

BITCOIN AND BLOCKCHAIN

Robin Ye:

"目前的阶段就像 2000 年 PC 转向互联网时代，大量的 PB / VB / Delphi 程序员要么继续学习，要么被淘汰。而现在是互联网转向AI、物联网和区块链"

我们将聊哪些内容

- 货币的演进
- 什么是比特币
- 比特币发展史
- 比特币交易
- 区块链
- 挖矿与共识
- 比特币安全

我们不聊哪些内容

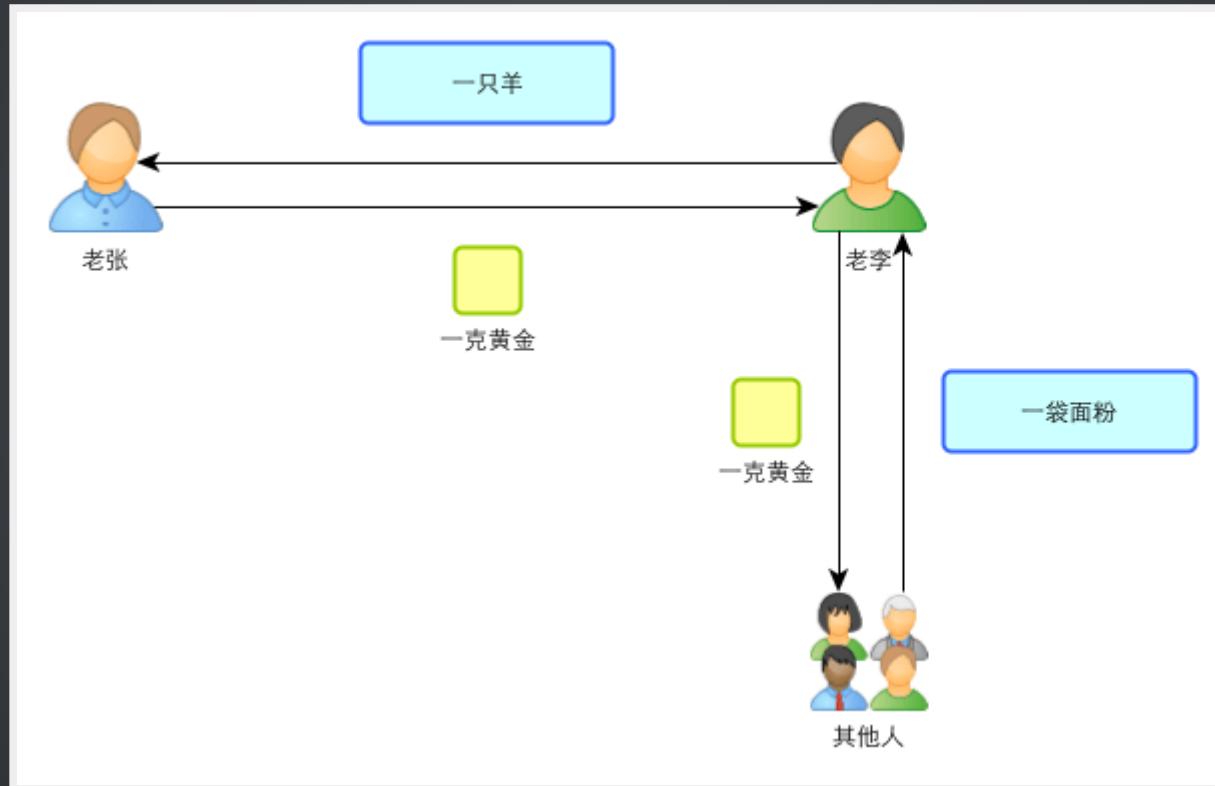
- Alt Coin 竞争币与山寨币
- Ethereum 以太坊
- Elliptic Curves Cryptography 椭圆曲线加密
- Digital Signatures (ECDSA) 数字签名

货币的演进

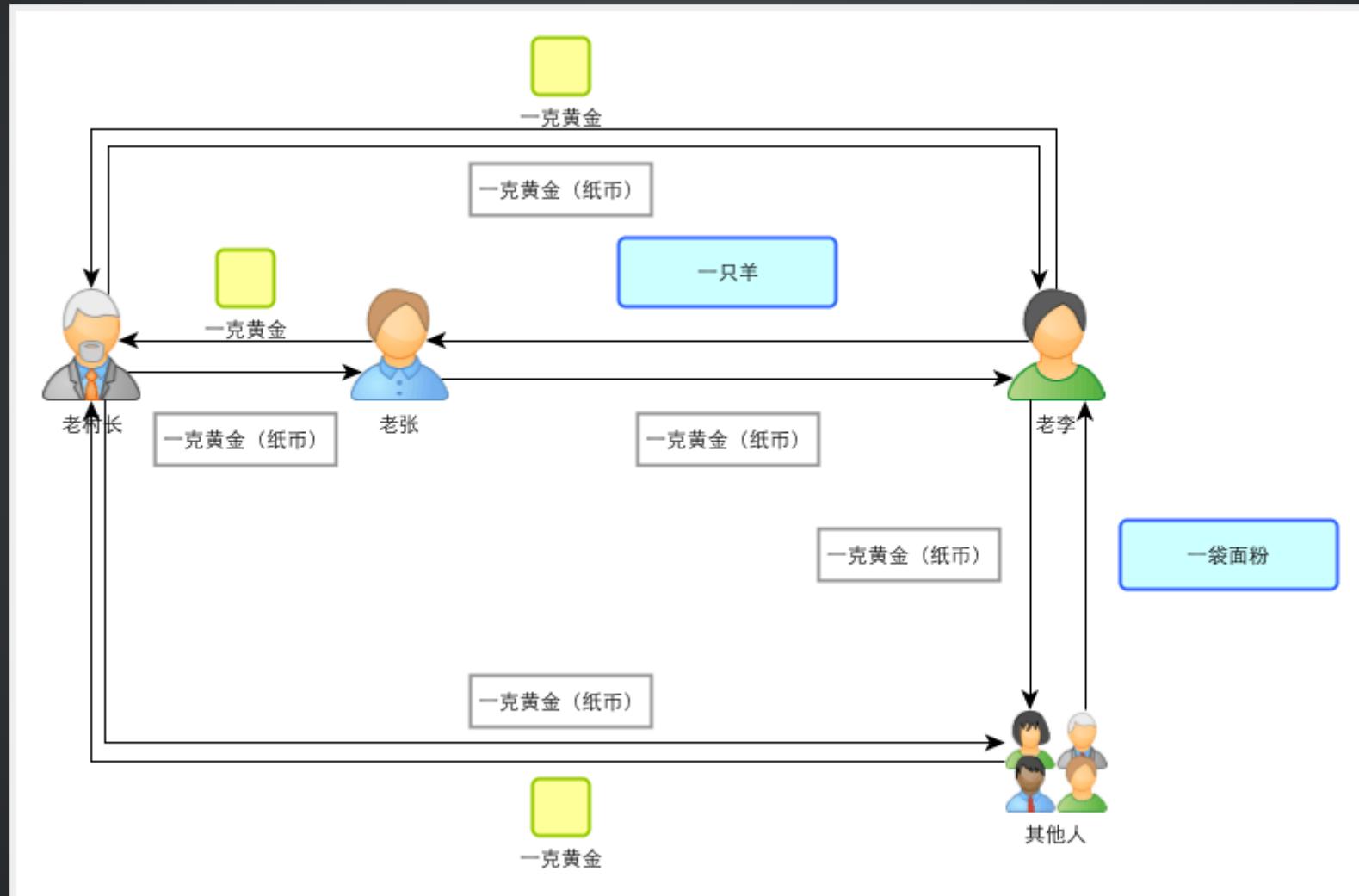
以物易物



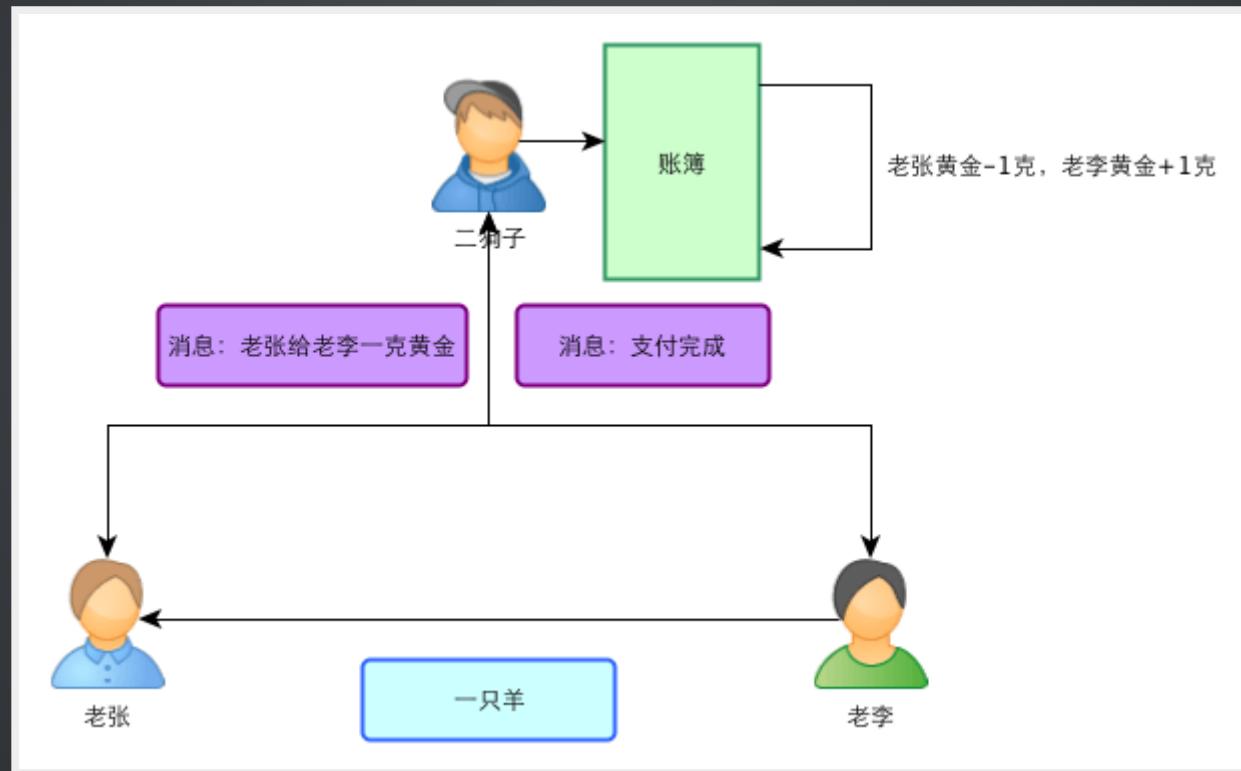
实物货币



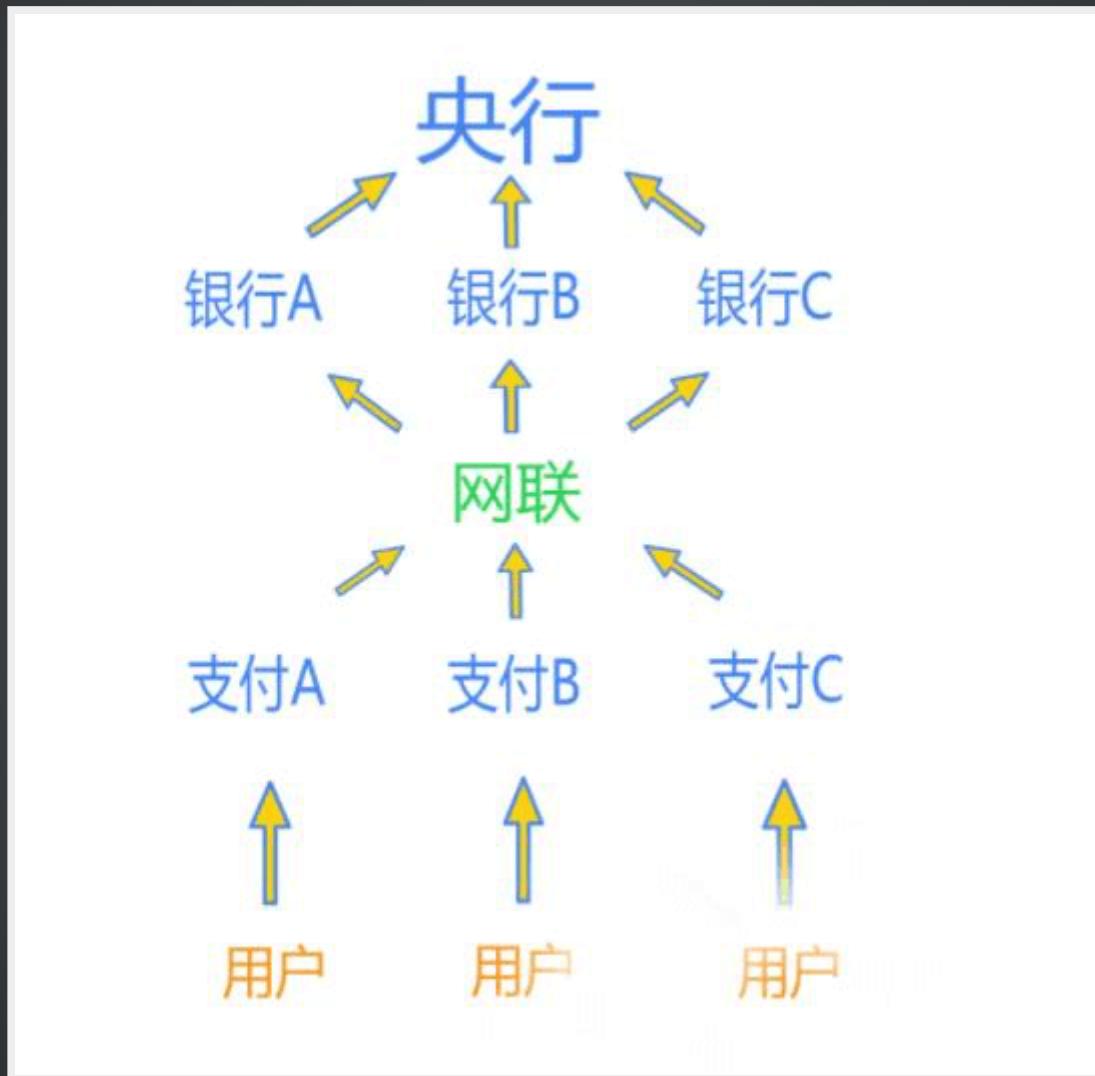
符号货币



无现金社会



中心化的网联



什么是比特币

什么是比特币

- 一种基于互联网的去中心化的**密码学货币**
- 一个分布式、去中心化的点对点网络系统
- 一种协议、一种网络、一种分布式计算创新的代名词
- 一个分布式问题（**拜占庭将军**）的解决方案

比特币诞生

- 2008年化名“中本聪”的人发表了《Bitcoin: A Peer-to-Peer Electronic Cash System》，描述了一个完全去中心化的电子现金系统
- 2009年一群工作量不饱和的程序员根据这篇论文，修订并发布了比特币网络
- 2011年“中本聪”退出公众视野，比特币网络由社区维护和发展

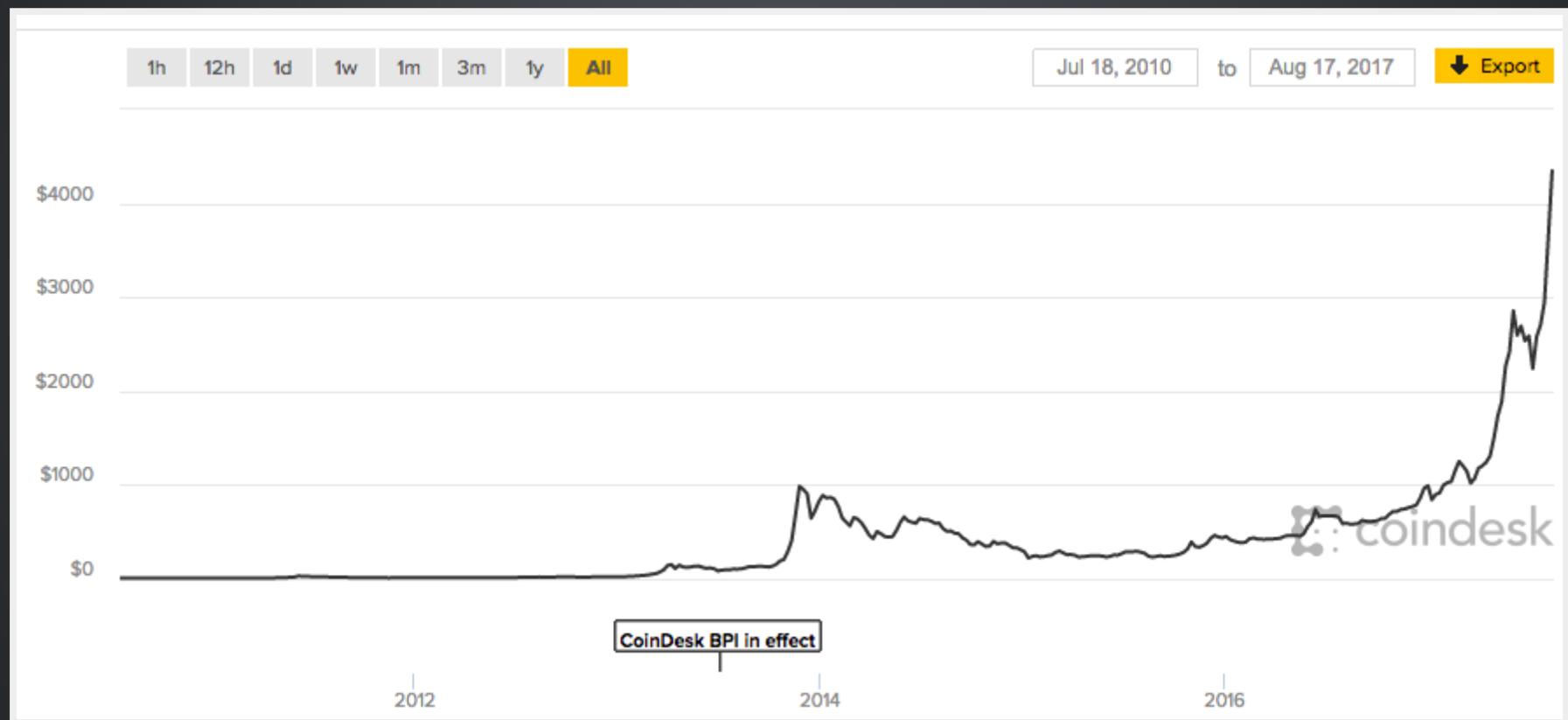
比特币发展史

2013 我们讨论比特币

网友：

- “有多少人接受使用外星人的货币来买你的房子和汽车？”
- “Q币可以买到TX的服务！而比特币什么也买不到！一文不值！”

2013 - 2017



5年后的今天

新闻：

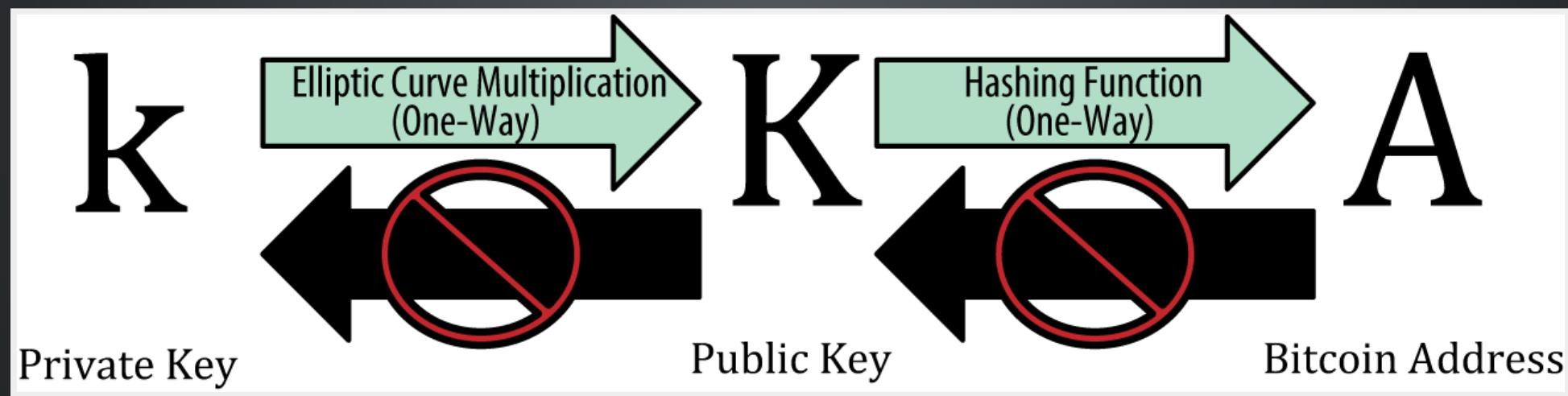
- 80后宝妈投资并通币给家庭添宝马
- 北邮区块链EMBA国际总裁研修班
- 陈满疑在“总裁班”接触虚拟货币，投资百万无法提现
- 薛蛮子：“中国还有80%的人没听过比特币”

比特币交易

言归正传

地址与钱包

- 比特币的所有权是通过密钥，地址和签名来确立的
- 一个人可以有多对密钥，钱包是这些密钥的容器



交易模板

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC
-			
<i>Inputs</i>	<i>0.55 BTC</i>		
<i>Outputs</i>	<i>0.50 BTC</i>		
<i>Difference</i>	<i>0.05 BTC (implied transaction fee)</i>		

交易链

每一次交易是比特币所有权的转移

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From

From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To

Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

INPUTS From

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18:0
Alice 0.1000 BTC

OUTPUTS To

Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

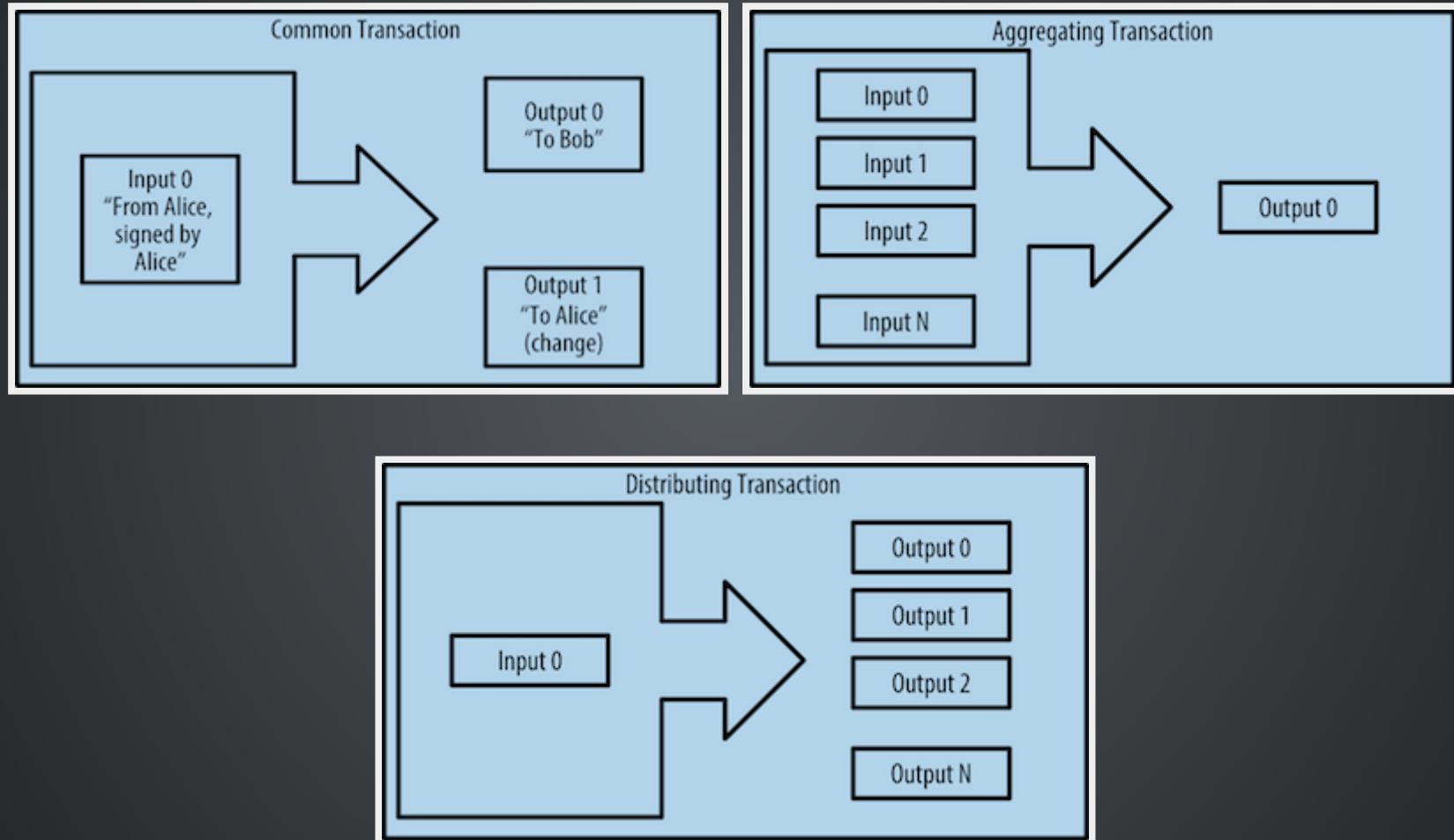
INPUTS From

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2:0
Bob 0.0150 BTC

OUTPUTS To

Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

常见交易形式



交易记录查询

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

[1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK](#) (0.1 BTC - Output)



[1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA](#)
- (Unspent) 0.015 BTC
[1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK](#) -
(Unspent) 0.0845 BTC

97 Confirmations

0.0995 BTC

Summary

Size 258 (bytes)

Received Time 2013-12-27 23:03:05

Included In
Blocks [277316](#) (2013-12-27 23:11:54 +9
minutes)

Inputs and Outputs

Total Input 0.1 BTC

Total Output 0.0995 BTC

Fees 0.0005 BTC

Estimated BTC Transacted 0.015 BTC

blockchain.info

UTXO

- Unspent Transaction Outputs 未消费交易输出
- 最小单位是 Satoshi (0.00000001 BTC)
- 交易输入是被消耗的 UTXO，输出是产生的新 UTXO
- 比特币世界没有记录用户的余额，只有分散在若干交易中的 UTXO，比特币钱包通过扫描区块链聚合属于用户的所有的 UTXO 来计算余额

交易费

```
Fees = Sum(Inputs) - Sum(Outputs)
```

- 按照交易尺寸，以千字节计算得来，与交易额无关
- 是矿工处理交易的优先级因素之一
- 钱包会根据网络中最近交易自动计算恰当的交易费

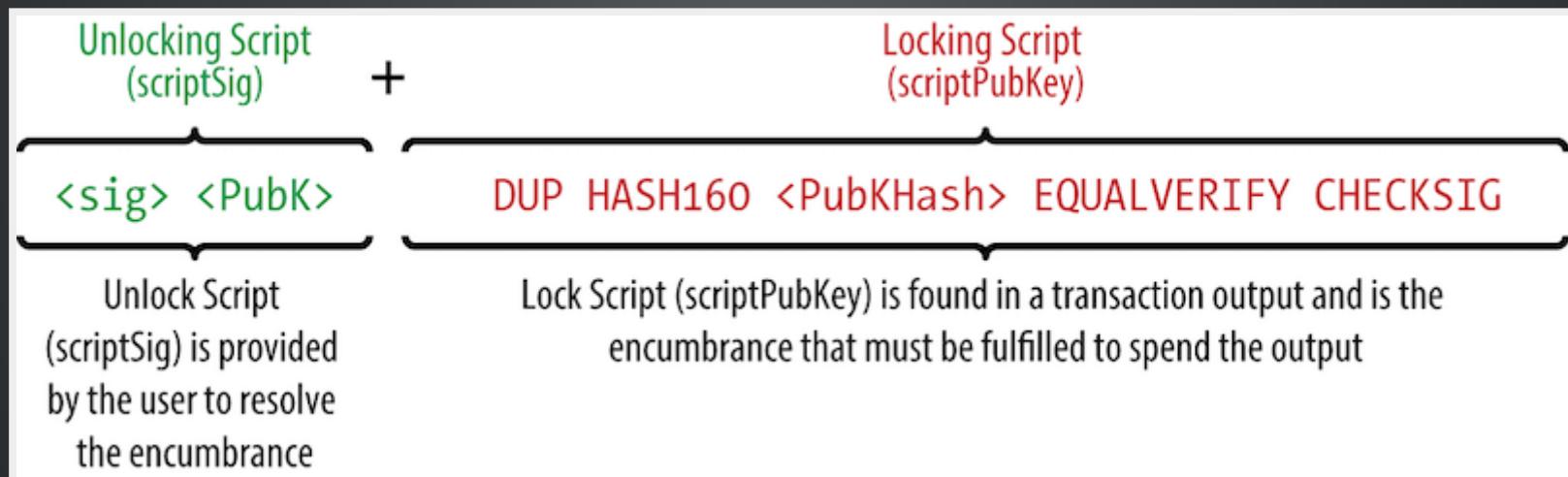
交易费估算



<https://bitcoinfees.21.co/>

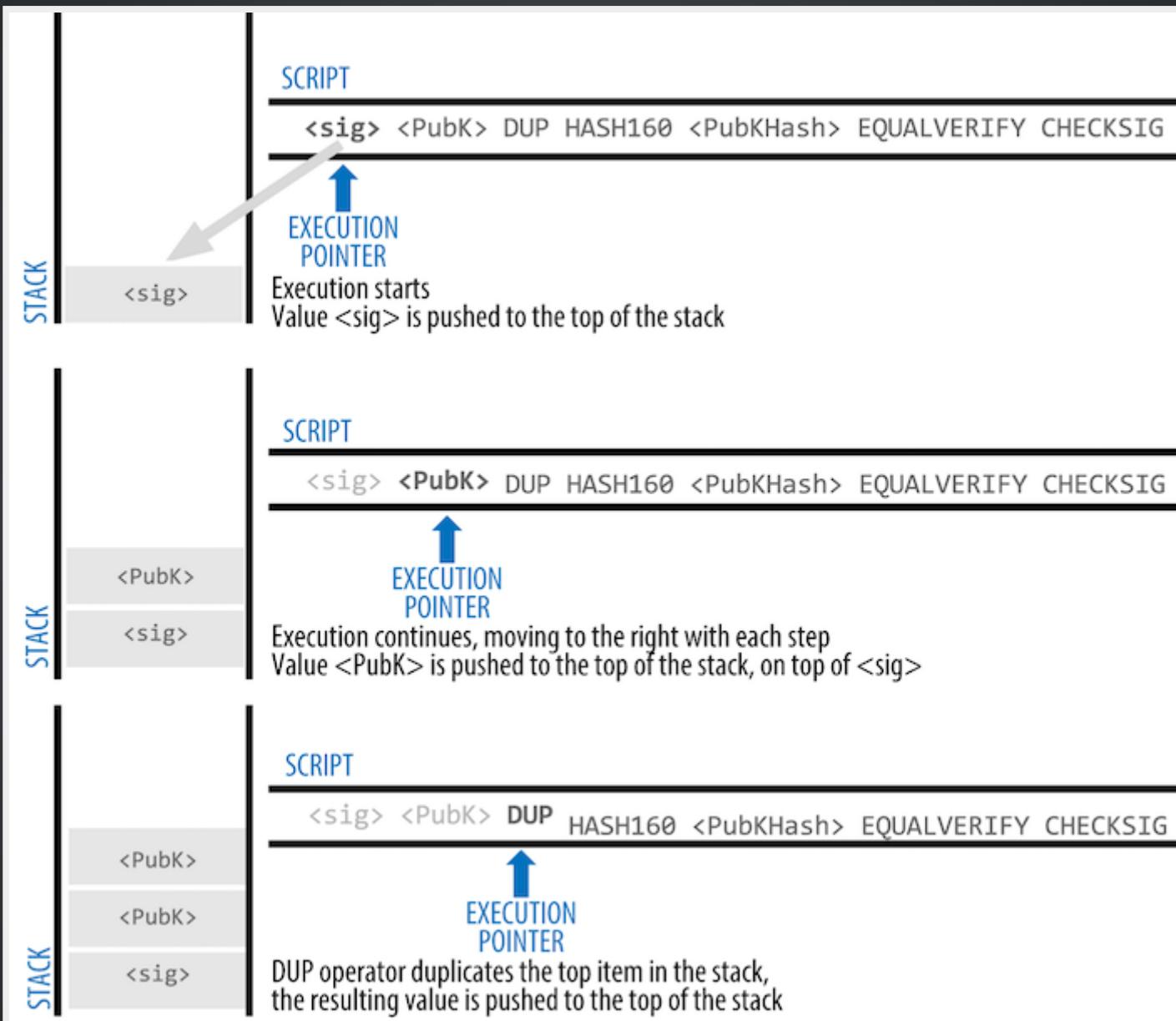
锁定和解锁脚本

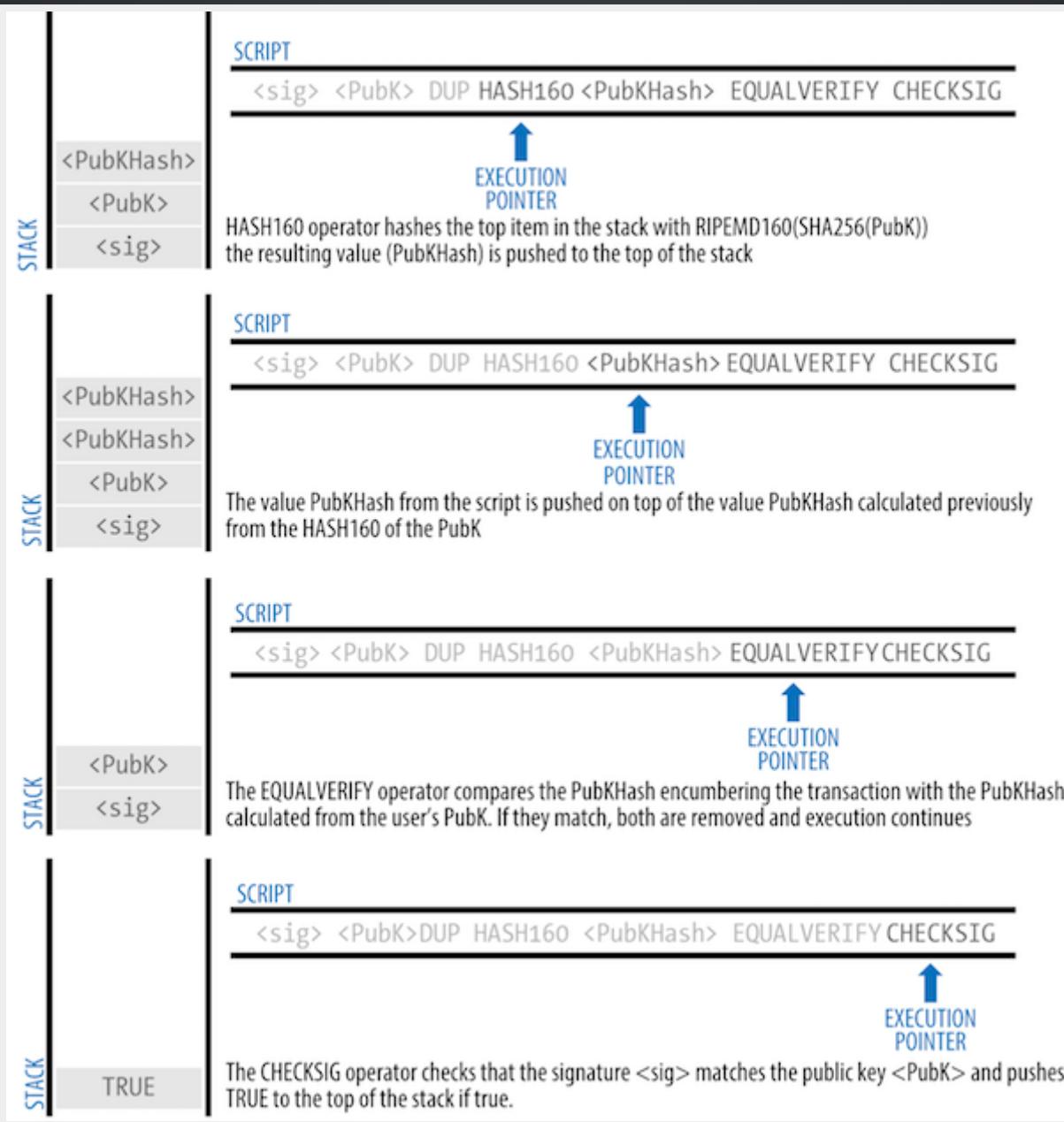
- 比特币客户端使用一种基于堆栈的，非图灵完备的脚本语言来验证交易
- 交易验证依赖于两类脚本：锁定和解锁脚本



一次 P2PKH 交易的脚本验证过程

比特币网络中的大多数都是 P2PKH (PAY-TO-PUBLIC-KEY-HASH) 交易





区块链

区块与区块链

- 区块是一种聚合了交易信息的容器数据结构
- 每个区块都会指向一个父区块，形成一个有序链表
- 区块链就是比特币世界中的公共账簿

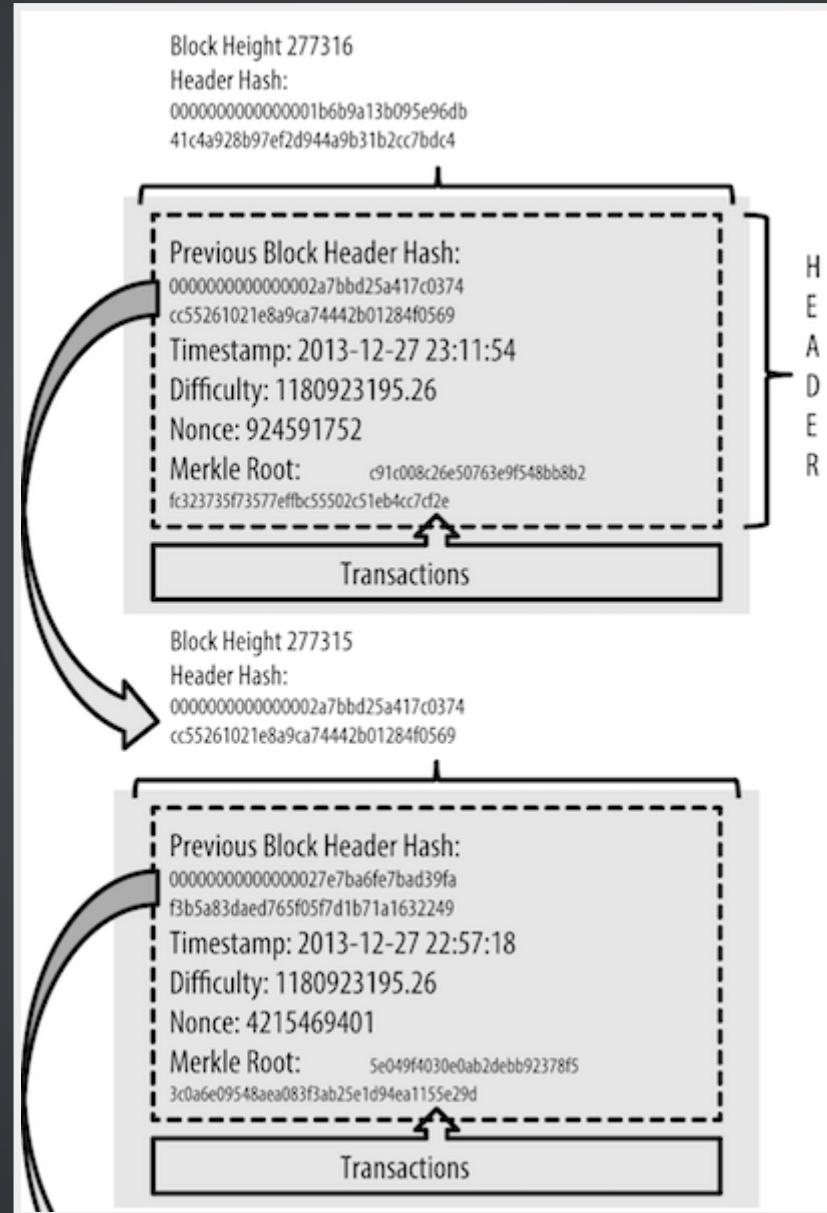
区块结构

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
VarInt	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

区块头

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block
4 bytes	Difficulty	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

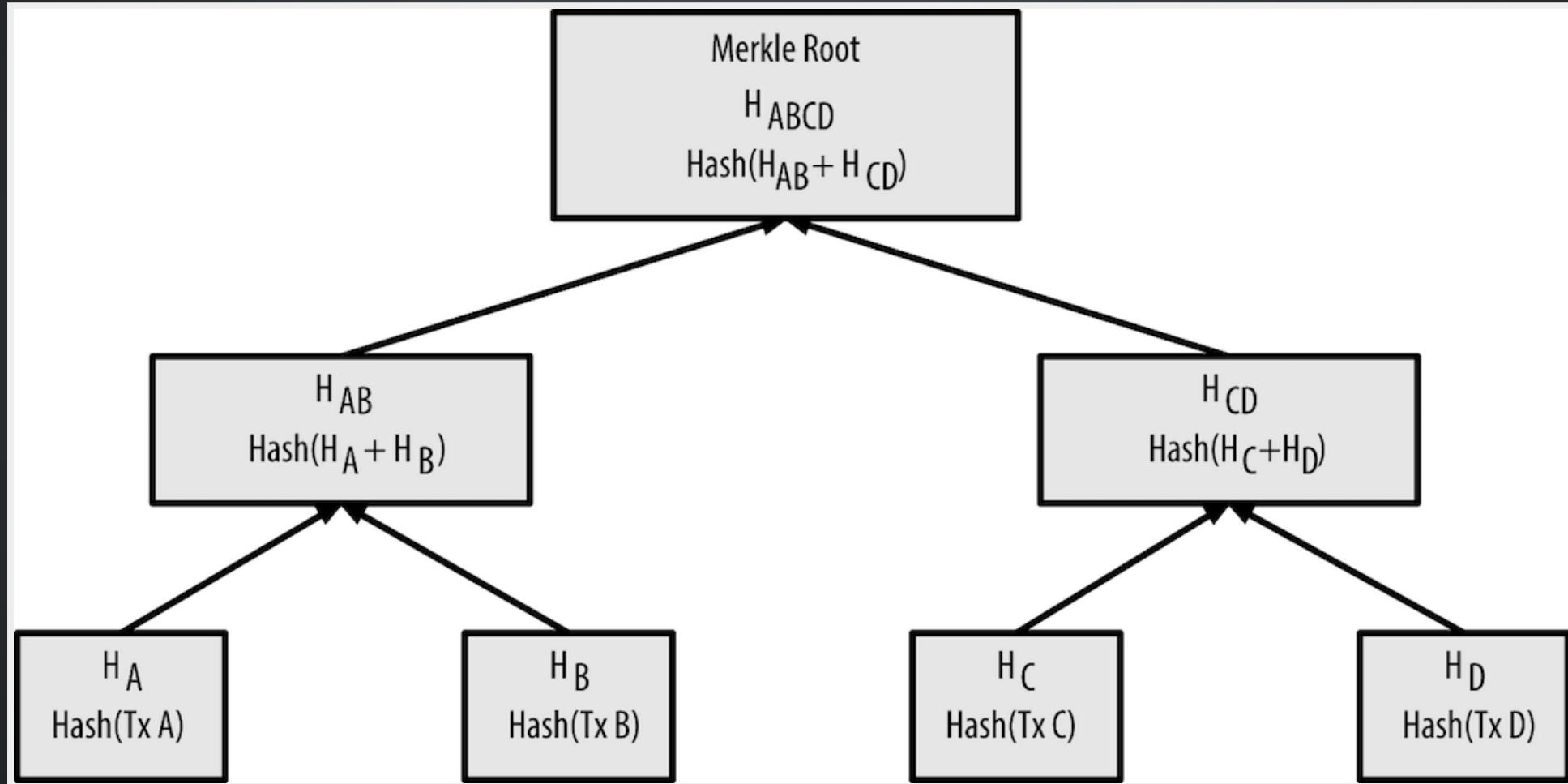
区块的连接



创世区块

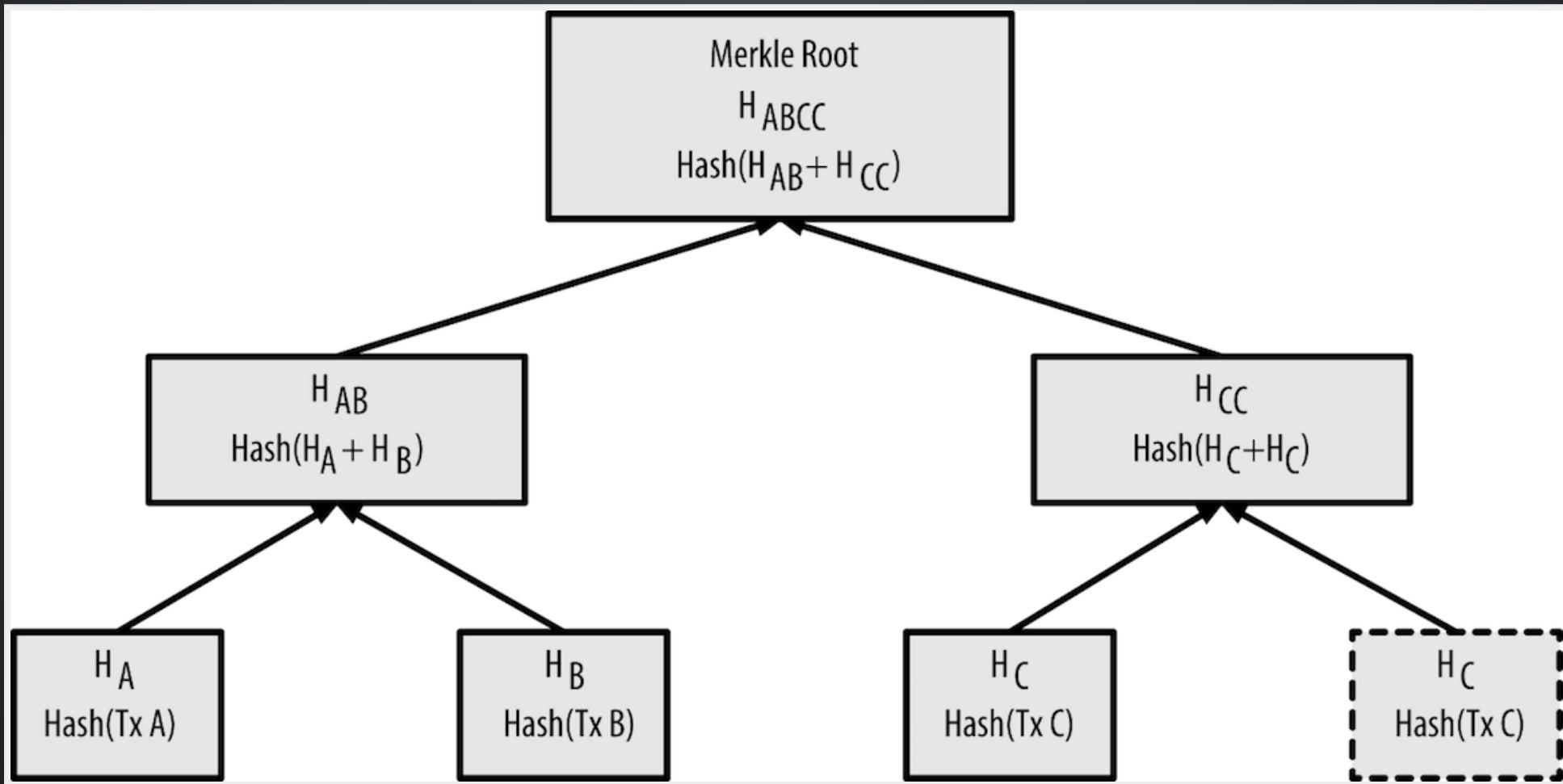
区块链中的第一个区块创建于 2009 年，称为创世区块。创世区块中包含了一个彩蛋，在其 Coinbase 交易中包含这样一句话：“首相第二次对处于崩溃边缘的银行进行紧急救助”，这是当天泰晤士报的头版，也是对现有货币制度的嘲讽

MERKLE TREE

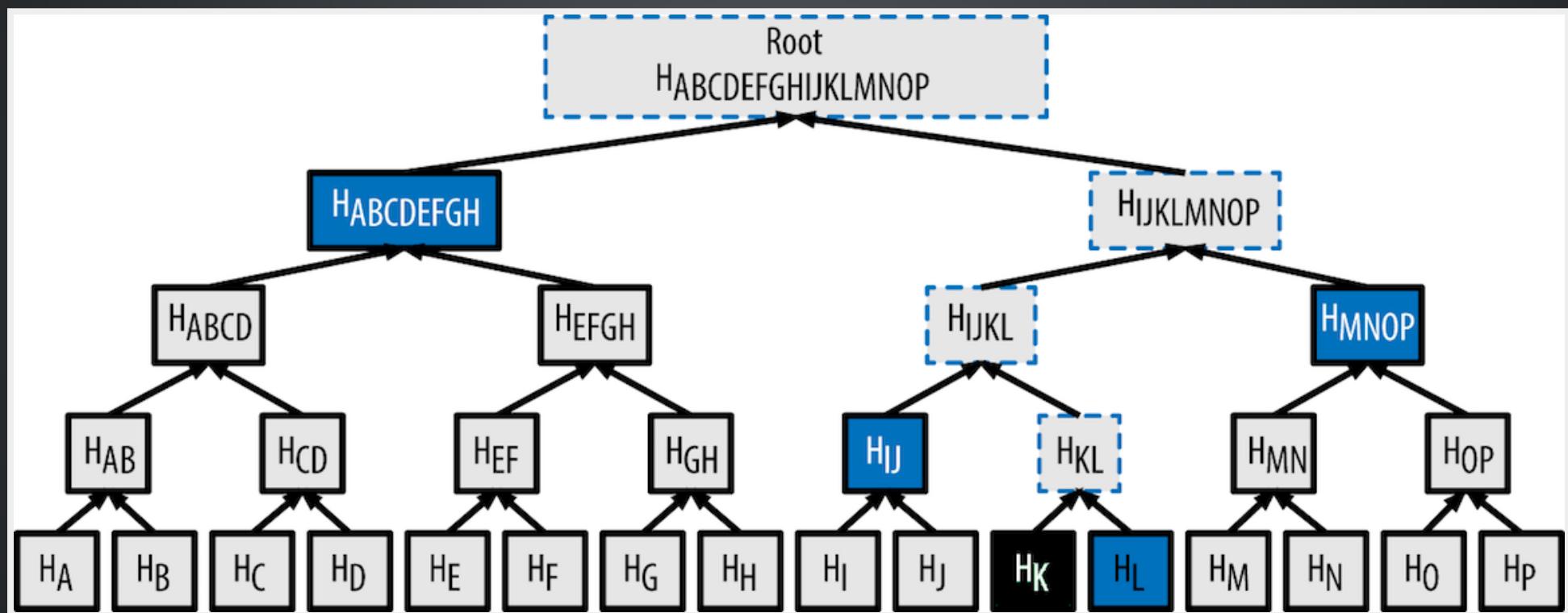


MERKLE TREE

Even number of nodes



MERKLE PATH



MERKLE TREE 效率

Number of Txns	Approx. size of block	Path size (hashes)	Path size (bytes)
16 txs	4 KB	4 hashes	128 bytes
512 txs	128 KB	9 hashes	288 bytes
2048 txs	512 KB	11 hashes	352 bytes
65535 txs	16 MB	16 hashes	512 bytes

挖矿与共识

矿工干什么， 收入来自哪里？

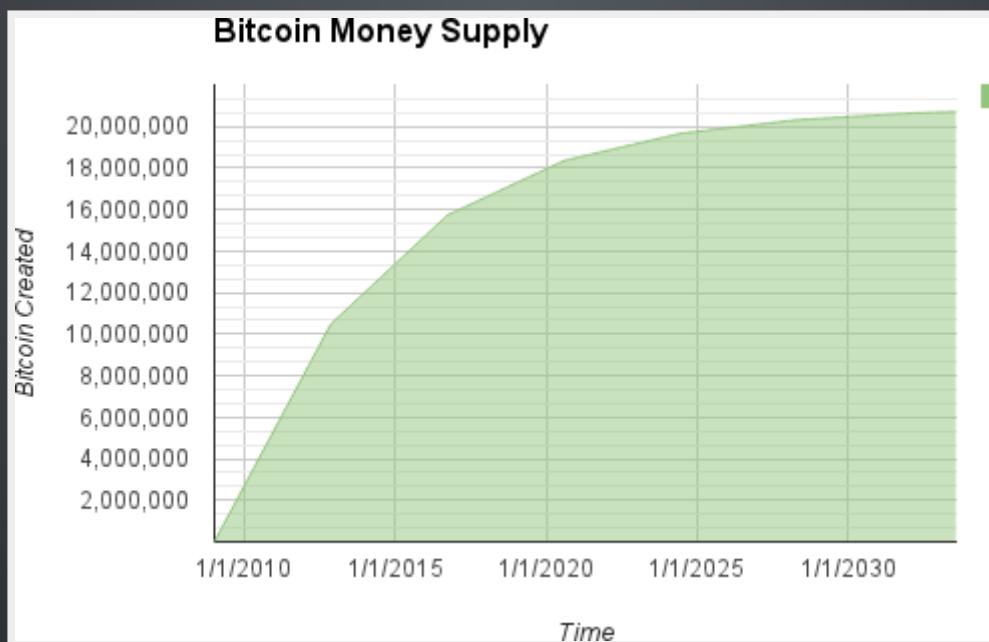
矿工验证收到的每笔新交易，并将它们构建在区块中。每成功构建一个新区块并添加到区块链中，矿工将获得创建区块的奖励和区块中所有交易的交易费。

比特币经济学与货币创造

比特币网络约每 10 分钟产生一个新区块，每个新区块的诞生会创造一定额度的新比特币（矿工奖励），这是比特币的唯一的发行方式

比特币发行速度和总量

每 210,000 个块（约 4 年），发行速率降低 50%，初始每个区块会产生 50 BTC，而现在 (2017) 已降低到 12.5 BTC。到 2140 年左右，比特币总量将达到 2,100 万，之后新区块将不再奖励比特币，货币发行停止，届时矿工收益仅来自交易费



COINBASE 交易

- 每个区块中的第一笔交易是 Coinbase (创币) 交易
- Coinbase 交易没有输入，而输出是当前区块奖励加所有交易费的总和，支付给构建此区块的矿工自己

工作量证明

让我们回忆下区块头中的 Difficulty Target 和 Nonce

Size	Field	Description
4 bytes	Difficulty	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

工作量证明

```
# example of proof-of-work algorithm
max_nonce = 2 ** 32 # 4 billion

def proof_of_work(header, difficulty_bits):

    difficulty_target = 2 ** (256-difficulty_bits)

    for nonce in xrange(max_nonce):
        block_hash = hashlib.sha256(str(header)+str(nonce)).hexdigest()

        if long(block_hash, 16) < difficulty_target:
            print "Success with nonce %d" % nonce
            return (block_hash, nonce)
```

要成功构建一个区块，矿工必须穷举出一个合适的
Nonce，使区块头的哈希值小余难度目标

难度目标与难度调整

- 每 10 分钟产生一个新区块，这是比特币的发行速率和交易达成速度的保证，需要在长期内保持恒定
- 每个矿工节点将独立完成难度调整，公式如下

```
New Difficulty = Old Difficulty *  
(Actual Time of Last 2016 Blocks / 20160 minutes)
```

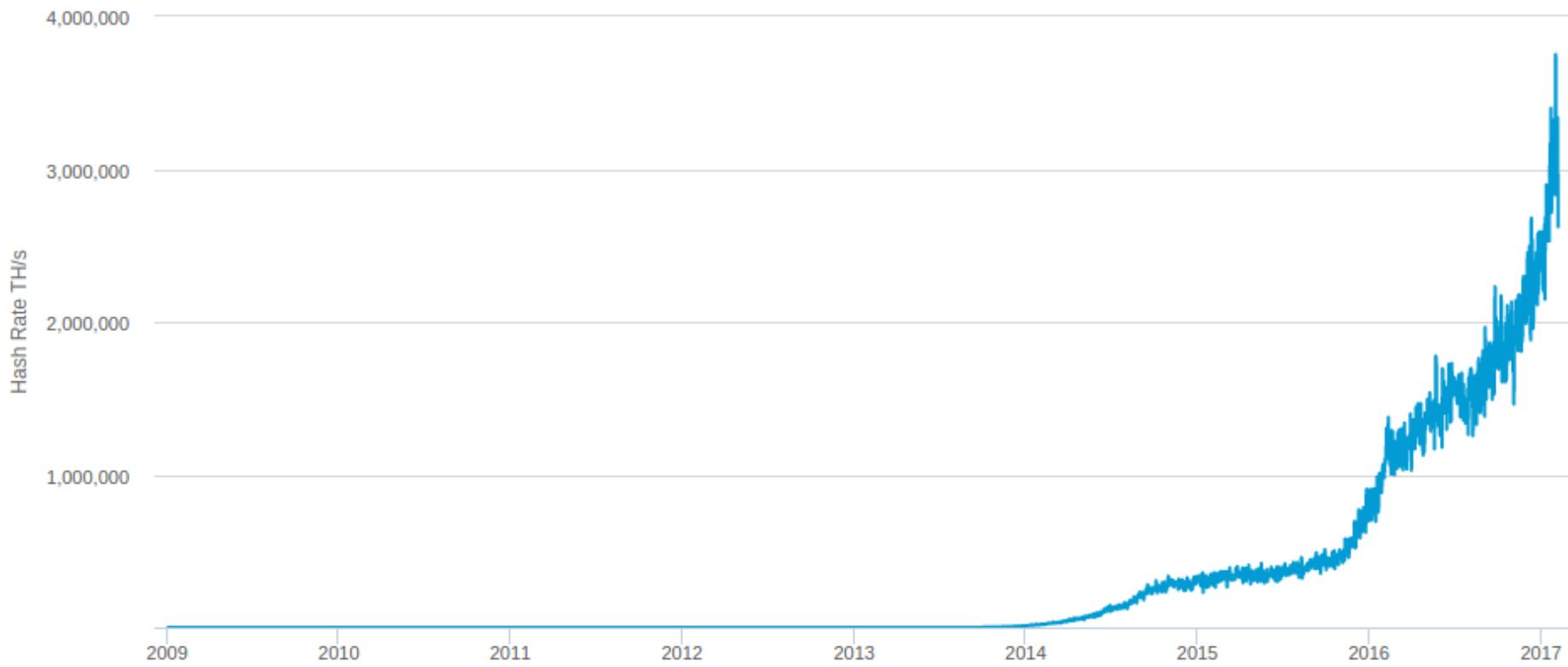
总哈希算力

Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.

Source: blockchain.info

Export ▾



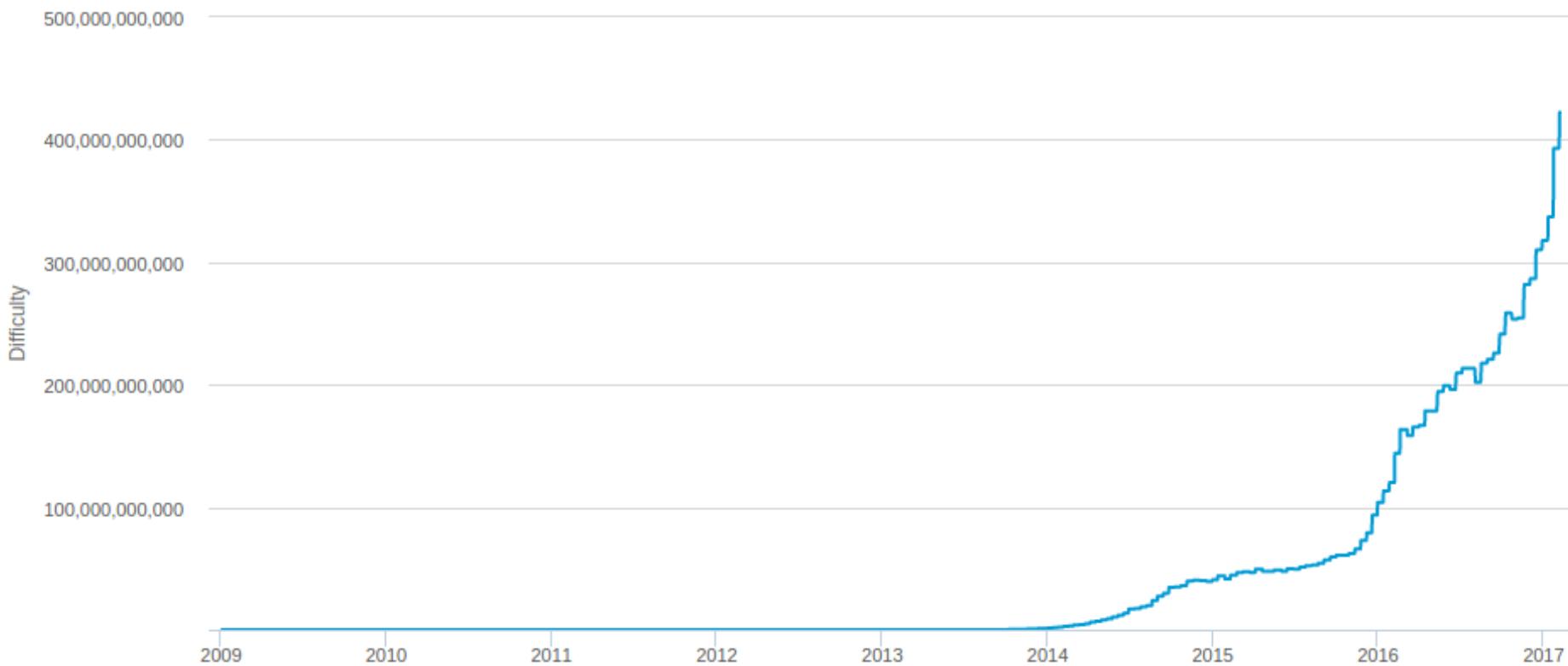
难度目标

Difficulty

A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Export ▾

Source: blockchain.info



矿工间的竞争

当一位矿工成功构建出区块（解出Nonce），传播给其它节点时，其它矿工会立刻停止计算，转而投入下一个区块构建的竞争中，一轮竞争的结束也代表着下一轮竞争的开始

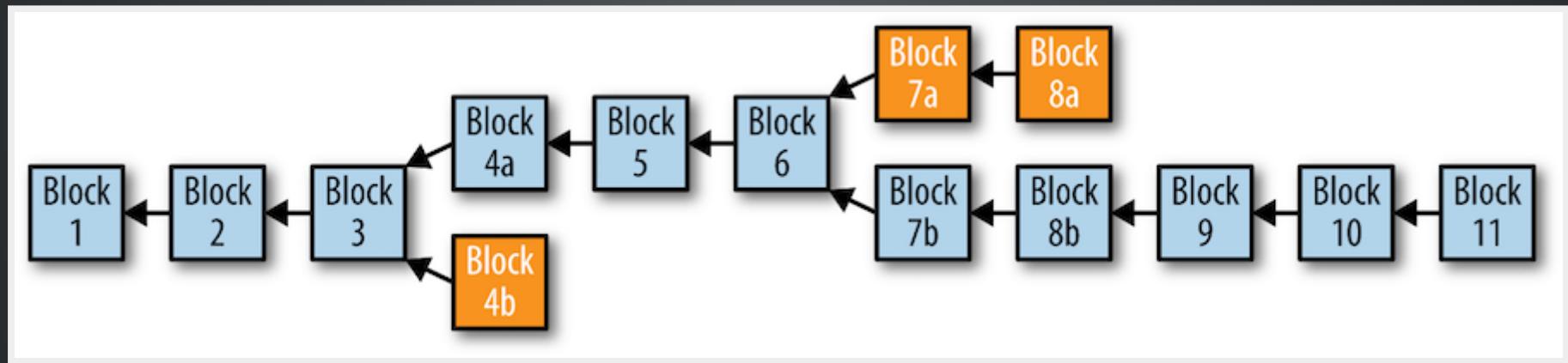
去中心化共识

共识来自独立发生在每个网络节点的 4 种过程相互影响

- 每个节点依据综合的标准列表对每个交易进行独立验证
- 每个节点独立将交易记录打包进新区块，并通过工作量证明算法进行验算
- 每个节点独立的对新区块进行校验并组装进区块链
- 每个节点对区块链独立选择，在工作量证明机制下选择累计工作量最大的链

区块链分叉

由于区块链是去中心化的，每个节点的视角不是总保持一致，两个节点可能同时传播了经过工作量证明的新区块，试图去延长区块链



只要所有节点遵循选择最长累计难度链的原则，整个网络最终会收敛到一致的状态

硬分叉

协议、方案的升级，守旧派和革新派

- Bitcoin Core
- Bitcoin XT
- Bitcoin Classic
- Bitcoin Unlimited
- Bitcoin Cash

共识攻击：51% 攻击

如果拥有了整个网络 51% 的哈希算力，我可以

- 造成分叉使自己的交易撤销，实现双重支付
- 阻止区块确认部分或全部交易
- 阻止部分或全部矿工构建区块

说了这么多，现在挖矿还来得及吗？

GPU MINER



Nvidia GTX1080 GPU = 2.83GH/s for 200w

ASIC: Application-Specific Integrated Circuit



AntMiner S2 ASIC = 1000GH/s for 120w

投资回报率

ROI = Miner costs / (Income per day - Power costs)

你的对手：川西深山里的“淘金客”



在激烈竞争的环境下，个体矿工只能选择加入矿池

比特币安全

“人类使用物理的安全措施已经有数千年之久。相比之下，我们的数字化安全经验还不满50年”

参考

- 一个故事告诉你比特币的原理及运作机制
- 云风的BLOG: Bitcoin 的基本原理
- Mastering Bitcoin

THE END

讨论环节