

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

图片使用的著作权在笔记栏详细说明

▪ 放弃金本位 CC-SA 3.0: Will O'Neil



什么是钱？

CC0: <http://maxpixel.freegreatpicture.com/Cash-Exchange-Financial-Currency-Banknote-Money-1309887>



纸币能吃饱吗？
为五斗米而折腰有听过吗

Public Domain:

https://commons.wikimedia.org/wiki/File:%E0%B4%AC%E0%B4%B8%E0%B5%81%E0%B4%AE%E0%B4%A4%E0%B4%BF_%E0%B4%85%E0%B4%B0%E0%B4%BF.JPG



一般商品都易腐 (盐也有被当成过货币，政府规定不能私自提炼盐这事情居然有存在过 哈哈)

量多 - 携带不便

难以标准化

国际交易兴起和需求 (用米的话用航运都烂光了，何况老外不吃米？)

Public Domain: <https://commons.wikimedia.org/wiki/File:China-1Yuan-1914.jpg>

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冲击
- 20世纪生产力高速上升
- 战争

旧金山 (三藩市)，在1848年发现金矿

如果挖矿比生产力增幅慢，存着的钱或金子在未来购买力更大的话，即是通缩。大家就不愿消费，把钱存着就好。

针对实物货币的问题，两个措施: 部份准备金、纸币

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%

差不多同期的玩法



纸币

20世纪初战事频繁，要真金白银支付军饷 – 无论是国共内战、美国内战、第一次世界大战...

纸币一开始，通常起初都承诺可以兑换实物 (金、银)

强势点的国家又或者会强制地徵收实物兑换

无论如何，一般政府自己是认可的 – 可以用来交税

但战争后都会被挤兑或通货过份膨胀、因为根本没有足够生产力去滥发的货币，然后就会贬值

1948年還改发金圆券、49年银圆券。

https://zh.wikipedia.org/wiki/File:ROC_Fabi.jpg

Believed to be in Fair Use

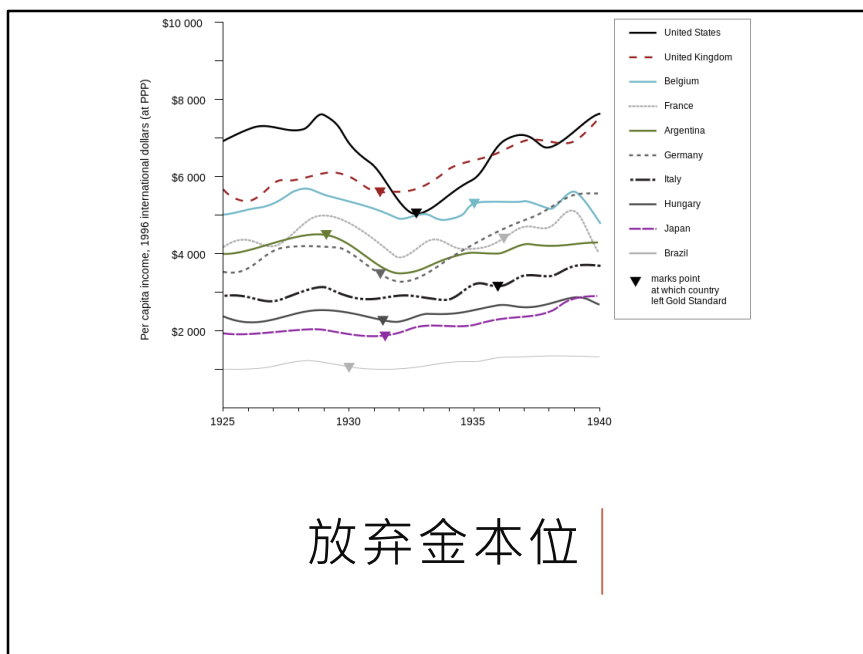


大幅贬值、通胀以支军响



两大说法:

1. 股灾、信心危机、挤兑
2. 一战之后收紧银根 (因为通胀太多、太多“热钱”)、回复战前兑换率、一不為意收得太紧导致流动性问题、大幅通缩
滚雪球



放弃金本位，自由浮动，自由印钞
基本上是谁一放弃就恢复过来

CC-SA 3.0: Will O'Neil

https://commons.wikimedia.org/wiki/File:Graph_charting_income_per_capita_througout_the_Great_Depression.svg



打够了没有...

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

在二战时自由浮动太可怕，但金本位也很可怕。
当时美国就是最强，因为没有怎样参与战事，草草丢了原子弹就完。德、英、法、中、日这些直接参与战事的都没什么元气。

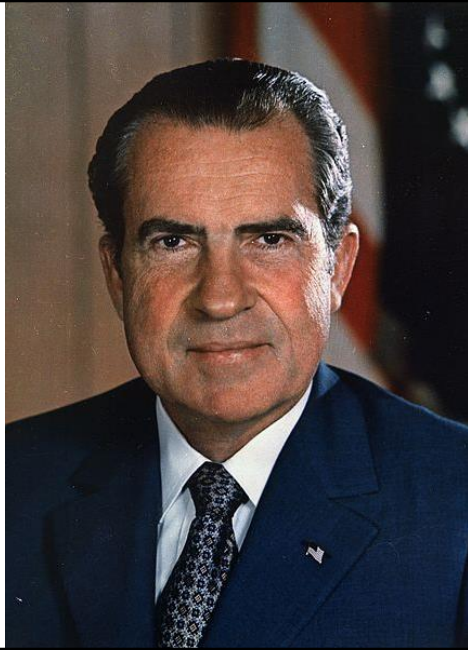
所以盟国去开个会，都依靠美元 – 尤如相信黄金一样去相信美元的GDP，变相回到差不多是金本位。



这次到美国要支付军响
外国信心不足，纷纷兑换黄金

尼克松冲击 NIXON SHOCK

1971



一句话: 禁止外国兑换黄金、加进口税
本来说是90天的短期政策，但根本回不来

全世界货币从始变成自由浮动

Public Domain:

https://commons.wikimedia.org/wiki/File:Richard_M._Nixon,_ca._1935_-_1982_-_NARA_-_530679.jpg

法定货币 FIAT CURRENCY

不能吃、什么也不是
但至少能用来交税

1987年也有股灾 – 当日香港股票跌幅比得上经济大萧条那次，但这次大家都用法币，所以能通过货币政策调节避过去，民生没什么影响，甚至日本也创造了她的盛世。

后面2000金融风暴、2008次按危机、QE量化宽松、美国启动印钞机、中国央行调整存款准备金等，大家都比较熟

货币总结

钱值多少只是信心，由一国的GDP支持。

现代经济学认为，维持2%低通胀是最好。

比特币 |

比特币

BITCOIN/BTC

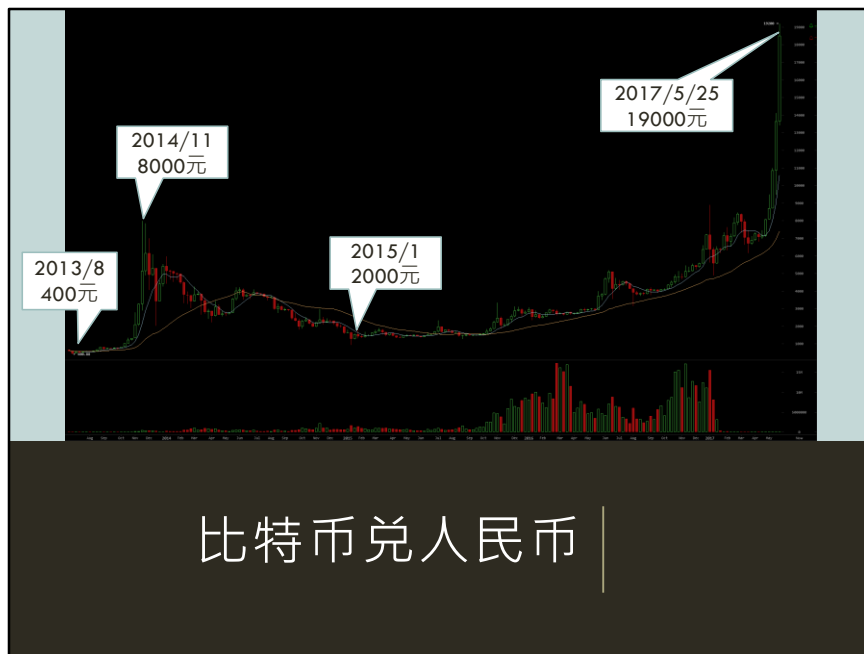
首只Cryptocurrency (加密货币)

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一一个BTC，亦称一个Shatoshi
▪ 但技术上可以更细

中本聪只是网名，真人是谁不知道。



Bitcoin在Okcoin.cn上的价格

2013年8月 – 400

2014年11月 – 8000

2017年5月25日 – 19000

2017年5月26日 – 16000 (单天就掉了15%)

(截自bitcoinwisdom.com)

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

定价和外汇、股票一样，就和黄金差不多。谁愿意卖、愿意买，就是了。虽不能用来交税，但有上十万商号接受消费。或者用来支付WannaCry？信就有？不信就没有。

没有涨停、没有跌停

与黄金有纸黄金ETF不一样，目前都声称是完全准备制，未见部份准备制的比特币交易所。某些交易所公开Audit – 当然信不信由你。也有试过很大的交易所被黑而倒闭 (mt.gox事件)

是不是1637年荷兰郁金香狂热的翻版？

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)

先不要问为什么规则是长这样，为什么是10分钟？为什么是每四年减半？中本聪一开始说是这样就这样。

就像剪刀石头布，为什么剪刀能赢布？跟着玩就是...别问这么多。

后面会说明为什么大家都愿意跟着玩。

PROOF OF WORK (POW)

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

$$x = 6 \text{ or } x = 9$$

Proof of Work

算出答案有点难，但验证答案是正确的很容易

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"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

- 找一个nonce而使sha256(区块内容+nonce)是小于难度值
- 找到后向其他电脑广播这区块+nonce内容

问: 如果我黑了某挖矿电脑，也刚好算出nonce，也刚好把他的nonce抢走，抢先广播，那我会抢到他奖励金吗？

答: 不会。他算的nonce只适用于他所选择编成的交易数据，包括自己那条“12.5BTC进他的钱包”的交易信息

如果要是改成进别的钱包，所需要的nonce就完全不一样。

节点 NODE – 执行规则者

1. 接收挖矿结果
2. 验证规则
 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

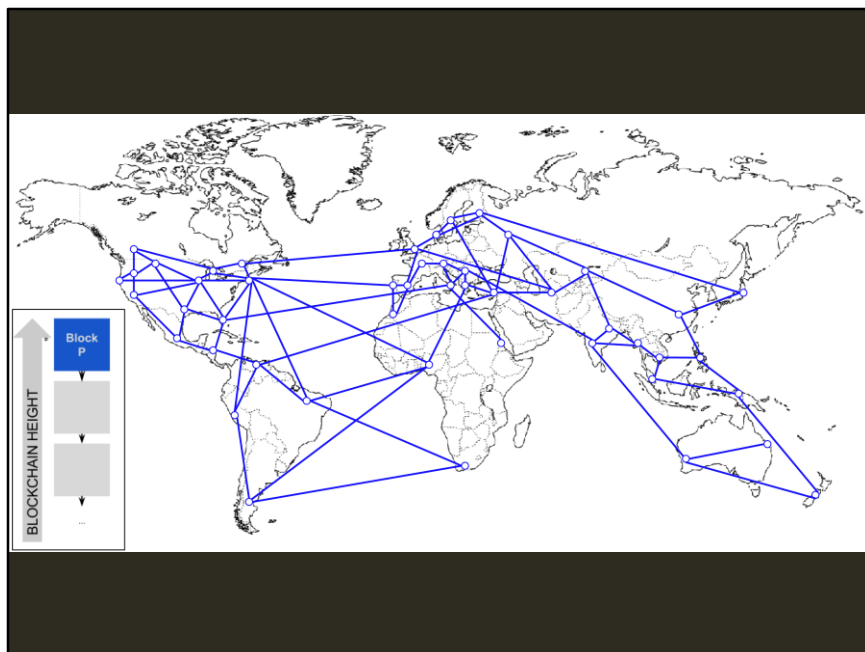
挖矿电脑在知道新区块出现了，就会在放弃当前的并转到新区块上挖 – 不然会浪费自己时间。因挖旧的区块出来的结果也不会被节点认同。

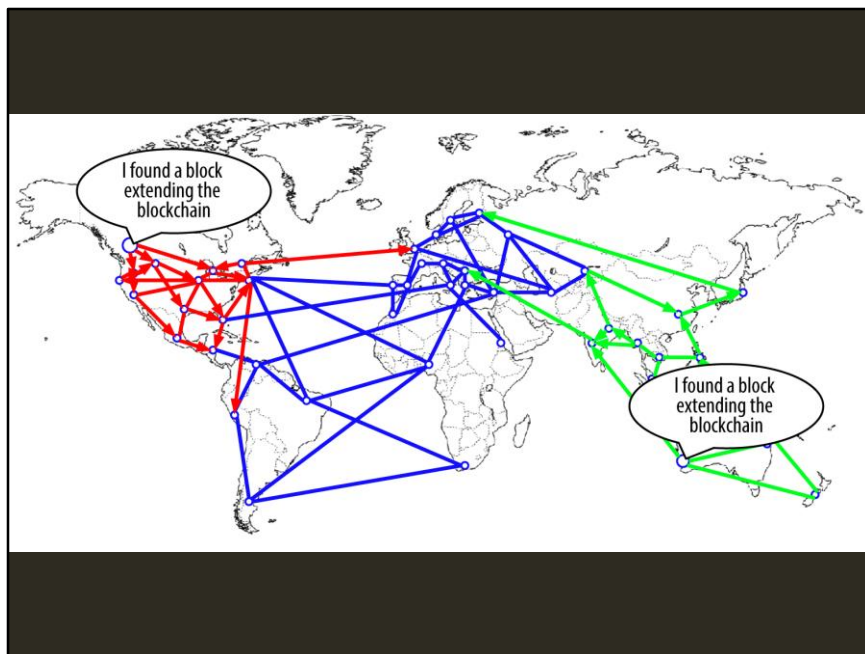
难度值 - 就是根据规则算出来的那个，每两周(2016个区块)重新调整一次，希望难度大约等于十分钟挖出一个区块。

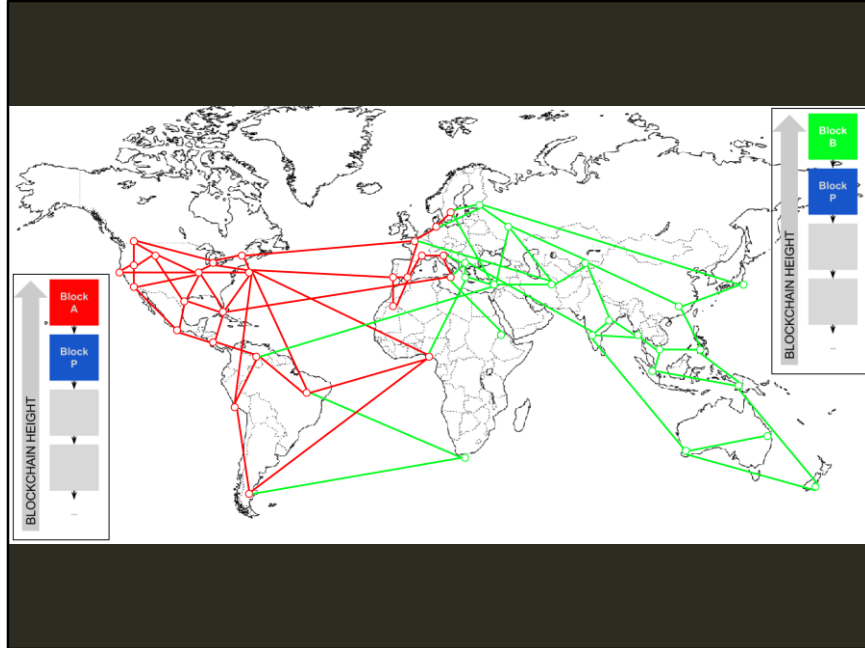


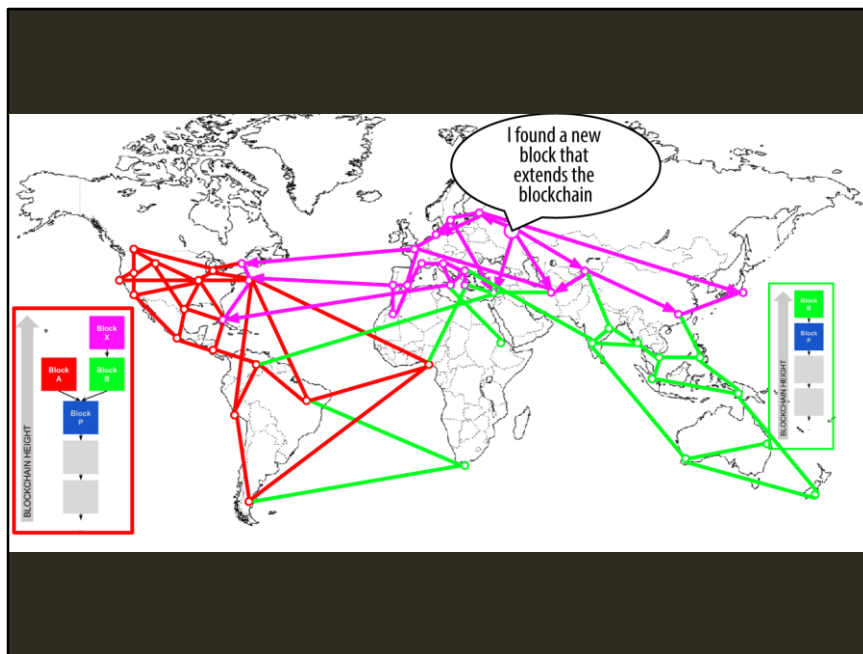
BLOCKCHAIN分岐

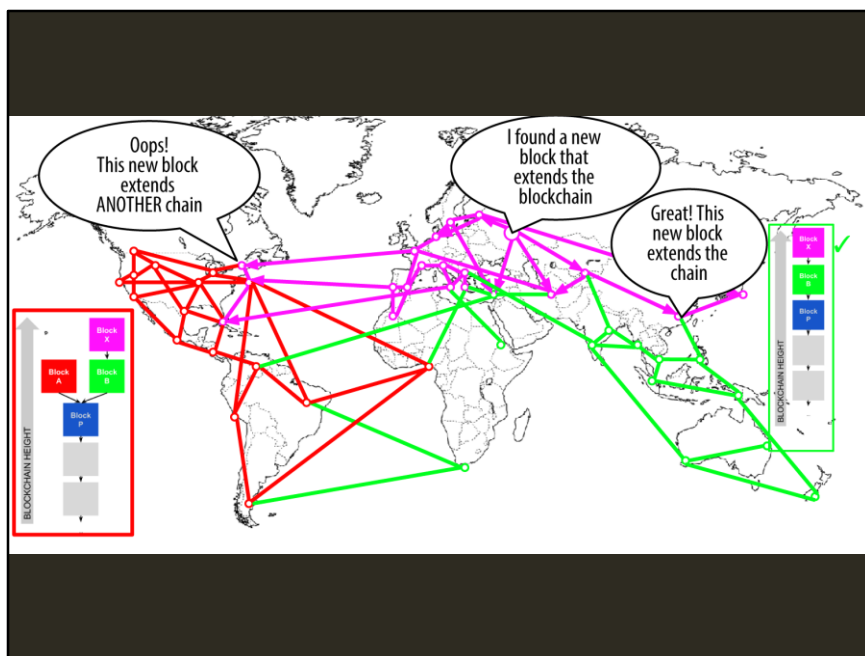
那如果同时挖出东西，会怎样？同步也要时间啊。











最后终会归为单一条链，因为大家按规则玩的都会在最长的链上继续算。红色那一区块A就等同不存在也没发生过。

出现一级分歧大约每周会发生一次。两级分歧机率微乎其微。所以如果一个交易是已经在第3~5个区块之下，基本上没可能推翻掉。

一般交易，例如充币到交易所可能是要等3个确认才会被“接纳”清算，这纯粹是双方在bitcoin框架之外所协议的事。

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)

“官方” (中本聪以及他交棒的人)是有个“组织”去商讨制定Bitcoin的技术，以及弄了一个公版 (Reference Client) – 像Nvidia的Founder's Edition? XD

公版是开源的。协议也是公开说明的。用不用倒是大家的自由，像HTTP就摆在这儿，大家可以用各家开发的浏览器...

著名的client好像有两三个。也有出现因为某版本出bug算不出东西。但只要>50%的运算力都支持某一个规则，那一套规则就是Bitcoin。

官方可以突然胡扯推一个新版本，全新协议，或者说改成一个block挖出50000个BTC...

但大家用不用，信不信是一个人控制不了。

也有可能出现以太坊这样弄出两个货币，两套规则各自有“信徒”去跑。

问1: 比特币的节点是服务器吗

答: 任何参与进去的电脑就是...服务器也不就是电脑? 可能是个莓树派、可能是Windows、可能是Linux、可能是路由器 (我就是不提Mac。噢，提了)。只是验证规则是否正确需要的电费、比起挖矿需要的低得多。

亦有点像Bittorrent (BT)一样，某人想下载东西所以有诱因去跑BT节点
越想守护bitcoin规则的人，就越有诱因去花点电费去跑这个节点，例如可能他是商家、投资/投机者...

问2: 出bug的时候，hard fork可以直接更新节点上的源码吗

答: 需要大家跑的去升级。有些client可能有自动升级机制，可能你要下载...等等。就靠大家去做。

例如某天发现BT因为版本协义变了下载不到，但你又很想下载某文件 - 就自然会去升级。

挖矿的也想相安无事继续挖，所以也会有诱因去升级去一个符合自己理想的一个版本

问3: 感觉就像一个游戏，BTC就是里面的游戏币...

除了这里没有运营商。不能胡扯SSR今天抽奖机率是啥就是啥。而是所有玩家说了算。

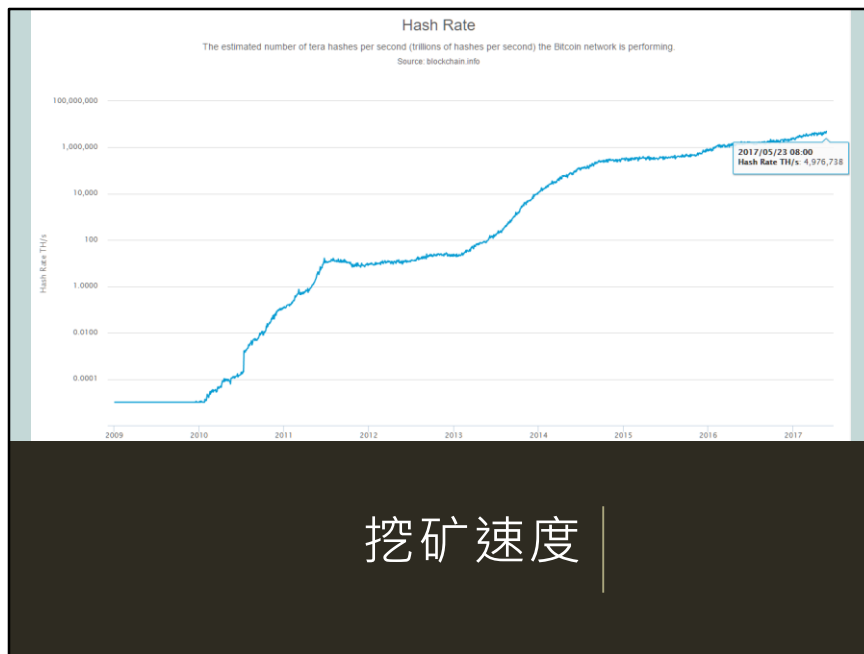


怎么得到BTC？

三个入手方法: 交易所买卖、挖、交易收款

交易所买卖

存入法币，买卖贵金属、股票一样



自己一个挖矿几乎不太可能中奖

一台电脑可能就是以百K哈希/s的速度，现在(2017-05-23)是4976738T哈希/s的速度。

机率自己算。

1T=1000G

1G=1000M

1M=1000K

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**

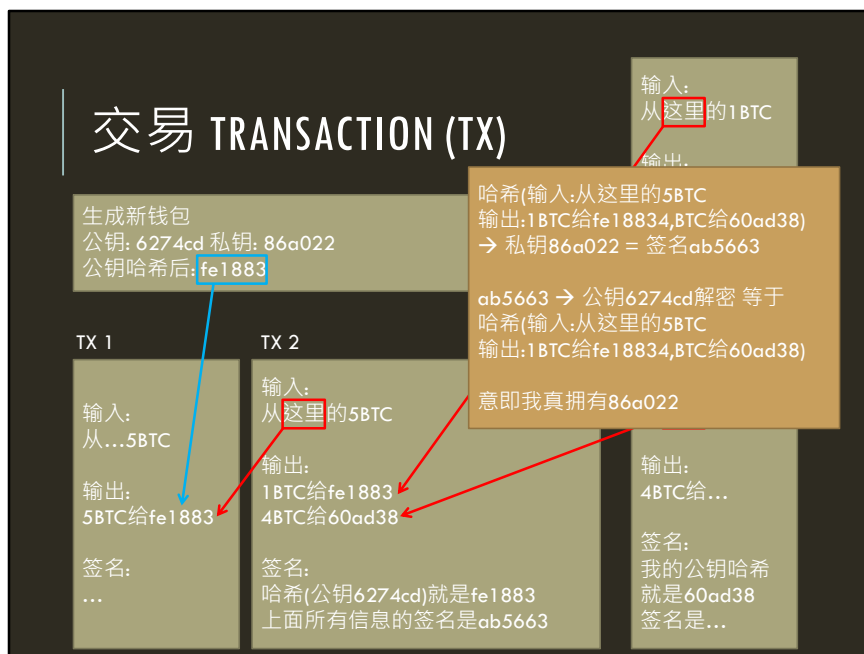
第三就是别人给你BTC (可能你卖了某东西)
这里要先解释公私钥加密算法的概念

像公章一样

其他人看到我盖上了章的文件(如同签名一样)，就意会到我是拥有这一个章(私钥)，但我从来不要把章秀出来给大家看。

最多是在工商局登记章盖出来的样子(如同公钥)，那下次看到时就知道那个是我的。

通过数学保证，(几乎)不可能单从观察过盖章的文件，复制出那个章。



简单版 - 先不讨论脚本(Script)

生成新钱包，把哈希(基本上就是钱包地址)给到想给BTC你的人

那拿到BTC后又怎样它花掉？看图解，其实每个TX是一个扣一个。

节点会验证TX是否合法，合法才会纳入Blockchain:

- 公钥的哈希就是钱包地址，且签名正确
- 输入总金额小于输出总金额 (除了奖励金交易是没有上一个输入)
- 还有剩余的会给到挖矿的人

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

然后含有你的TX的区块挖好了，广播出去，就成为历史的一部份了

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

一个交易数据的内部其实要复杂一点点，大概是上面这样。

脚本可以是别的，它只是一个bitcoin特定汇编语言，例如可以写成

- 需要多个签名
- 直接return true也行

(这语言故以设计成非Turing Complete)

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

回顾为什么比特币有这些特性

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

投资、投机？
价格可跌可升...

法币的历史是从**1971**年起，**Bitcoin**是**2009**年。未来两种东西怎样走，谁知道？
早期曾经有人花上万个**BTC**买一块**Pizza**。

BTC和法币的购买力是什么？反正都不能吃进肚子的，说到底都只是人相信不相信。