

# 区块链技术

# Course Overview

## 上次课程内容

1 史前

2 初识

3 回顾

4 剖析

- 交易
- 交易历史
- 金融创新
- 记账历史

- 区块链定义
- 账本集vs.分
- 区块链结构
- 租车例子

- 区块链起源
- 比特币
- 区块链发展
- 智能合约
- ICO

- 计算视角
- 网络视角
- 社会视角
- 面临挑战

# Course Overview

## 本次课程内容

1 区块

- Hash算法
- Hash指针
- 梅克尔树
- 区块结构

2 密码

- 密码学
- 公钥密码学
- 公钥管理
- 数字签名

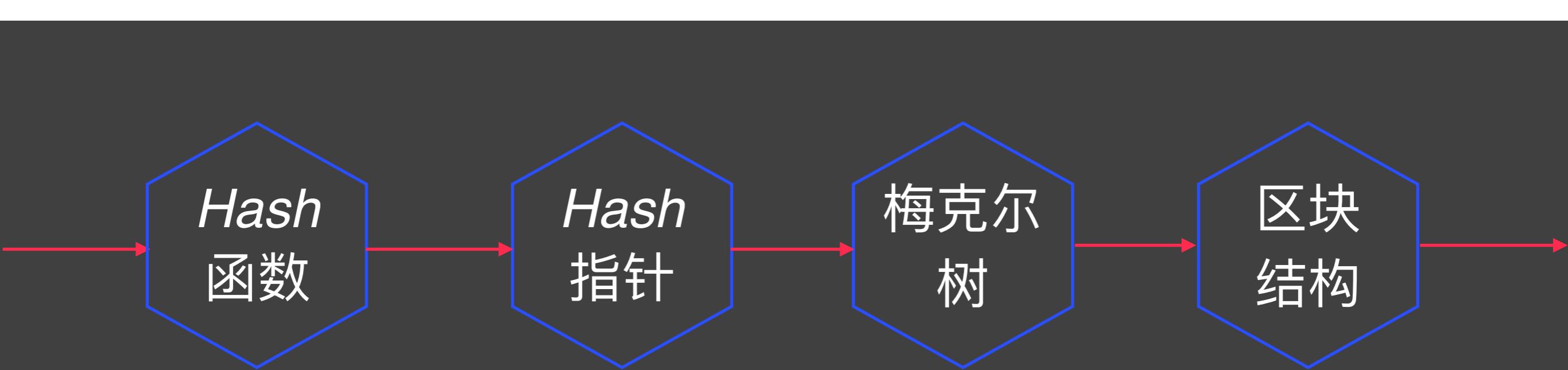
3 共识

- P2P
- 分布共识
- 比特币共识
- 隐性共识

4 挖矿

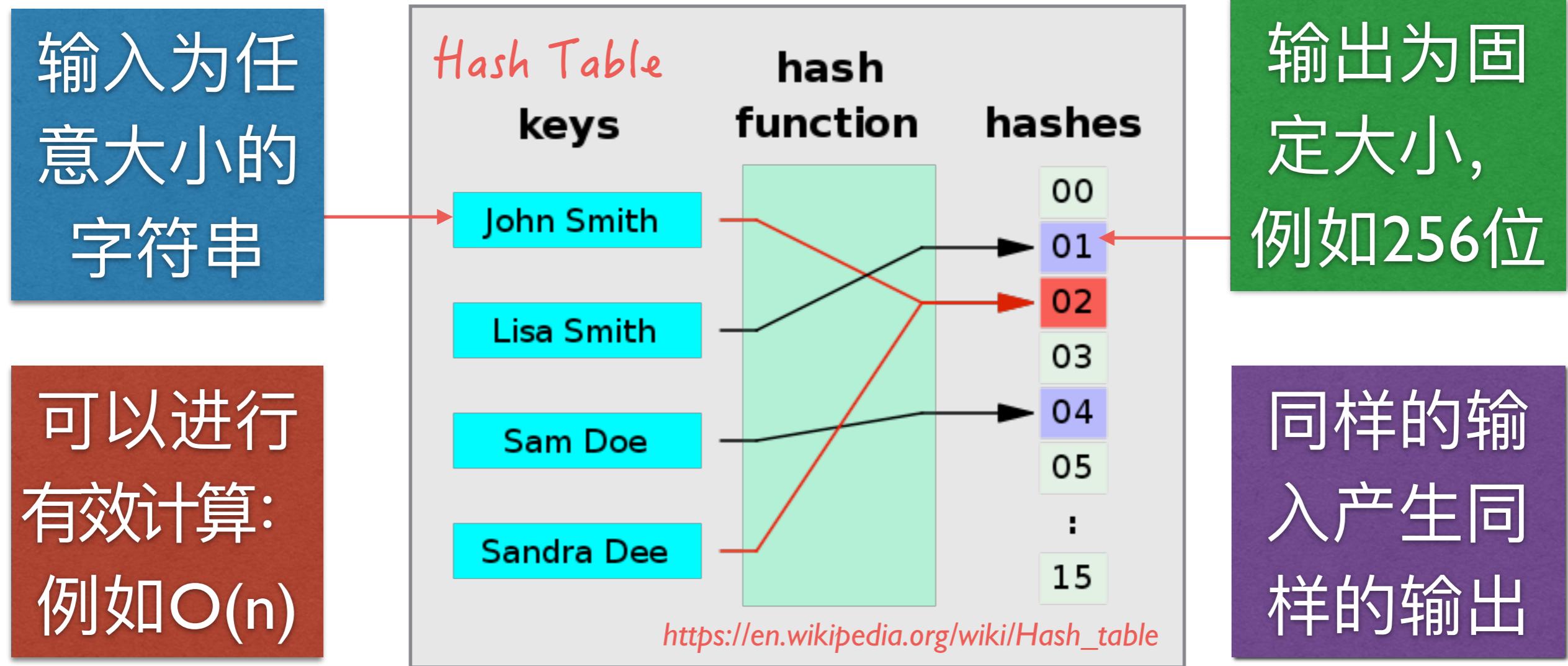
- 矿工任务
- 有效区块
- 激励机制
- 矿机矿池

# 区块



# Hash函数

[https://en.wikipedia.org/wiki/Hash\\_function](https://en.wikipedia.org/wiki/Hash_function)



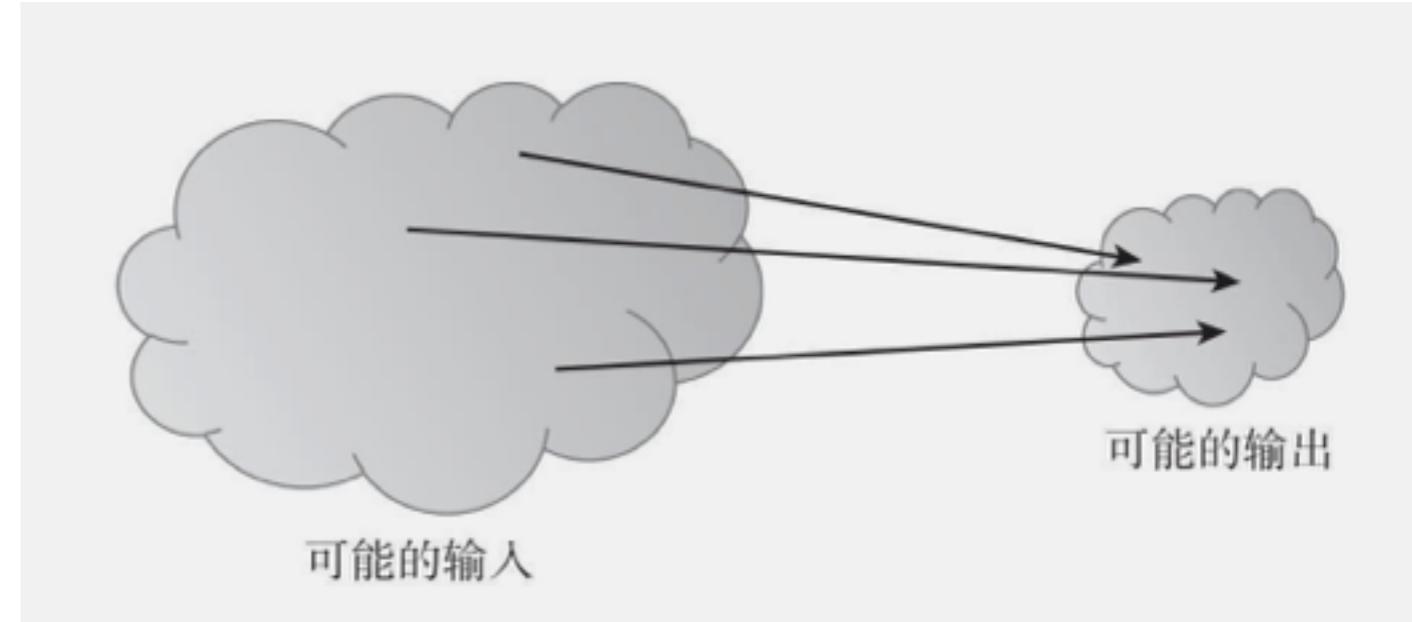
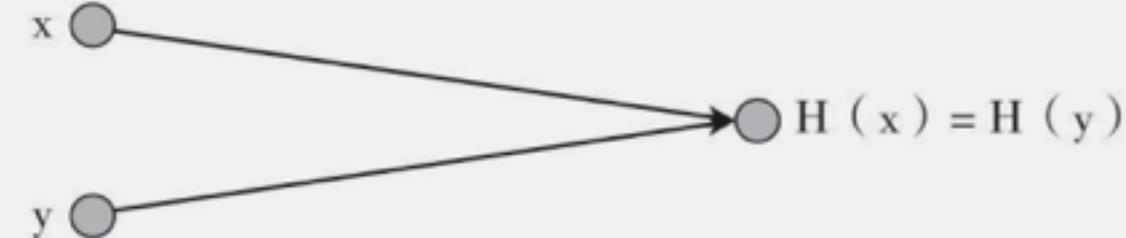
可以进行有效计算：  
例如 $O(n)$

同样的输入产生同样的输出

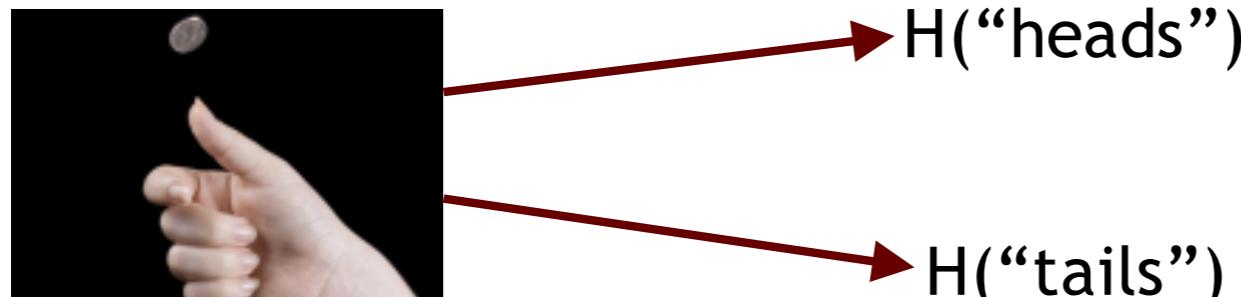


## Hash函数

抗碰撞



隐匿性



给出 $H(x)$ , 不能找到 $x$

单向性

已知 $x$ , 计算 $H(x)$ 容易

已知 $H(x)$ , 求 $x$ 困难

难题友好

## Hash指针

Hash指针：  
是一个指向存储数据  
及其数据Hash的指针

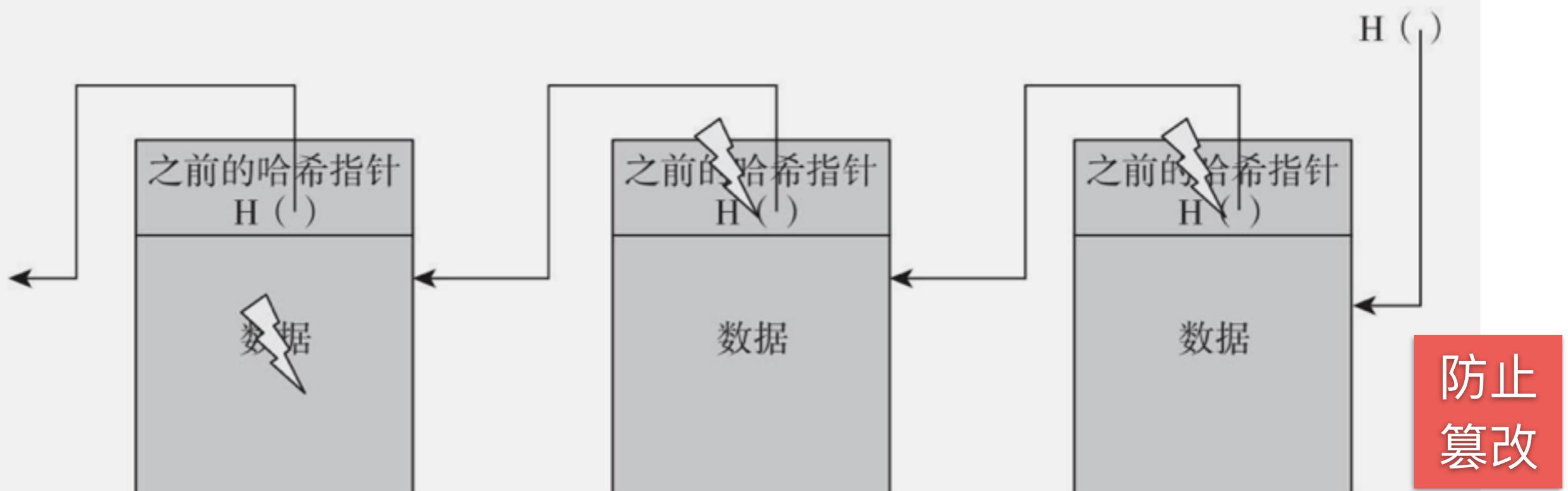
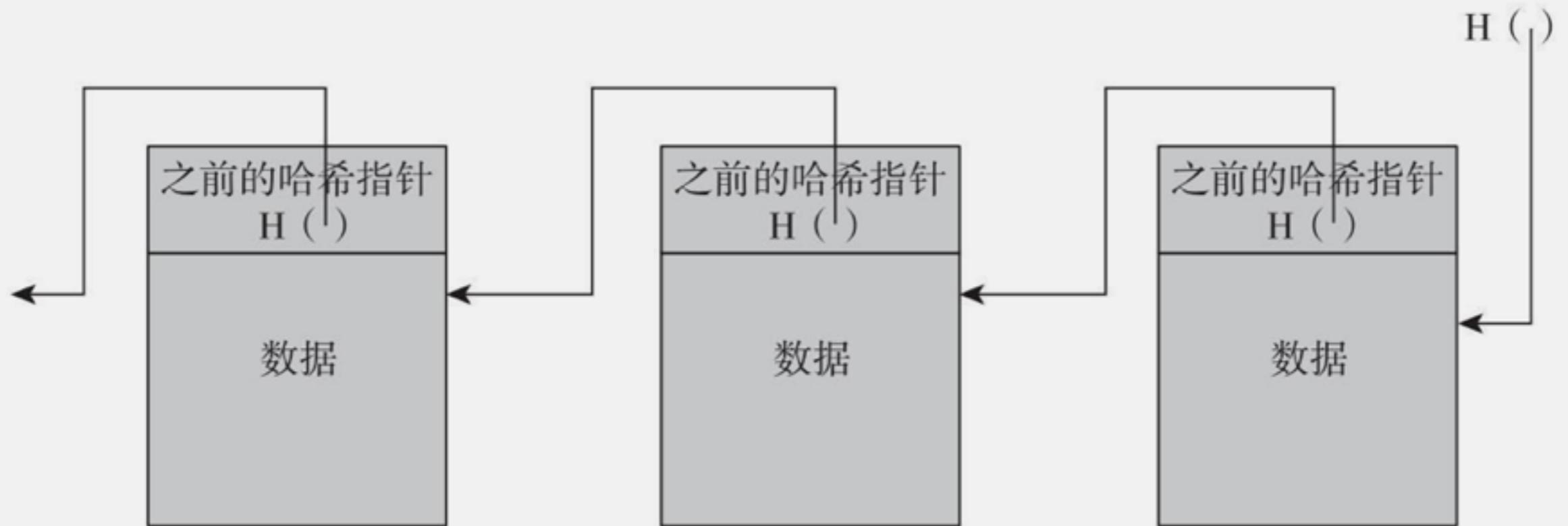
取回数据  
验证数据是否改变

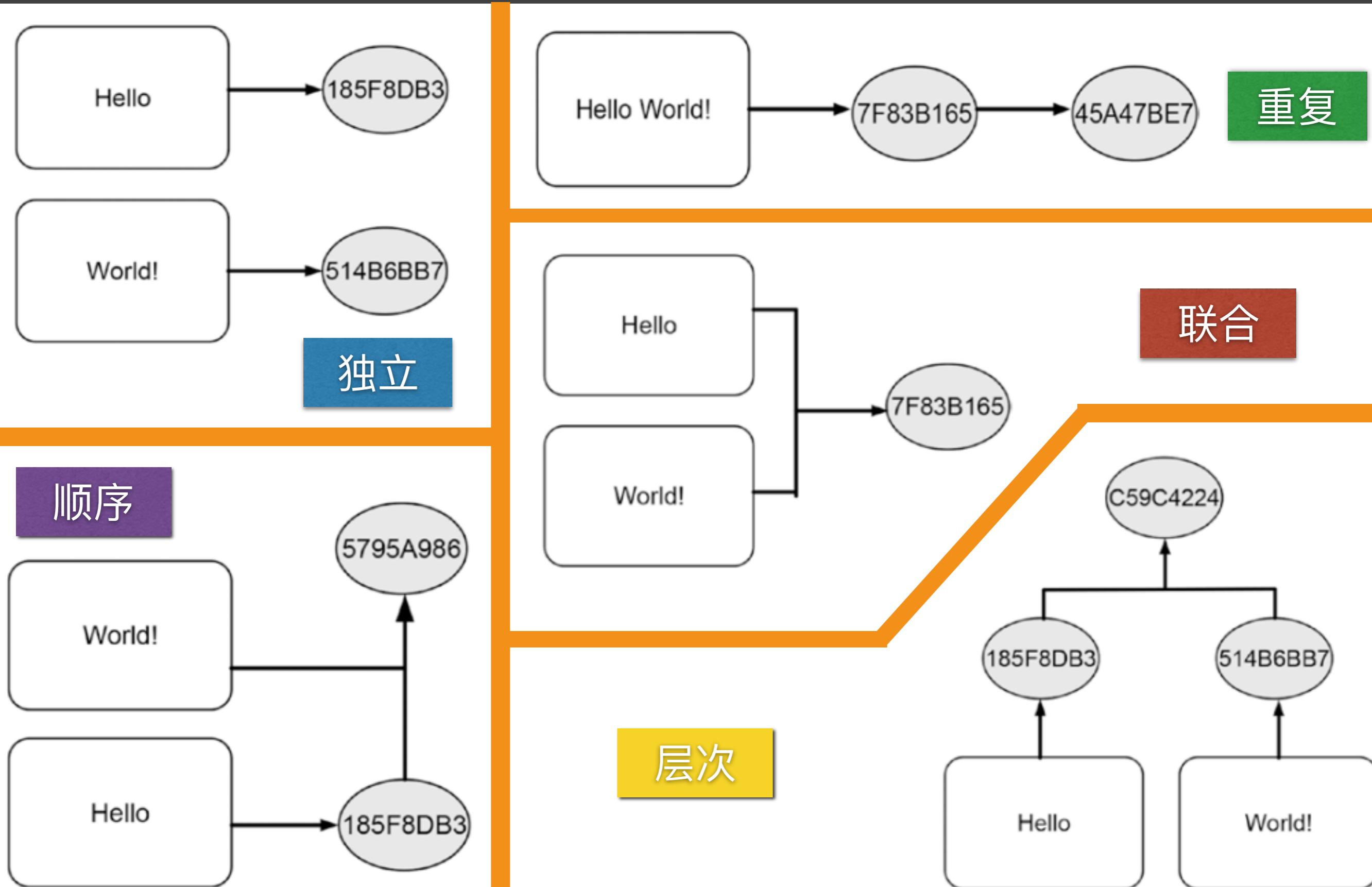
区块链的关键思想



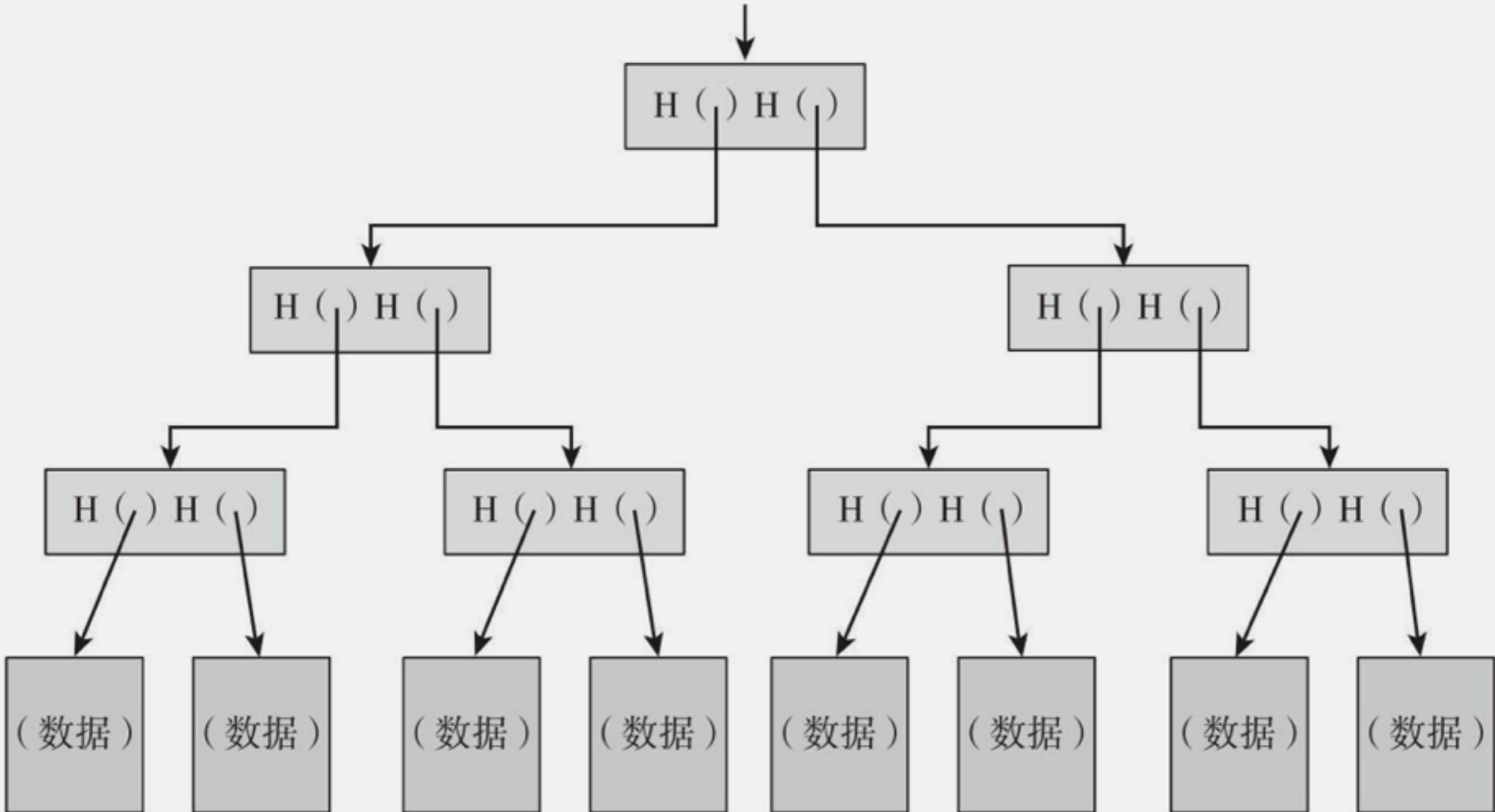
( 数据 )

# 区块链



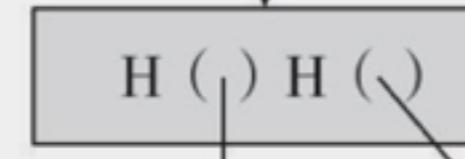
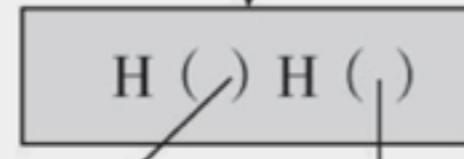
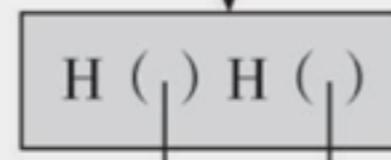
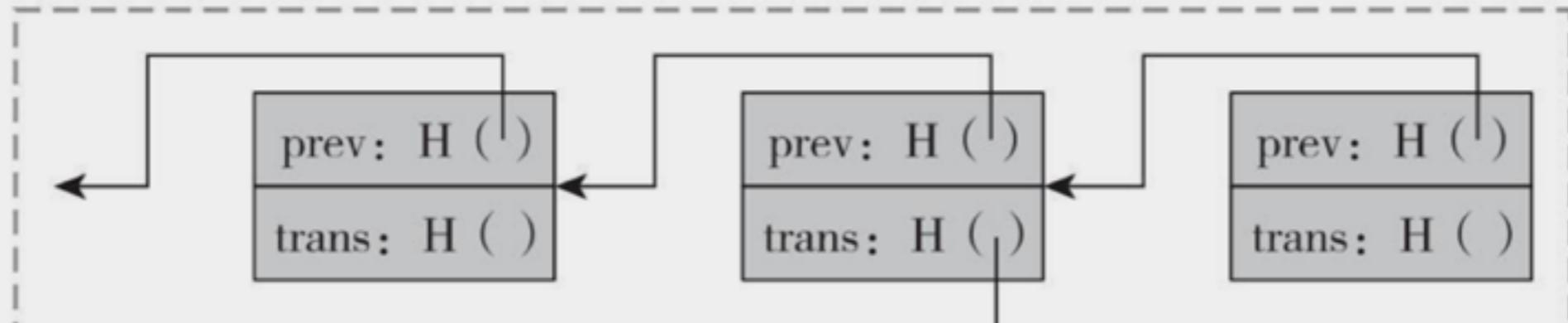


# 梅克尔树



# 区块结构

区块的哈希链



交易

交易

交易

交易

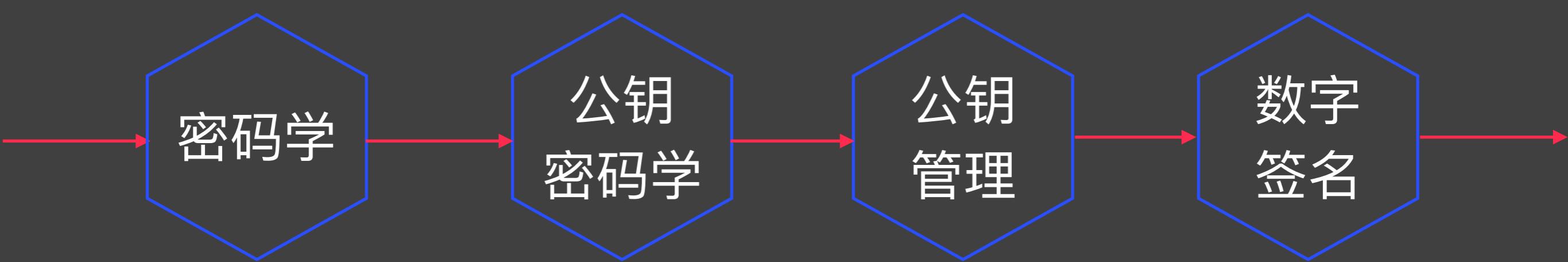
比特币

每个区块中各笔交易的哈希树（梅克尔树）

图3.7 比特币的区块链有两个哈希结构

注：一个就是把区块联结在一起的哈希链，另一个就是区块内部的交易哈希值梅克尔树。

# 密码



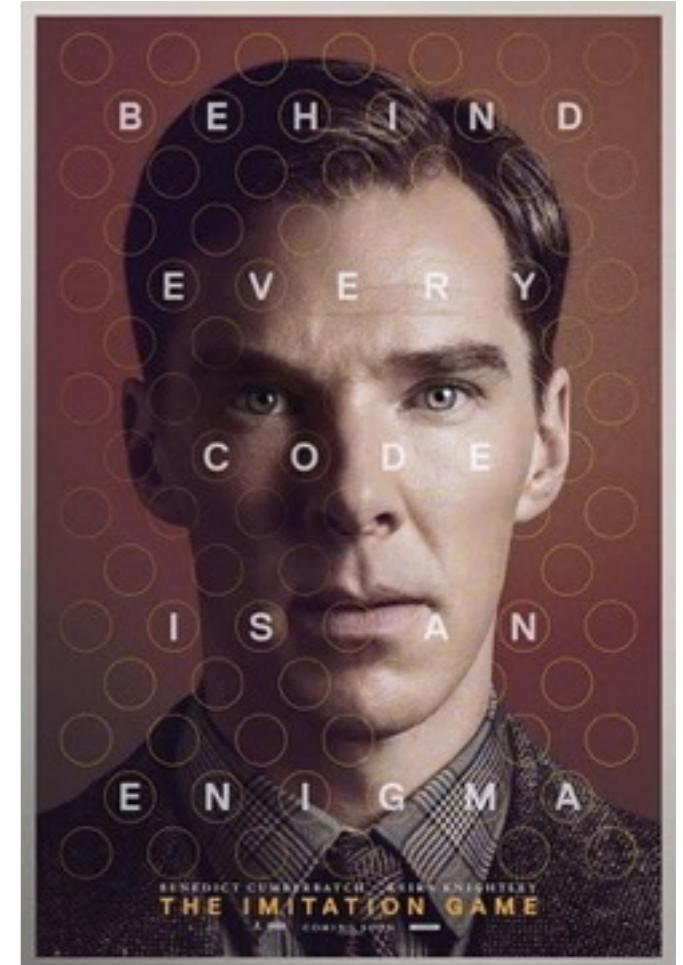
### 图灵



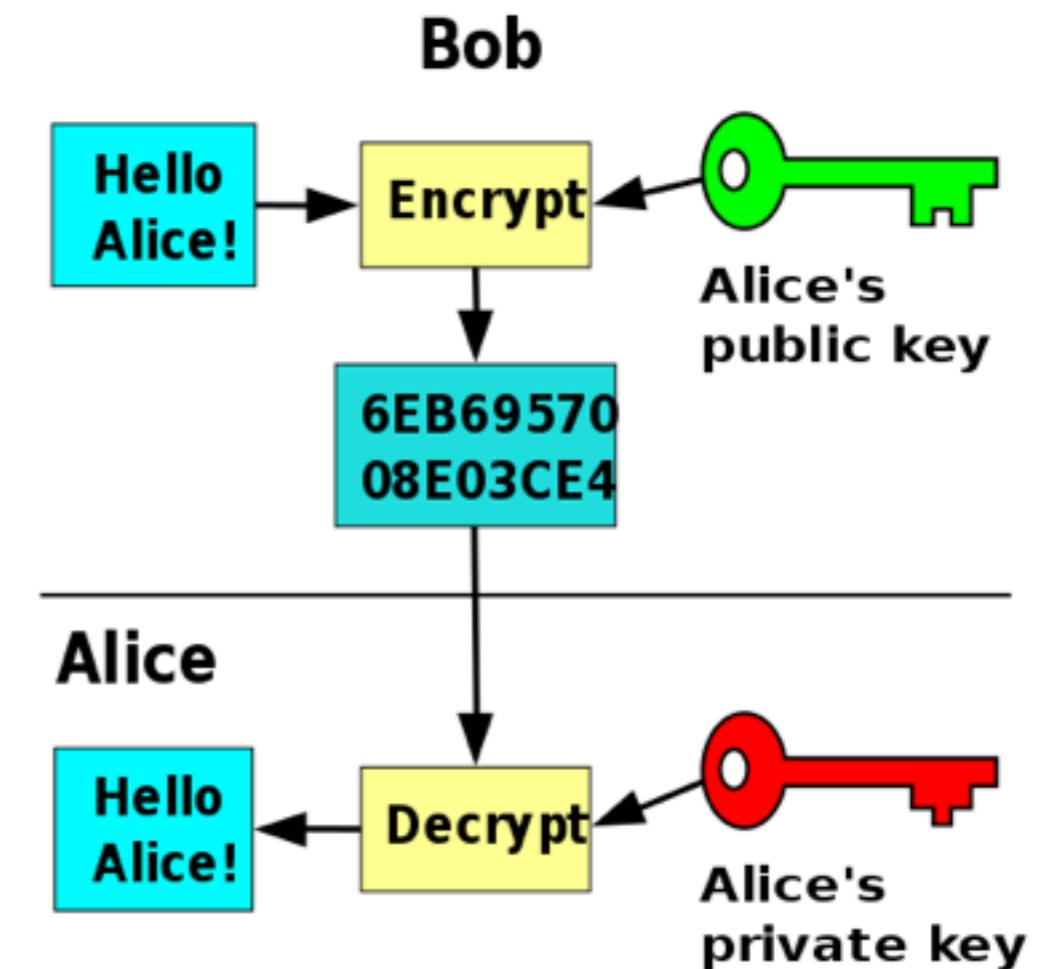
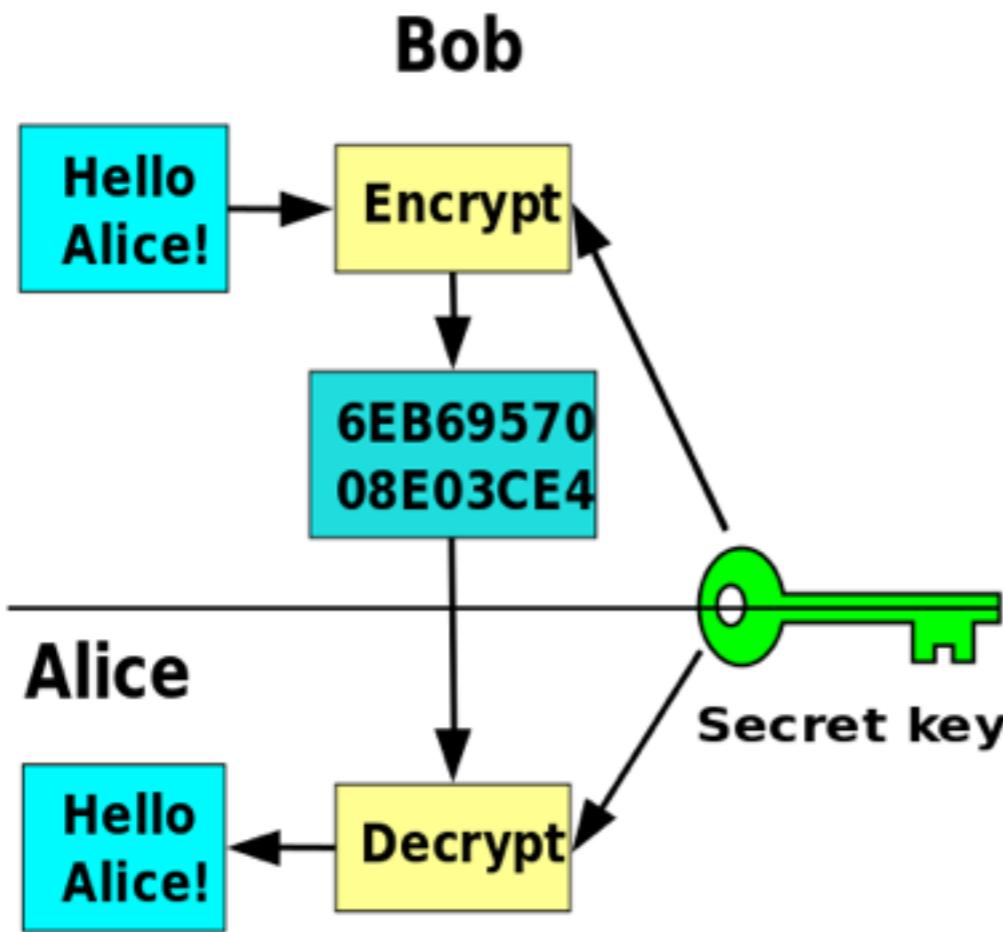
### 恩尼格玛密码机



### 模仿游戏



# 对称密码学 vs. 非对称密码学



对称密码学

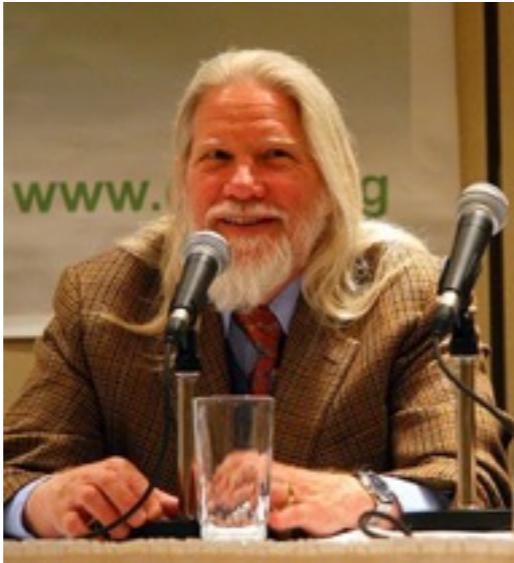
非对称密码学

# Blockchain Technology

## DH vs. RSA

2015年  
图灵奖

1976



*Whitfield Diffie*



*Martin Hellman*



*Ralph Merkle*

1978

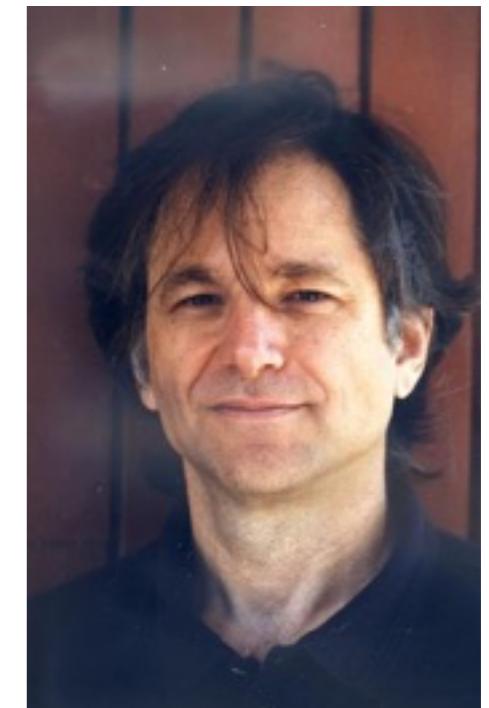
2002年  
图灵奖



*Ronald L. Rivest*



*Adi Shamir*



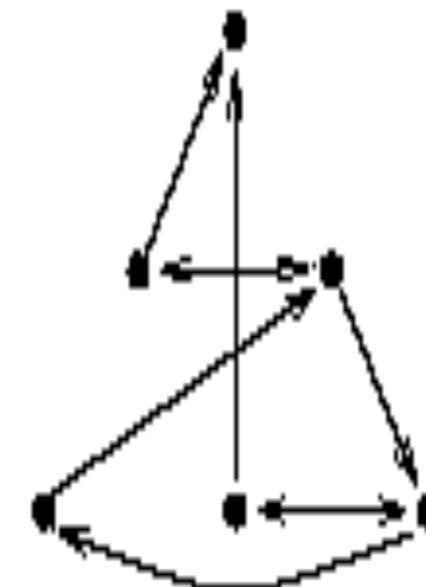
*Leonard Max Adleman*

## 公钥管理: PKI vs. PGP

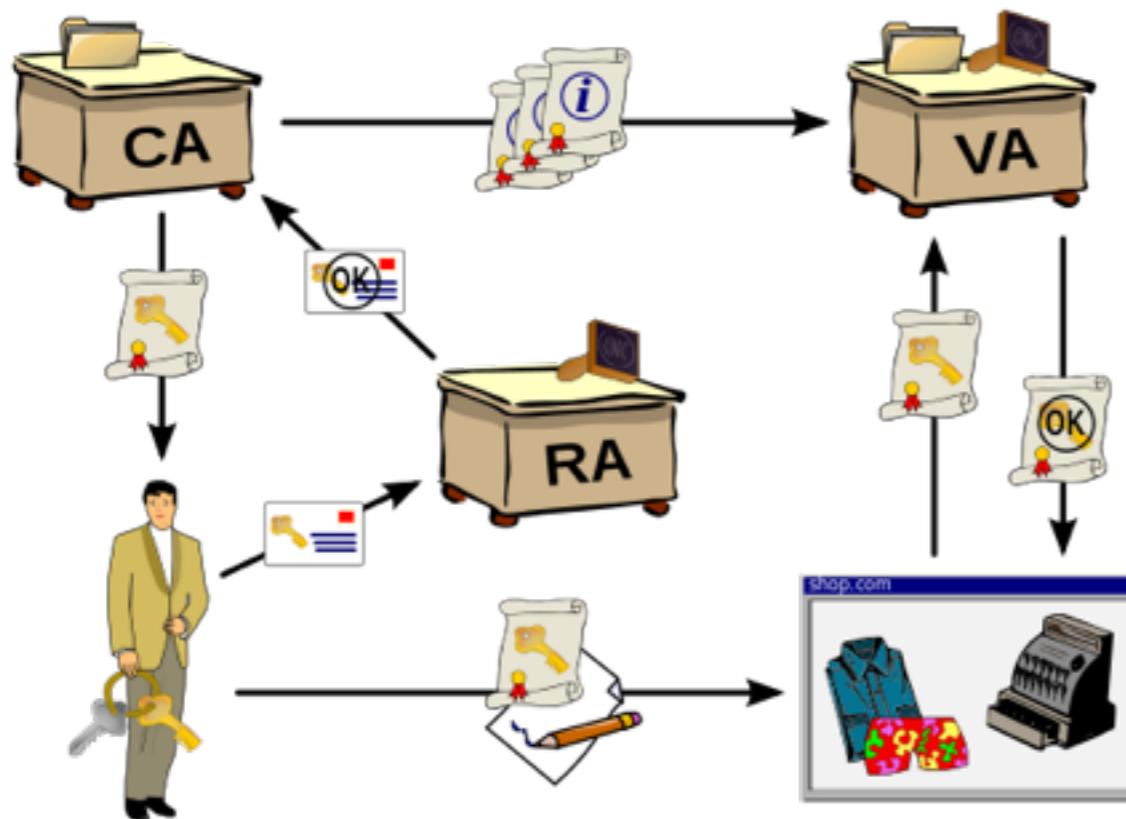
RSA



VERISIGN™



公钥管理  
的P2P版本



P G P®

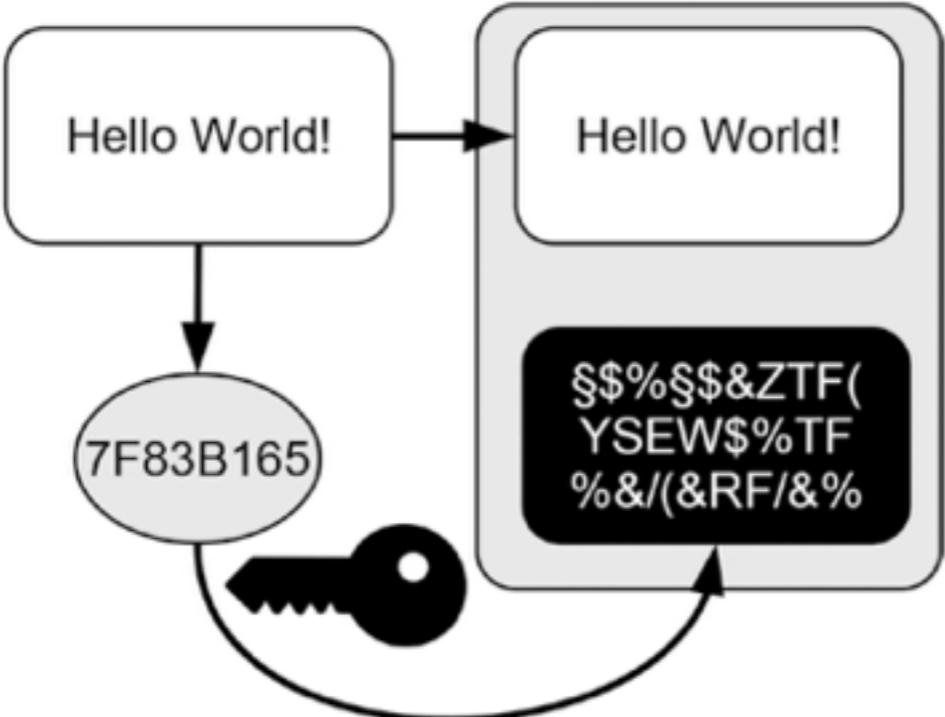
1991

GnuPG  
1999

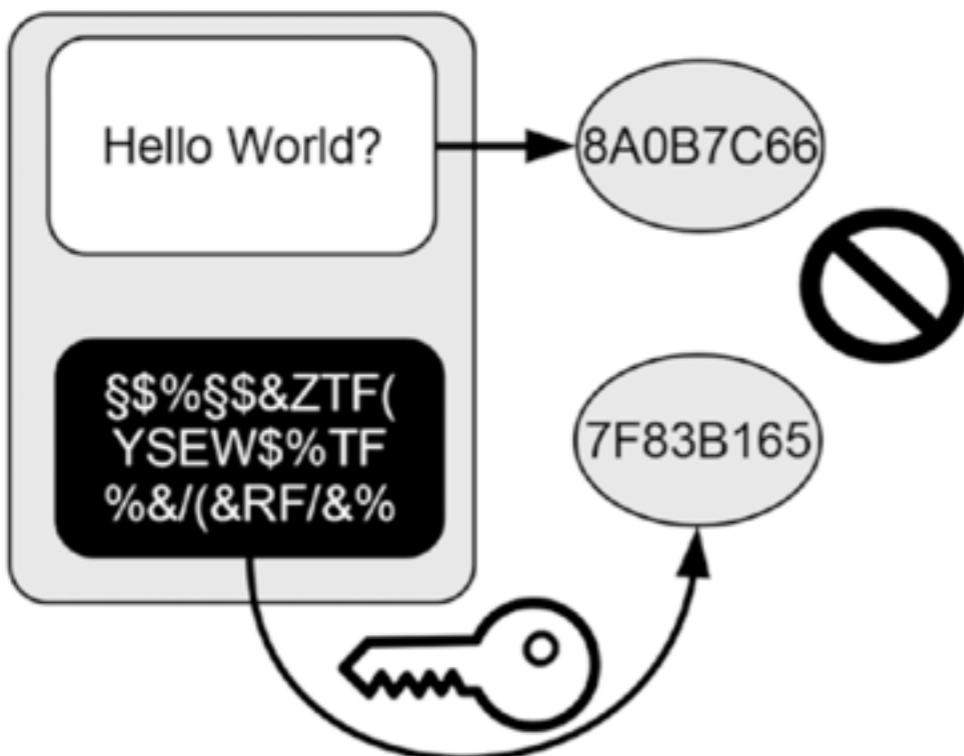


Phil Zimmermann

产生签名

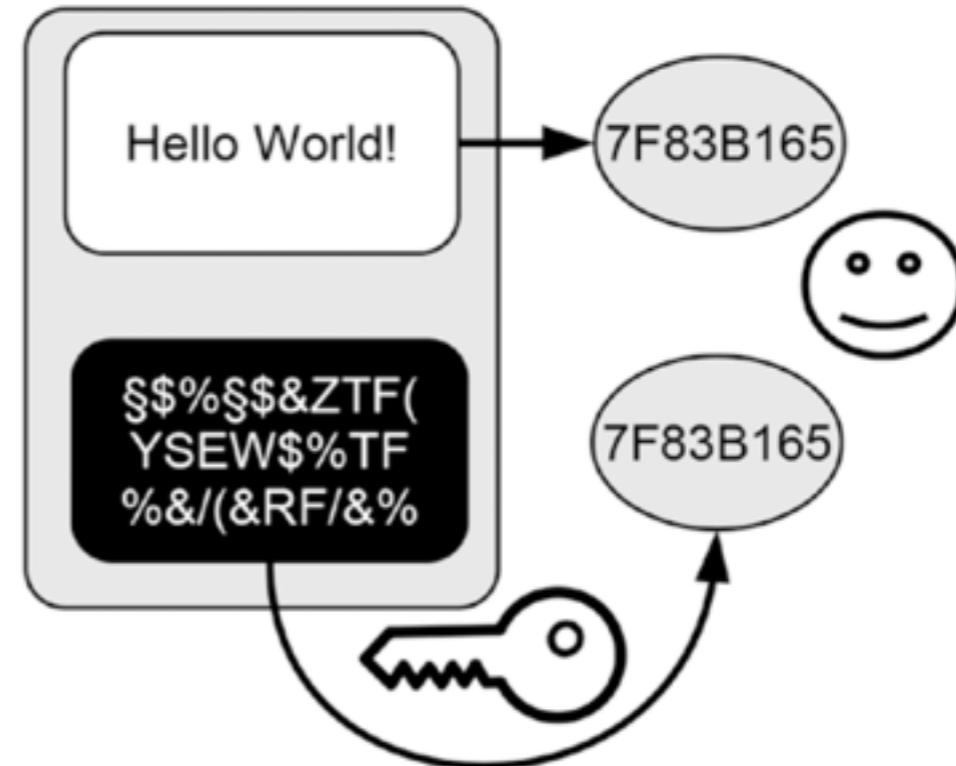


发现欺骗



## 数字签名

验证签名

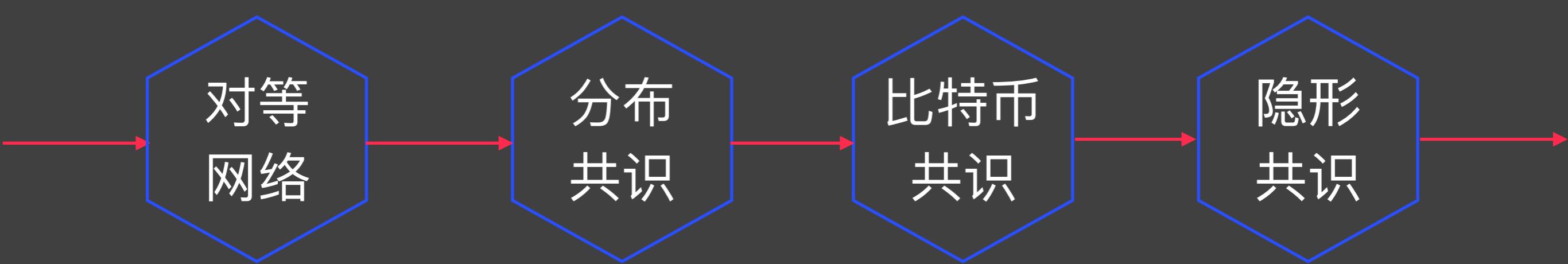


自己签名，任何人都可以验证（公钥分发）

不可伪造，公钥私钥

签名信息的大小

# 共识



# Blockchain Technology

## Peer to Peer

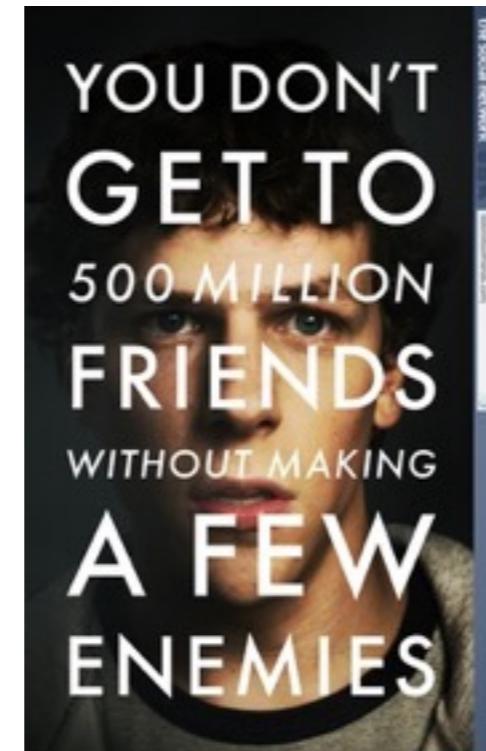


napster™

1999



**Sean Parker**



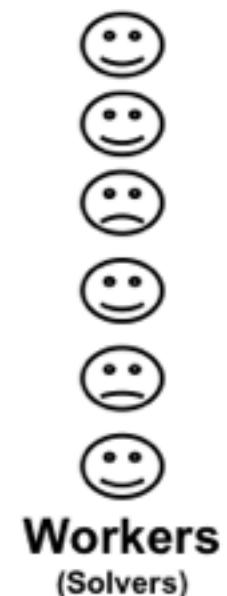
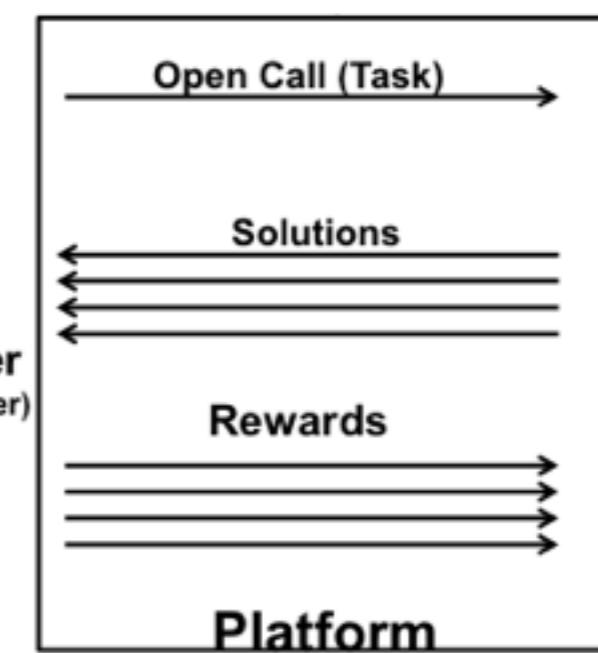
**The Social Network**



2003



众包



# Blockchain Technology

## BitTorrent

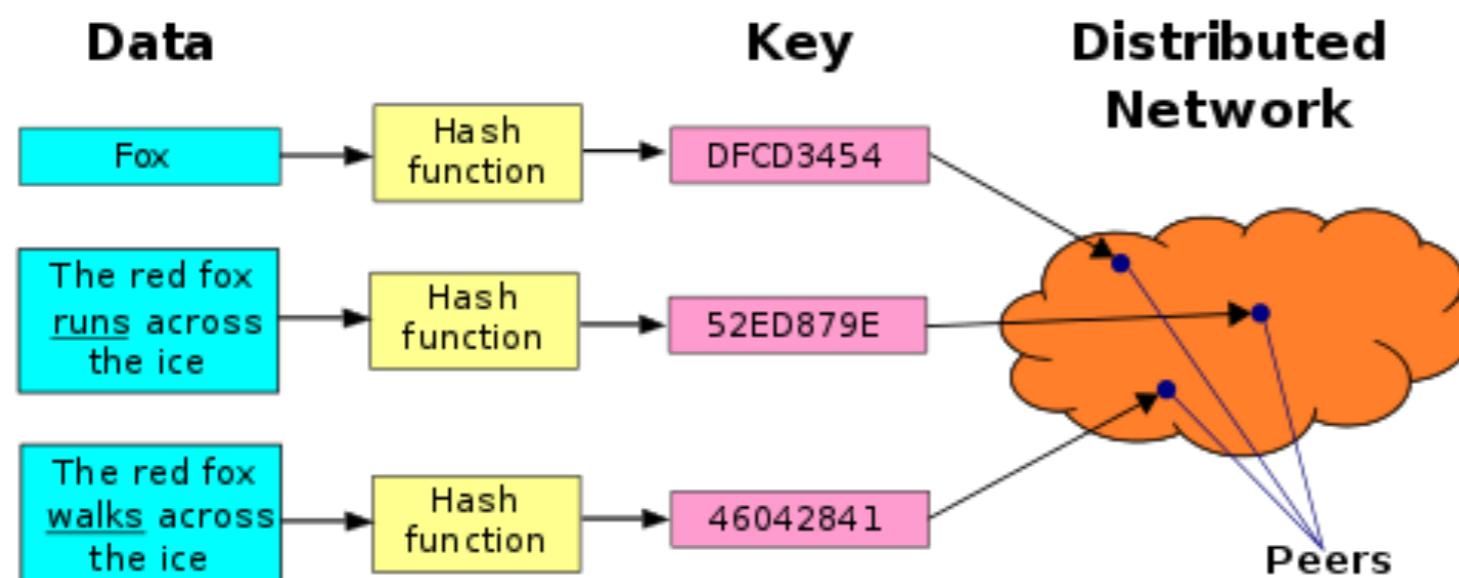


2001

*Bram Cohen*

**BitTorrent**

## Distributed Hash Table



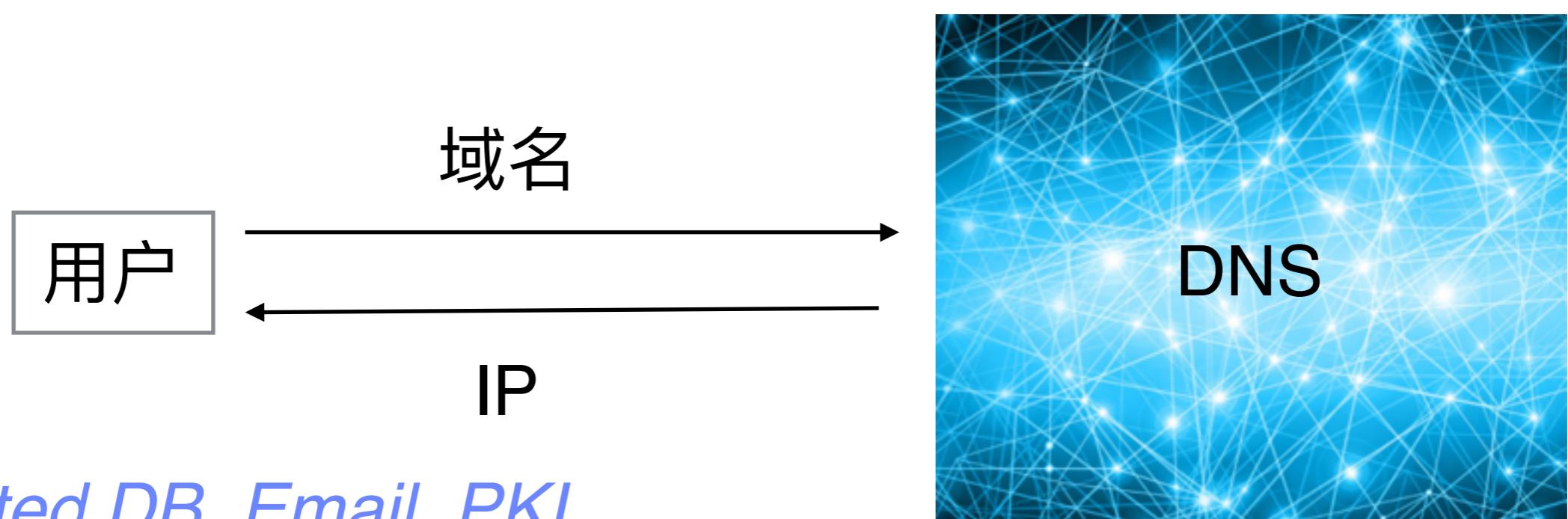
激励

[https://en.wikipedia.org/  
wiki/BitTorrent](https://en.wikipedia.org/wiki/BitTorrent)

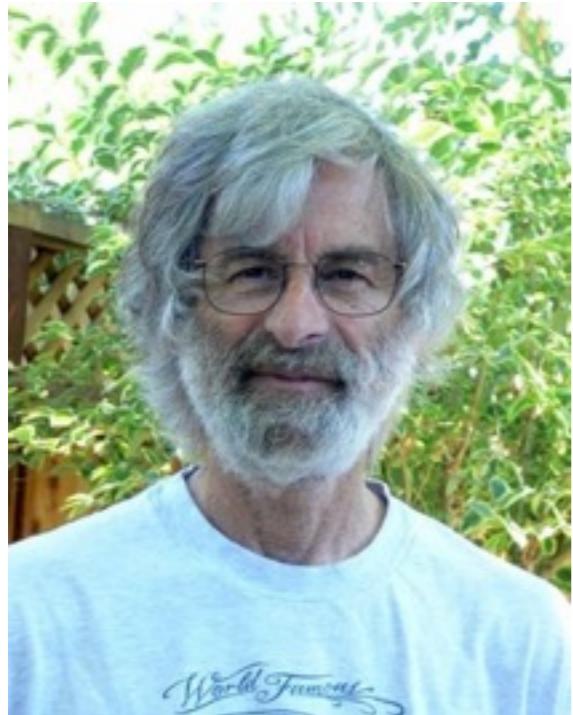
[https://en.wikipedia.org/  
wiki/Distributed\\_hash\\_table](https://en.wikipedia.org/wiki/Distributed_hash_table)

## 分布共识

- 在一个有 $n$ 个节点的系统中，每一个节点都有一个输入值，其中有一些节点是错误的或者恶意的。一个分布式共识协议具有如下两个属性：
  - \* 结束时所有诚实的节点均认同该值；
  - \* 该值由诚实节点产生



# 拜占庭将军问题和Paxos



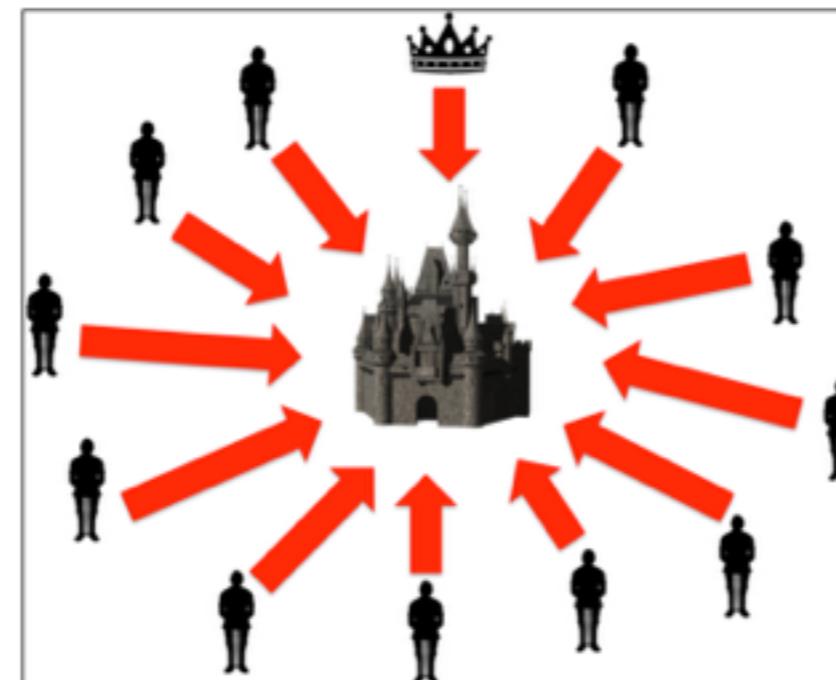
LESLIE LAMPORT

2013图灵奖

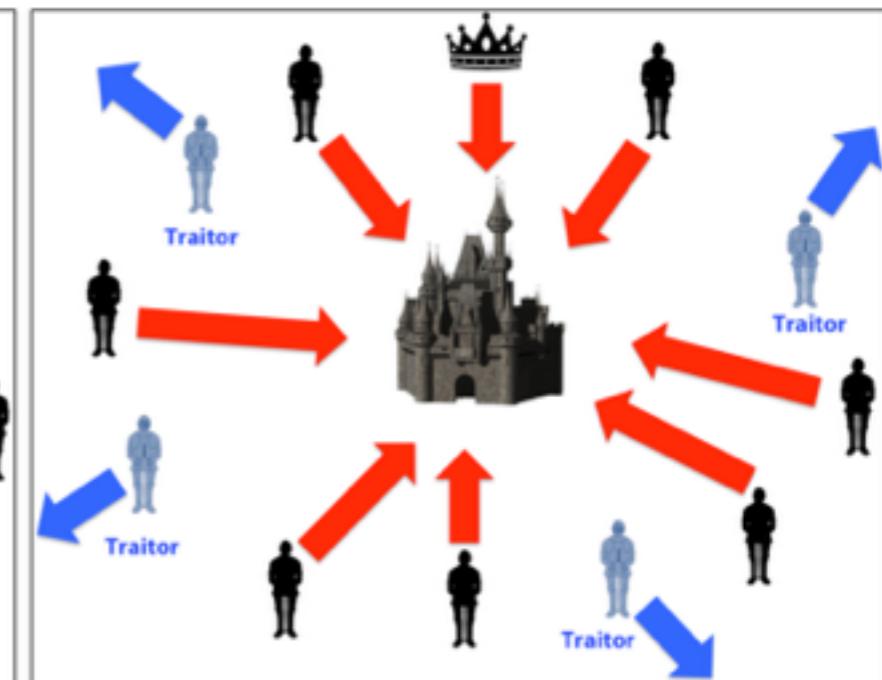
## The Byzantine Generals Problem

1982

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE  
SRI International



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

## Paxos Made Simple

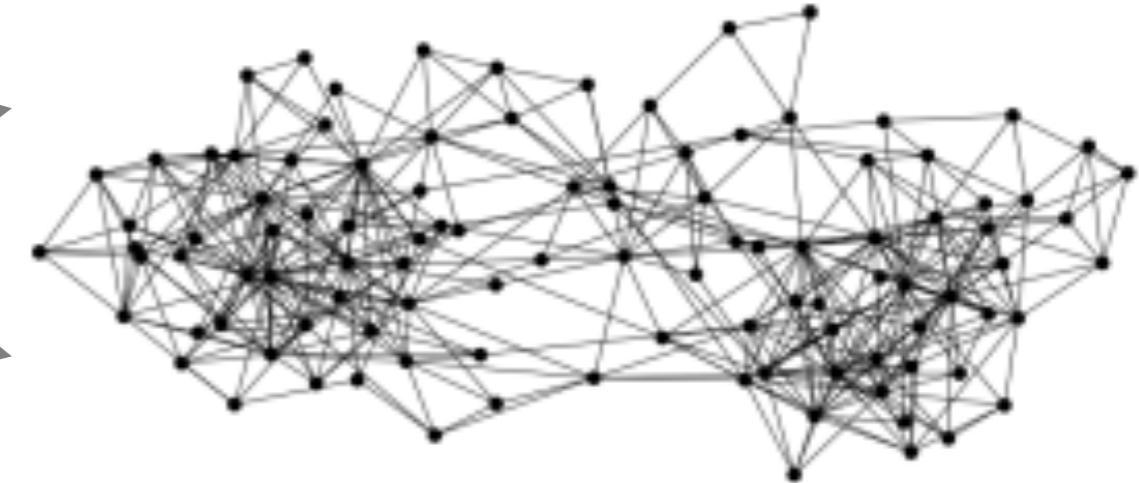
2001

The Paxos algorithm, when presented in plain English, is very simple.

# 比特币的交易传播



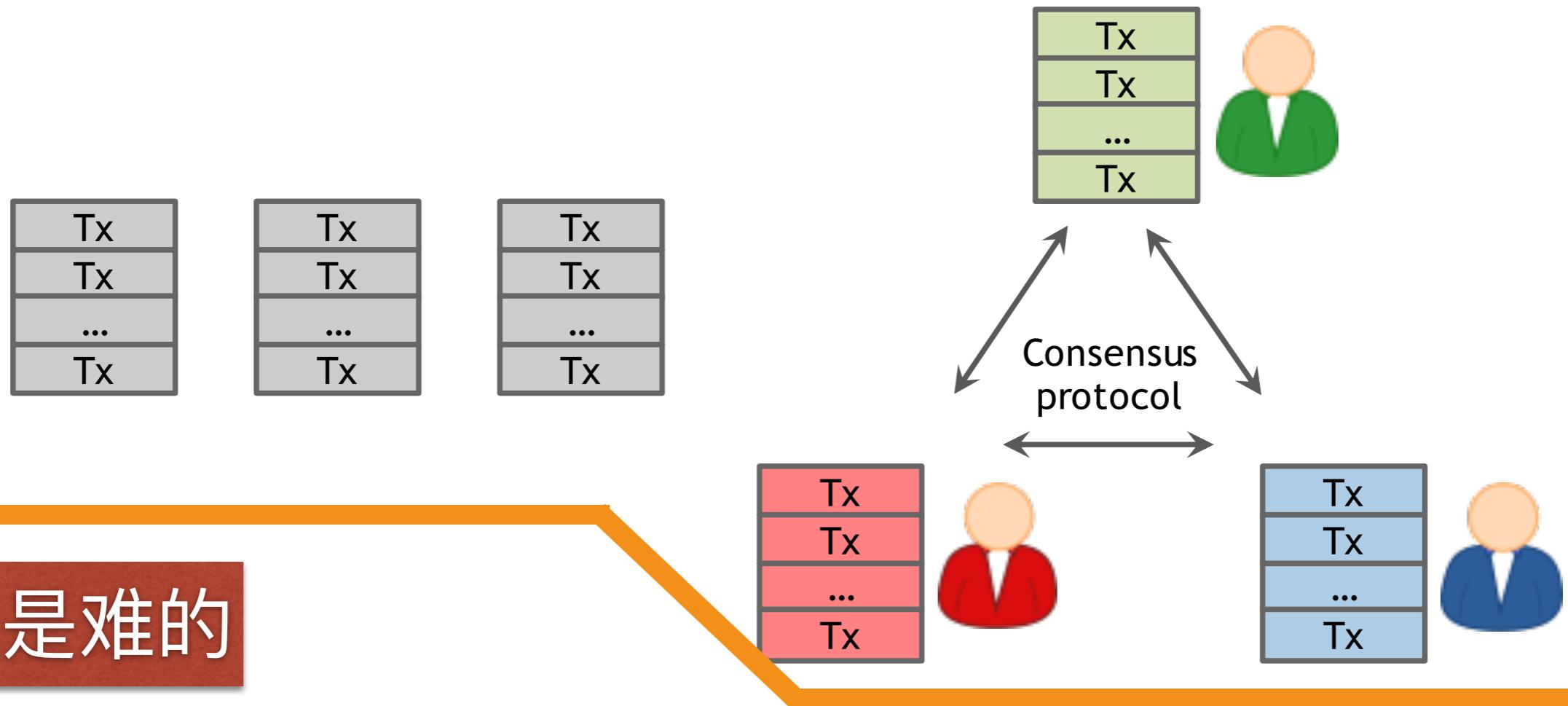
signed by Alice  
Pay to  $pk_{Bob} : H( )$



- 比特币是一个P2P网络
- Alice 需要广播她完成的交易給所有的节点
- Bob计算机当时可以不在P2P网络中
- *A single, global ledger for the system*
- 等待共识的业务、已共识的业务

# 比特币的分布共识

每一个节点输出它的未共识的业务竞争下一个Block



→ *Node: crash, malicious*

→ *Network: Imperfect (online, latency)*

**Global Time**

## 比特币和身份

- 比特币节点需要身份 (*ID*)
- 比特币假设恶意节点小于 50%
- 但是 P2P 系统中，*ID* 面临很大问题
  - \* *Sybil Attack*
- *Pseudonymity* 是比特币的目的
- 比特币跟踪和验证 *ID* 是困难的
- 比特币采用的应对方法：随机的选择节点

## 比特币的隐形共识机制

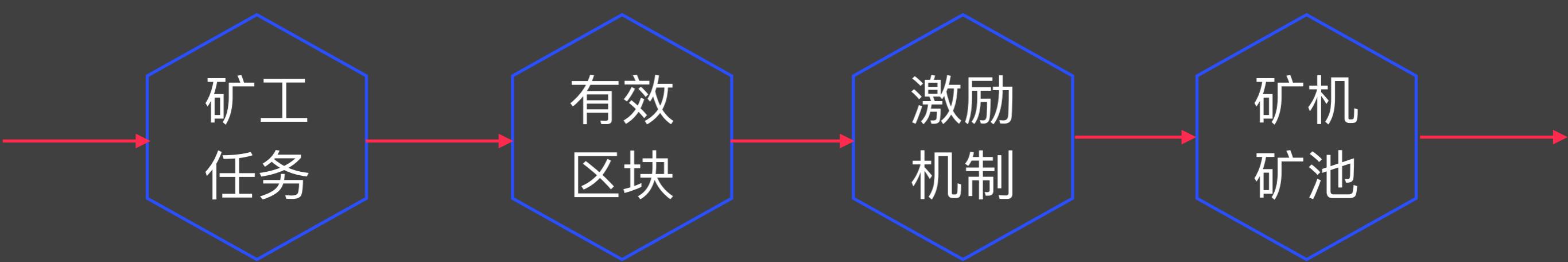
- 新的交易被广播到所有节点
- 每个节点将新的交易放进一个区块
- 在每一轮中，一个随机的节点被选择可以广播它的区块
- 其余节点可以选择接受这个区块，前提是区块的交易是可验证的
- 节点将以上区块的Hash放进自己的区块，表示它认可这个新区块

隐形共识：接受该块并扩展 vs. 拒绝该块，扩展前面的块

## 比特币的共识总结

- 理论落后于实践
- 引入了 *Incentive*
  - \* 是电子货币
- 利用了随机性
  - \* 很长时间后才取得共识，1小时
  - \* 随着时间的增加，对某一块的共识的概率越来越大

# 挖矿

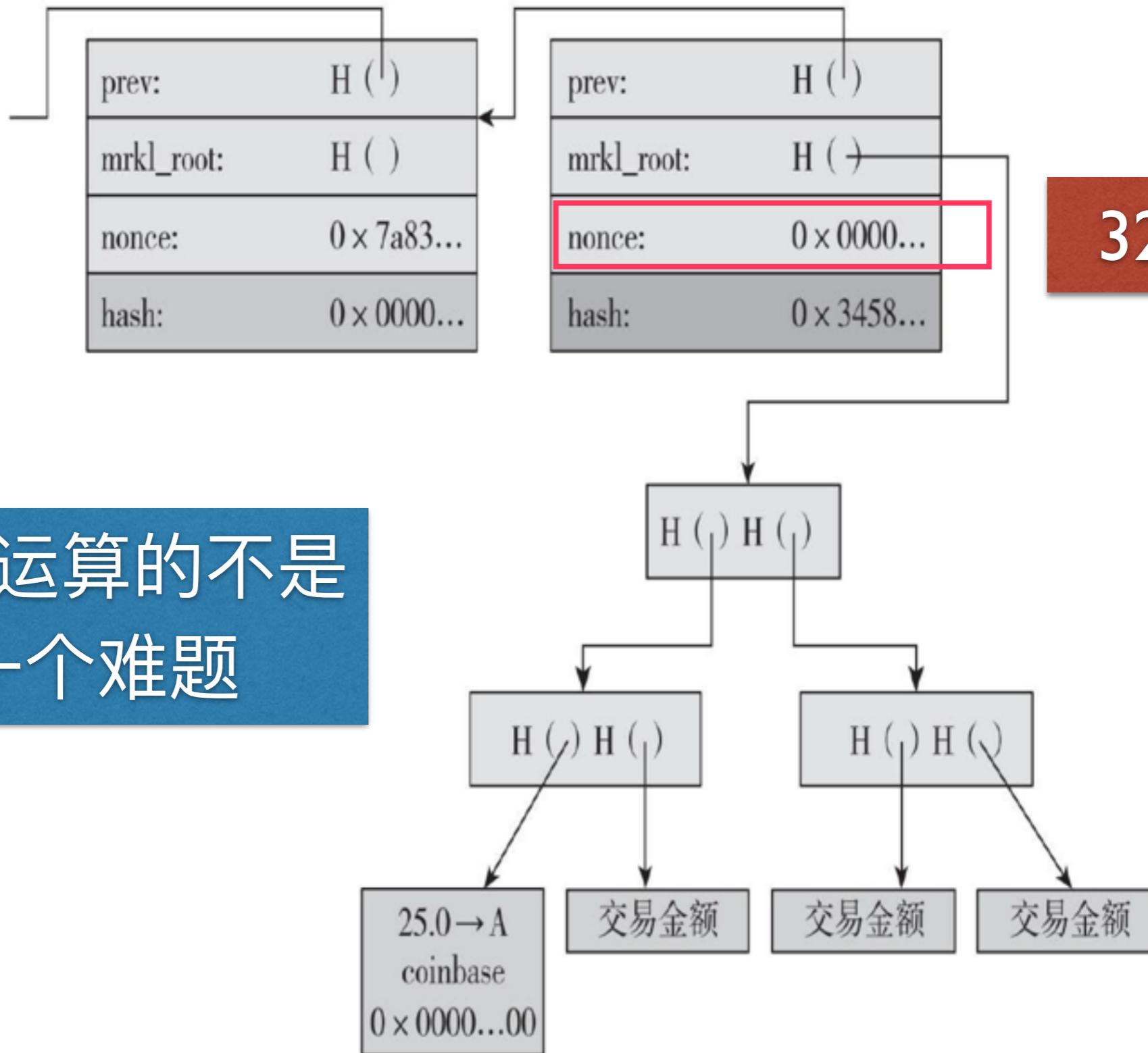


## 矿工的任务

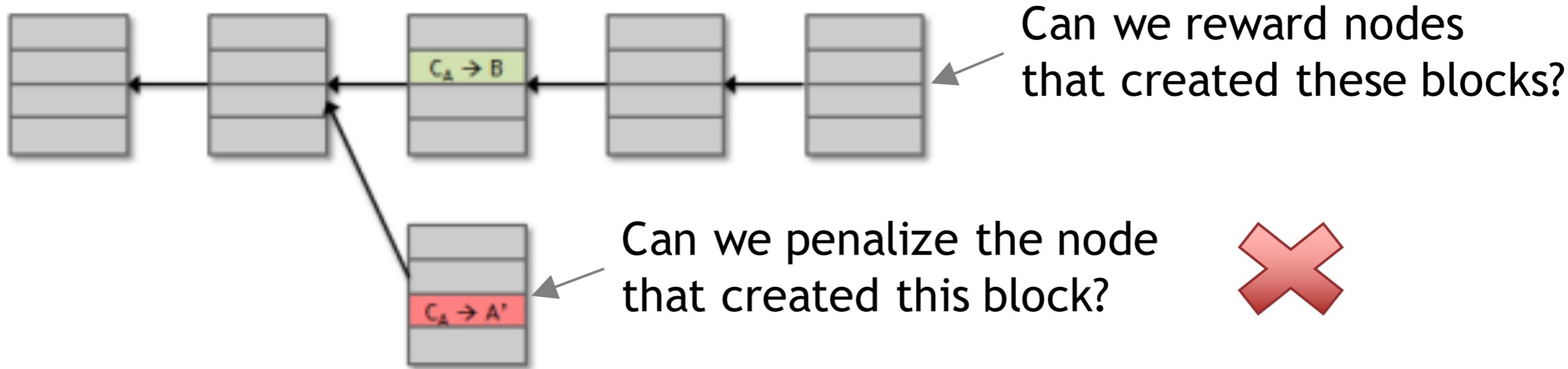
- 监听交易广播
- 维护区块链网络和监听新的区块
- 组装一个备选区块
- 找到一个让你的区块有效的随机数
- 希望你的区块被全网接受
- 利润

验证交易和区块 vs. 和其余矿工竞争

# 寻找有效区块



## 激励节点诚实

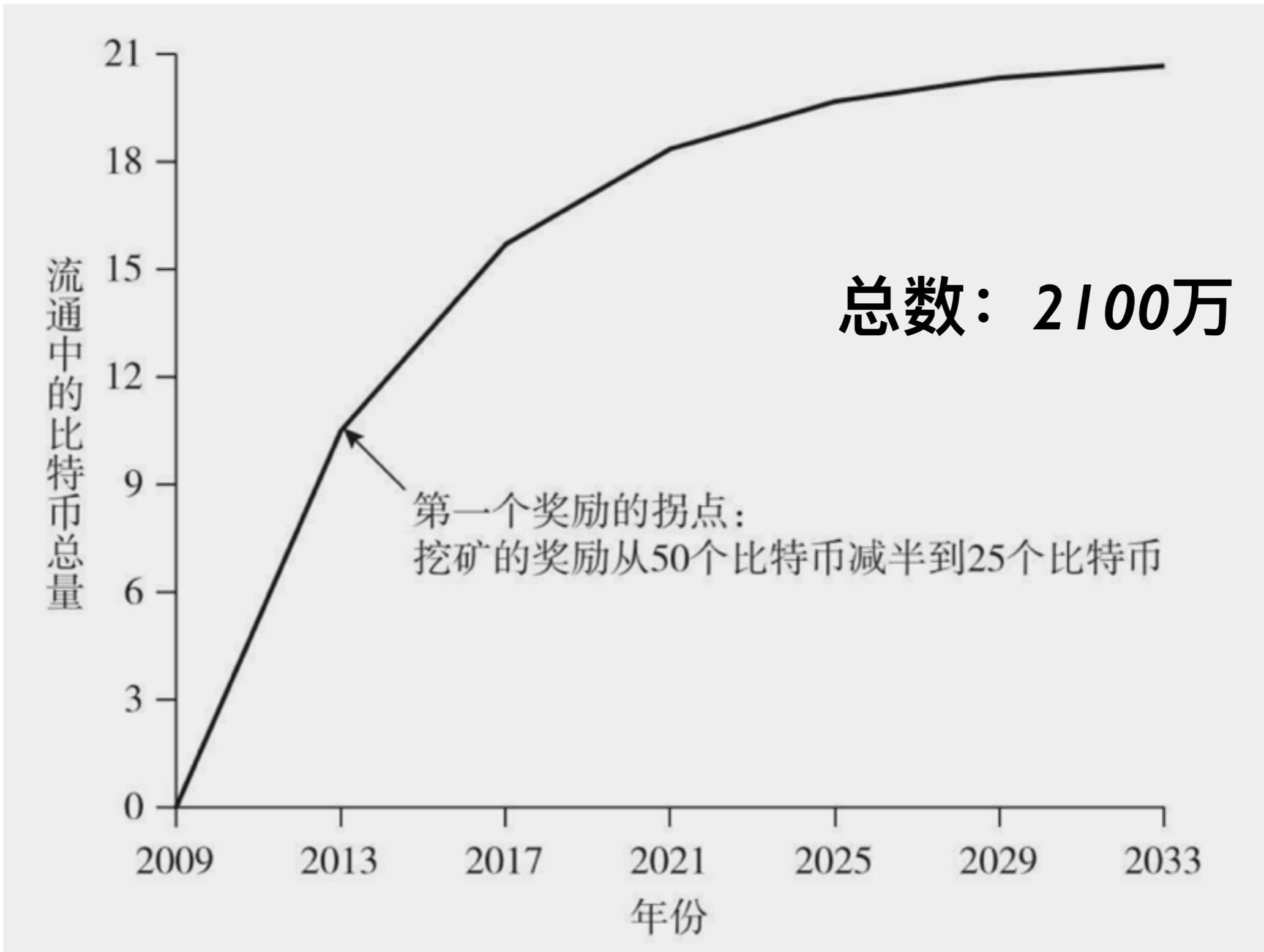


---

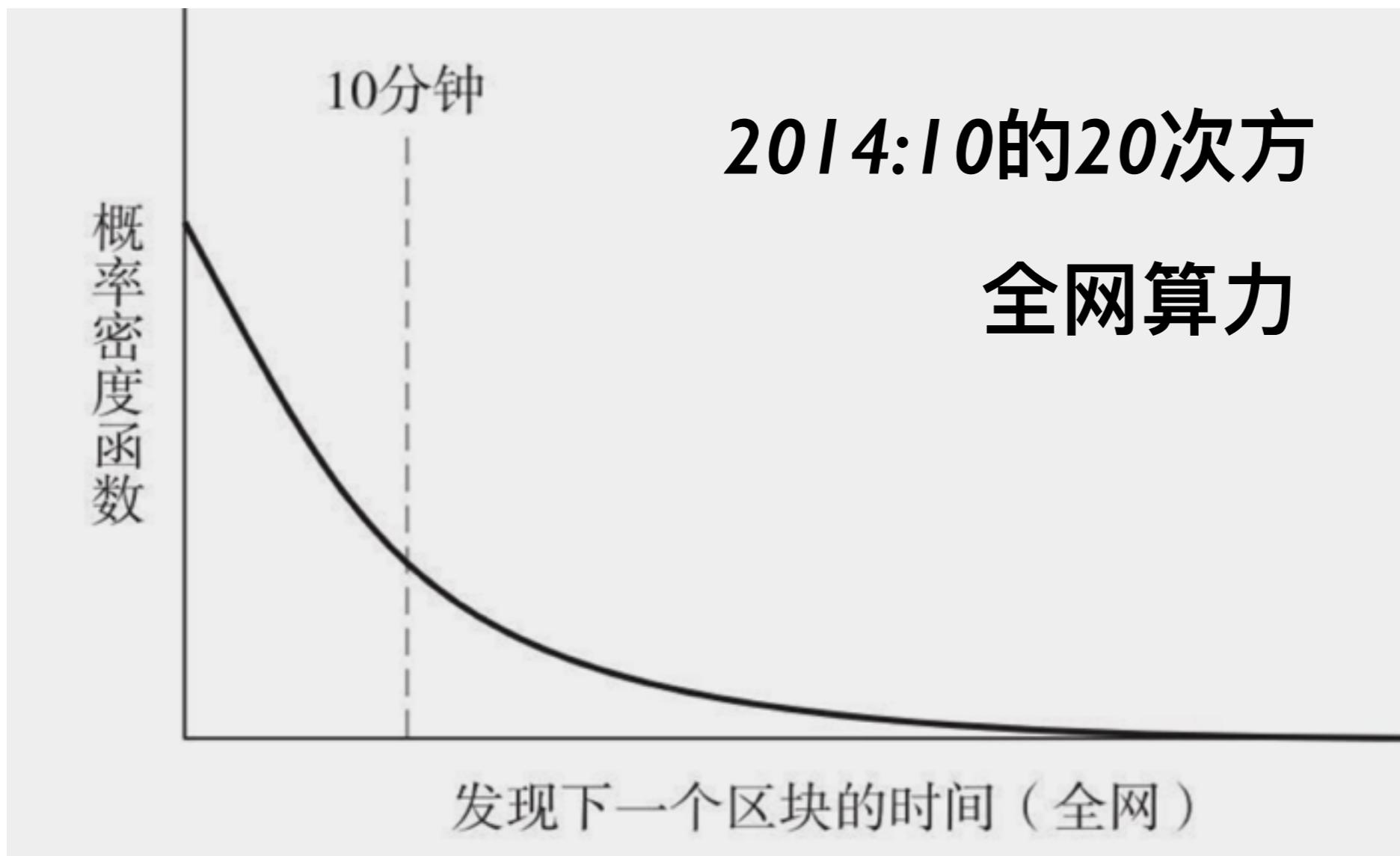
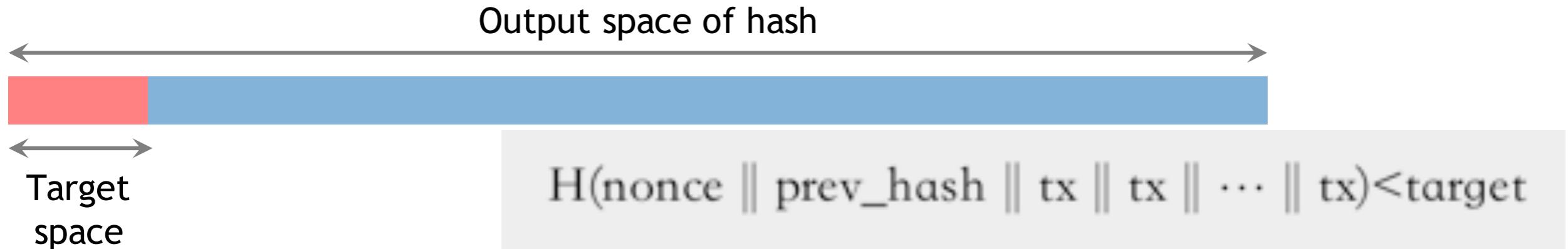
区块奖励 vs. 交易费奖励

交易费：输入和输出不等

## 比特币奖励



## 工作量证明



限定Hash的  
输出范围

临时随机数

PoW:  
工作量证明

PoS:  
权益证明

# 挖矿发展



CPU



GPU



FPGA



ASIC



gold pan



placer mining



pit mining

Blockchain  
Technology

# 专业矿场

温度

电费

网速

中国

# Blockchain Technology

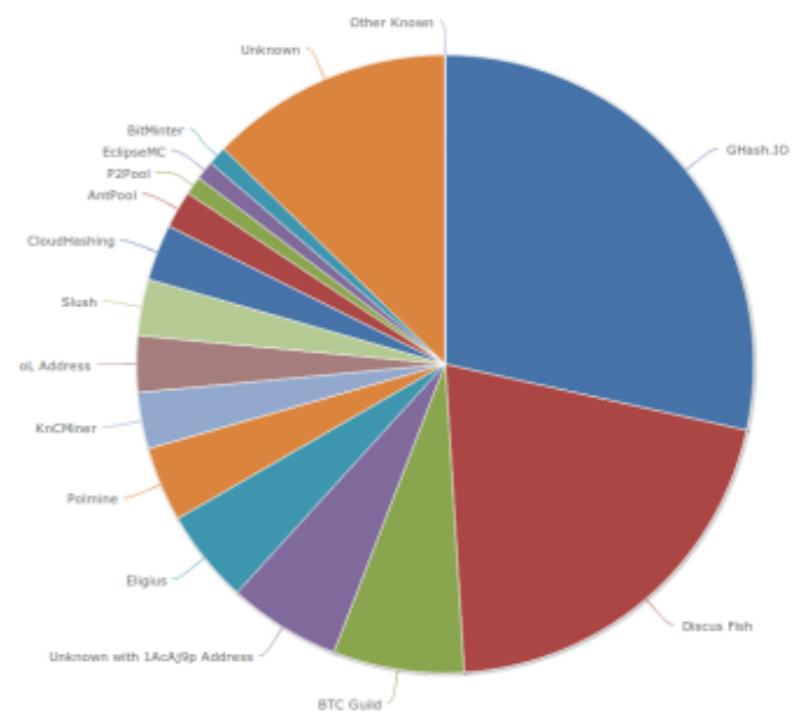
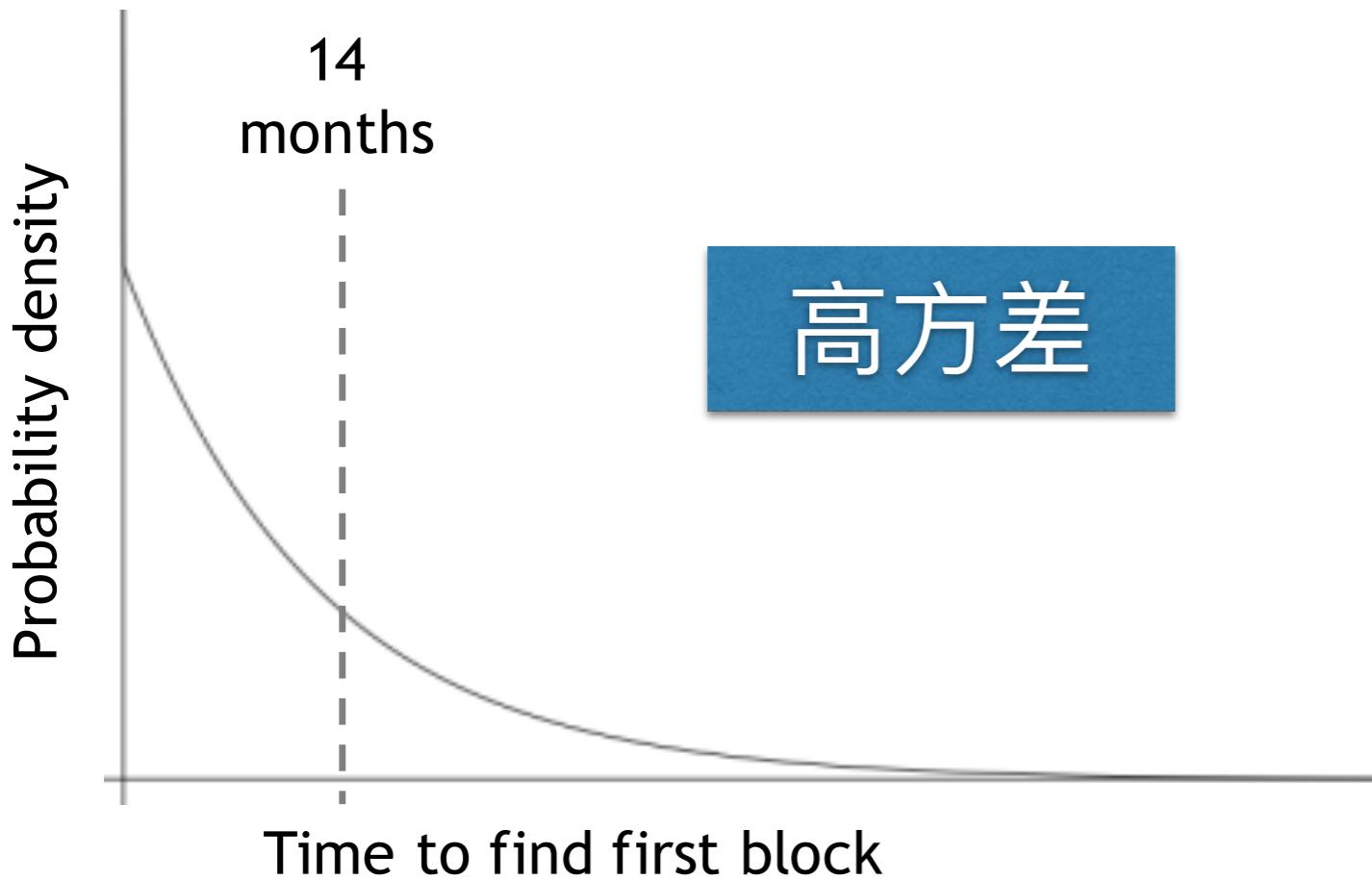
矿池



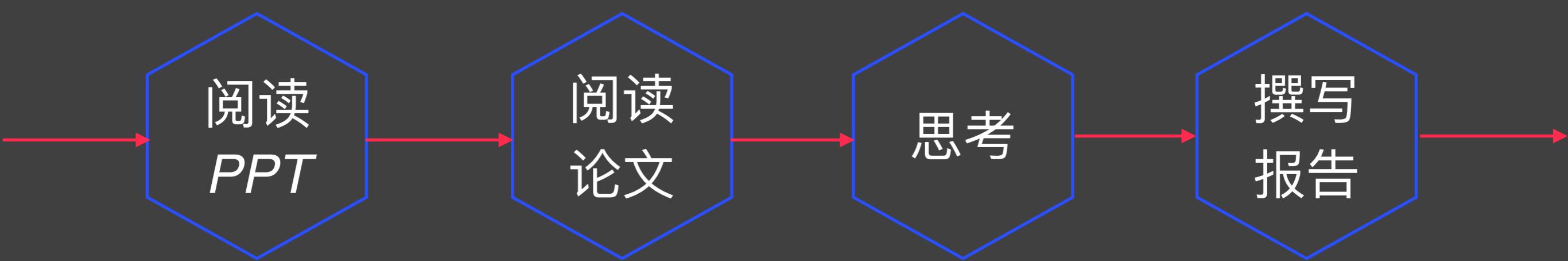
TerraMiner IV

Cost: ≈US\$6,000  
Expected time to find a block: ≈14 months  
Expected revenue: ≈\$1,000/month

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



# 课后作业



要求阅读如下论文，写论文阅读报告

### Majority Is Not Enough: Bitcoin Mining Is Vulnerable

By Ittay Eyal and Emin Gün Sirer

In CACM 2018.

选择一篇该文的参考文献，阅读该参考文献，在论文报告中简单介绍

- 1、论文概述
- 2、主要收获
- 3、存在疑问
- 4、所思所感
- 5、一篇引用

下周一日晚上  
12点前提交

謝謝 !

*Huijing Sun*

[sunhp@ss.pku.edu.cn](mailto:sunhp@ss.pku.edu.cn)

<https://huijingsun.github.io>