区块链与数字货币

浙江大学 杨小虎

2019年11月11日

教学安排（共8周）

- 区块链技术原理
- 数字货币和区块链生态
- 以太坊技术原理与架构
- 智能合约概念及开发实践
- 区块链应用开发案例
- HyperLedger技术架构
- 企业级联盟链技术平台（Hyperchain、Libra）
- 数字货币和区块链发展趋势

课程考核

- 课程平时作业与课堂表现：50分
- 课程大作业：50分

作业	占总成绩比例	备注
作业1	10%	比特币
作业2	10%	数字货币
作业3	10%	以太坊
作业4	10%	HyperLedger
作业5	10%	Libra
大作业	50%	以太坊

蔡亮、李启雷、梁秀波著，

《区块链技术进阶与实战》，

人民邮电出版社，2018.

毛德操著，

《区块链技术》，

浙江大学出版社，2019.

参考资料：比特币、以太坊、HyperLedger、Libra等网上资料

推荐网站： http://book.8btc.com/

授课教师

杨小虎，浙江大学计算机软件研究所副所长、区块链研究中心副主任。

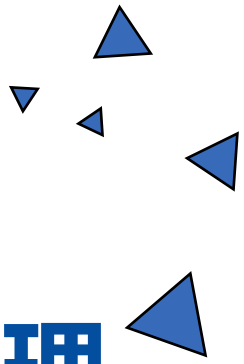
戎佳磊，浙江大学计算机学院硕士，以太坊go-ethereum客户端核心开发者，趣链科技高级架构师

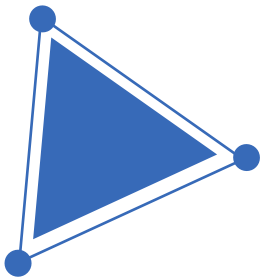
宣章炯 ，浙江大学软件工程硕士，HyperLedger Fabric开源项目重要贡献者，趣链科技高级架构师

2019冬区块链课程群

该二维码7天内(11月18日前)有效，重新进入将更新

01 区块链技术原理





起源

- 中本聪(Satoshi Nakamoto)，2008
- 比特币:一种点对点的电子现金系统

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

总共将发行2100万个比特币
目前已生成1800万个，目前市值约9000美元，
总市场规模估计在1600亿美元左右。

迄今最成功的区块链应用:
10年来没有出现过任何一次服务暂停
任何交易均可被追溯

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

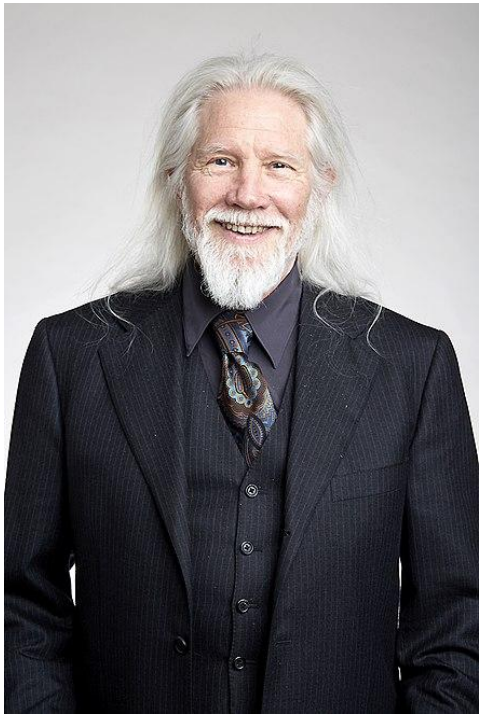
数字货币面临的2个问题

- **什么是货币？货币的基本属性？**

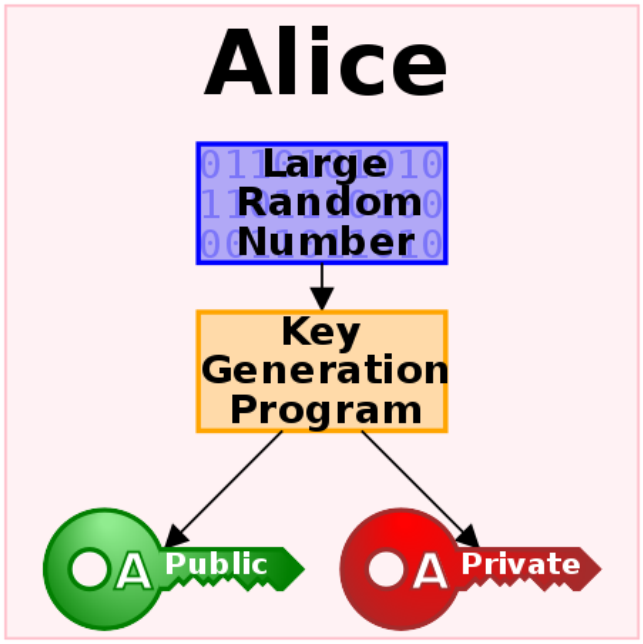
- **问题1：虚假货币**
  - 解决方案：数字签名（非对称加密技术）
- **问题2：多重支付**
  - 解决方案：分布式账本

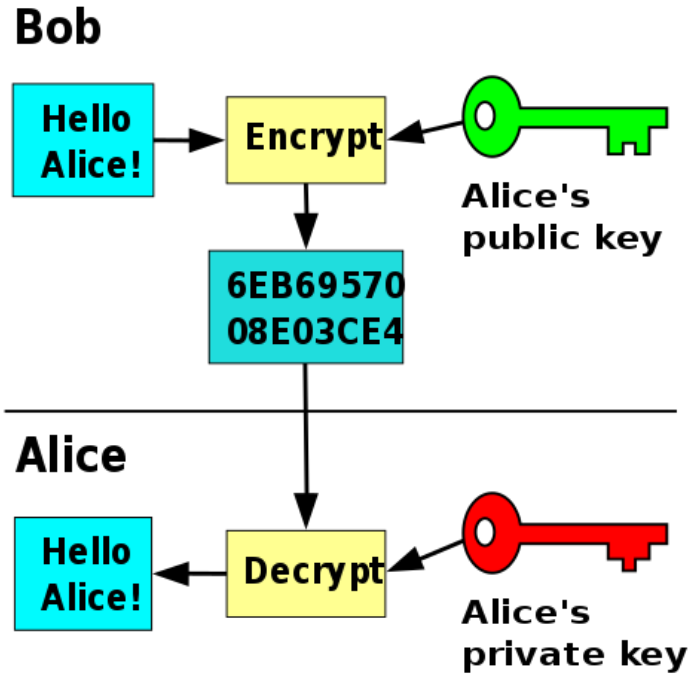
非对称加密算法

- 1970年，英国学者James H. Ellis提出设想
- 1976年，美国学者Whitfield Diffie and Martin Hellman首次提出一种可实现的非对称加密算法——exponentiation in a finite field

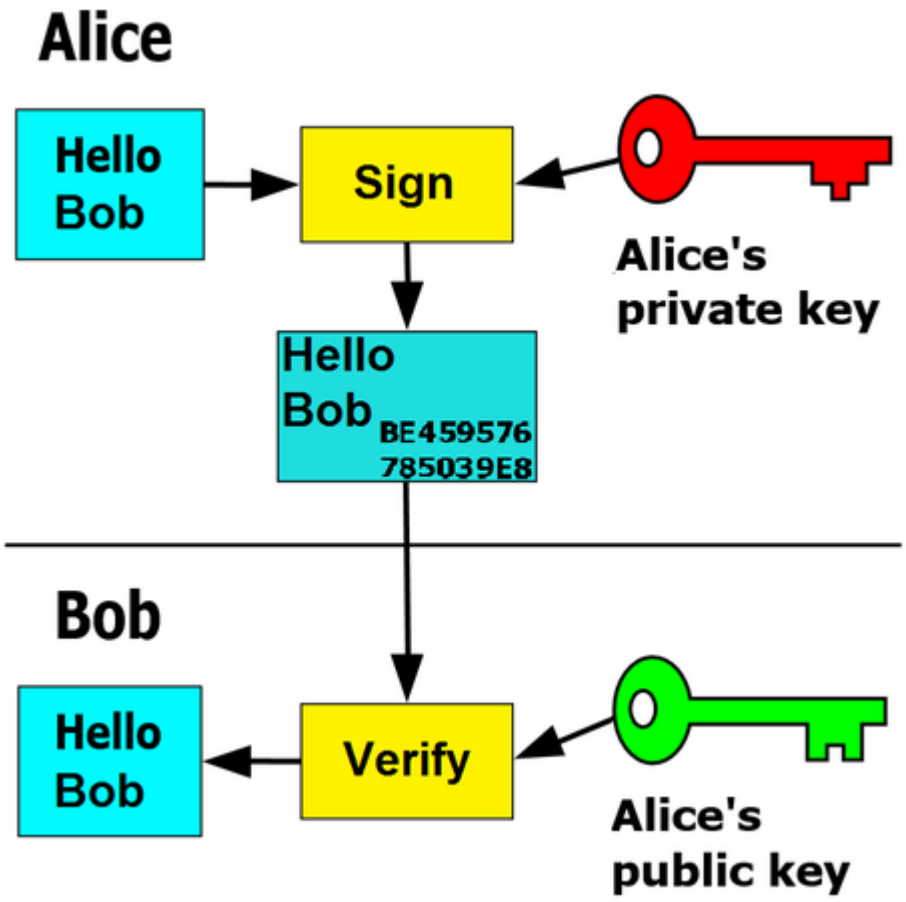


非对称加密算法


Alice
Large Random Number
Key Generation Program
Public
Private


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

数字签名


Alice
Hello
Bob
Sign
Alice's
private key
Hello
Bob
BE459576
785039E8
Bob
Hello
Bob
Verify
Alice's
public key

非对称加密算法

- 基于大素数分解难题：
  - RSA
- 基于离散对数难解问题：
  - 椭圆曲线加密
  - Diffie-Hellman 加密

数字货币面临的2个问题

- **问题1：虚假货币**
  - 解决方案：数字签名（非对称加密技术）
- **问题2：多重支付**
  - 解决方案：分布式账本

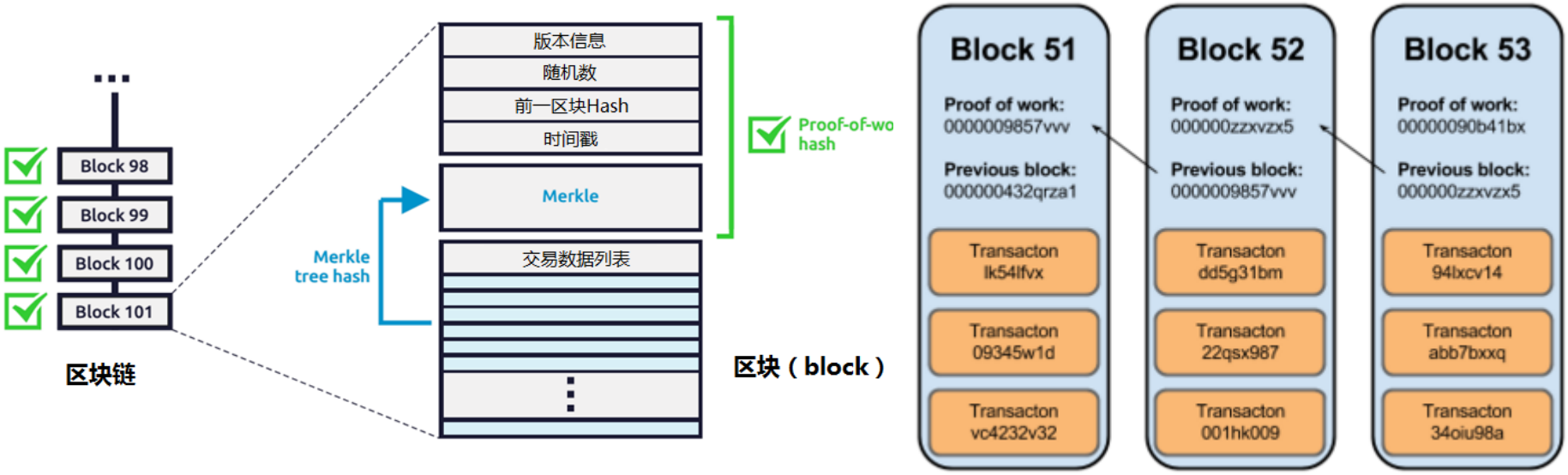
分布式账本技术原理

- 将交易向全网所有节点进行广播
- 由记账节点竞争记账权，胜出者把记账区块发布给全网
- 所有账本数据完整存储于区块链网络的每个节点
- 所有节点都对账本数据的合法性和完整性进行验证

- 两个核心技术：
  - 以链式区块组织账本数据实现账本数据的不可篡改
  - 分布式的可信记账机制

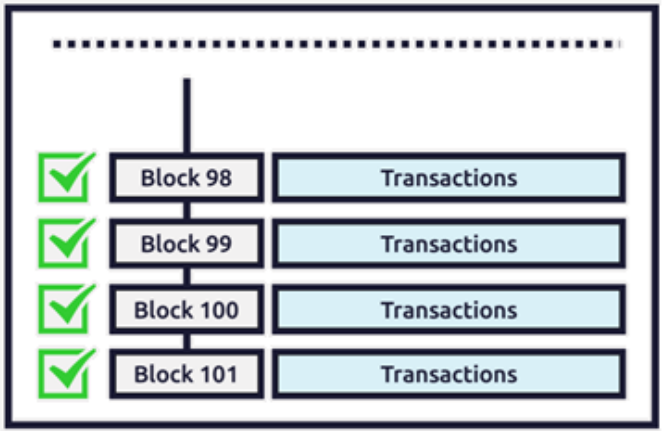
区块的微观结构

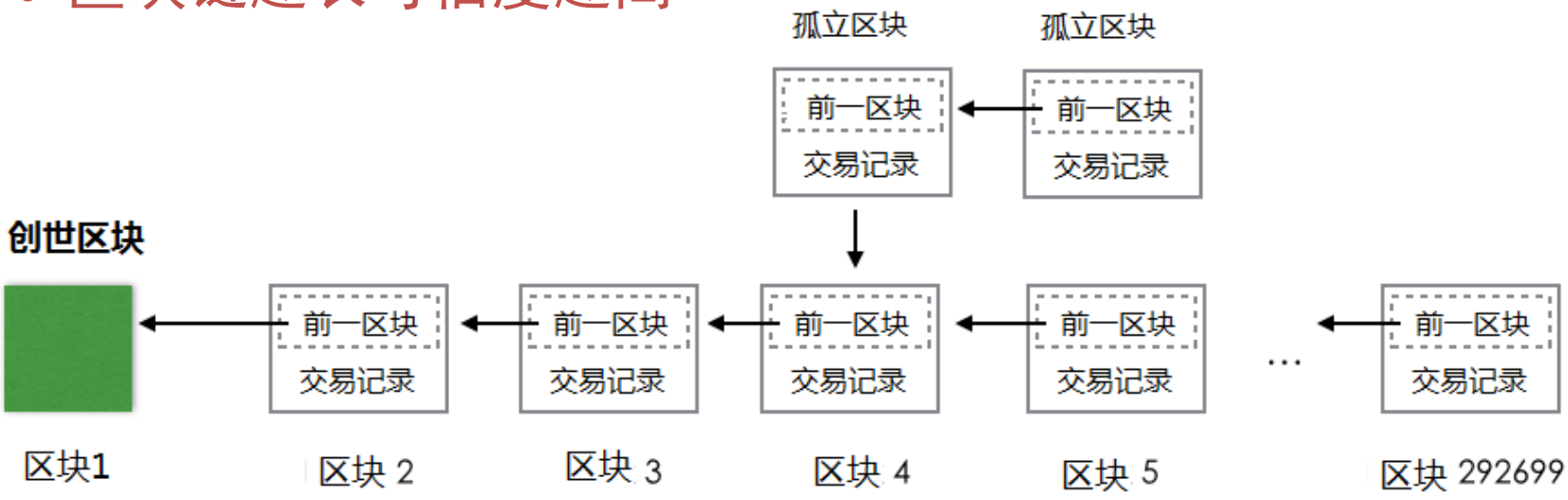
- 每个区块包括区块头和交易数据两个部分
  - 区块头由当前区块的元数据和前一区块的Hash值构成
  - Merkle树用于对交易数据列表进行快速寻址



区块链宏观结构

- **区块链**
  - 基于哈希值进行链接
- **特点**
  - 区块链中数据无法篡改或删除
  - 区块链越长可信度越高





区块的微观结构

区块的结构

大小	字段	描述
4字节	区块大小	用字节表示的该字段之后的区块大小
80字节	区块头	组成区块头的几个字段
1-9 字节（可变整数）	交易计数器	交易的数量
可变的	交易	记录在区块里的交易信息

区块头的结构

大小	字段	描述
4字节	版本	版本号，用于跟踪软件/协议的更新
32字节	父区块哈希值	引用区块链中父区块的哈希值
32字节	Merkle根	该区块中交易的merkle树根的哈希值
4字节	时间戳	该区块产生的近似时间（精确到秒的Unix时间戳）
4字节	难度目标	该区块工作量证明算法的难度目标
4字节	Nonce	用于工作量证明算法的计数器

区块的微观结构

区块标识符：区块头哈希值和区块高度

- 区块主标识符是它的加密哈希值，一个通过SHA256算法对区块头进行二次哈希计算而得到的数字指纹。例如:000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f是第一个比特币区块的区块哈希值。
- 区块哈希值实际上并不包含在区块的数据结构
- 第二种识别区块的方式是通过该区块在区块链中的位置，即“区块高度（block height）”。例如：高度为0的区块就是创世区块。
- 和区块哈希值不同的是，区块高度并不是唯一的标识符，因为有可能出现区块链分叉。

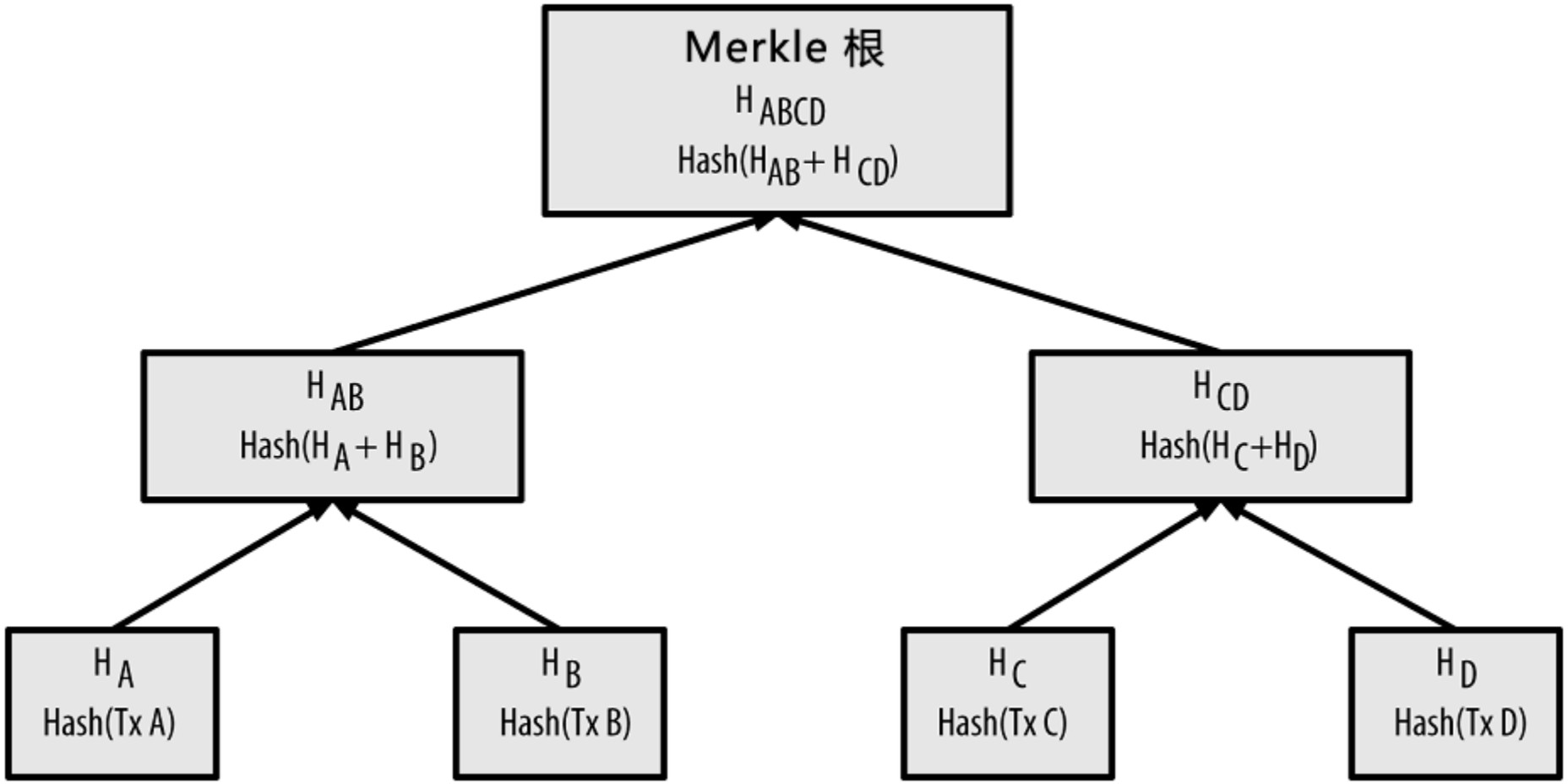
SHA256算法

- Hash算法，是一种从任何一种数据中创建小的数字“指纹”的方法，将数据打乱混合，重新创建一个叫做Hash值的指纹（摘要）。
- SHA-2，Secure Hash Algorithm 2的缩写，一种安全hash算法标准，由美国国家安全局National Security Agency研发。
- SHA256是SHA-2下细分出的一种算法，对于任意长度的输入数据，SHA256都会产生一个256bit长的哈希值，通常用一个长度为64的十六进制字符串来表示
  - 例如：A7FCFC6B5269BDCCE571798D618EA219A68B96CB87A0E21080C2E758D23E4CE9
- 算法的安全性：抗碰撞能力

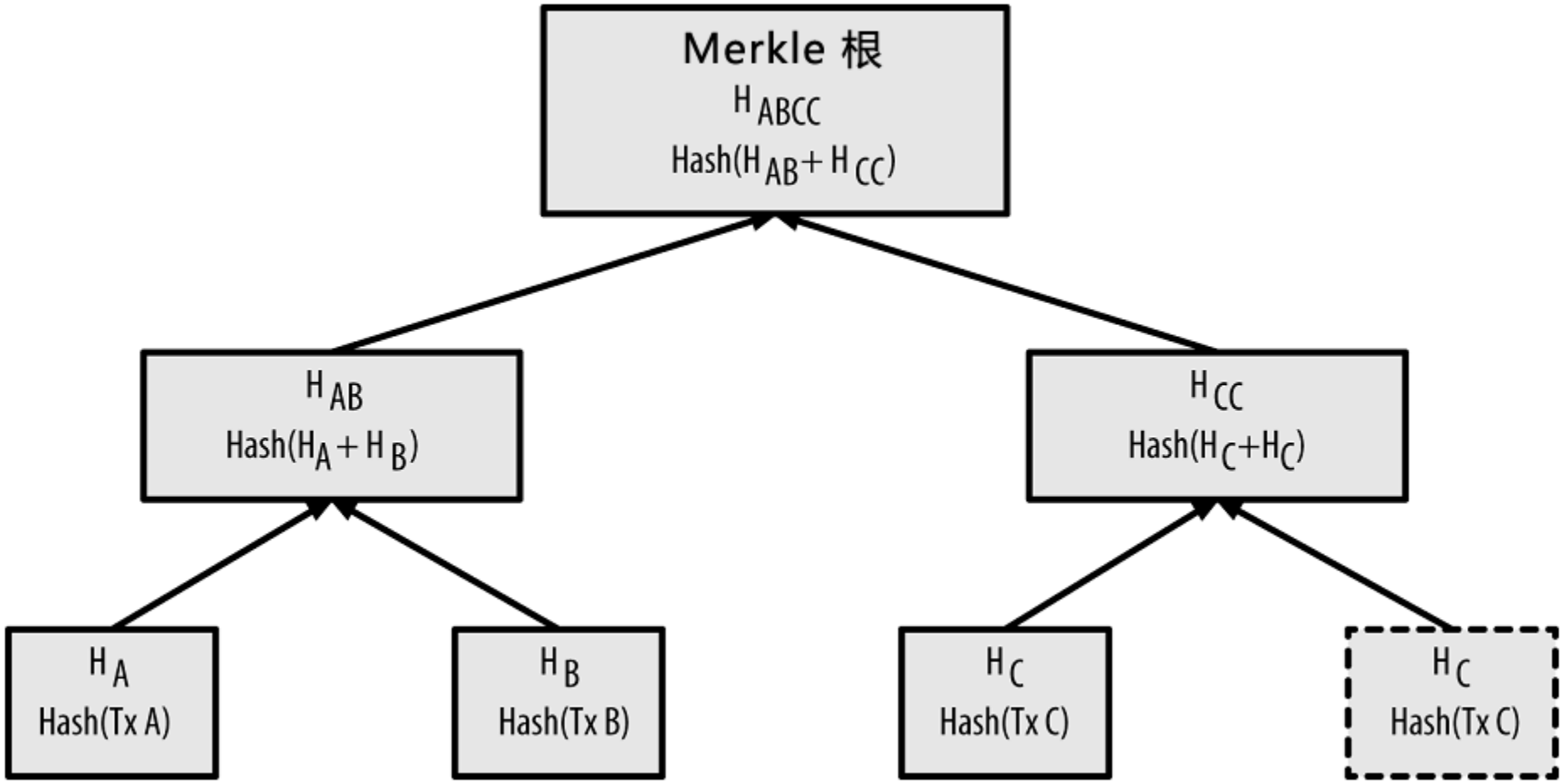
区块的微观结构：Merkle树

- Merkle树是一种哈希二叉树，它是一种用作快速归纳和校验大规模数据完整性的数据结构。这种二叉树包含加密哈希值。
- 在比特币网络中，Merkle树被用来归纳一个区块中的所有交易，同时生成整个交易集合的数字指纹，且提供了一种校验区块是否存在某交易的高效途径。
- Merkle树中使用两次SHA256算法计算结点的哈希值。
  - H~A~ = SHA256(SHA256(交易A))
- 当N个数据元素经过加密后插入Merkle树时，你至多计算log2(N)次就能检查出任意某数据元素是否在该树中，这使得该数据结构非常高效。

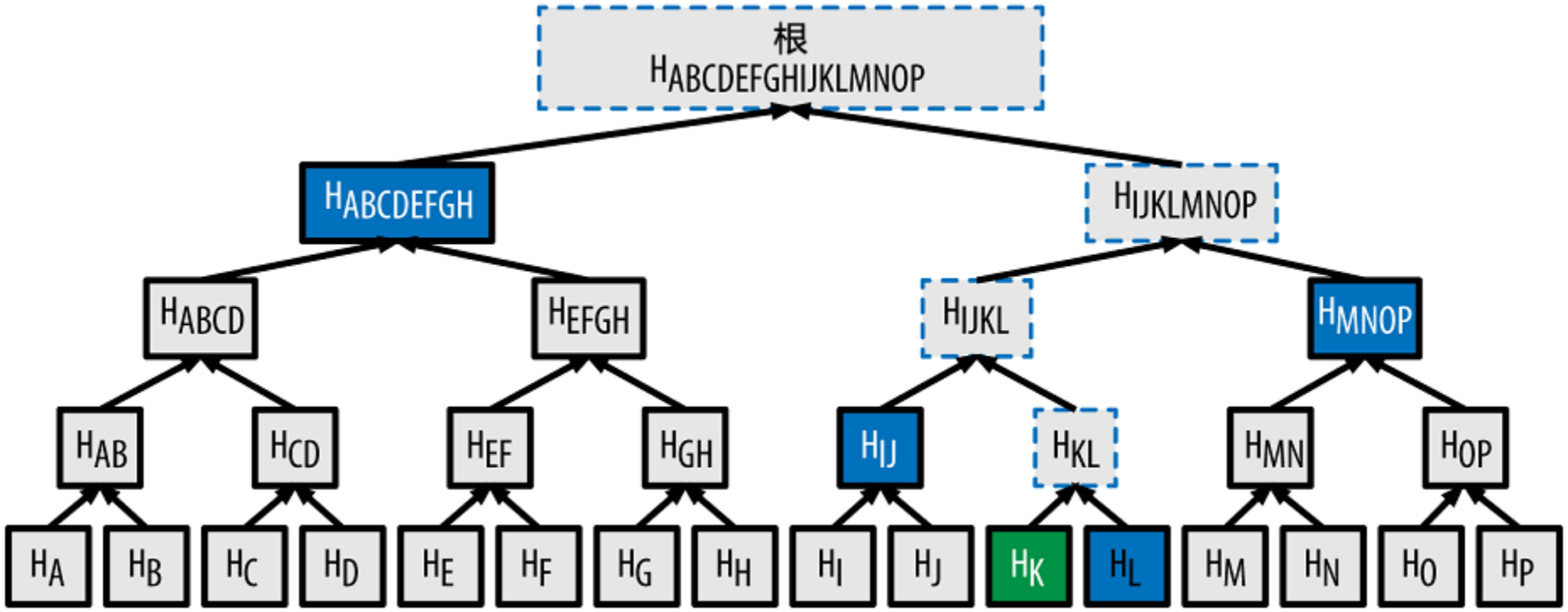
区块的微观结构：Merkle树



区块的微观结构：Merkle树



区块的微观结构：Merkle树



Merkle树的价值

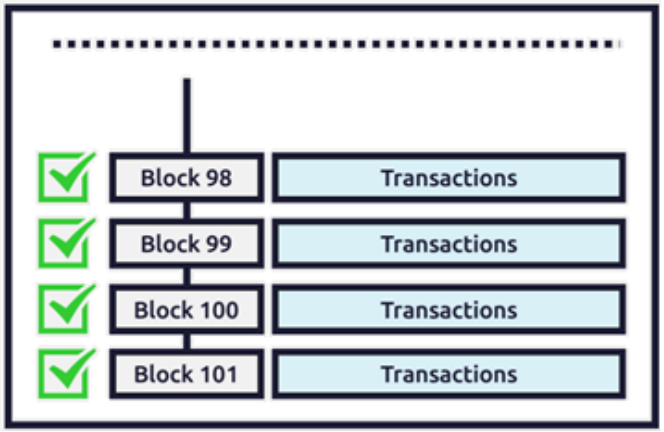
交易数量	区块的近似大小	路径大小（哈希数量）	路径大小（字节）
16笔交易	4KB	4个哈希	128字节
512笔交易	128KB	9个哈希	288字节
2048笔交易	512KB	11个哈希	352字节
65,535笔交易	16MB	16个哈希	512字节

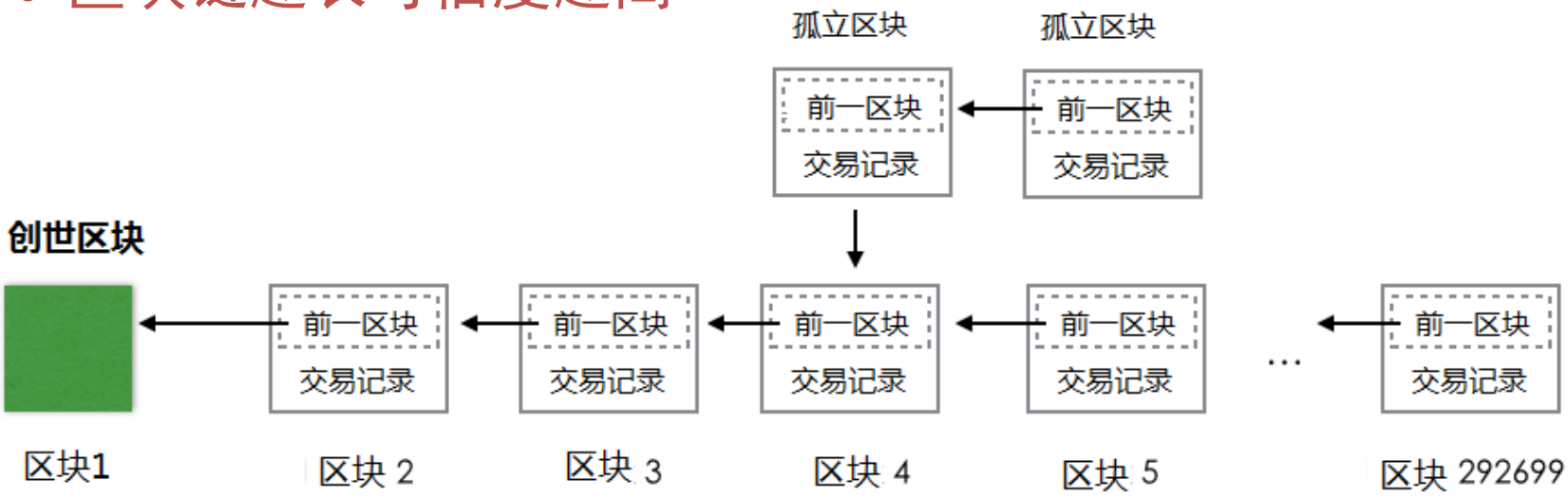
有了Merkle树，一个节点能够仅下载区块头（80字节/区块），然后通过从一个满节点回溯一条Merkle路径就能认证一笔交易的存在，而不需要存储或者传输区块链中大多数内容。

这种不需要维护一条完整区块链的节点，又被称作简单支付验证（SPV）节点，它不需要下载整个区块而通过Merkle路径去验证交易的存在。

区块链宏观结构

- **区块链**
  - 基于哈希值进行链接
- **特点**
  - 区块链中数据无法篡改或删除
  - 区块链越长可信度越高



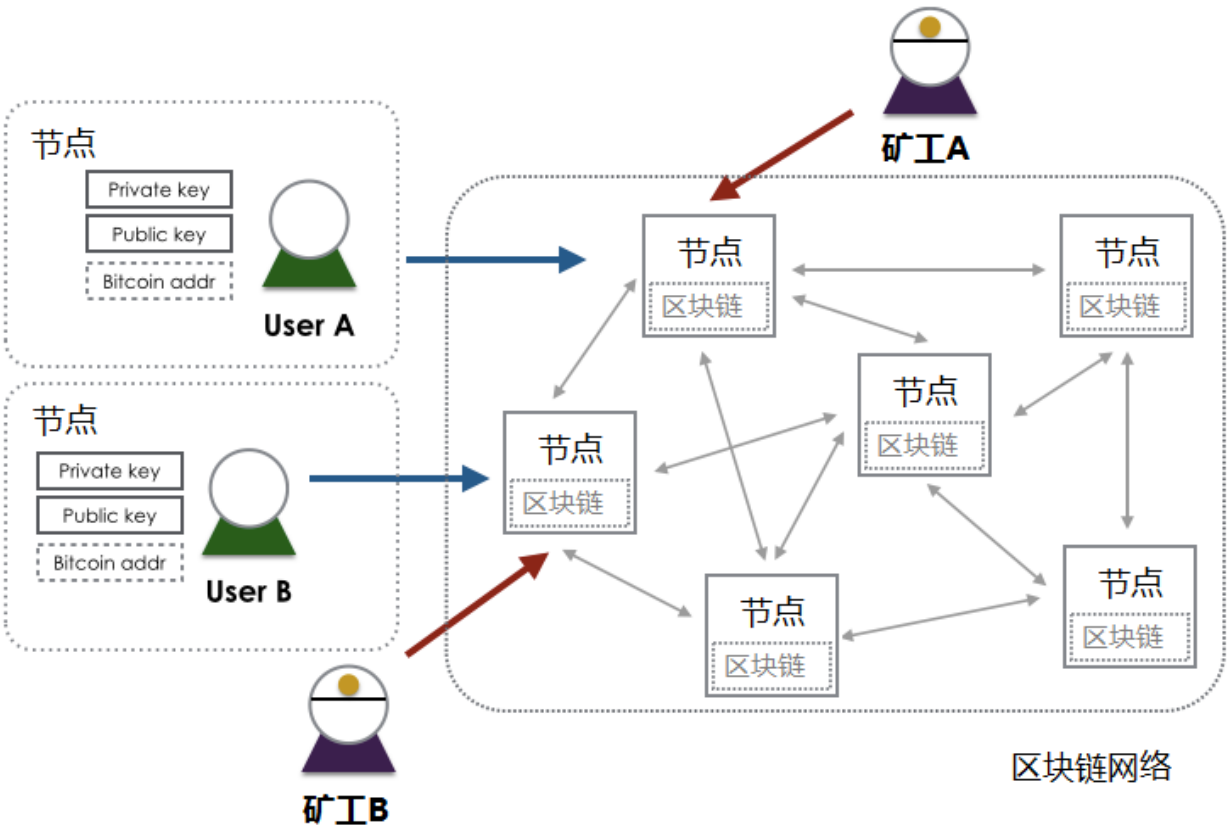


分布式账本技术原理

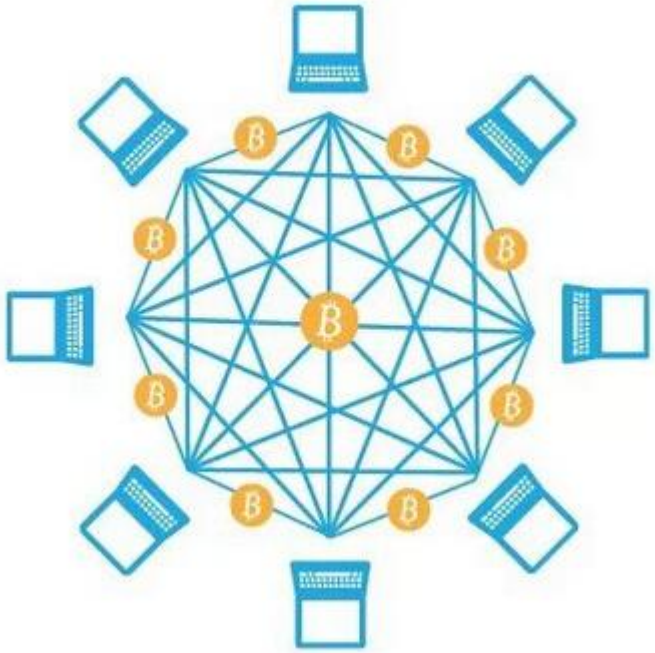
- 将交易向全网所有节点进行广播
- 由记账节点竞争记账权，胜出者把记账区块发布给全网
- 所有账本数据完整存储于区块链网络的每个节点
- 所有节点都对账本数据的合法性和完整性进行验证

- 两个核心技术：
  - 以链式区块组织账本数据实现账本数据的不可篡改
  - 分布式的可信记账机制

共识机制：由谁记账

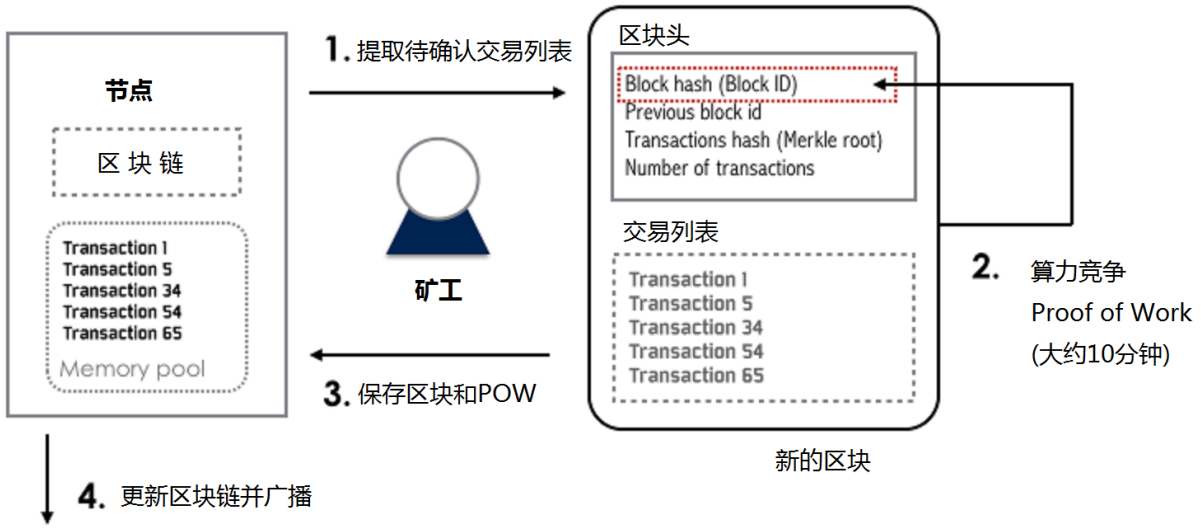

节点
Private key
Public key
Bitcoin addr
User A
节点
Private key
Public key
Bitcoin addr
User B
矿工B
矿工A
节点
区块链
节点
区块链
节点
区块链
节点
区块链
节点
区块链
节点
区块链
区块链网络

拜占庭将军问题（共识机制）



共识机制：由谁记账

- **目的**
  - 解决记账权——分布式系统中的拜占庭将军问题
- **技术原理**
  - 工作量证明（proof of work）：高强度哈希计算(SHA256)进行算力竞争解决记账权



SHA256算力竞争

- I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
- I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
- I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
- I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
- I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
- I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
- I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
- I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
- I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
- I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
- I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
- I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
- I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
- I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
- I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
- I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
- I am Satoshi Nakamoto16 => 8fa4992219df33f50834465d3047429...
- I am Satoshi Nakamoto17 => dca9b8b4f8d8e1521fa4eaa46f4f0cd...
- I am Satoshi Nakamoto18 => 9989a401b2a3a318b01e9ca9a22b0f3...
- I am Satoshi Nakamoto19 => cda56022ecb5b67b2bc93a2d764e75f...

工作量证明的难度设定和调整

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

- 例如：
  - target =0x00000000000000003A30C00000000000000000000000000000000000000000

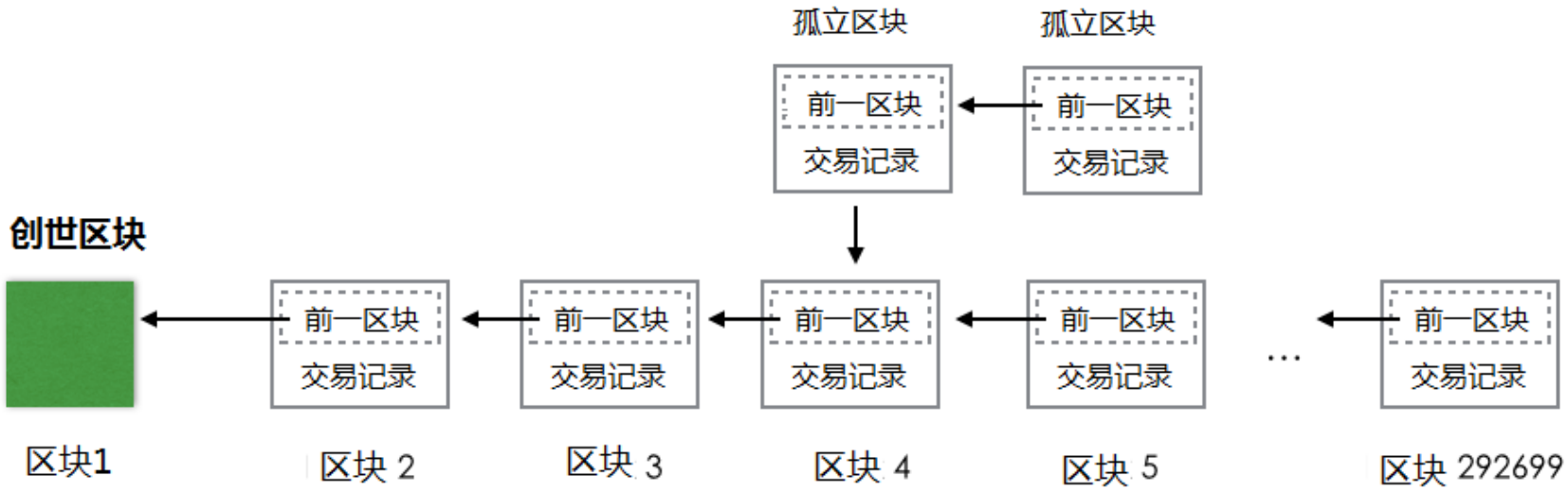
- 在每个完整节点中独立自动发生的。每2,016个区块中的所有节点都会调整难度。难度的调整公式是由最新2,016个区块的花费时长与20,160分钟（两周，即这些区块以10分钟一个速率所期望花费的时长）比较得出的。难度是根据实际时长与期望时长的比值进行相应调整的（或变难或变易）。简单来说，如果网络发现区块产生速率比10分钟要快时会增加难度。如果发现比10分钟慢时则降低难度。

区块生成和组装

- 竞争胜出的节点创建区块并广播
- 其他独立节点校验新区块
- 区块链的组装和选择（根据父区块hash值查找父区块）
  - 连接到主链上
  - 分叉（备用链）
  - 孤立区块

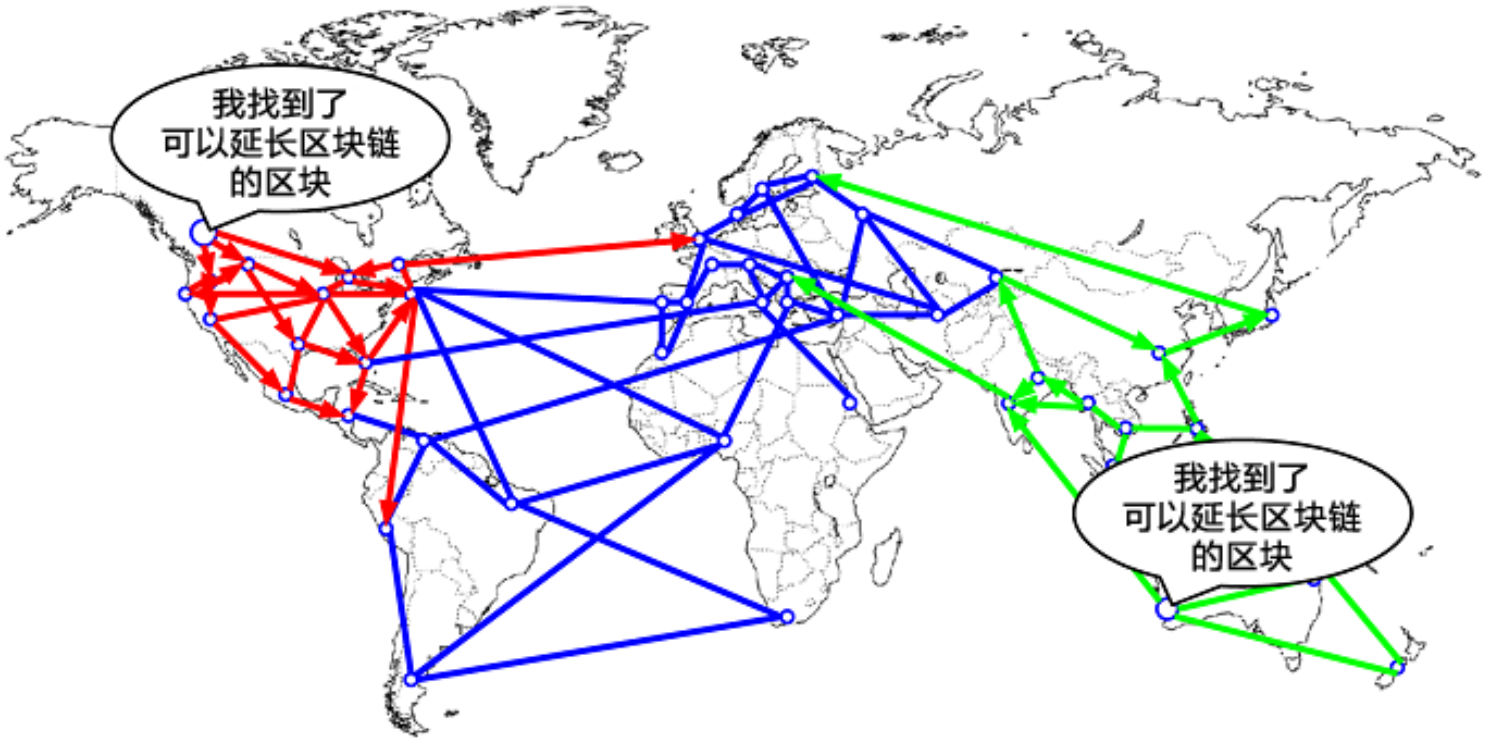
区块链分叉解决方案

- 把当前同一个父区块下的若干有效子区块都记录，形成兄弟区块（产生分叉）
- 后续区块（第3代、第4代……）到达后，依次加在前序区块后，若没有其他竞争性区块，这一分支最长，成为主链。

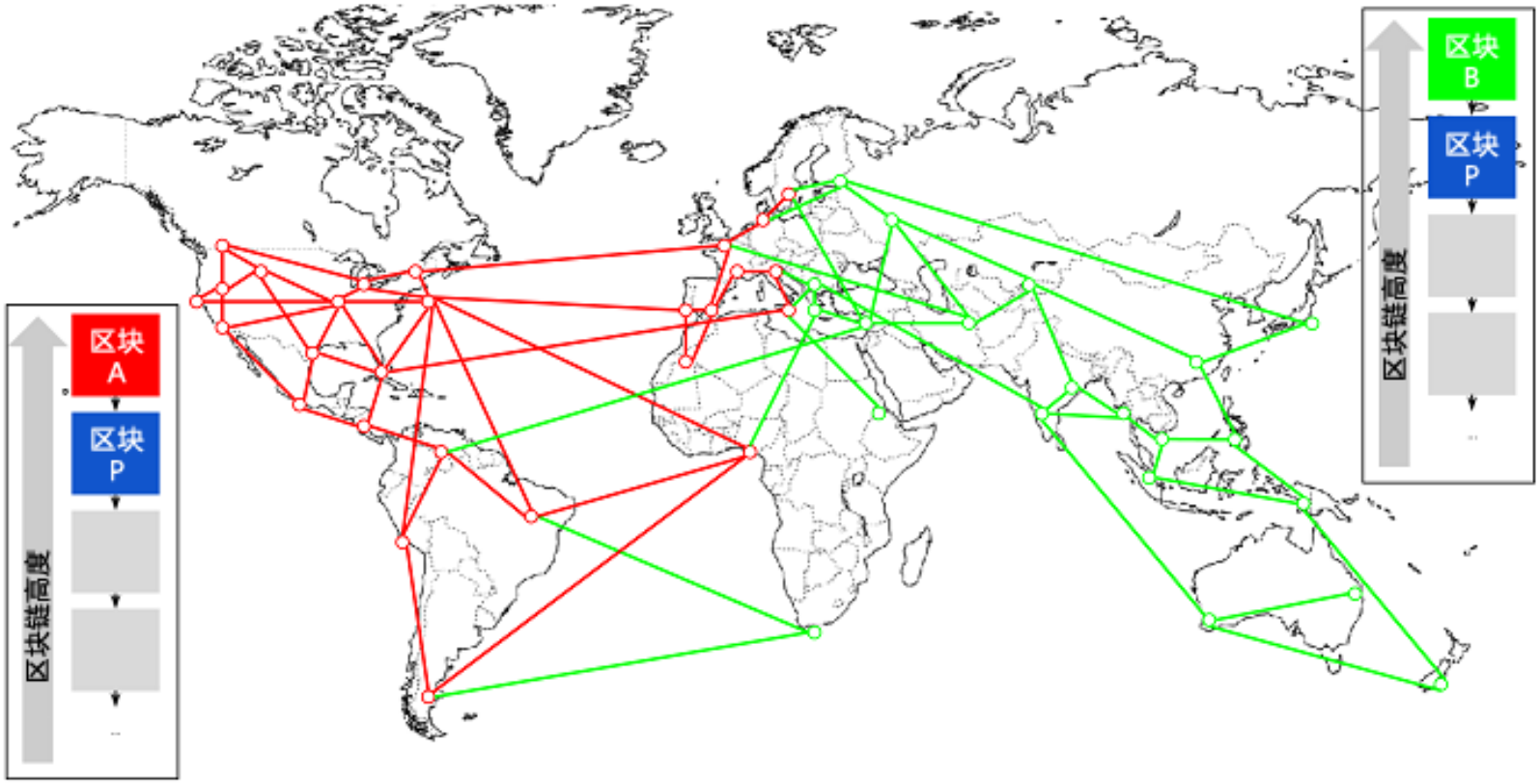


区块链分叉

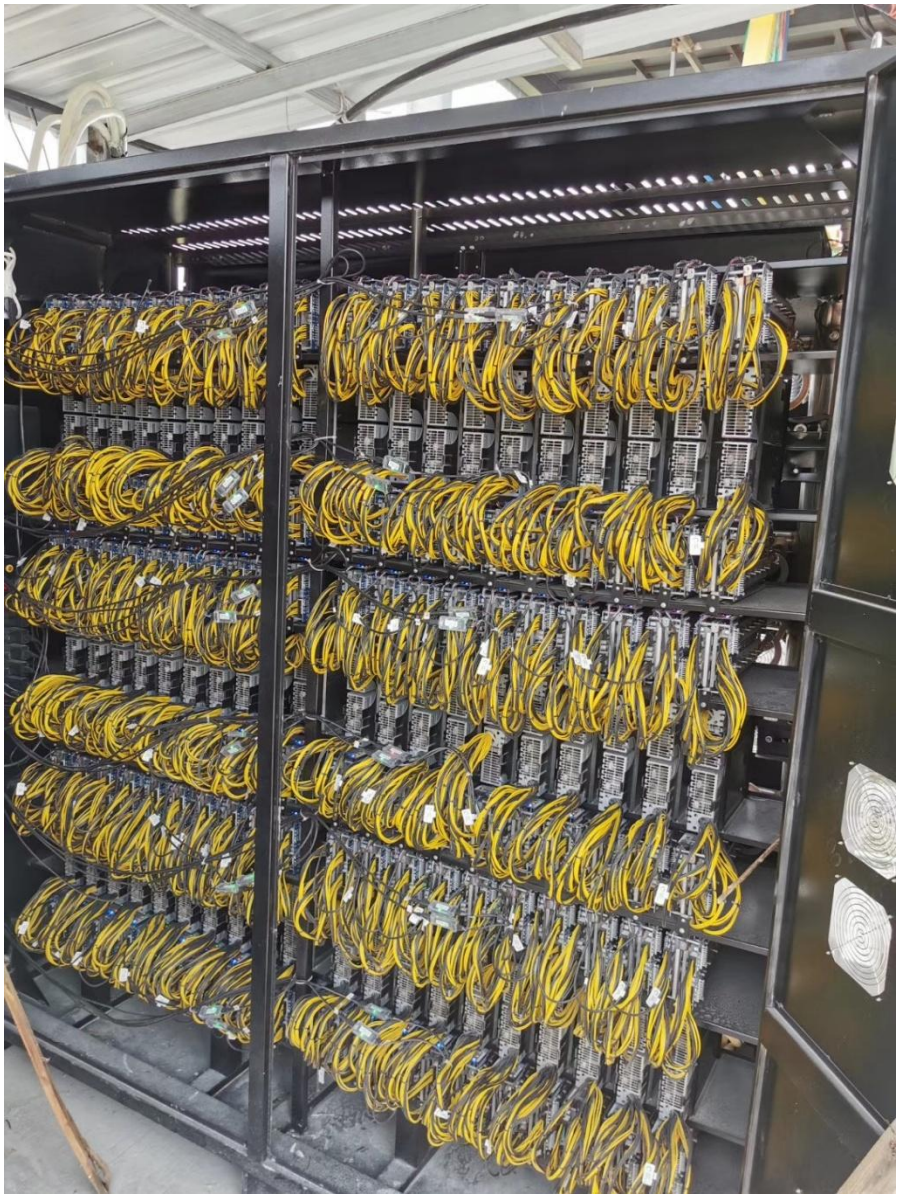
区块链分叉



区块链分叉



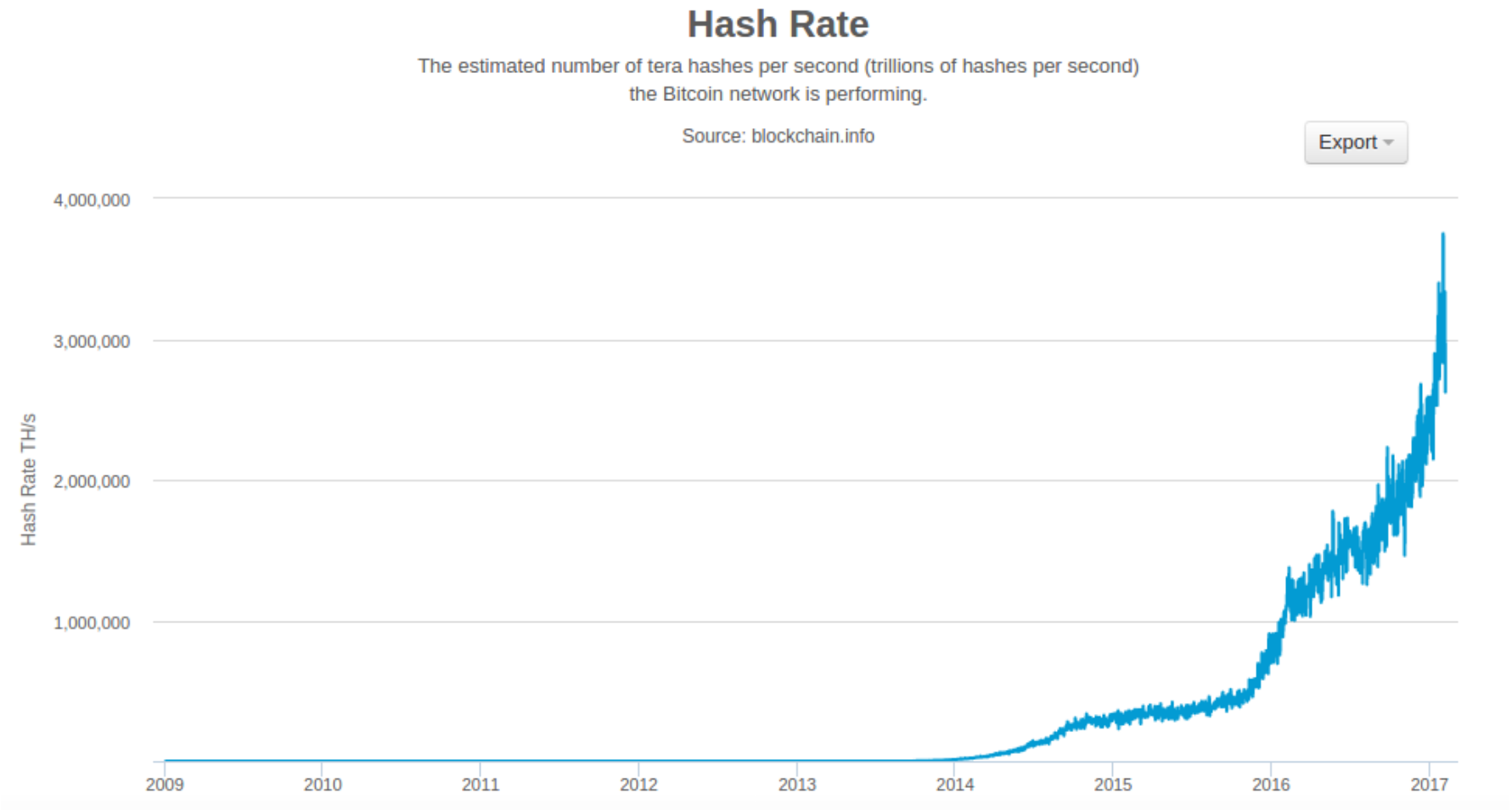
挖矿



挖矿：算力竞争

- 2009 0.5 MH/sec－8 MH/sec （16× growth）
- 2010 8 MH/sec－116 GH/sec （14,500× growth）
- 2011 16 GH/sec－9 TH/sec （562× growth）
- 2012 9 TH/sec－23 TH/sec （2.5× growth）
- 2013 23 TH/sec－10 PH/sec （450× growth）
- 2014 10 PH/sec－300 PH/sec （3000× growth）
- 2015 300 PH/sec-800 PH/sec （266× growth）
- 2016 800 PH/sec-2.5 EH/sec （312× growth））

挖矿：算力竞争


Hash Rate
The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.
Source: blockchain.info
Export
Hash Rate TH/s
4,000,000
3,000,000
2,000,000
1,000,000
2009
2010
2011
2012
2013
2014
2015
2016
2017

共识记账机制

- 每个全节点依据综合标准对每个交易进行独立验证
- 通过完成工作量证明算法的验算，挖矿节点将交易记录独立打包进新区块，
- 每个节点独立地对新区块进行校验并组装进区块链
- 每个节点对区块链进行独立选择，在工作量证明机制下选择累计工作量最大的区块链

UTXO——比特币账户模型

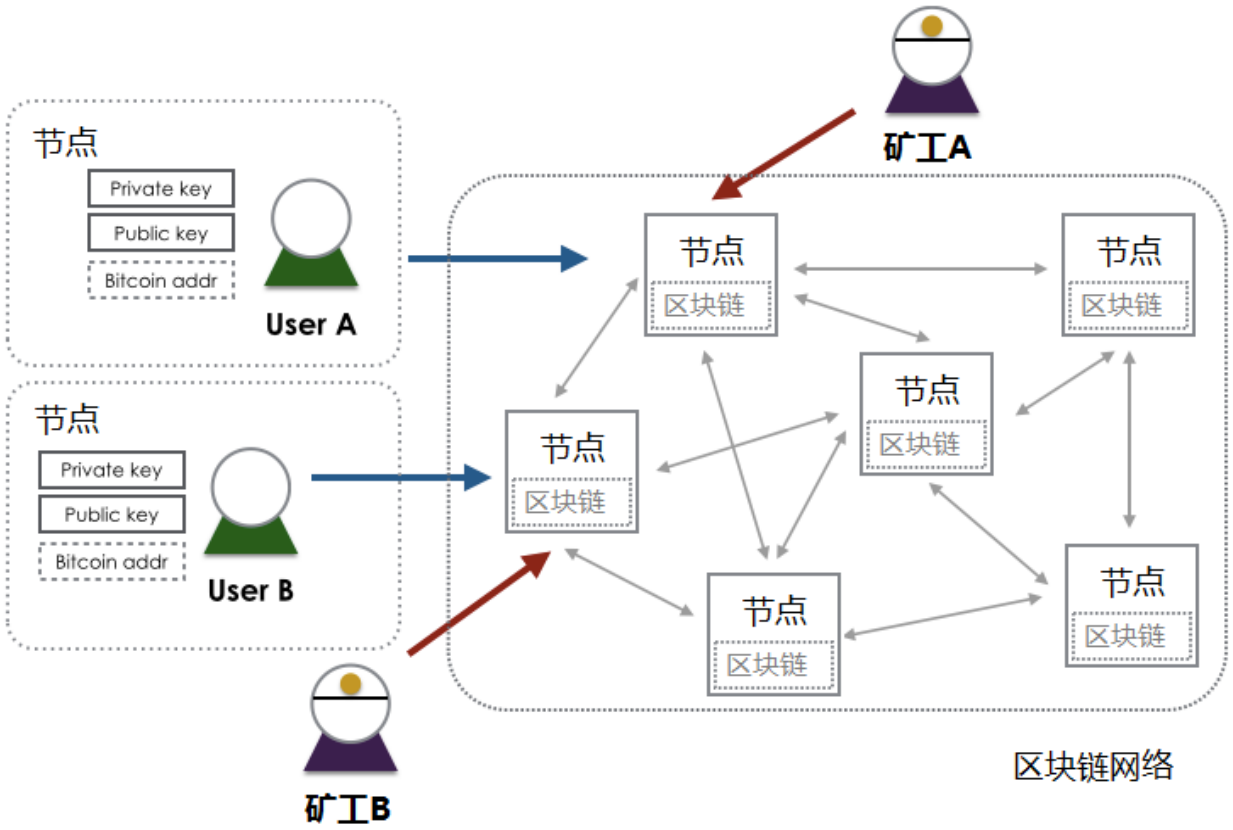
- 每个比特币用户有一个160位（20字节）长度的地址，产生的过程：
  - 用户生产一对非对称密钥
  - 公钥经hash计算产生160位的地址
  - 私钥自己保存，用于数字签名
- 这个160位地址，是用户在比特币网络中交易的唯一标识。
- 与一般的银行账户模型不同，比特币不维护每个账户的资金余额。

UTXO——比特币账户模型

- UTXO（Unspent Transaction Output），未花费的交易输出
- 比特币中有两类交易：
  - 常规交易，有交易输入（支付者地址和金额）、交易输出（收入者地址和金额）
  - 挖矿交易（Coinbase），产生比特币，只有交易输出（挖矿者地址和金额）
- 每个地址的资金余额就是散布在账本中所有UTXO的总和，使用时把自己名下的UTXO作为交易输入，可能需要拼凑找零。

区块链技术的定义

- 区块链技术是一种以非对称加密技术对交易进行数字签名，通过工作量证明等共识机制进行记账节点协调，数据以链式区块形式组织存储的分布式账本技术。



区块链支撑技术

- 非对称加密与数字签名
- 哈希计算：SHA256算法
- 链式区块结构
- Merkle树
- 共识机制
  - 拜占庭将军问题（Byzantine Generals Proglem）
  - PoW, PoS, DPoS, PBFT
  - Paxos算法

区块链技术的优点

- **去中心化**：避免垄断，点对点交易，去代理
- **数据公开**：无暗箱操作，平等性，开放生态体系
- **可信**：数据永久可靠，记录可信
  - 信任体系、价值传递体系

区块链技术的问题

- **隐私问题**
  - 匿名地址如何监管
- **性能问题**
  - 交易确认时间长
  - 区块容量有限
- **系统性风险**
  - 区块链分叉和51%攻击

作业1

- 说明比特币区块链中区块的组装生成过程和验证入链过程。

- 提交格式：word文件
- 文件名：姓名+学号+作业1.docx
- 提交邮箱：csyxh@zju.edu.cn
- 提交截止日期：2019年11月20日中午12点

深入阅读

- 比特币白皮书
- 比特币源码
- 《精通比特币》，Andreas M. Antonopoulos
- *Mastering Bitcoin*, Andreas M. Antonopoulos

2019冬区块链课程群

该二维码7天内(11月18日前)有效，重新进入将更新

谢谢！