

2018.03.06

区块链基础



Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

课堂测试时间

- 1、简单描述比特币和区块链的区别和联系？
- 2、简单描述公开链和私有链的异同？
- 3、简单描述Hash和Hash指针在区块链中作用？
- 4、简单描述区块链的缺陷？
- 5、雄安新区已经上线了区块链租房应用平台，你认为与现在的租房应用平台相比有哪些优势？
- 6、结合论文内容，谈谈你对区块链的看法和感想（有新的想法更好）

- 课程简介
- 什么是区块链
- 区块链历史
- 为什么使用区块链
- 区块链如何工作
- 共享的分布式账本
- 比特币、以太坊、超级账本
- 密码、计算机、经济、社会
- 以物易物、货币、信用、银行
- 第三方、中心化
- Hash函数、Hash指针、梅克尔树

加密货币

去中心化

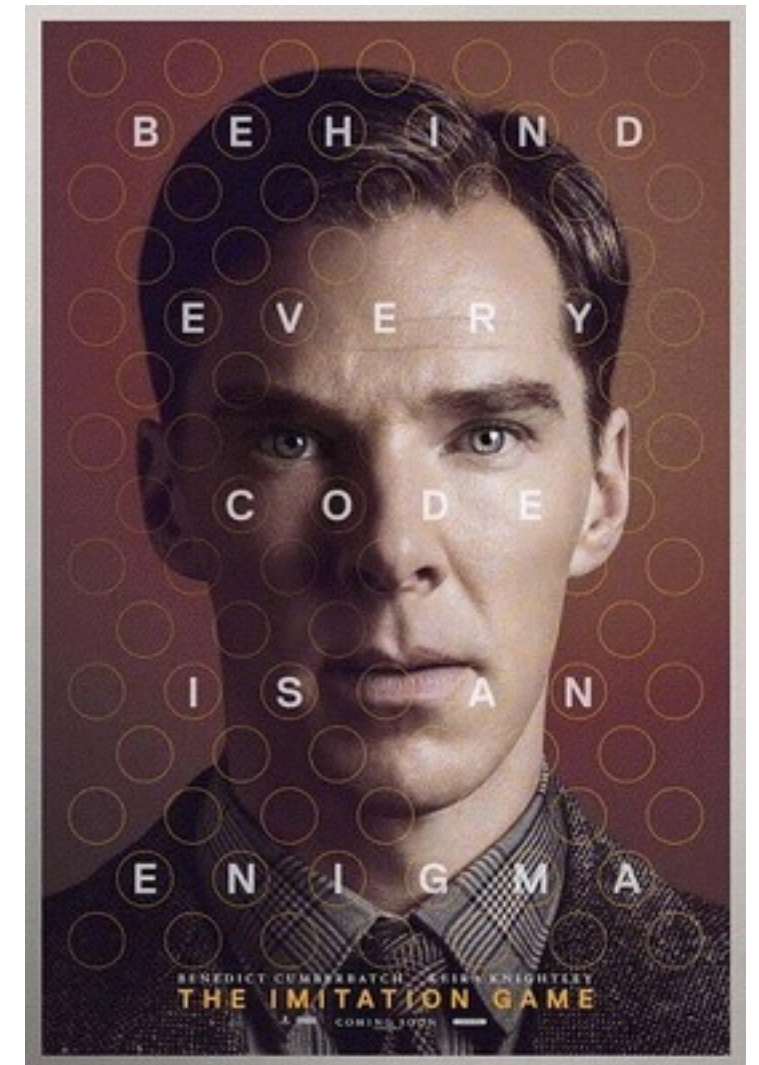
Crypto **Currency**



图灵

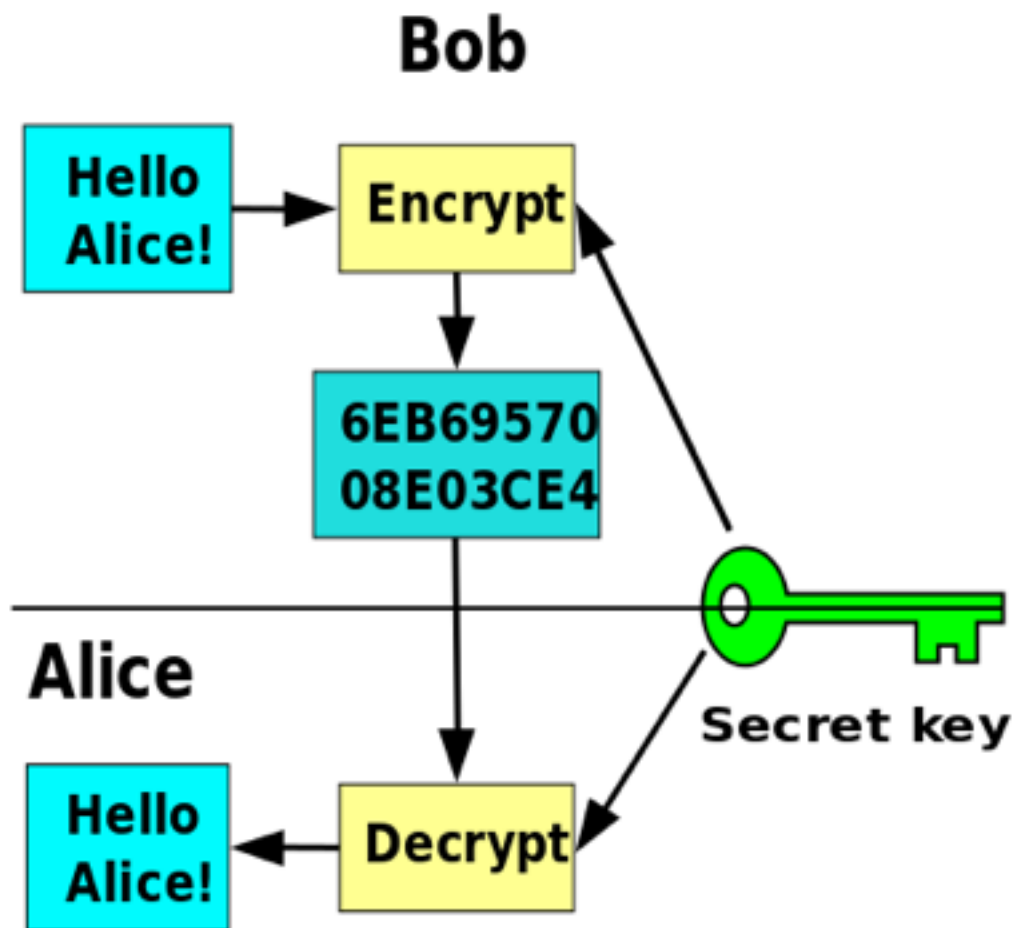


恩尼格玛密码机

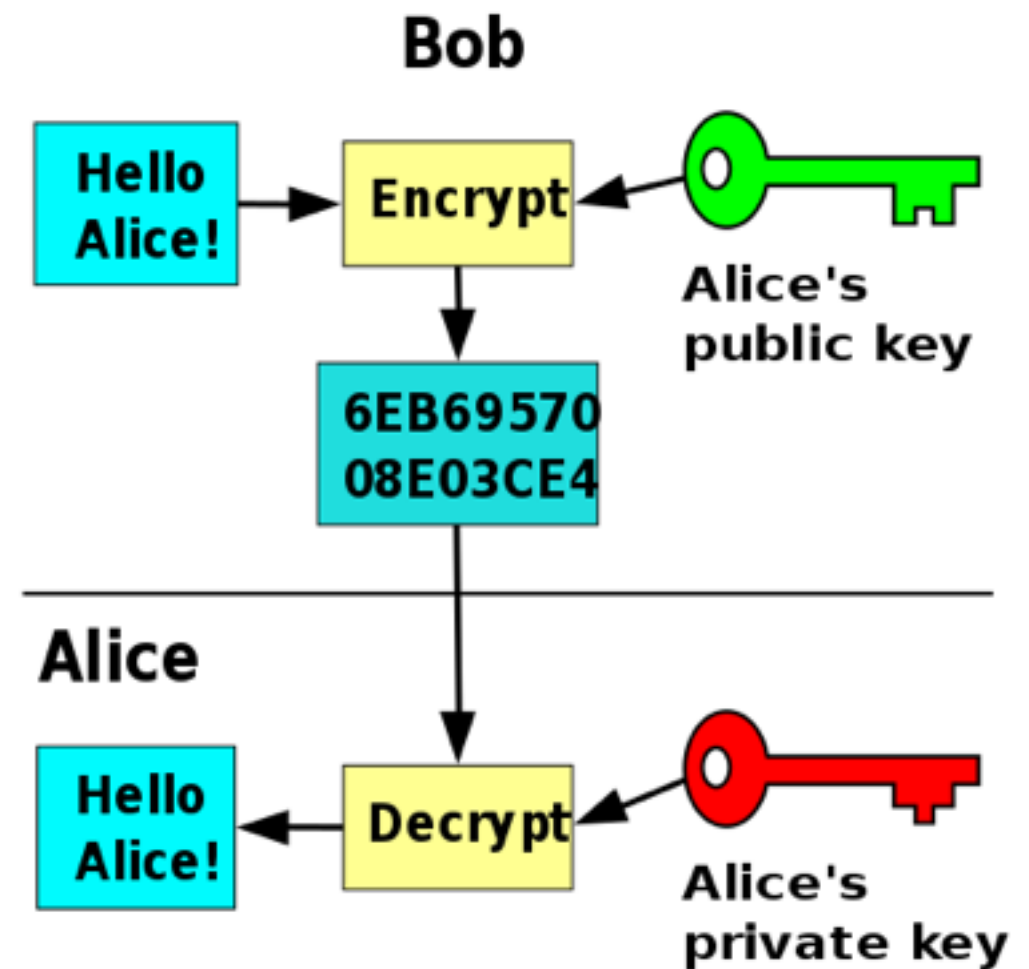


模仿游戏

CryptoCurrency 对称密码学 vs. 非对称密码学



对称密码学



非对称密码学

2015年
图灵奖



Whitfield Diffie



Martin Hellman



Ralph Merkle

1976

1978

2002年
图灵奖



Ronald L. Rivest



Adi Shamir

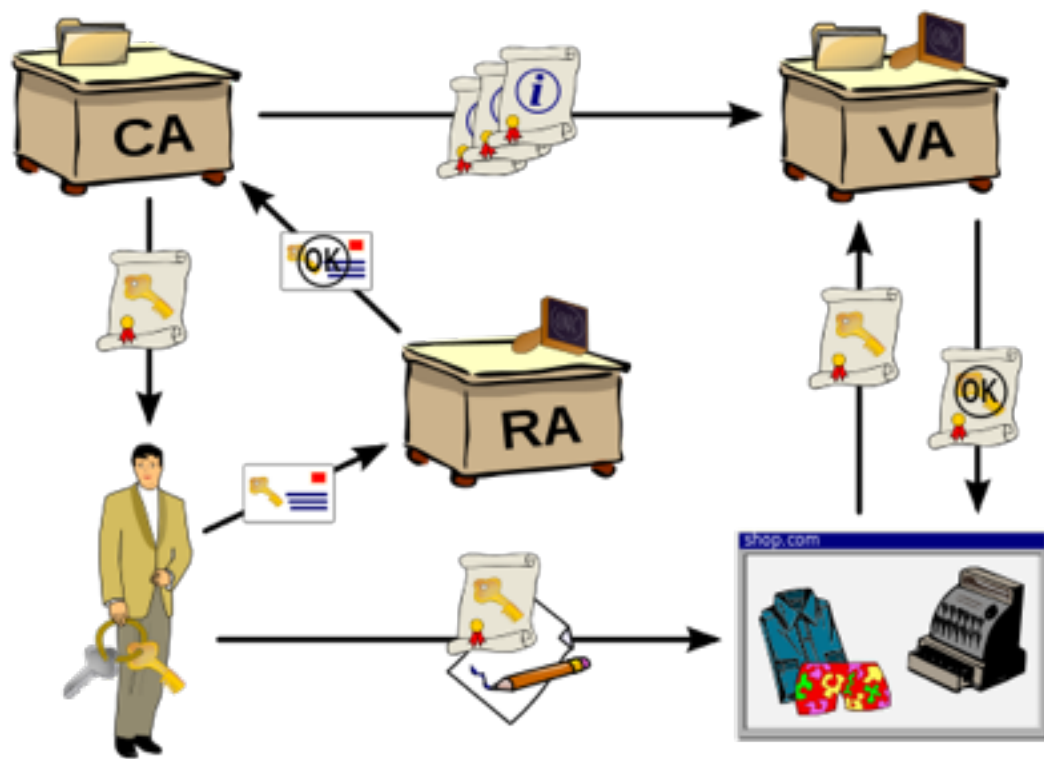
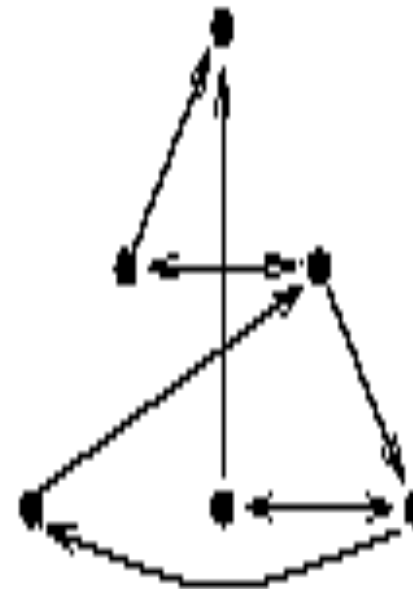


Leonard Max Adleman

RSA



VERISIGN™



1991



1999



Phil Zimmermann

新版人民币 2015年版第5套 那些事...



钞票正面



钞票背面

多一份金融了解 多一份财富保障

2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。

- 1 光变镂空开窗安全线**
位于票面正面右侧。垂直观察，安全线呈品红色；与票面成一定角度观察，安全线呈绿色；透光观察，该安全线中正反交替排列的镂空文字“¥100”。
- 2 雕刻凹印**
票面正面毛泽东头像、国徽、“中国人民银行”行名、左上角面额数字、盲文及背面人民大会堂等均采用雕刻凹印印刷，用手触摸有明显的凹凸感。
- 3 数字对印图案**
票面正反面下方和背面右下方均有面额数字“100”的局部图案。透光观察，正背面图案组成一个完整的数字“100”。
- 4 光彩光变数字**
位于票面正面中部。垂直观察，数字以金色为主；平视观察，数字以绿色为主。随着观察角度的改变，数字颜色在金色与绿色之间交替变化，并可见到一条亮光带上下滚动。
- 5 水印**
位于票面正面左侧下方。透光观察，可以看到透光很强的水印图案数字“100”。
- 6 人像水印**
位于票面正面左侧空白处。透光观察，可见毛泽东头像。
- 7 横竖双号码**
票面正反面左下方采用横号码，其前两位数字为暗红色，后六位数字为黑色；右侧竖号码为黑色。

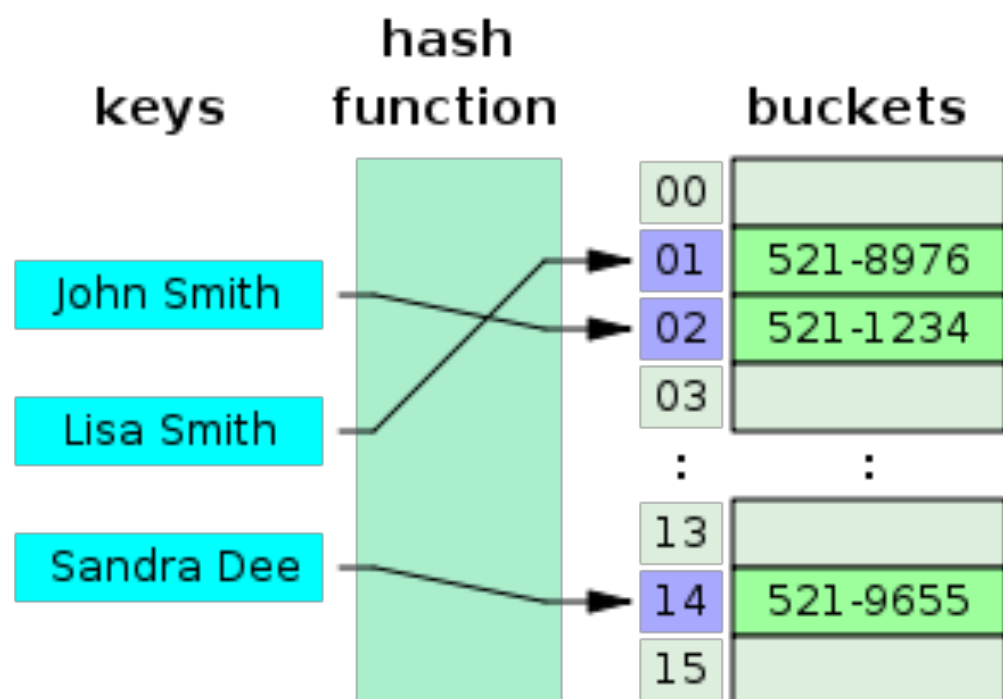


广发银行 CGB

- 输入为任意大小的字符串
- 输出为固定大小，例如256位
- 可以进行有效计算： $O(n)$
- 抗碰撞
- 隐匿性
- 难题友好

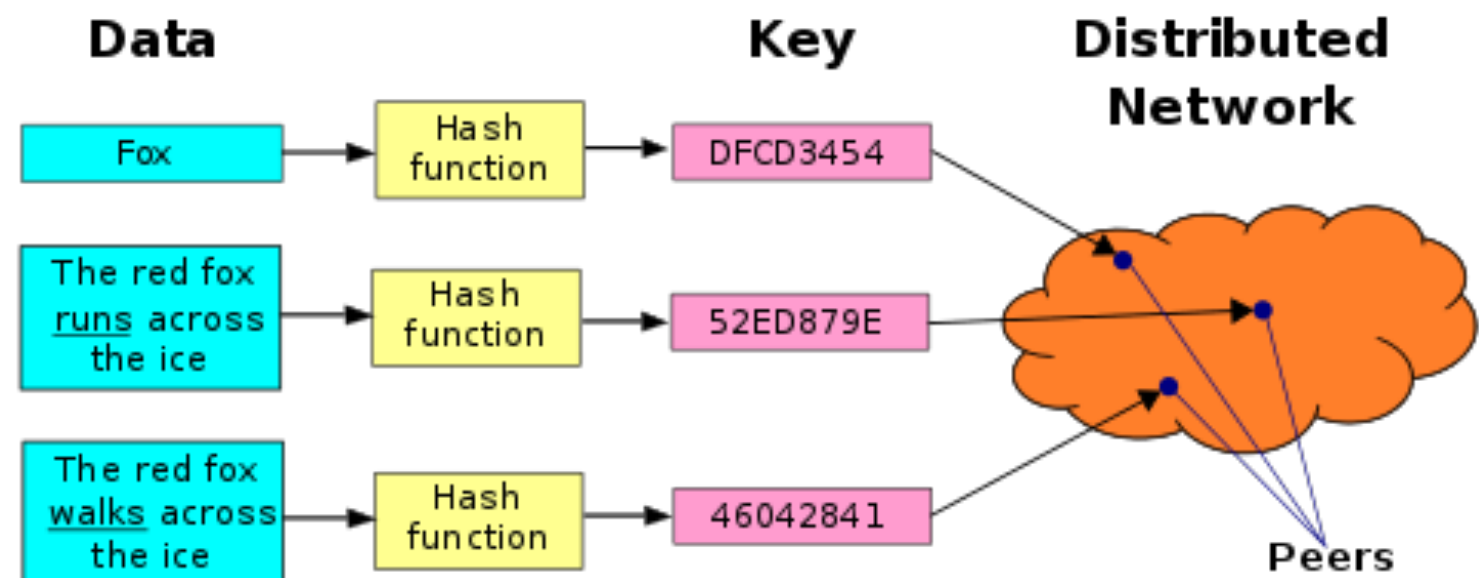
<http://www.fileformat.info/tool/hash.htm>

Hash Table

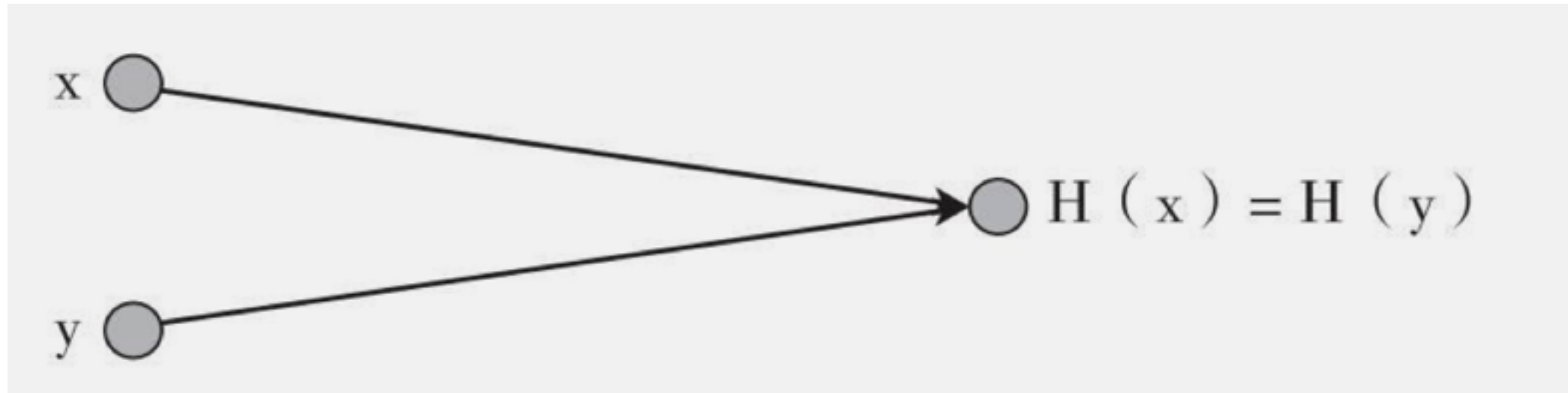


https://en.wikipedia.org/wiki/Hash_table

Distributed Hash Table

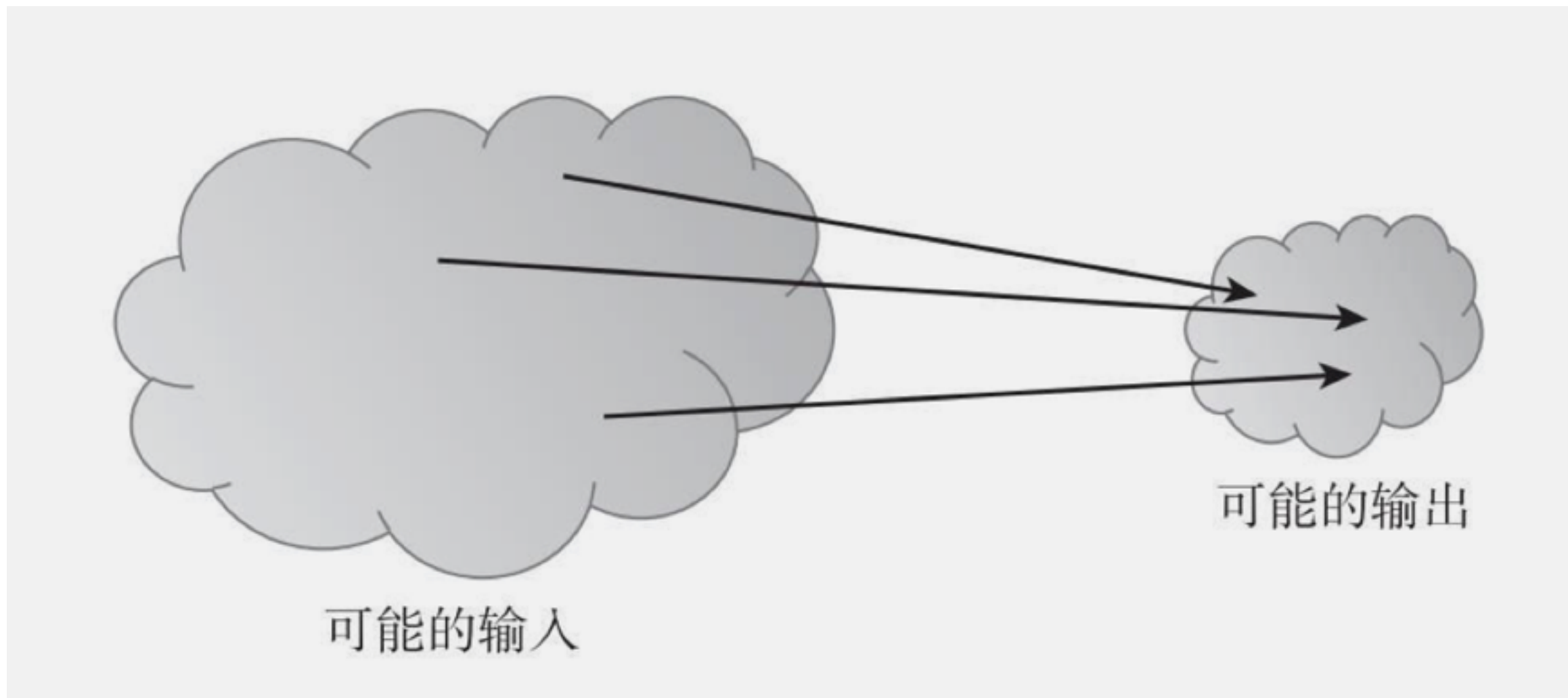


https://en.wikipedia.org/wiki/Distributed_hash_table

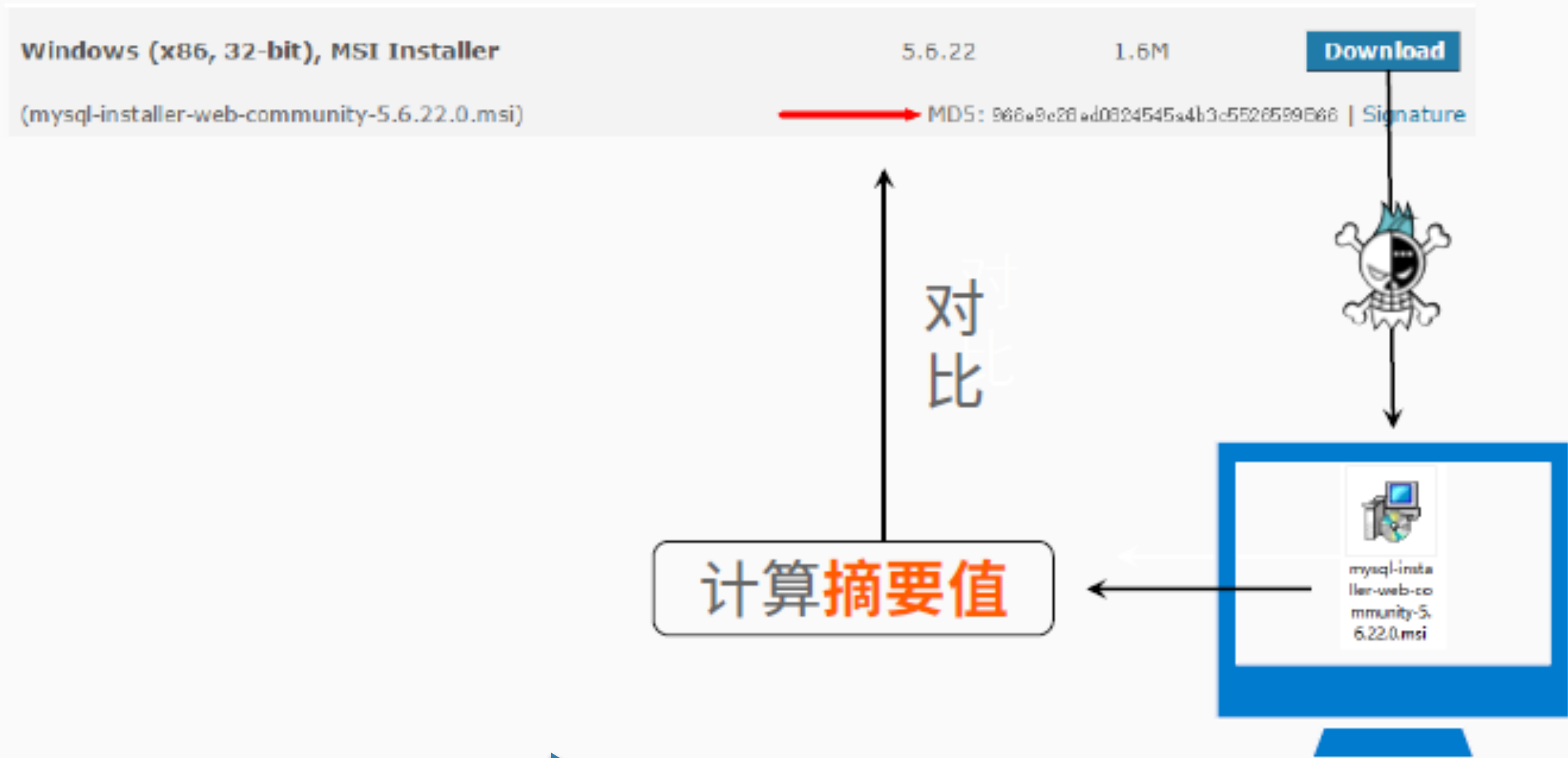


2^{130}

99.8%

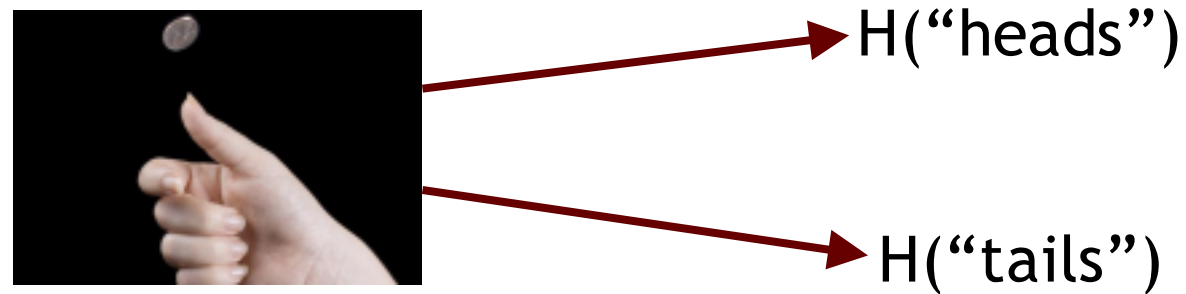


hash足够小



$$H(x) = H(y) \quad \longrightarrow \quad x = y$$

- 给出 $H(x)$, 不能找到 x
-



-
- 如果概率分布有高的最小熵, 非常分散, 则具有隐匿性

$com := \text{commit}(msg, nonce)$

公开 msg

$match := \text{verify}(com, nonce, msg)$

公开 key 和 msg

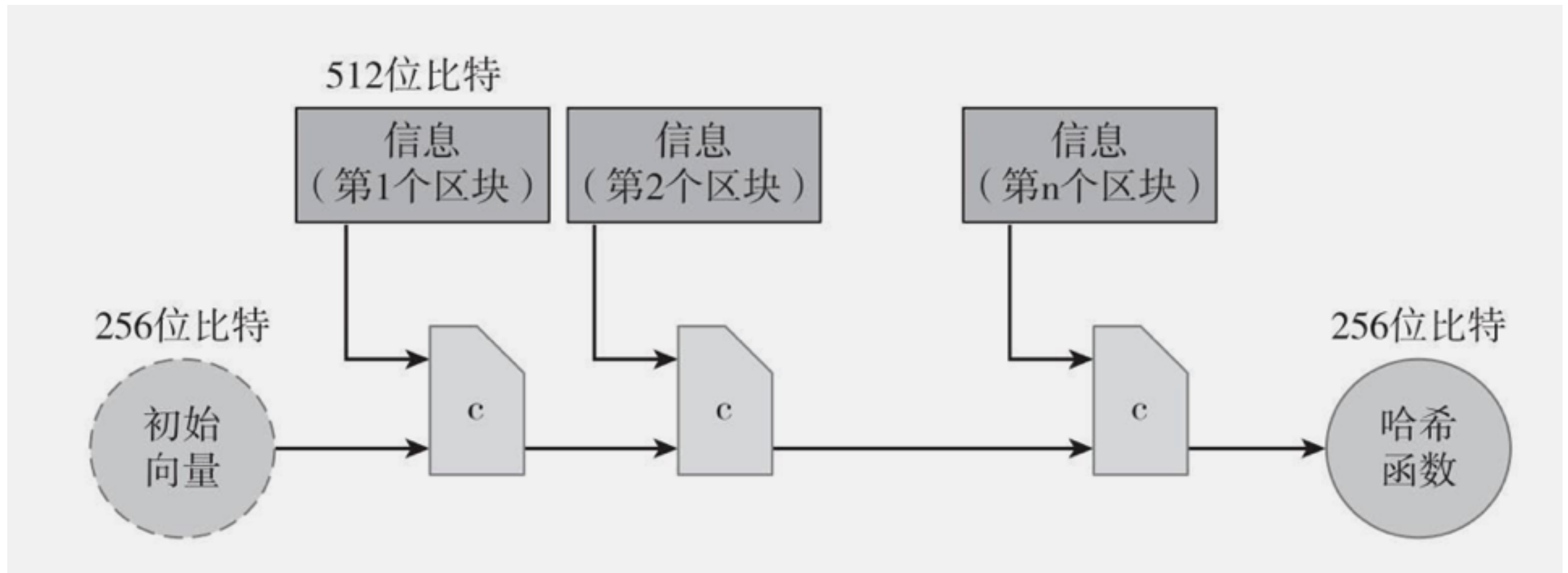
已知 com , 不能找到 msg

不能找到 $msg \neq msg'$, 但 $\text{commit}(msg, nonce) == \text{commit}(msg', nonce')$

$\text{commit}(msg) := (H(nonce \mid msg), H(nonce))$

$\text{verify}(com, nonce, msg) := (H(nonce \mid msg) == com)$

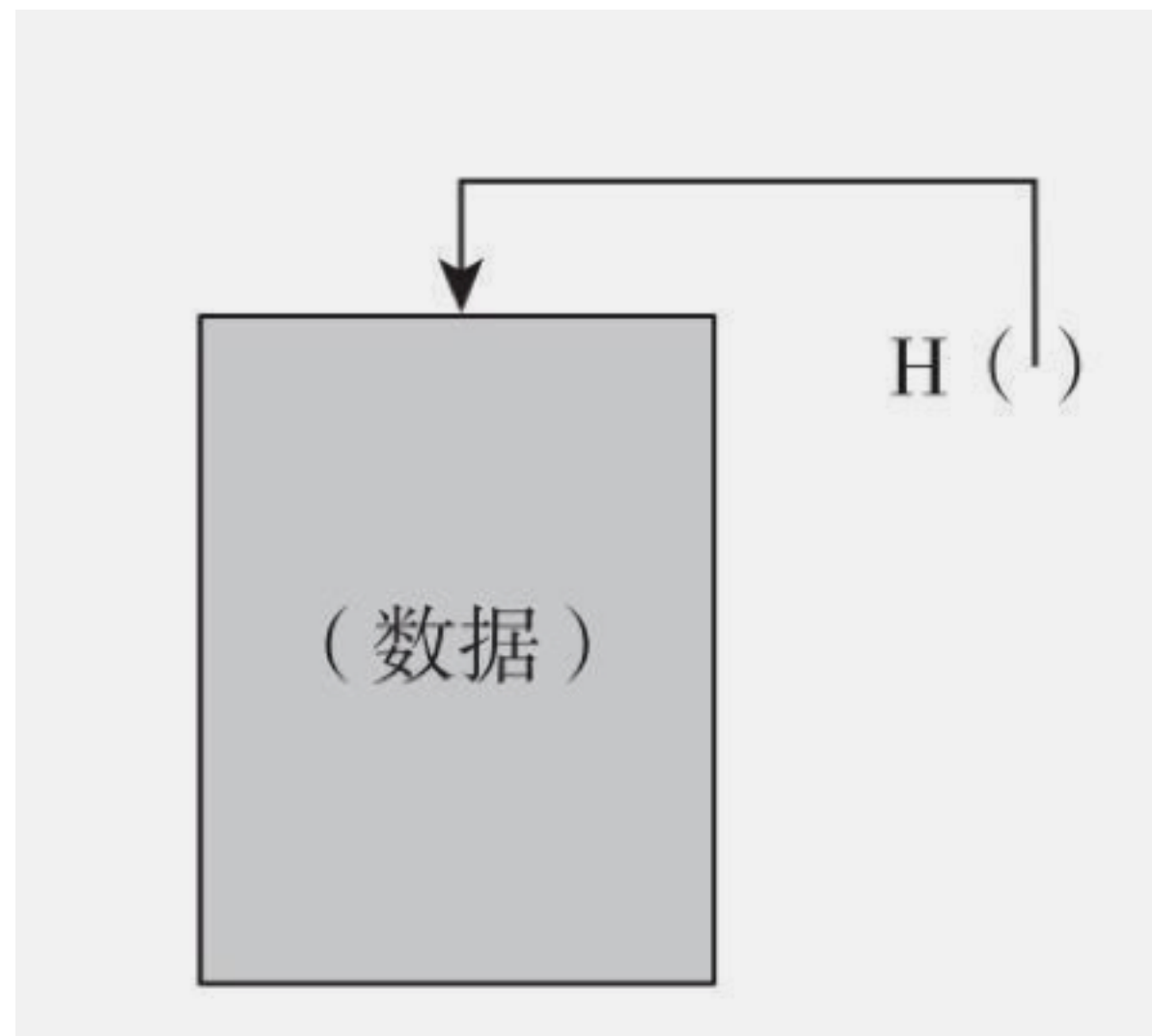


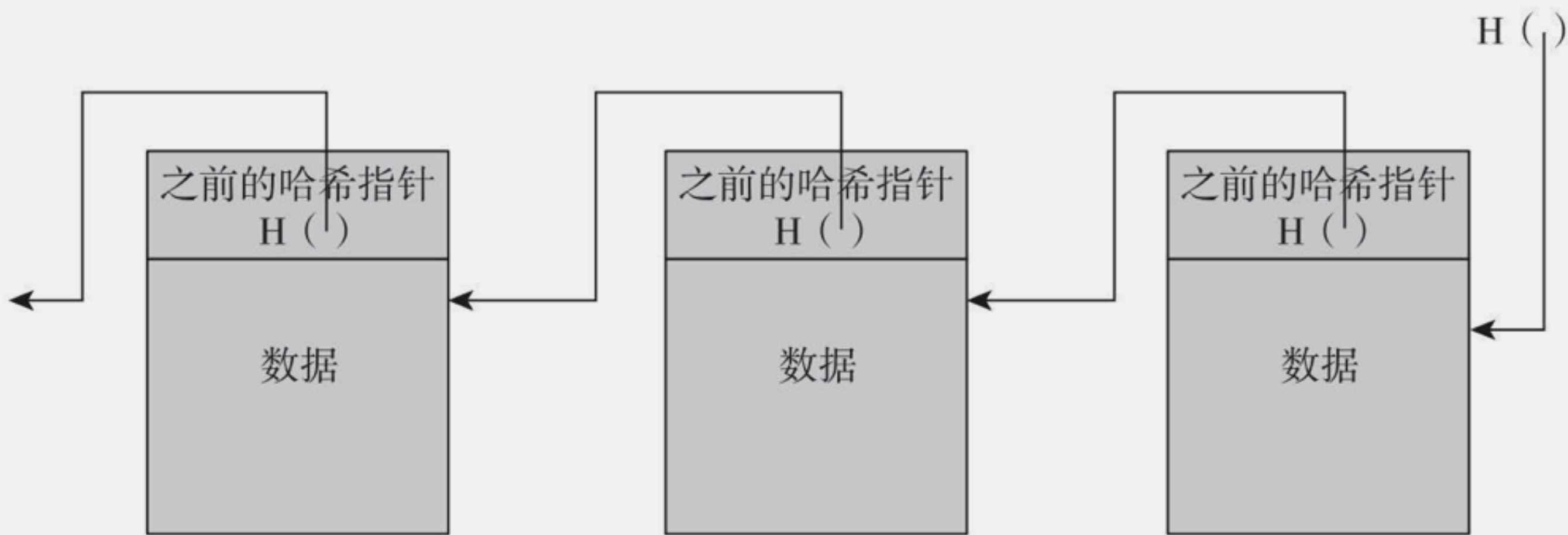


- **Hash指针是一个指向存储数据及其数据Hash的指针**

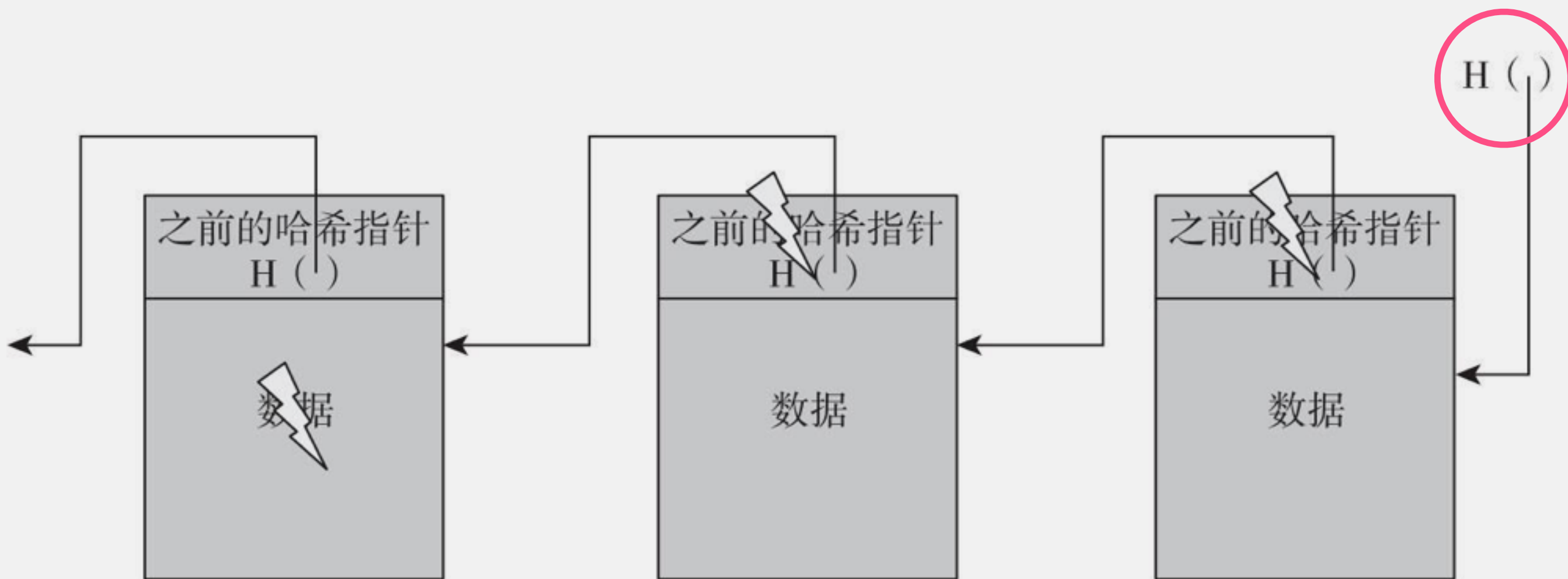
- **取回数据**
- **验证数据是否改变**

- **区块链的关键思想**

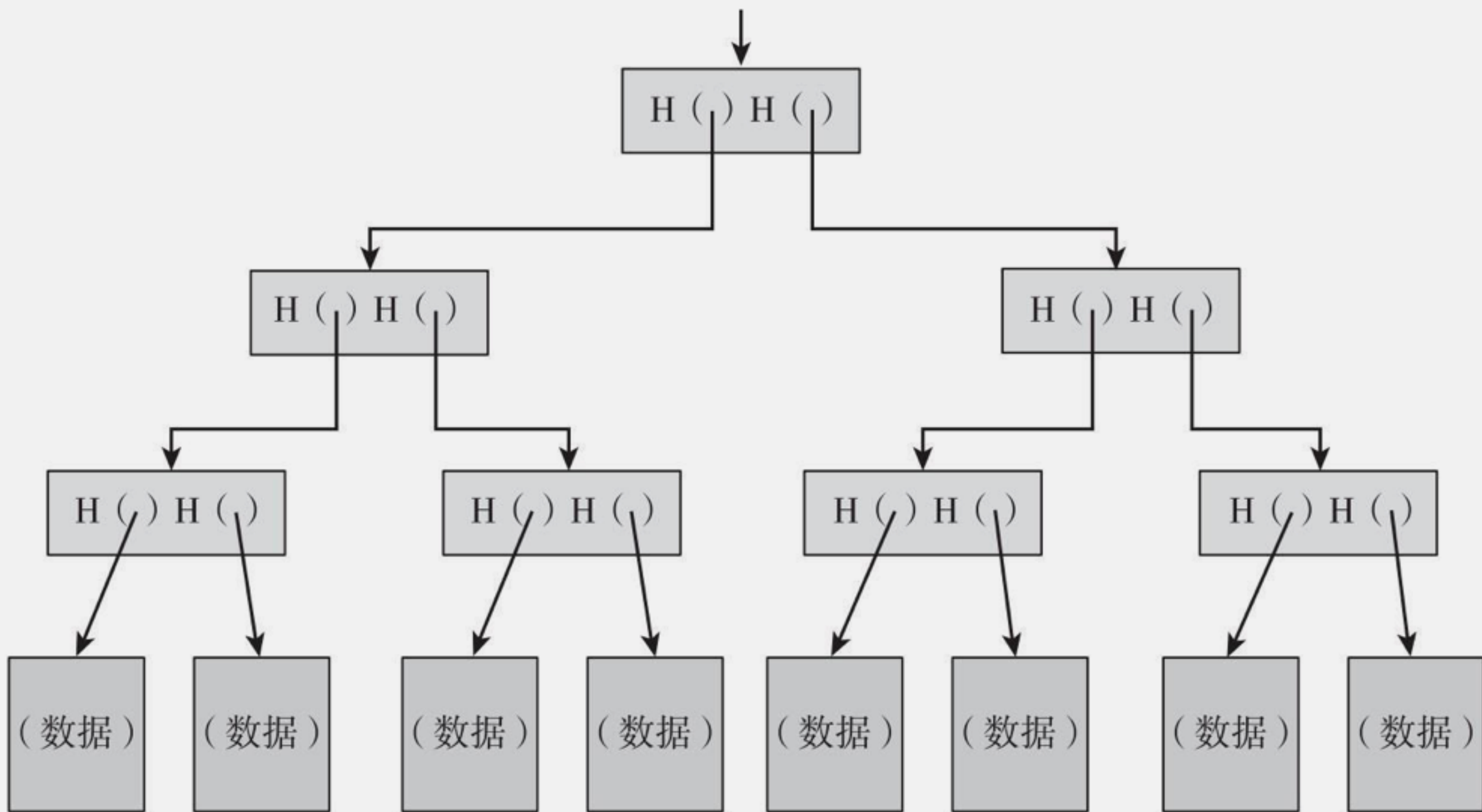




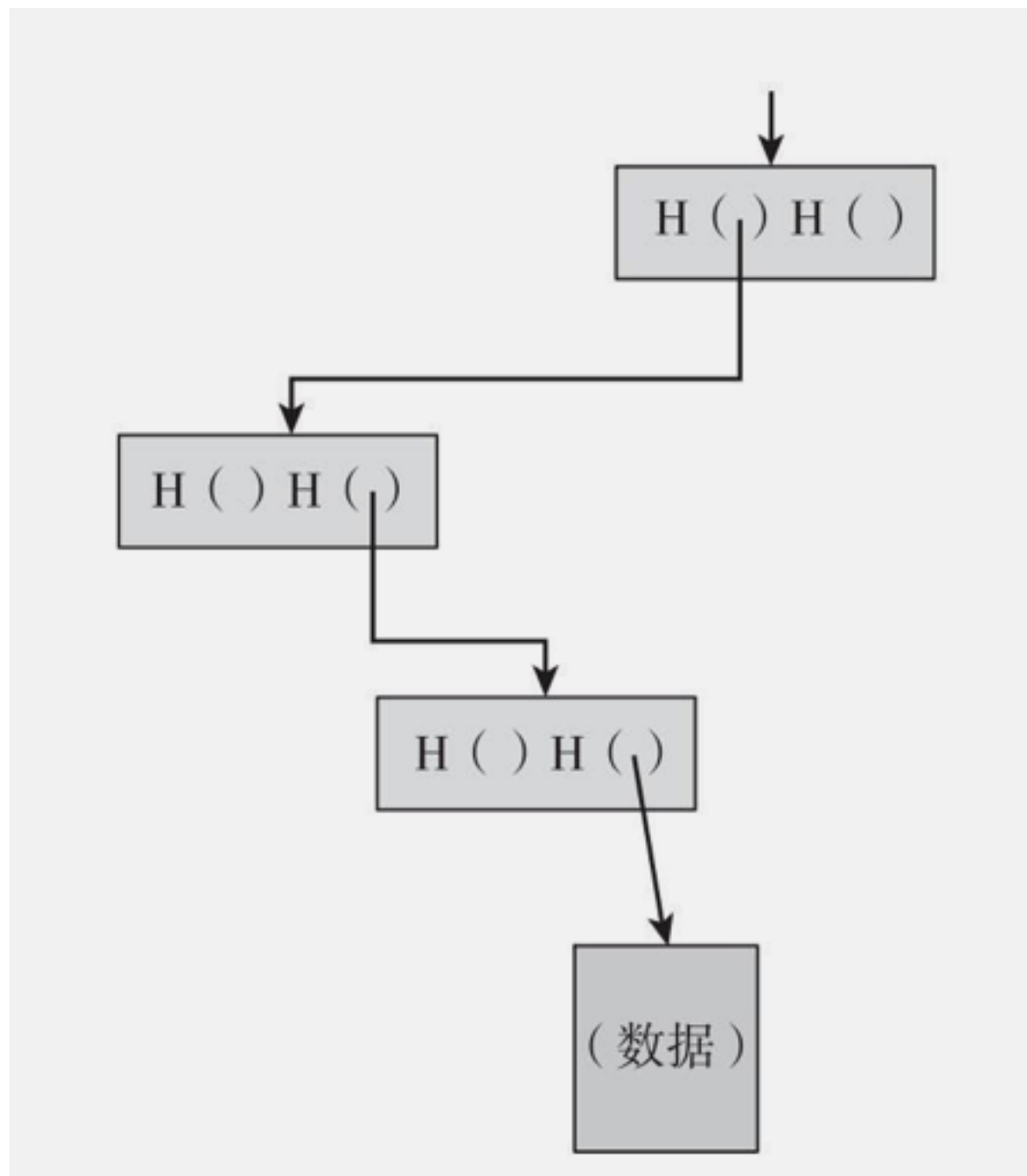
防止篡改



梅克尔树

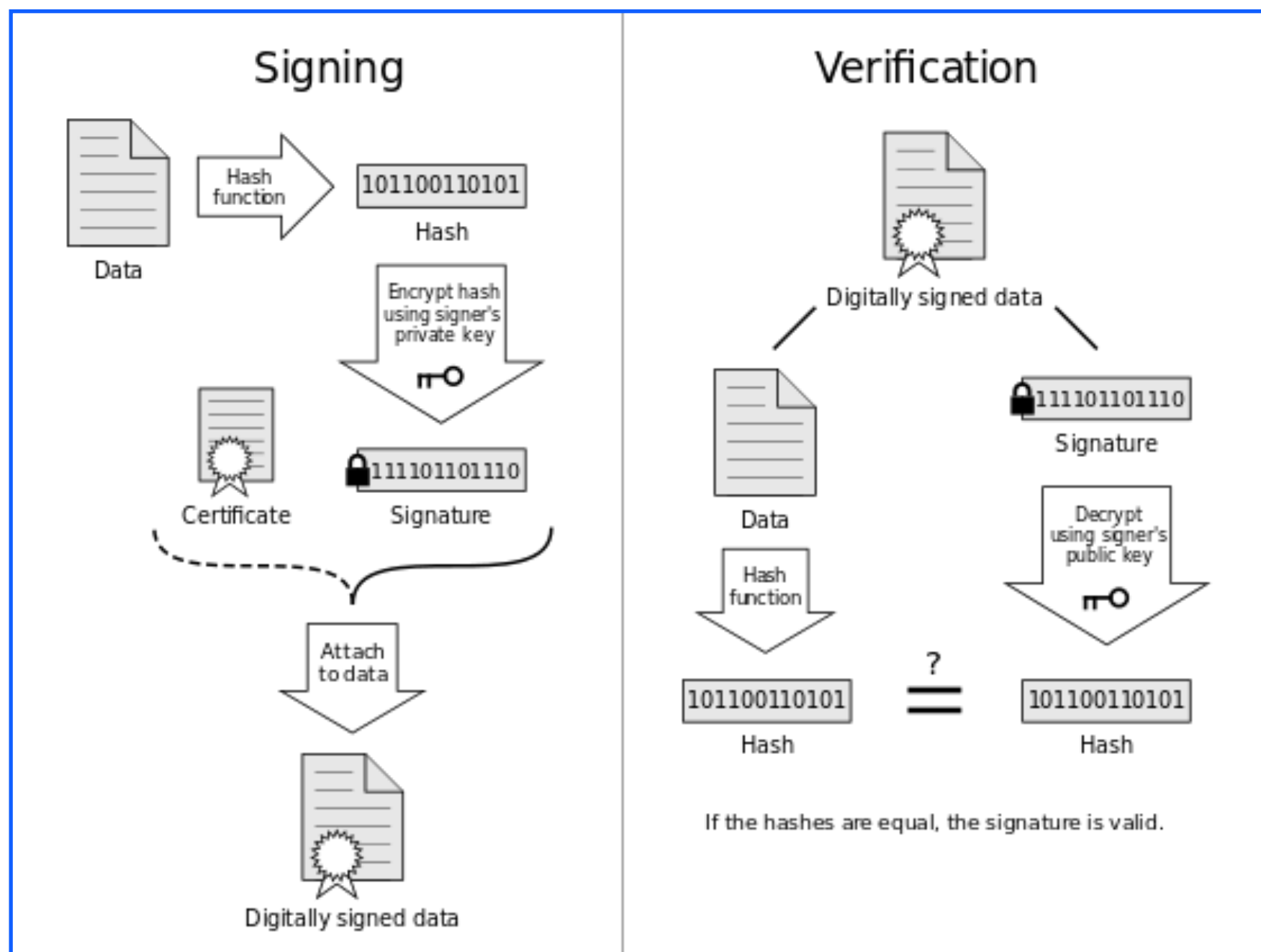


成员证明

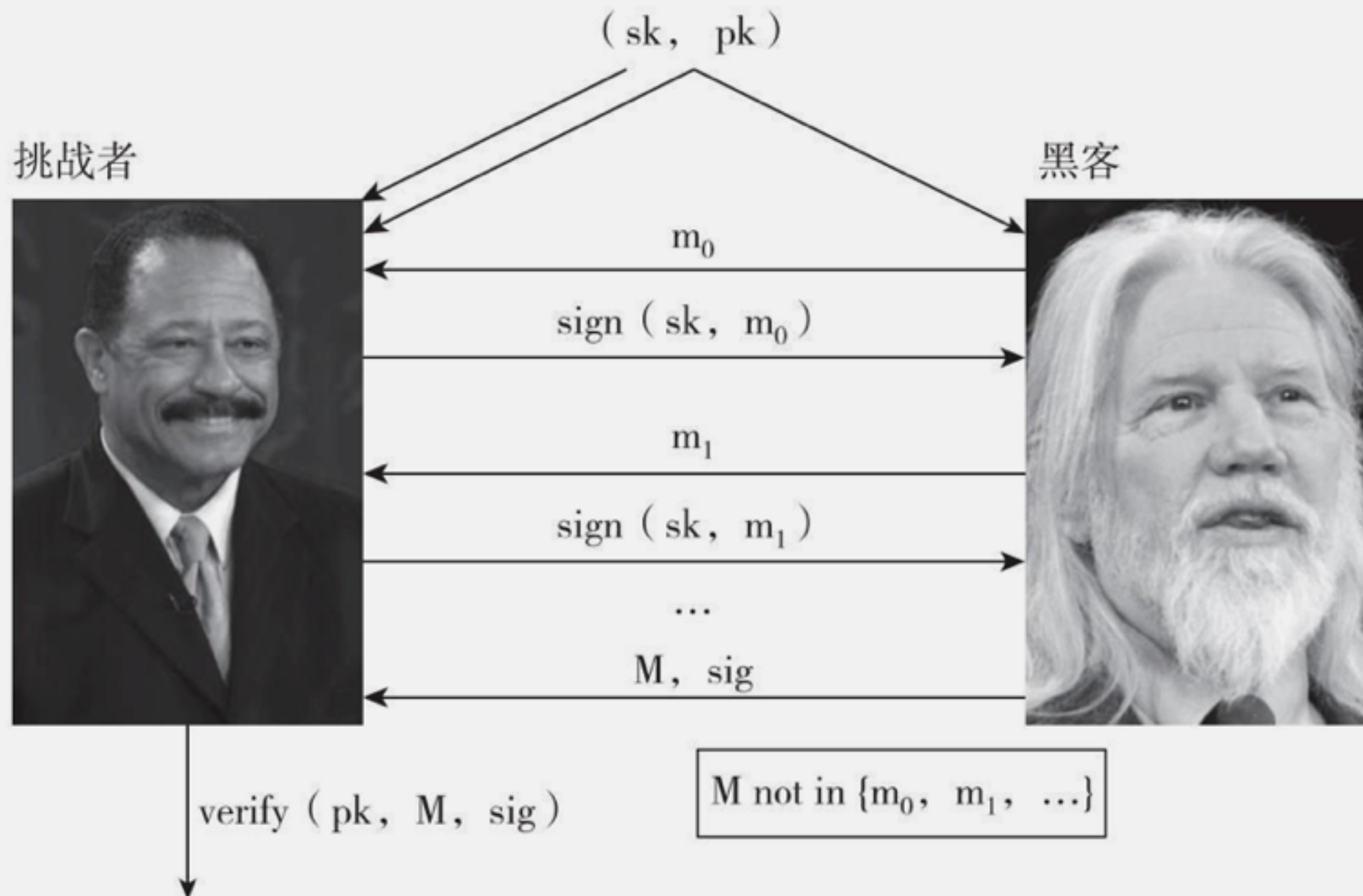


$O(\log n)$

- 自己签名，任何人都可以验证
- 公钥和私钥
- 不可伪造
- 信息大小

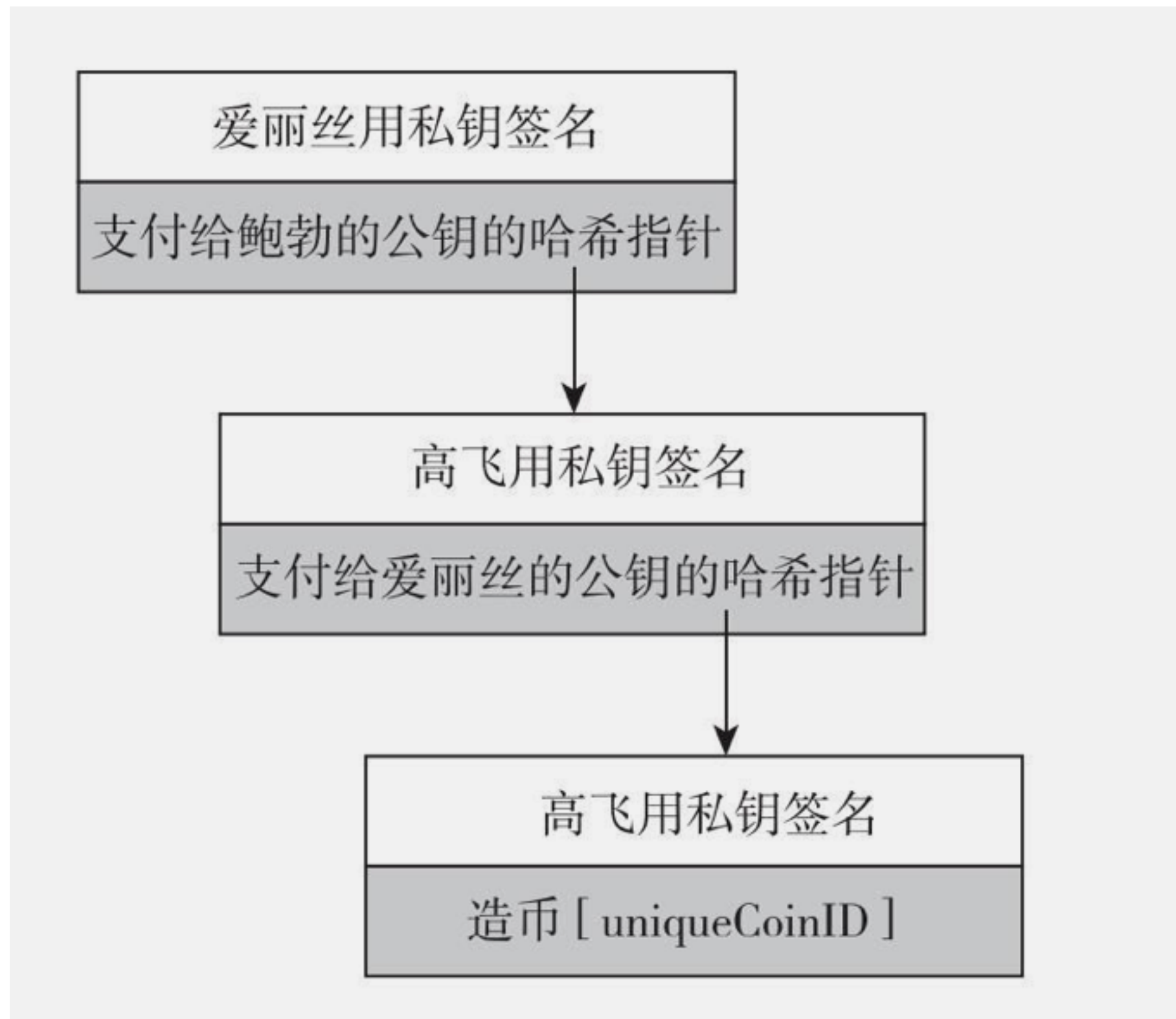


不可伪造游戏



如果是正确的，黑客赢得这个游戏

- 每人一个公钥、一个私钥
- 比特币：2的160次方
- 全球的沙子：2的63次方





交易ID: 73		类型: 造币	
被创造的货币			
序号	数量	造币记录	
0	3.2	0x...	
1	1.4	0x...	
2	7.1	0x...	

← 虚拟货币ID 73 (0)

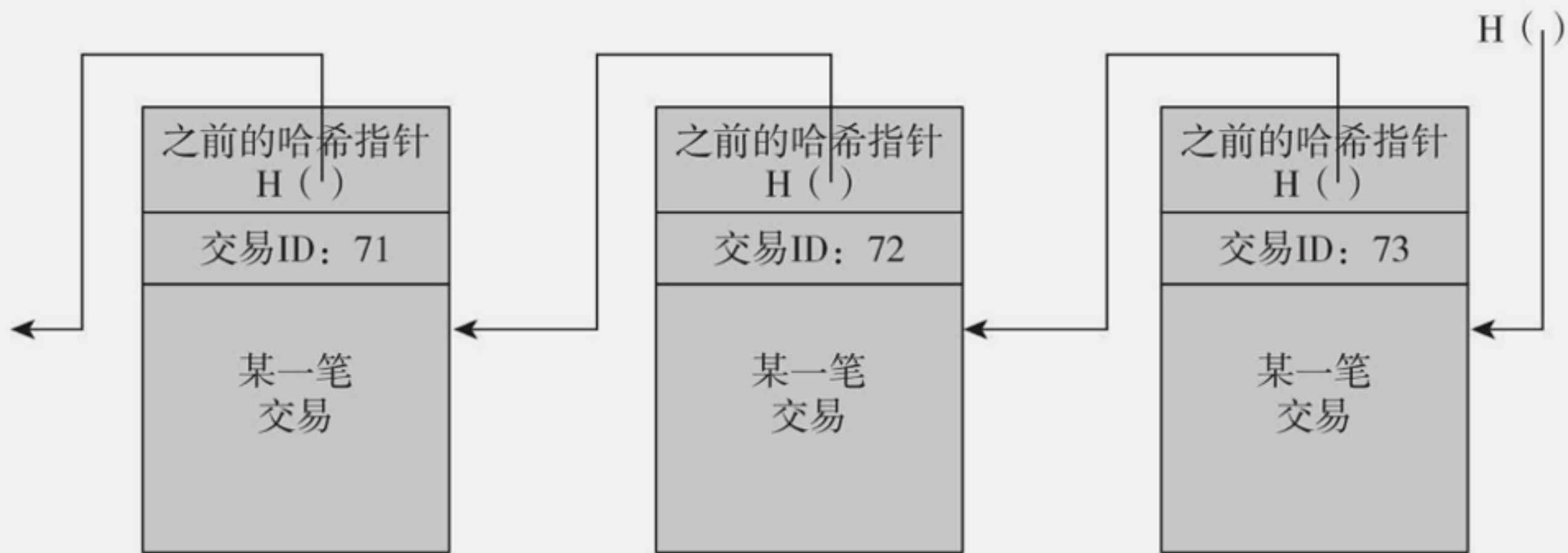
← 虚拟货币ID 73 (1)

← 虚拟货币ID 73 (2)

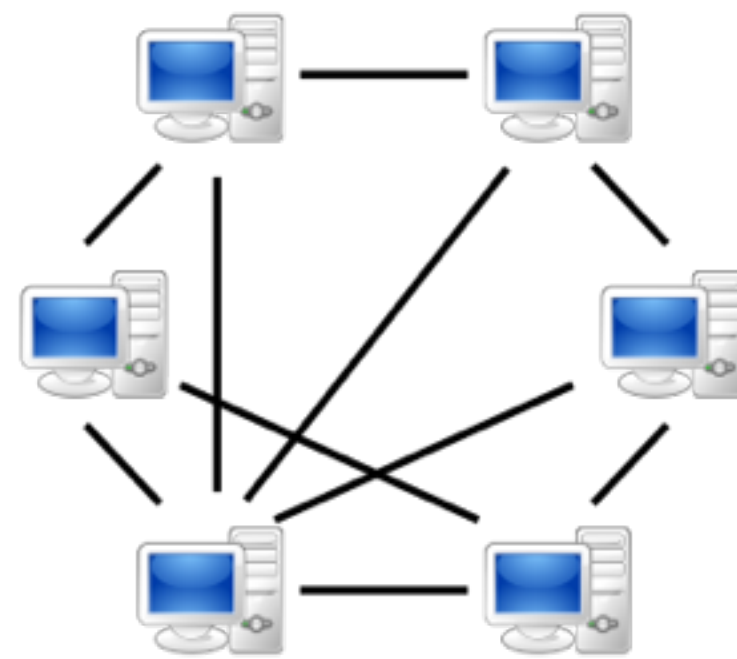
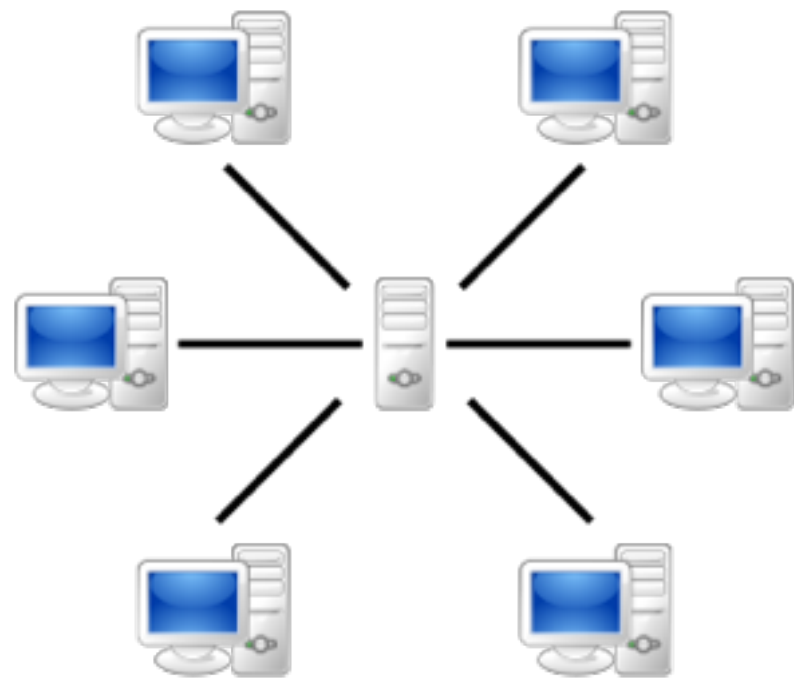
交易 ID: 73		类型: 付币
消耗的虚拟货币 ID: 68 (1), 42 (0), 72 (3)		
被创造的货币		
序号	数量	造币记录
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
签名		

提问时间！

Decentralization



- 比特币如何要去中心化?



神话

- 没有纯粹的中心化系统或者分布式系统
- 各有优缺点
- 大多数系统都是混合类型的

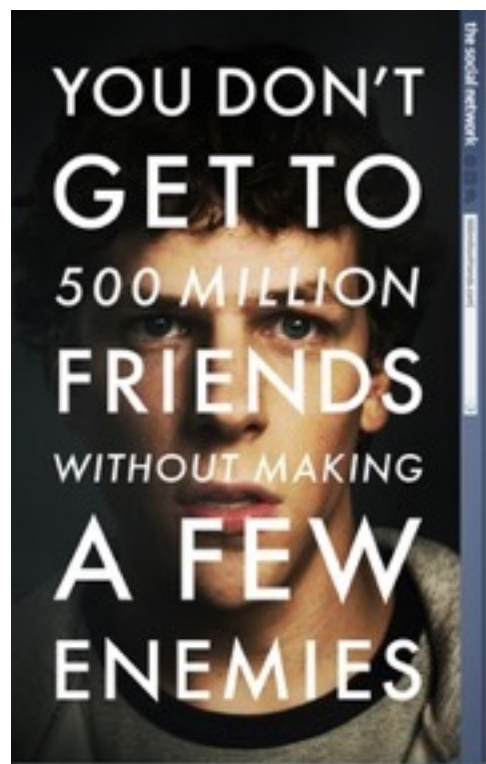
Internet, Email, IM, SNS

比特币?

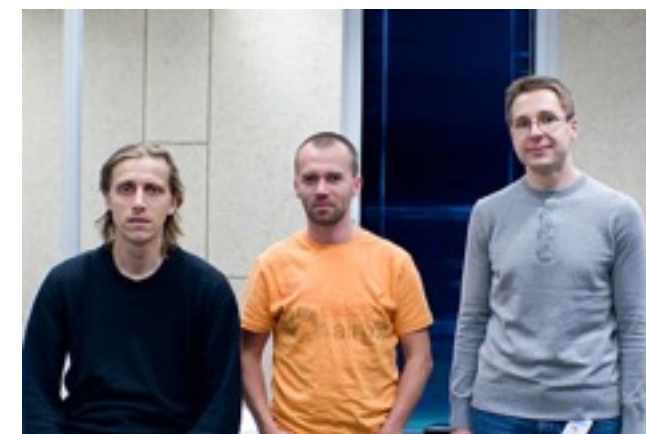


Sean Parker

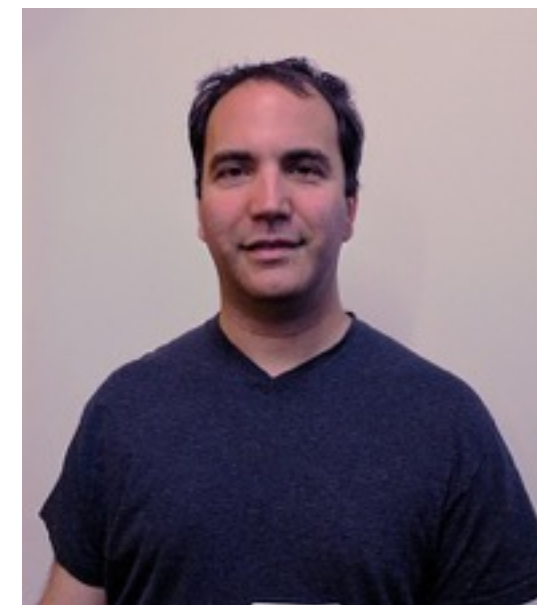
facebook



The Social Network



Bram Cohen



BitTorrent

- 谁维护交易账本?
- 谁有权限验证交易的有效性?
- 谁创造新的比特币?

- 谁决定系统如何改变规则?
- 比特币如何获得交易价格

技术

激励

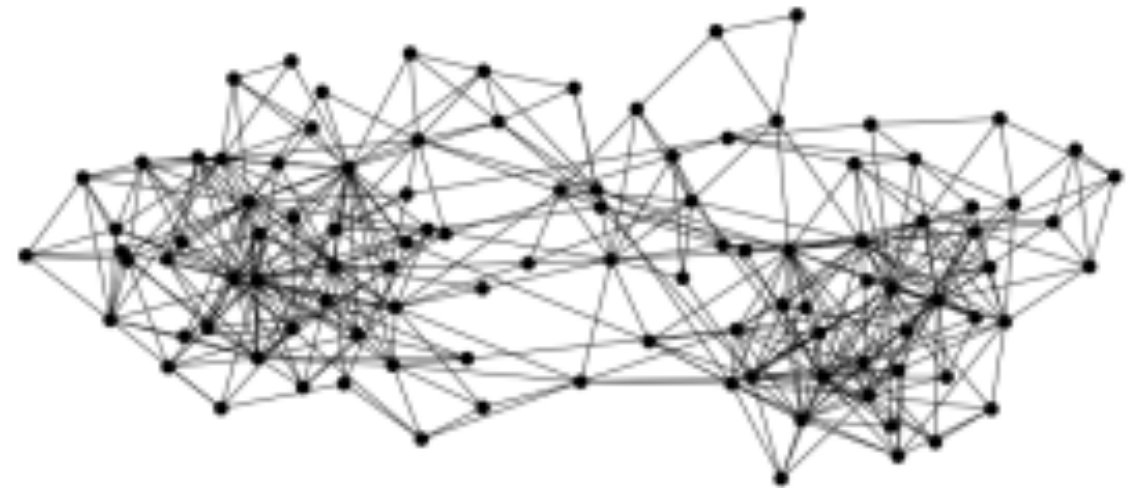
用户: 对等网络 / 矿工 挖矿 / 开发人员: 软件更新

- 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



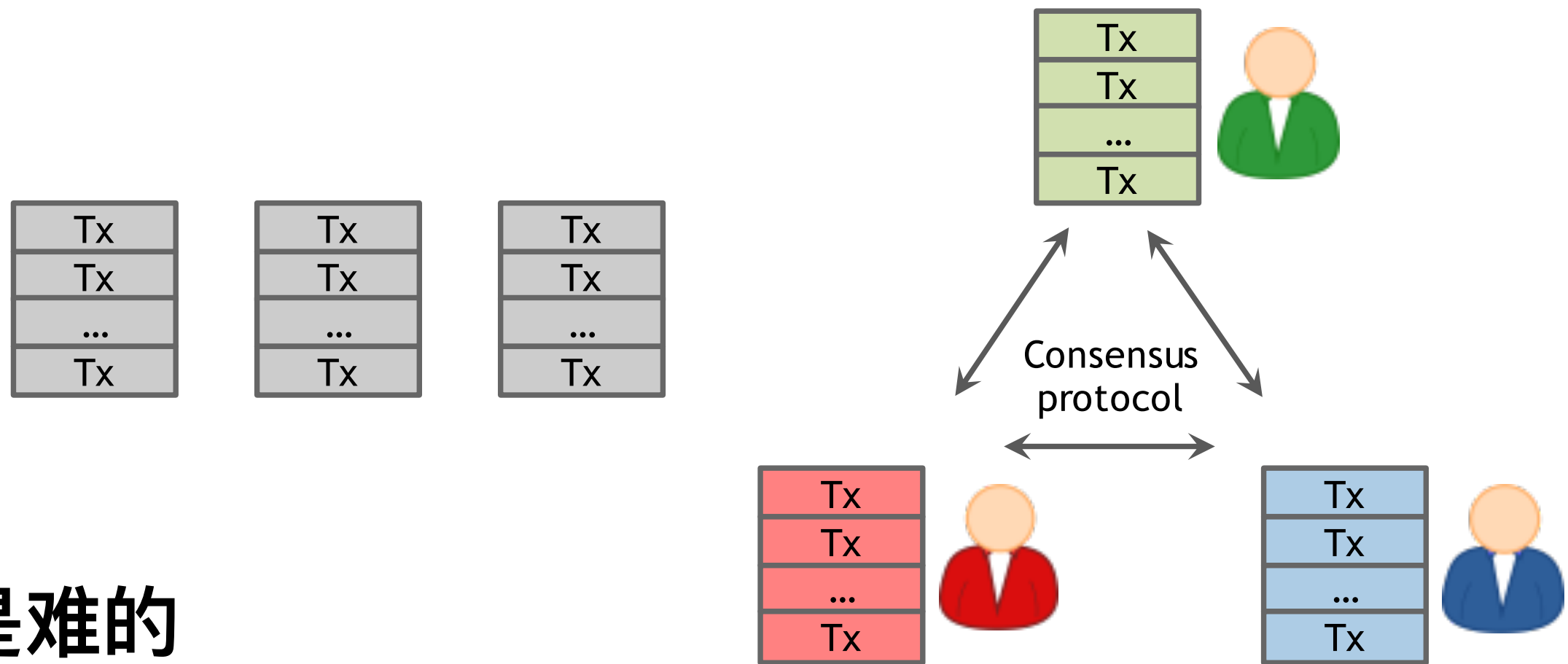


signed by Alice
Pay to $pk_{Bob} : H()$



- 比特币是一个P2P网络
- Alice 需要广播她完成的交易给所有的节点
- 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

- 每一个节点输出它的未共识的业务竞争下一个Block



- 共识是难的

➔ *Node: crash, malicious*

➔ *Network: Imperfect (online, latency)*

Global Time

The Byzantine Generals Problem

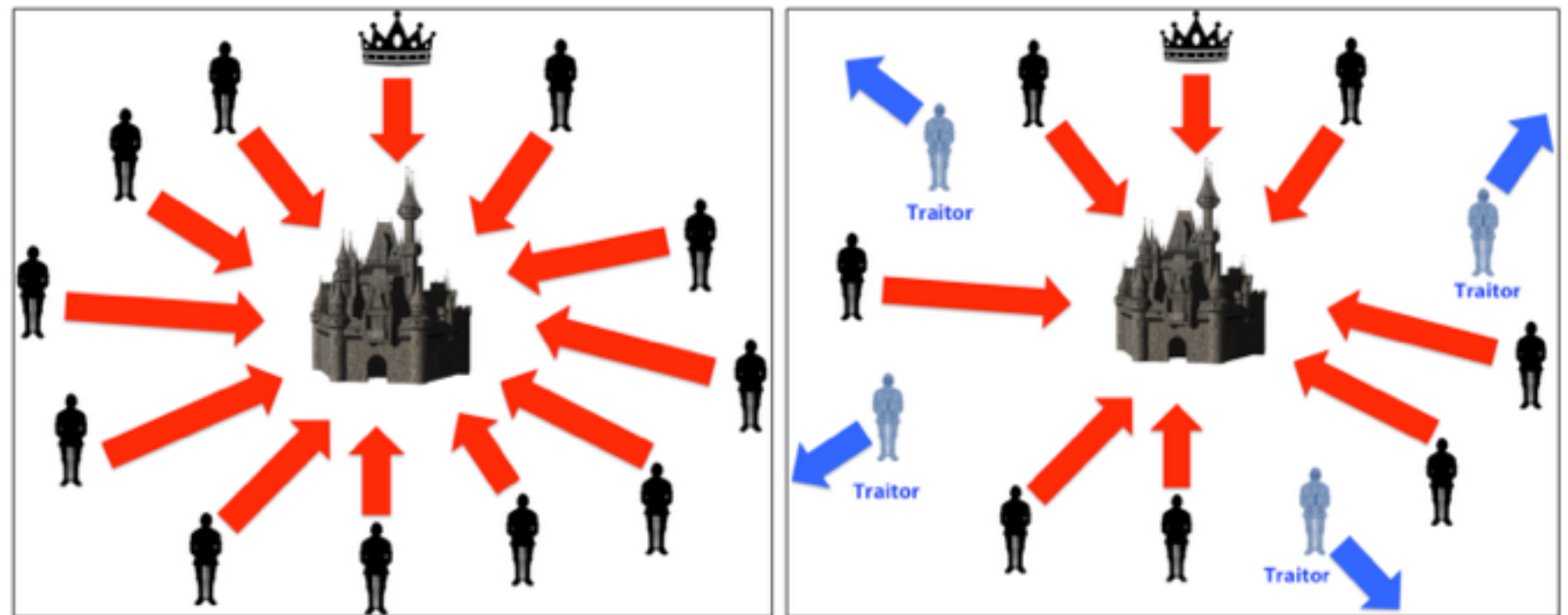
| 1982

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International



LESLIE LAMPORT

2013图灵奖



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

Paxos Made Simple Abstract

2001

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

- **理论落后于实践**
- **引入了 *Incentive***
 - * **是电子货币**
- **利用了随机性**
 - * **很长一段时间后取得共识，1小时**
 - * **随着时间的增加，对某一块的共识的概率越来越大**

- 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

- 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

- 窃取比特币
- 拒绝服务攻击
- 双重支付攻击

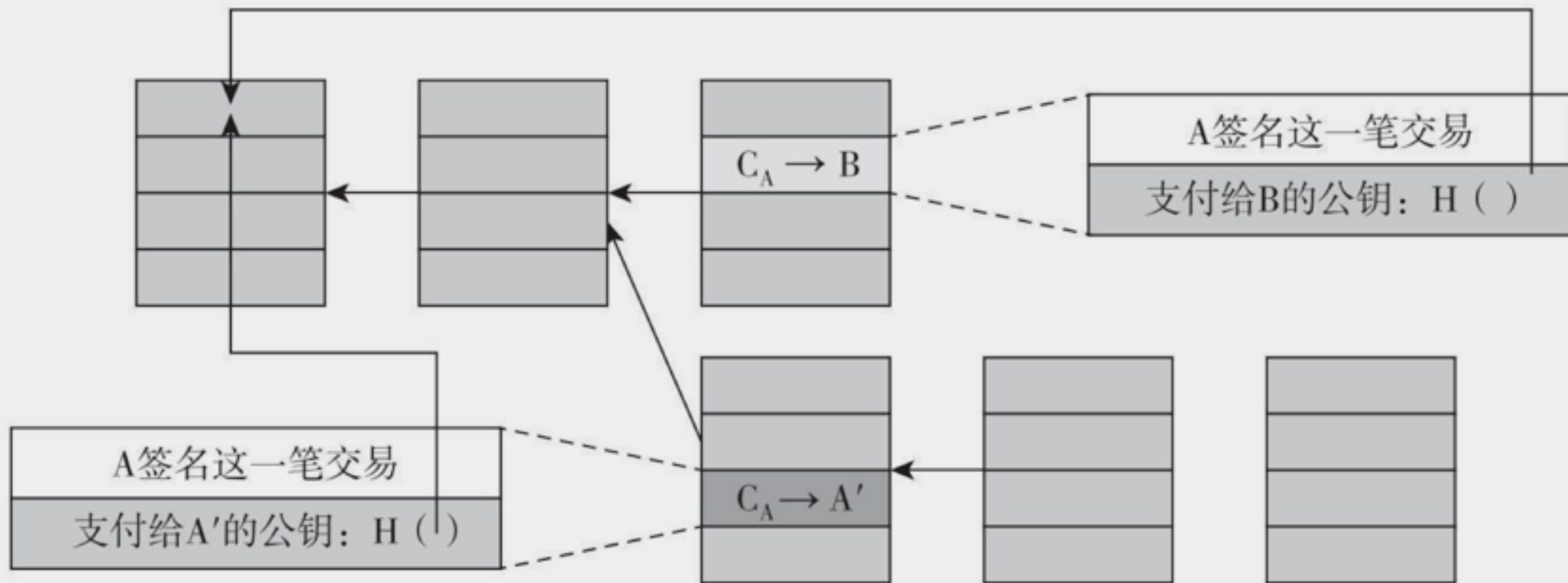


图2.2 双重支付攻击

注：爱丽丝创建了两笔交易：一笔是她付给鲍勃比特币的交易，另一笔是她将这笔比特币重复支付到她控制的另一个地址。因为这两笔交易用相同的比特币支付，所以只有一笔会被放进区块链。图中的箭头表示一个区块链接到前一个区块的指针，通过在前一个区块自己的内容中包含了一个哈希值进行了扩展。 C_A 代表爱丽丝拥有的币。

Decentralization 双重攻击防止：等待多次确认

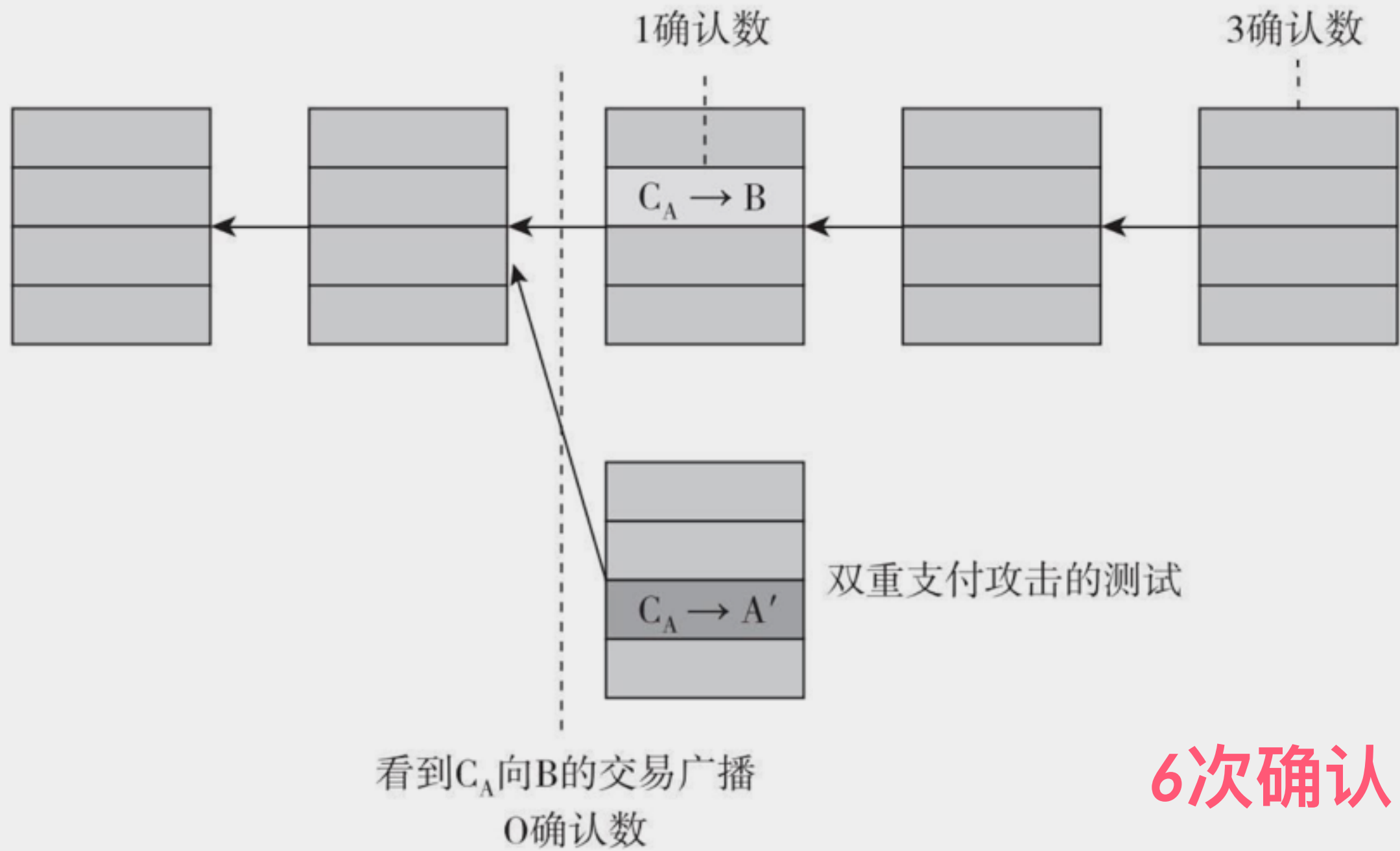
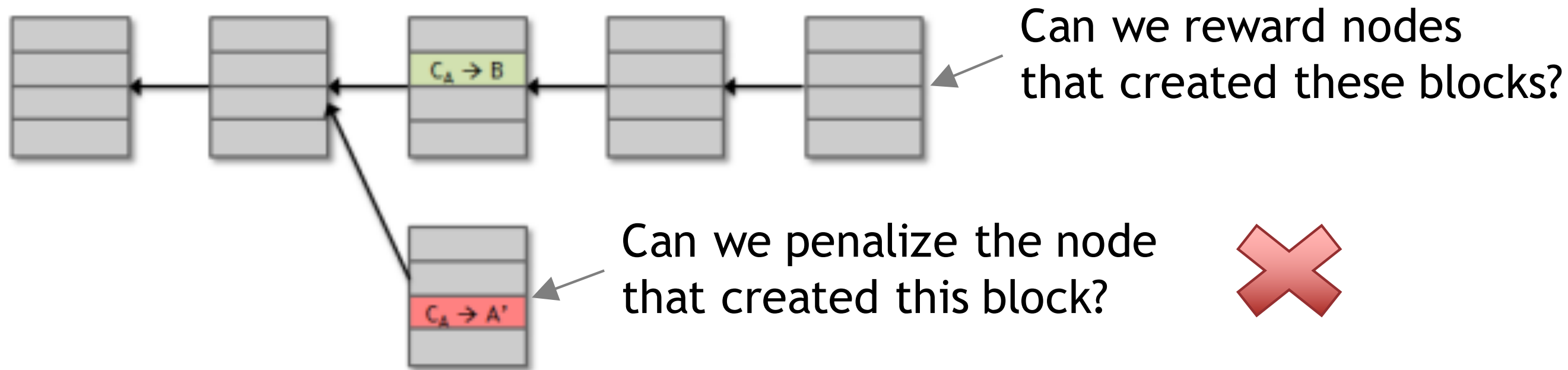


图2.3 从鲍勃立场来看双重支付

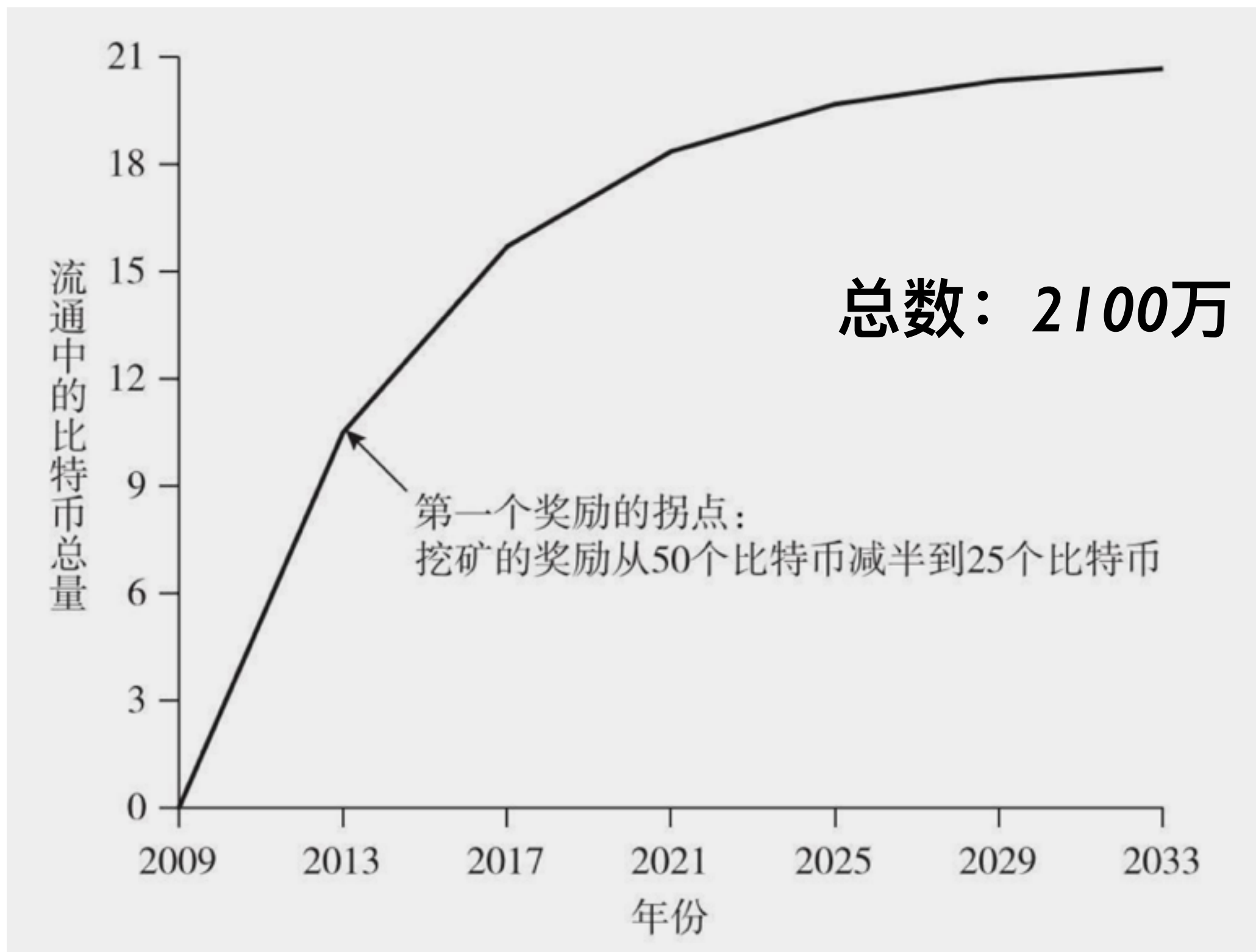
注：这是一个从商家鲍勃的立场来看爱丽丝做的双重支付尝试。为了保护自己免受双重支付攻击，鲍勃应当等爱丽丝向他支付的交易被区块链包含进去，并且多等几次确认。

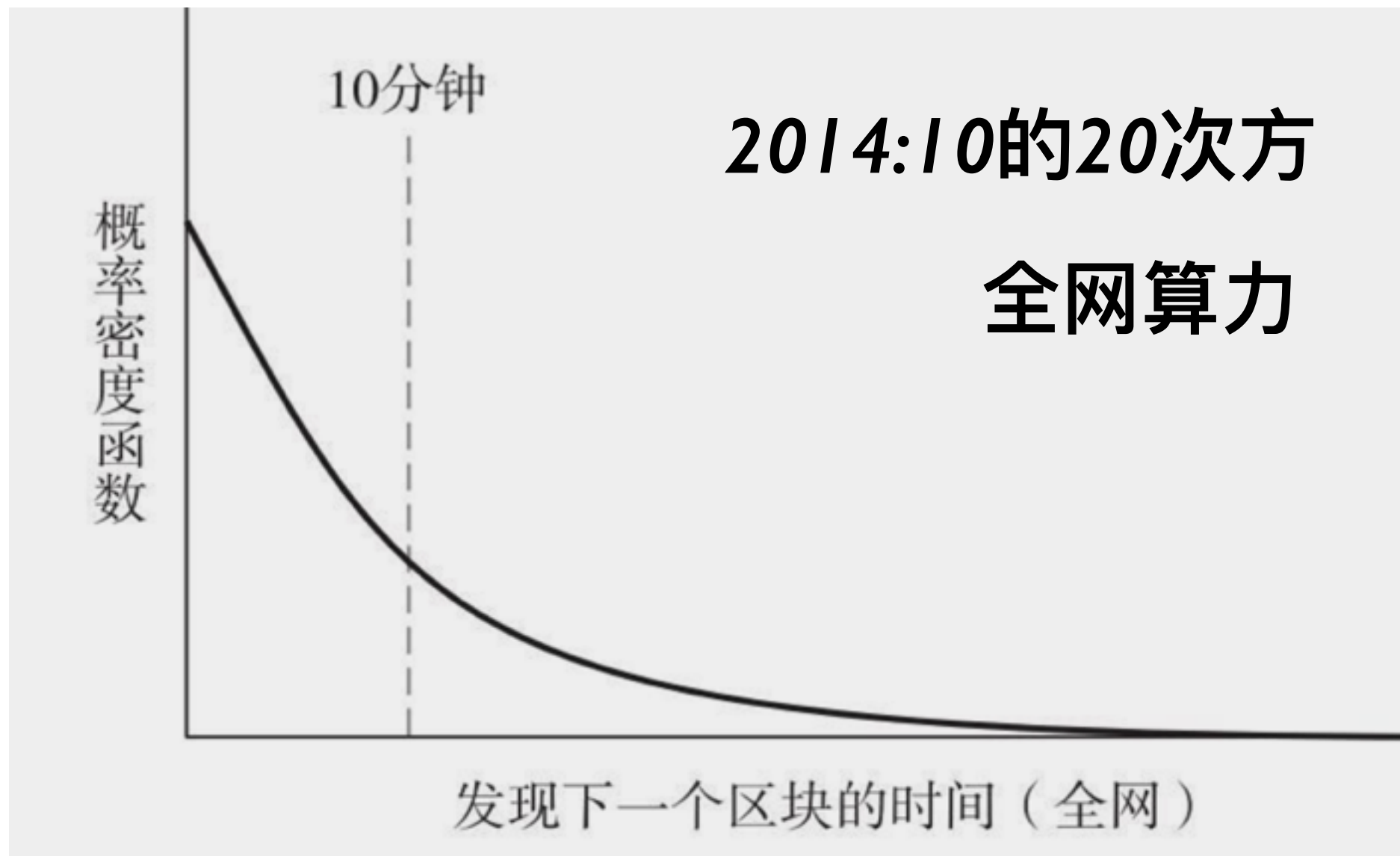
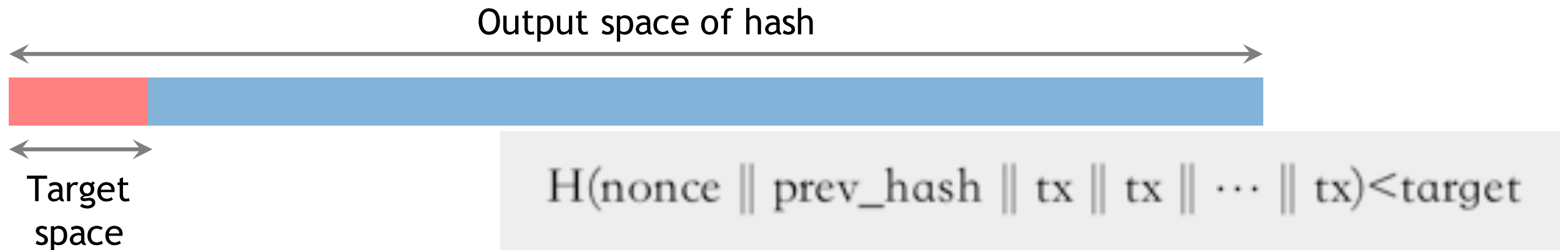


区块奖励 vs. 交易费奖励

交易费：输入和输出不等

比特币奖励





**2014:10的20次方
全网算力**

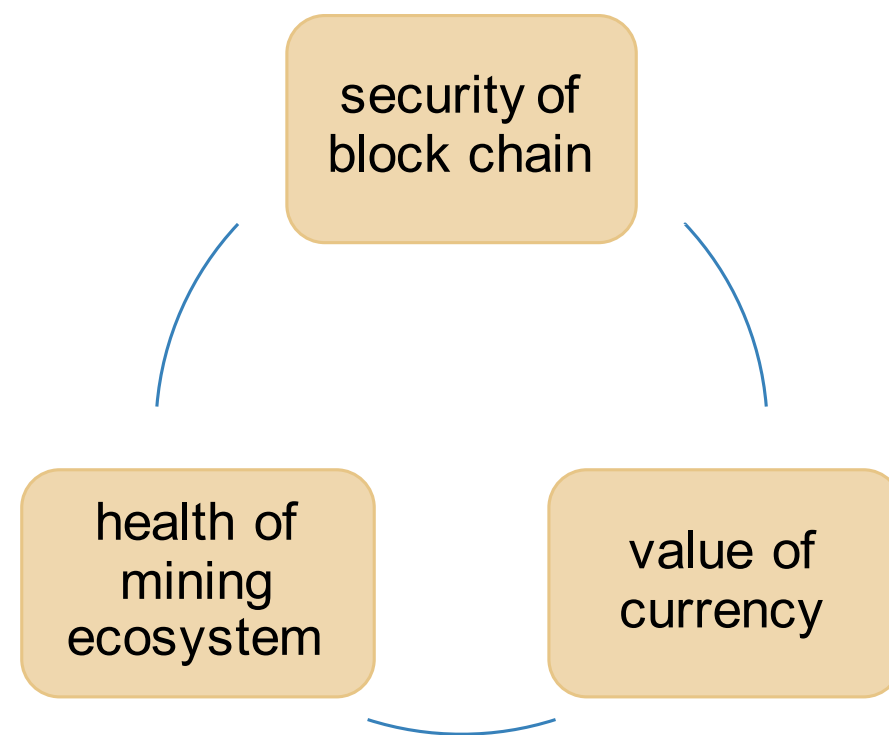
限定Hash的输出范围

临时随机数

**PoW:
工作量证明**

**PoS:
权益证明**

- 身份
- 交易
- P2P网络
- 区块链
- 共识
- Hash难题
- 挖矿
- 经济



- 51%攻击
 - ➔ 窃取币、操纵交易、改变激励、破坏信心

- 比特币现在的情况
- 比特币是分布式电子货币吗？
- 比特币实现匿名了吗？
- 比特币安全吗？
- 比特币不能操控吗？

提问时间！

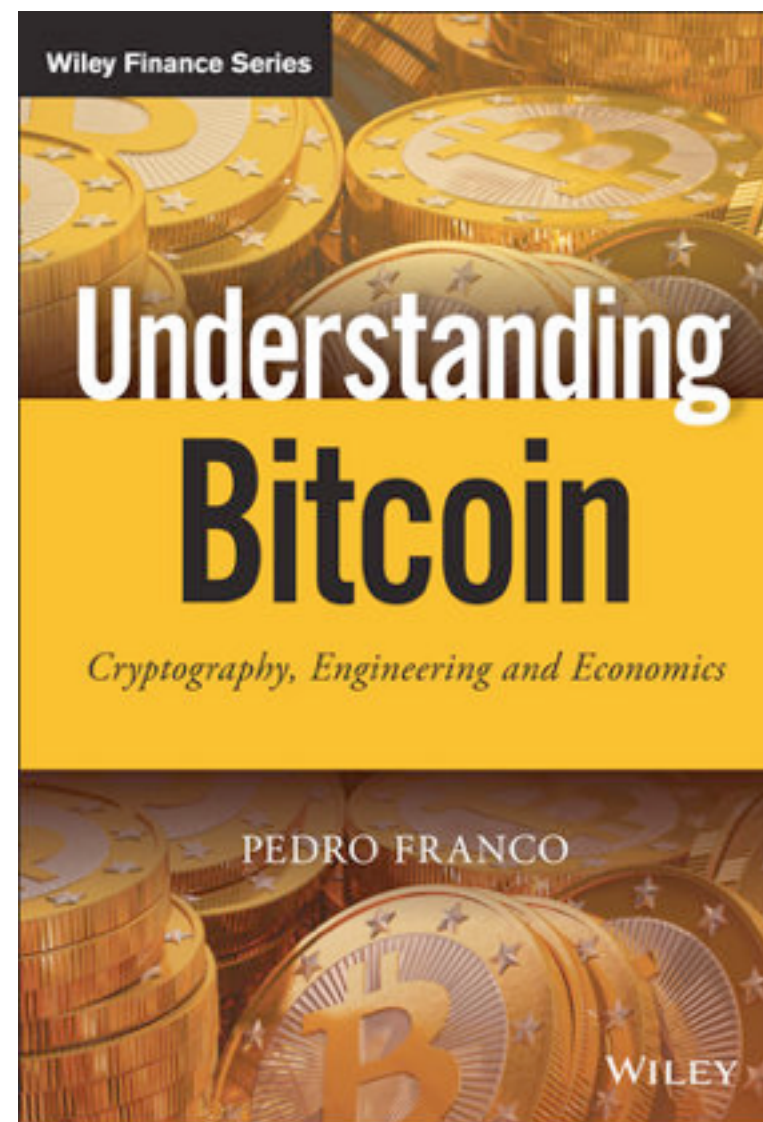
Projects

- 选择一个区块链应用相关的**项目**(平台类项目不行, 必须是具体的应用类项目), 每位同学一个, 不能重复, 发到课程群, **格式: 学号-姓名-项目名称-应用领域**; 先到先得。应用领域可以不准确
- 每个同学完成自己的**项目总结报告**, 总结报告要分析该项目的发展历程、发展趋势、优缺点、面临的问题, 你的所思所想;
- 根据项目对同学进行**分组**, 每个组对应一个区块链相关的应用领域;
- 每个组完成该应用**领域总结报告**; 总结报告要分析该领域的发展历程、发展趋势、优缺点、面临的问题, 小组讨论后的所思所想;
- 小组提出一个新的项目设计, 撰写完成**项目白皮书**;
- 最后一次课前提交项目总结报告、项目白皮书和**报告PPT**, 最后一次课报告 (具体时间待定);
- 所有参考资料、完成文档和PPT等上传Github。

Home **work**



第一章、第二章



第五章、第七章

- 要求阅读如下论文，写论文阅读报告：

➡ *In Harvard Business Review 2017.*

ARTICLE
TECHNOLOGY

The Truth About
Blockchain

It will take years to transform business,
but the journey begins now.

by Marco Iansiti and Karim R. Lakhani

**Harvard
Business
Review**

REPRINT R1701J
PUBLISHED IN HBR
JANUARY-FEBRUARY 2017

谢谢!

孙惠平

sunhp@ss.pku.edu.cn