Blockchain
区块链

2018.02.27

区块链简介

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

本次课程内容

- *What Is Blockchain ?*
- *Blockchain History.*
- *Why Use Blockchain ?*
- *How Blockchain Work ?*

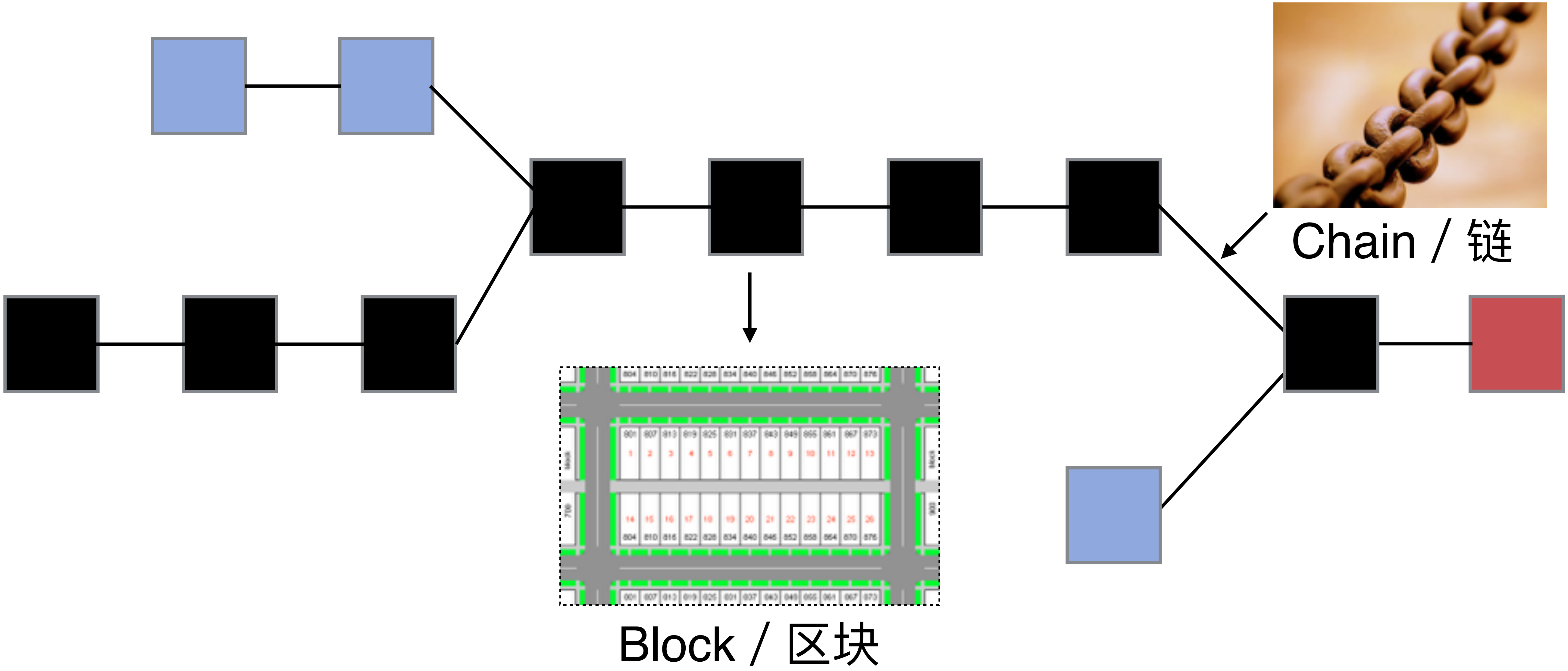
What
Is
Blockchain

What is Blockchain

区块链定义

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

- ***Blockchain:** a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. (originally block chain).*



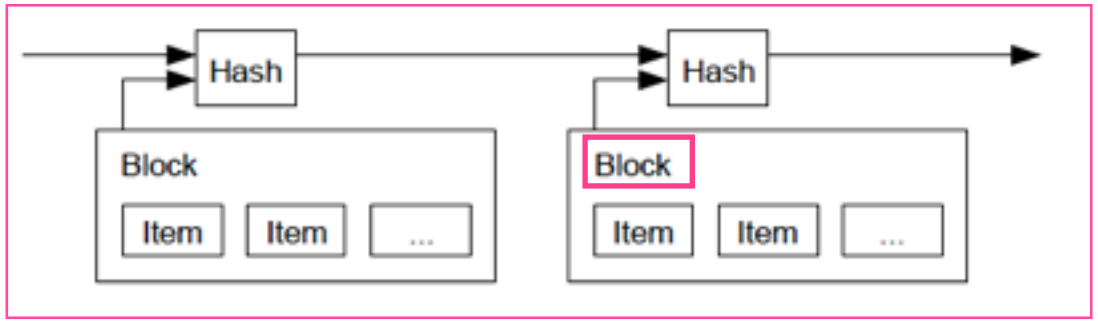
区块链起源

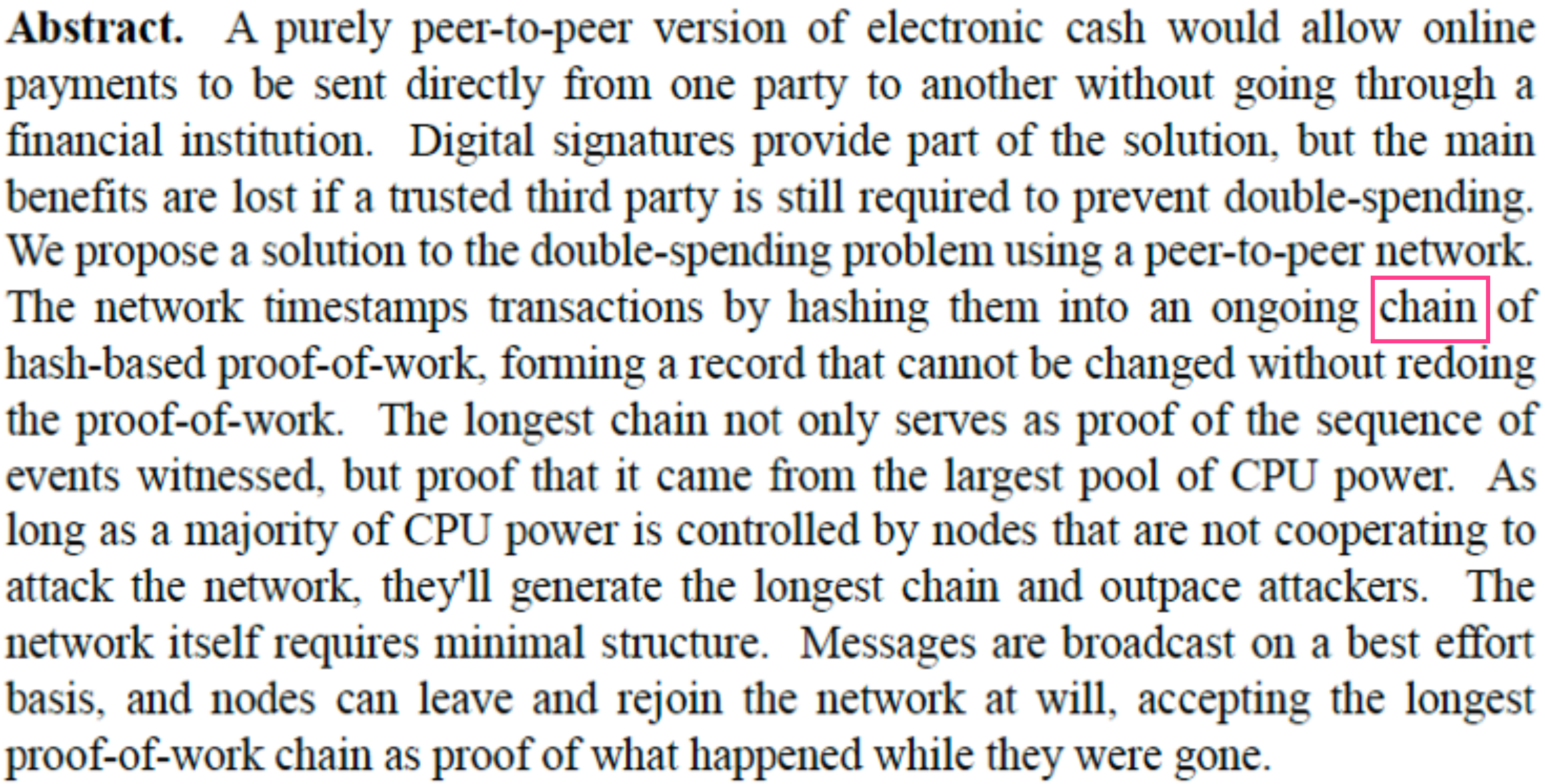
https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

2009

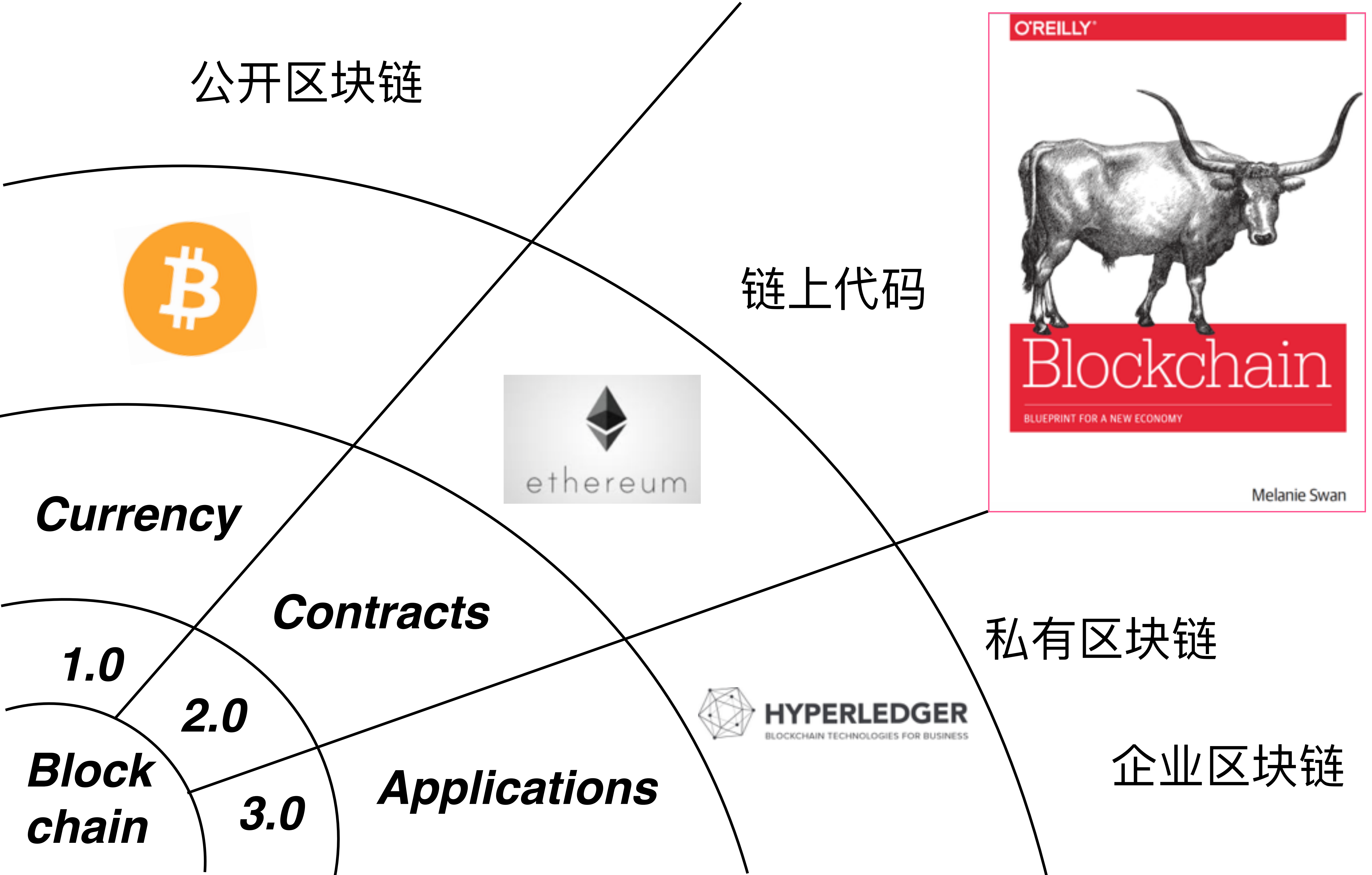
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org




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.

区块链
圣经

区块链发展



公开区块链

链上代码

私有区块链

企业区块链

Block chain

1.0

2.0

3.0

Currency

Contracts

Applications

ethereum
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS
O'REILLY
Blockchain
BLUEPRINT FOR A NEW ECONOMY
Melanie Swan

区块链的另一个定义

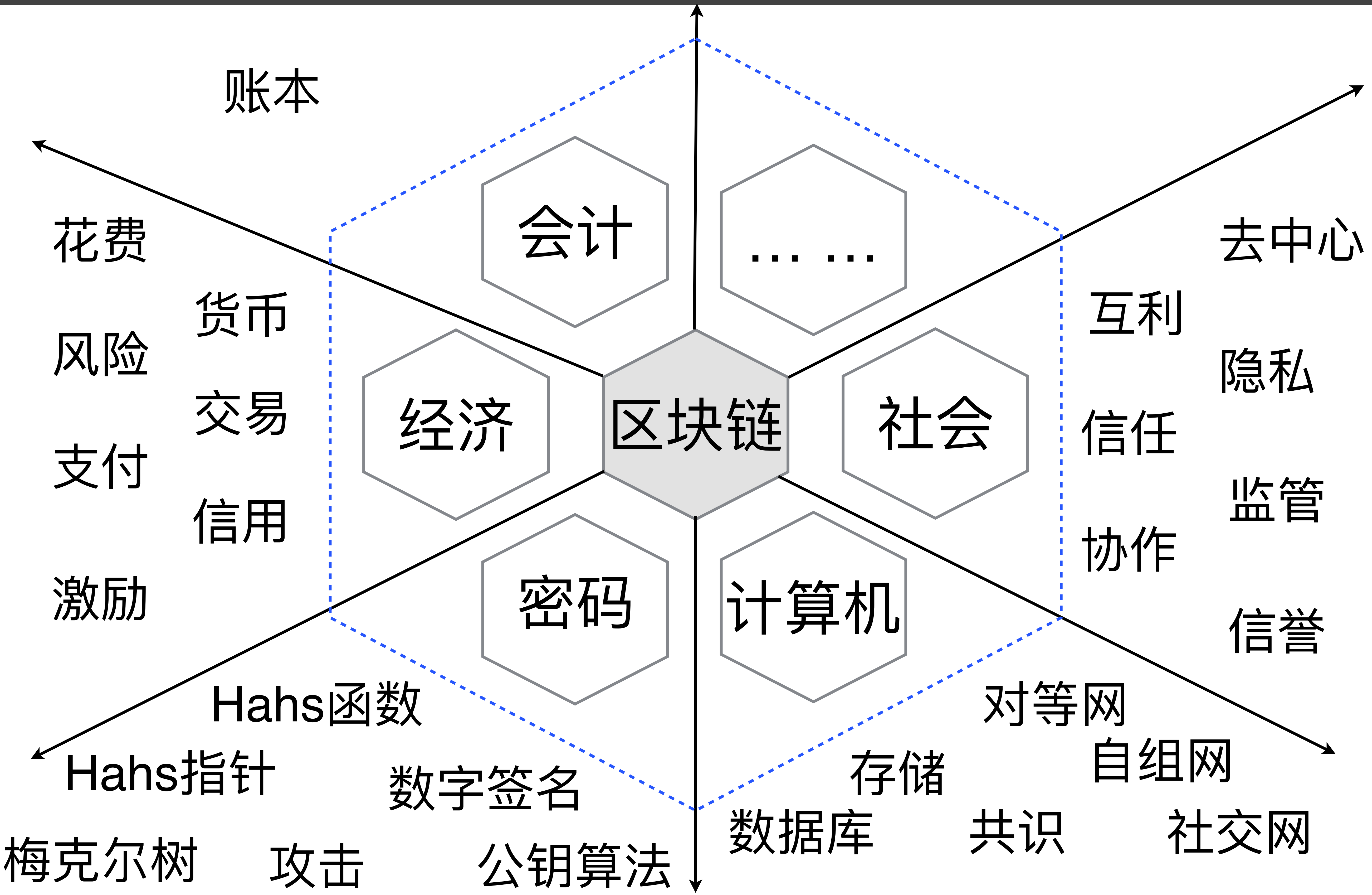
- **Blockchain** is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network.

- An asset can be tangible a house, a car, cash, land, or intangible like intellectual property, such as patents, copyrights, or branding.

- Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

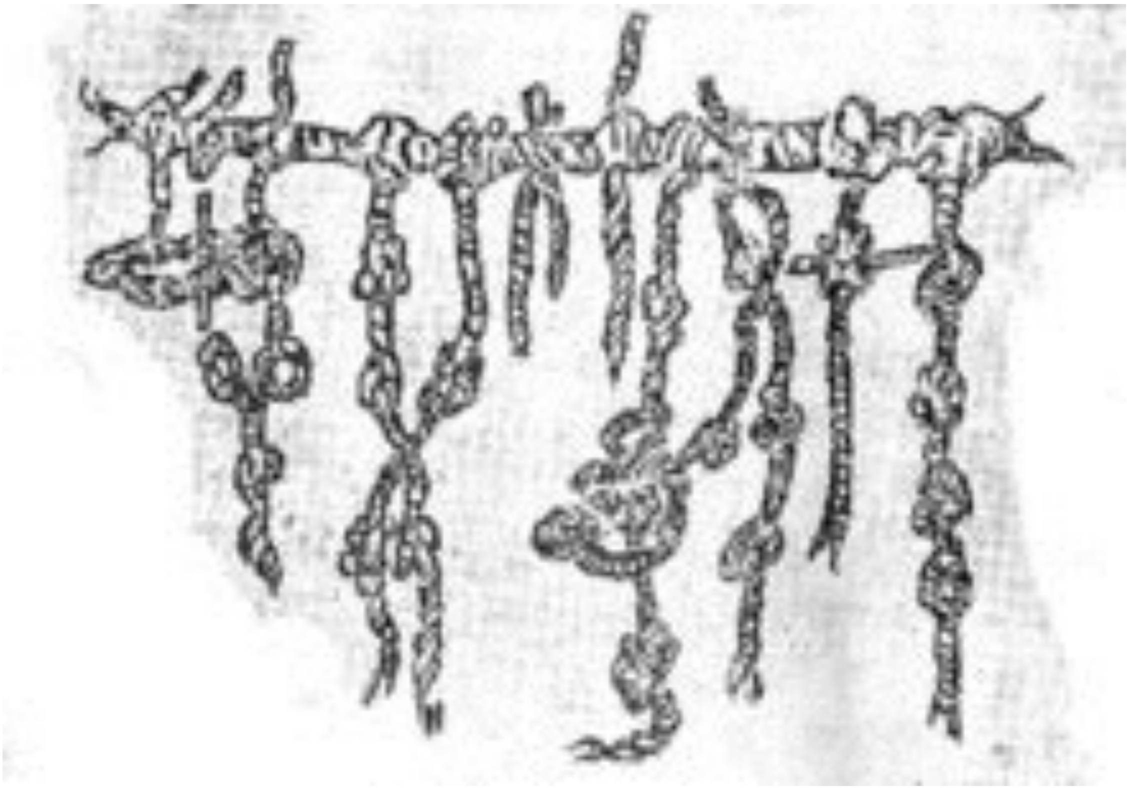
What is Blockchain

区块链涉及概念



Blockchain History

记账的历史

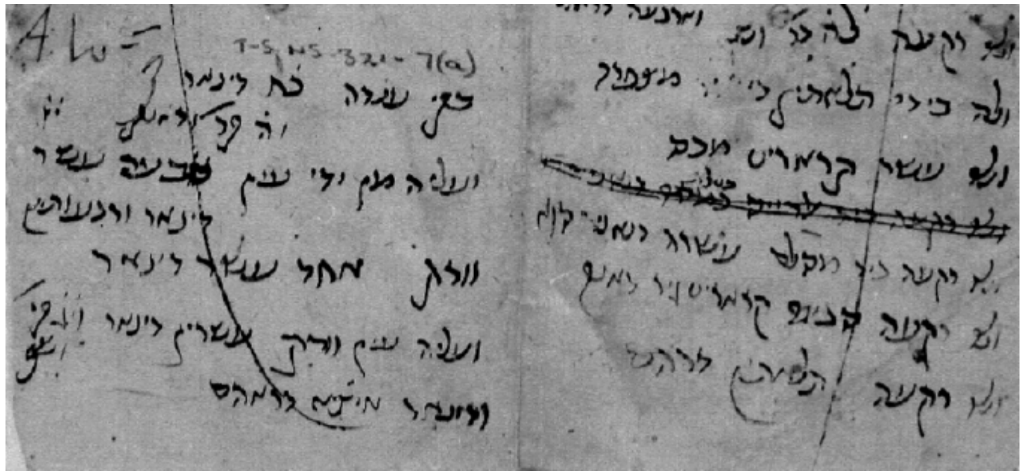


结绳纪事，中国

公元前3300，伊朗出土，
表示7罐油

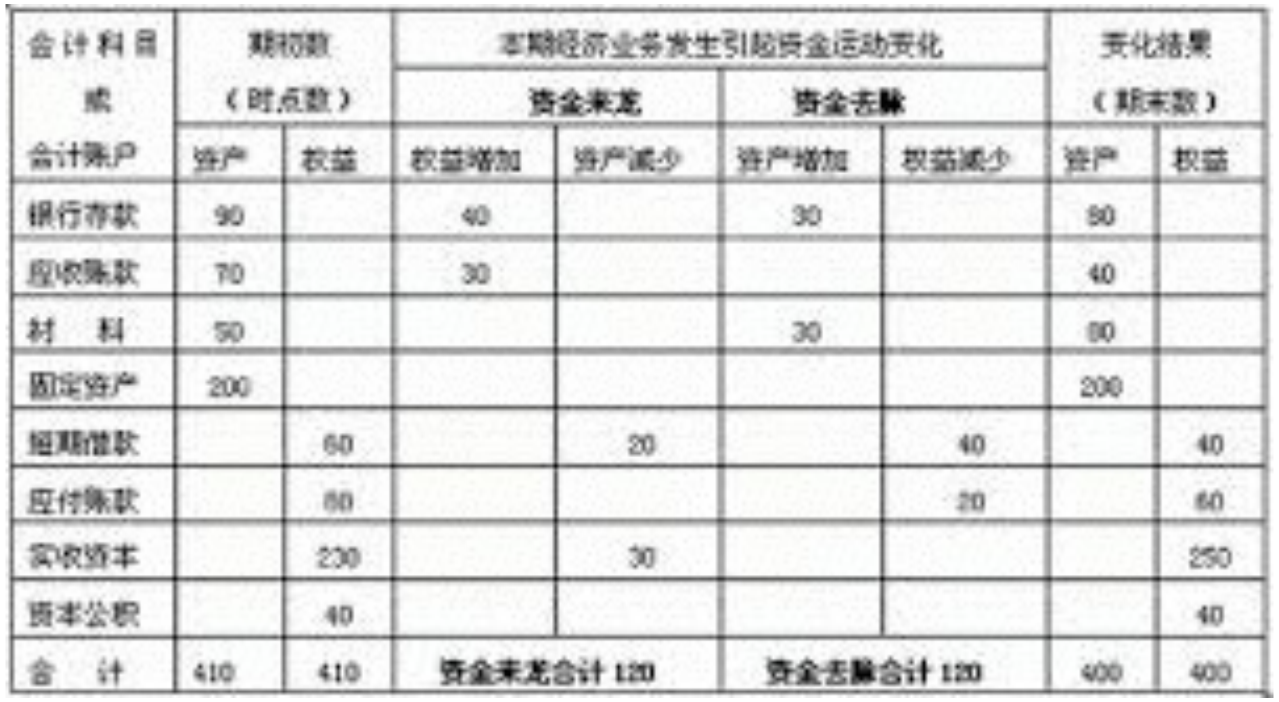
复式记账

- 复式记账法是指对每一笔经济业务都要以相等的金额，同时在两个或两个以上相互联系的账户中进行登记的记账方法。



T-S NS 321.7(a)

收支平衡　责任分离



会计科目 或 会计账户	期初数 （时点数）		本期经济业务发生引起资金运动变化				变化结果 （期末数）	
			资金来龙		资金去脉			
	资产	权益	权益增加	资产减少	资产增加	权益减少	资产	权益
银行存款	90		40		30		80	
应收账款	70		30				40	
材　料	50				30		80	
固定资产	200						200	
短期借款		60		20		40		40
应付账款		80				20		60
实收资本		230		30				250
资本公积		40						40
合　计	410	410	资金来龙合计 120		资金去脉合计 120		400	400

以物易物

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

- ***Bater:** a system of exchange where goods or services are directly exchanged for other goods or services without using medium of exchange.*

- *Double coincidence of wants*
- *No common measure of value*
- *Indivisibility of certain goods*
- *Lack of standards for delay payments*
- *Difficulty in storing wealth*

货币

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

- ***Money**: any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a particular country or socio-economic context.*

- *A medium of change*
- *A unit of account*
- *A Store of Value*
- *A standard of deferred payment*

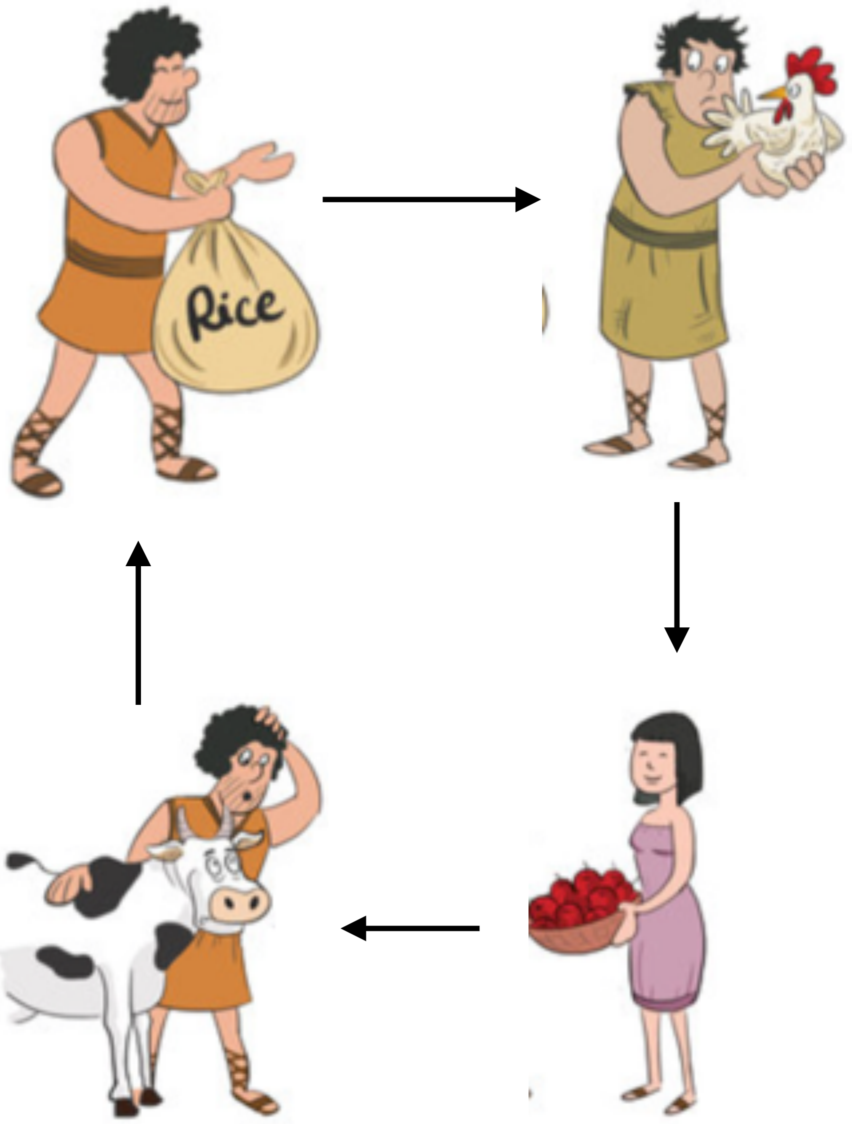
- *Fungibility*
- *Durability*
- *Portability*
- *Stability (Limited in supple)*
- *Divisible*
- *Acceptable*
- *Uniform*

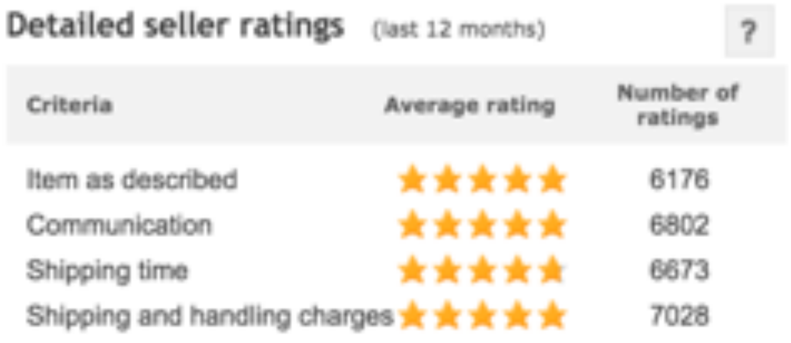
- *Commodity money*
- *Representation money*
- *Fiat money*

信用

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

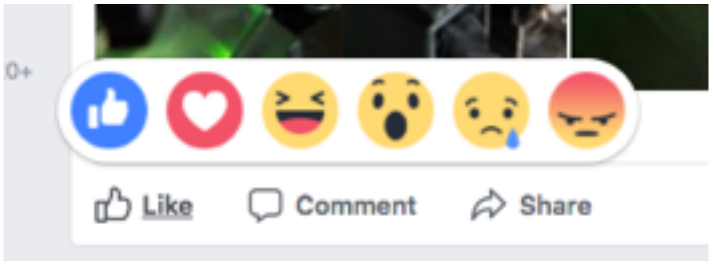
- ***Credit:*** *the trust which allows one party to provide money or resources to another party where that second party does not reimburse the first party immediately but instead promise either to repay or return those resources at a later date.*

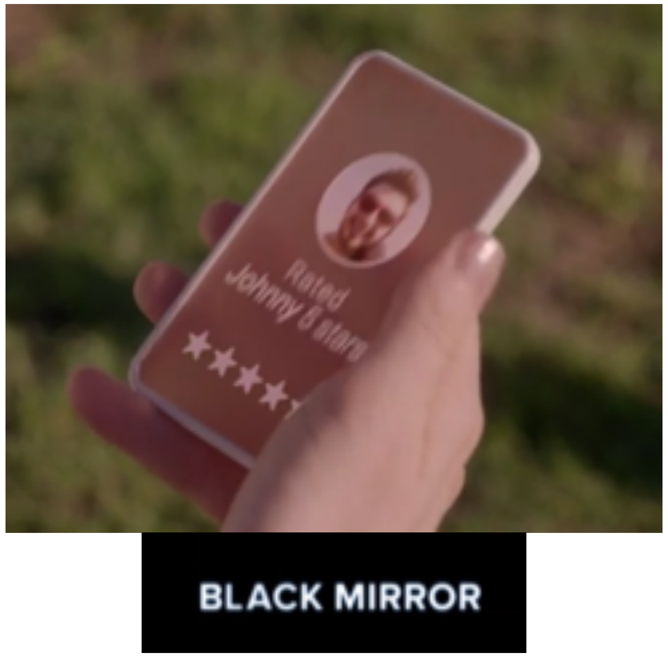




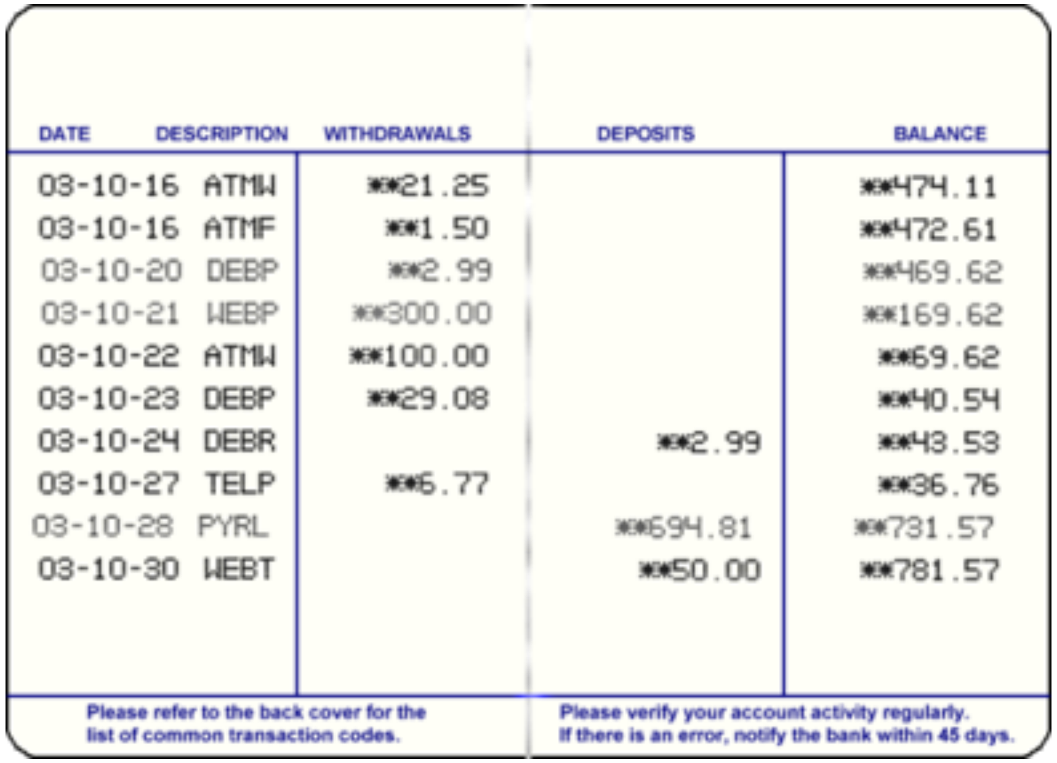
Detailed seller ratings (last 12 months) ?

Criteria	Average rating	Number of ratings
Item as described	★★★★★	6176
Communication	★★★★★	6802
Shipping time	★★★★★	6673
Shipping and handling charges	★★★★★	7028





银行

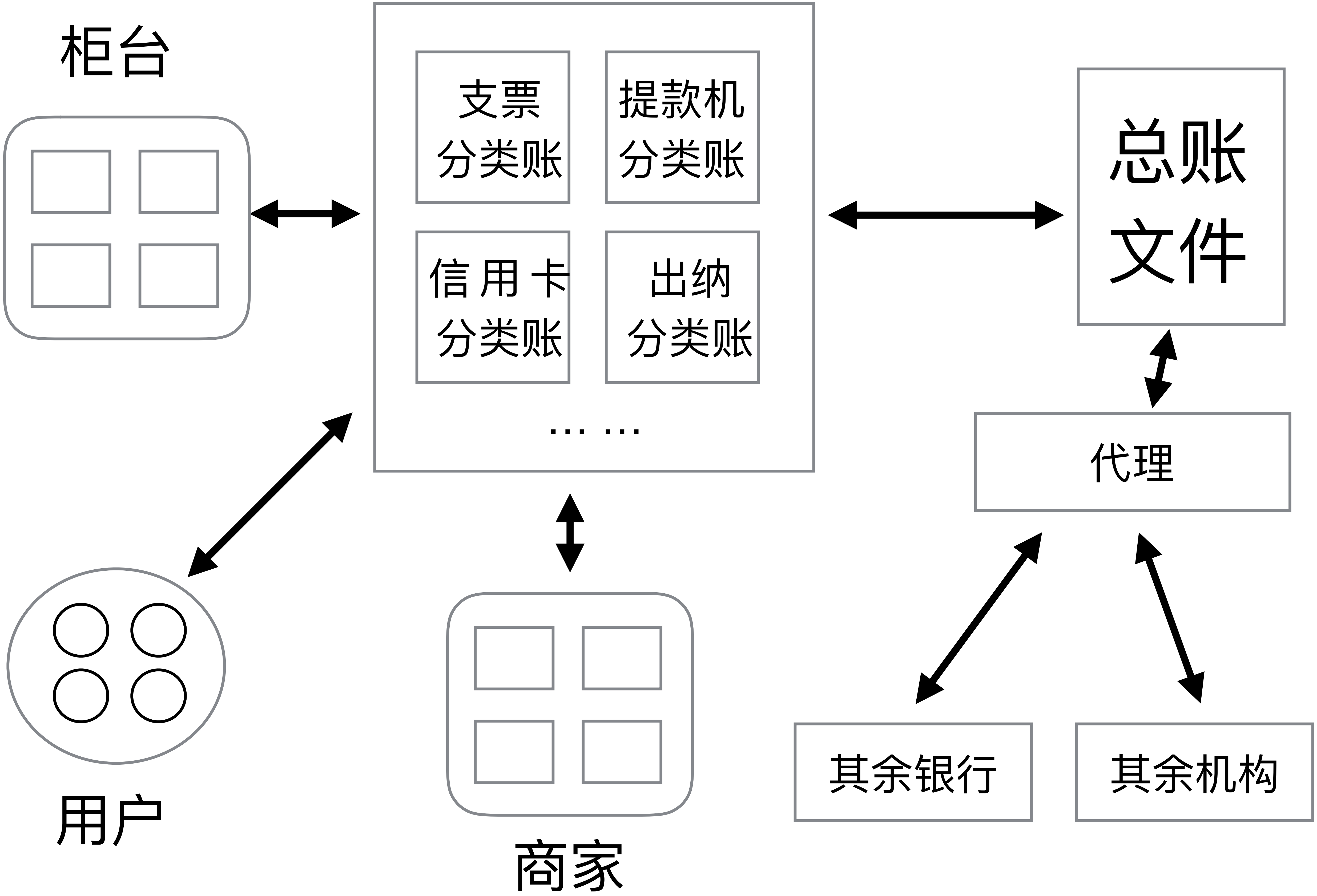


DATE	DESCRIPTION	WITHDRAWALS	DEPOSITS	BALANCE
03-10-16	ATMW	**21.25		**474.11
03-10-16	ATMF	**1.50		**472.61
03-10-20	DEBP	**2.99		**469.62
03-10-21	WEBP	**300.00		**169.62
03-10-22	ATMW	**100.00		**69.62
03-10-23	DEBP	**29.08		**40.54
03-10-24	DEBR		**2.99	**43.53
03-10-27	TELP	**6.77		**36.76
03-10-28	PYRL		**694.81	**731.57
03-10-30	WEBT		**50.00	**781.57

Please refer to the back cover for the list of common transaction codes.

Please verify your account activity regularly. If there is an error, notify the bank within 45 days.

银行记账



柜台

支票
分类账

提款机
分类账

信用卡
分类账

出纳
分类账

…… ……

总账
文件

代理

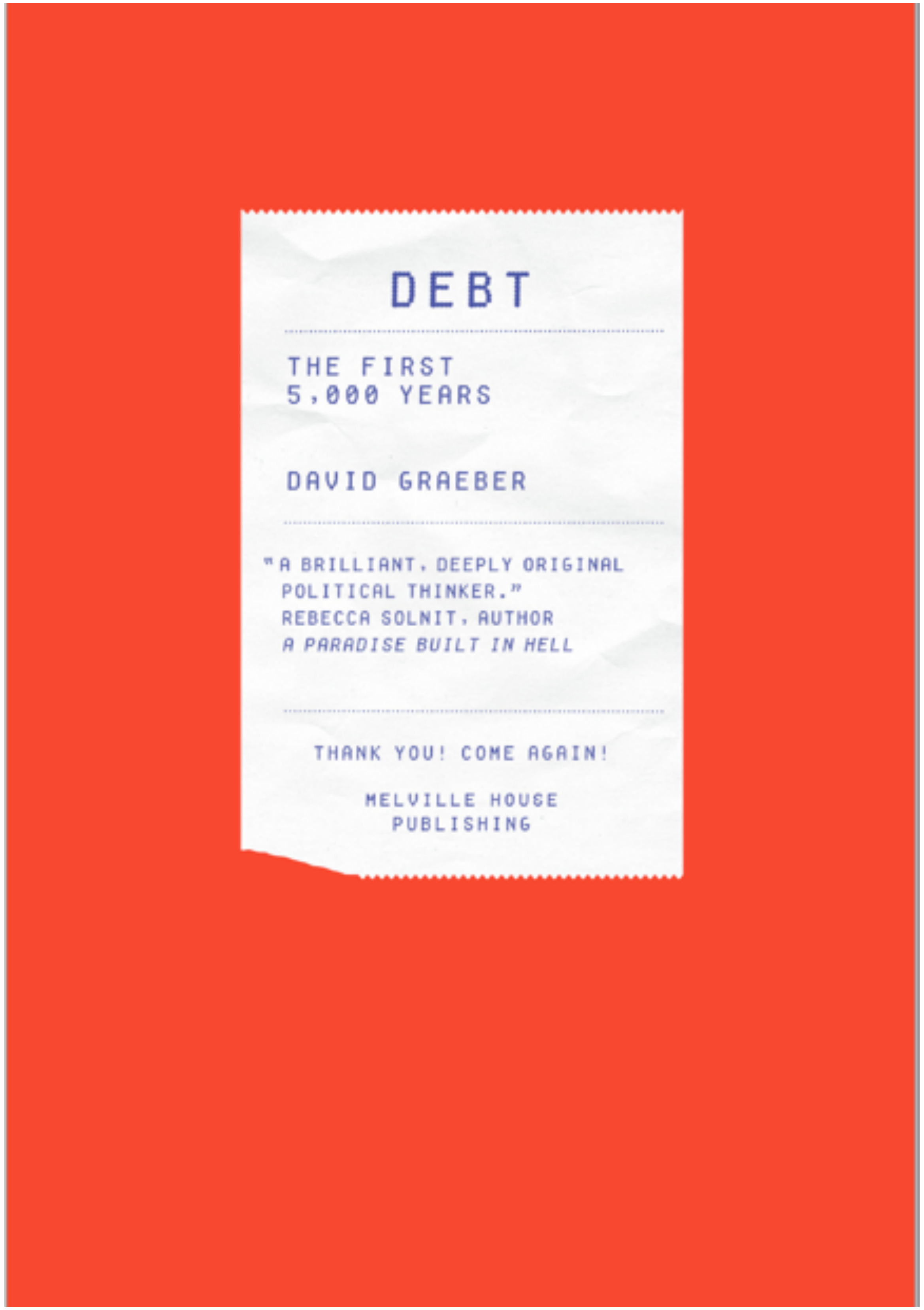
用户

商家

其余银行

其余机构

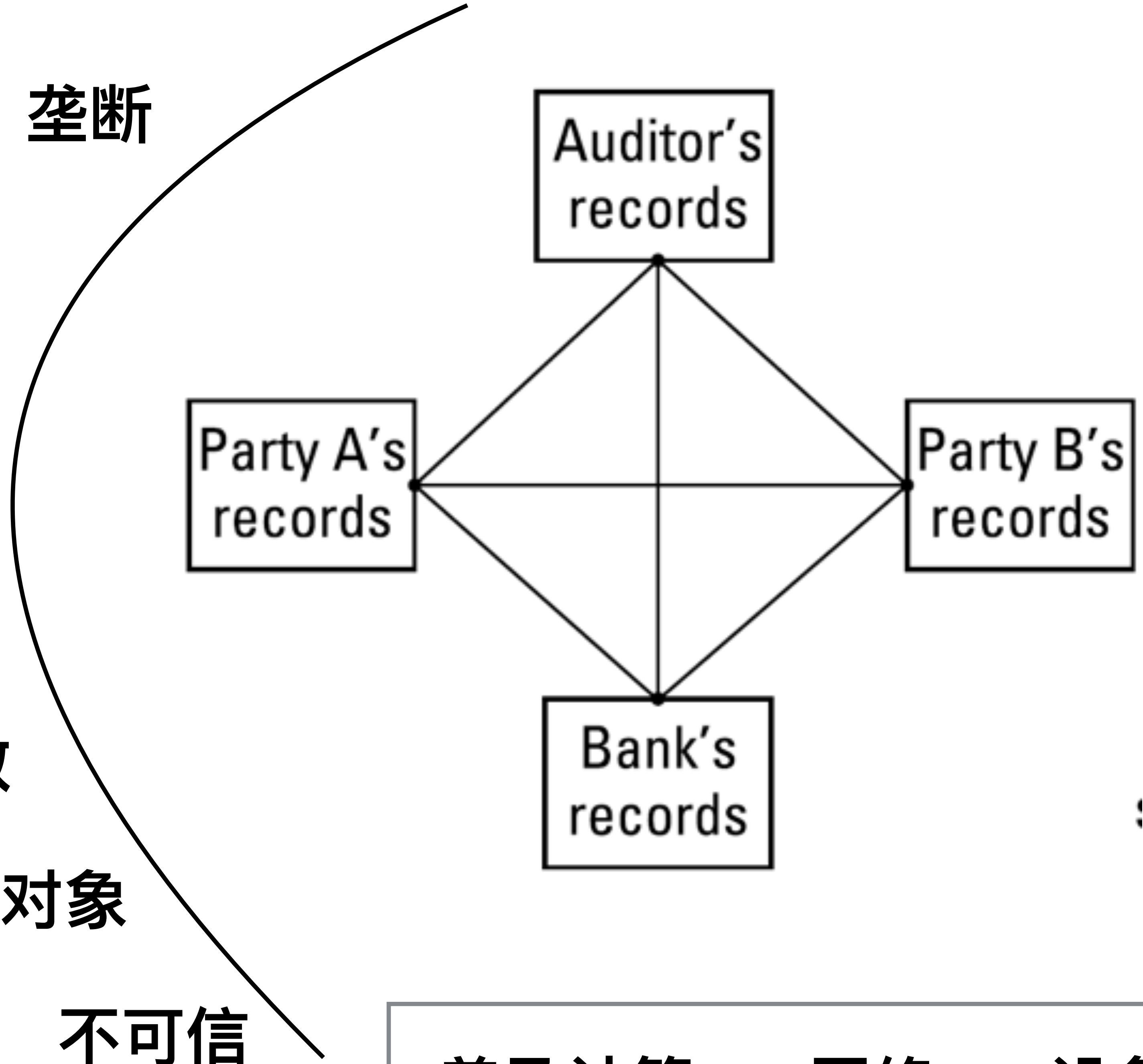
推荐一本书


DEBT
THE FIRST 5,000 YEARS
DAVID GRAEBER
"A BRILLIANT, DEEPLY ORIGINAL POLITICAL THINKER."
REBECCA SOLNIT, AUTHOR
A PARADISE BUILT IN HELL
THANK YOU! COME AGAIN!
MELVILLE HOUSE PUBLISHING

Why Use Blockchain

区块链之前的商业网络

- 需要第三方参与
  - ✳ 花费
- 执行延迟
  - ✳ 低效
- 中心机构
  - ✳ 脆弱



垄断

单点失败

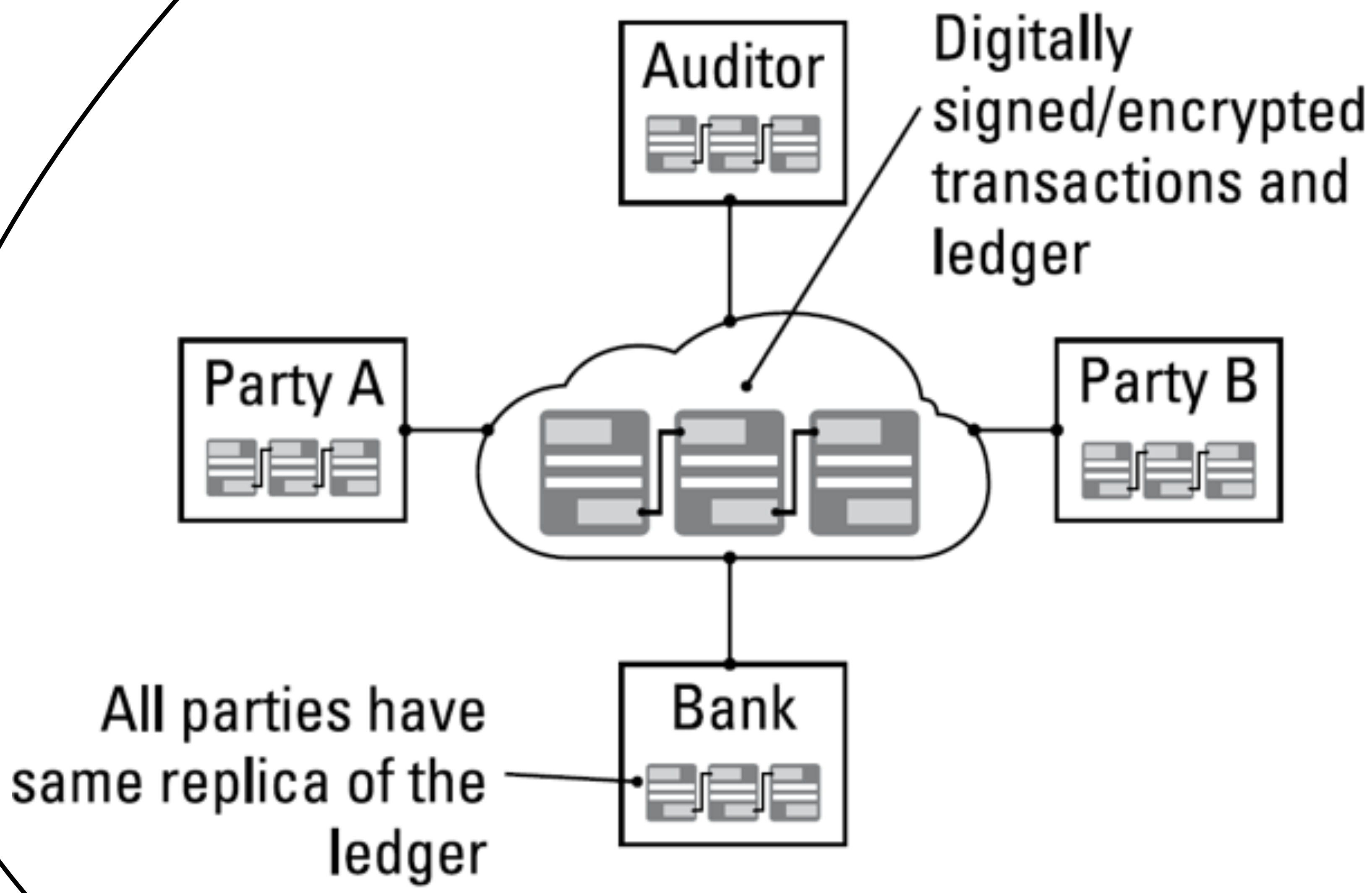
攻击对象

不可信

普及计算　网络　设备

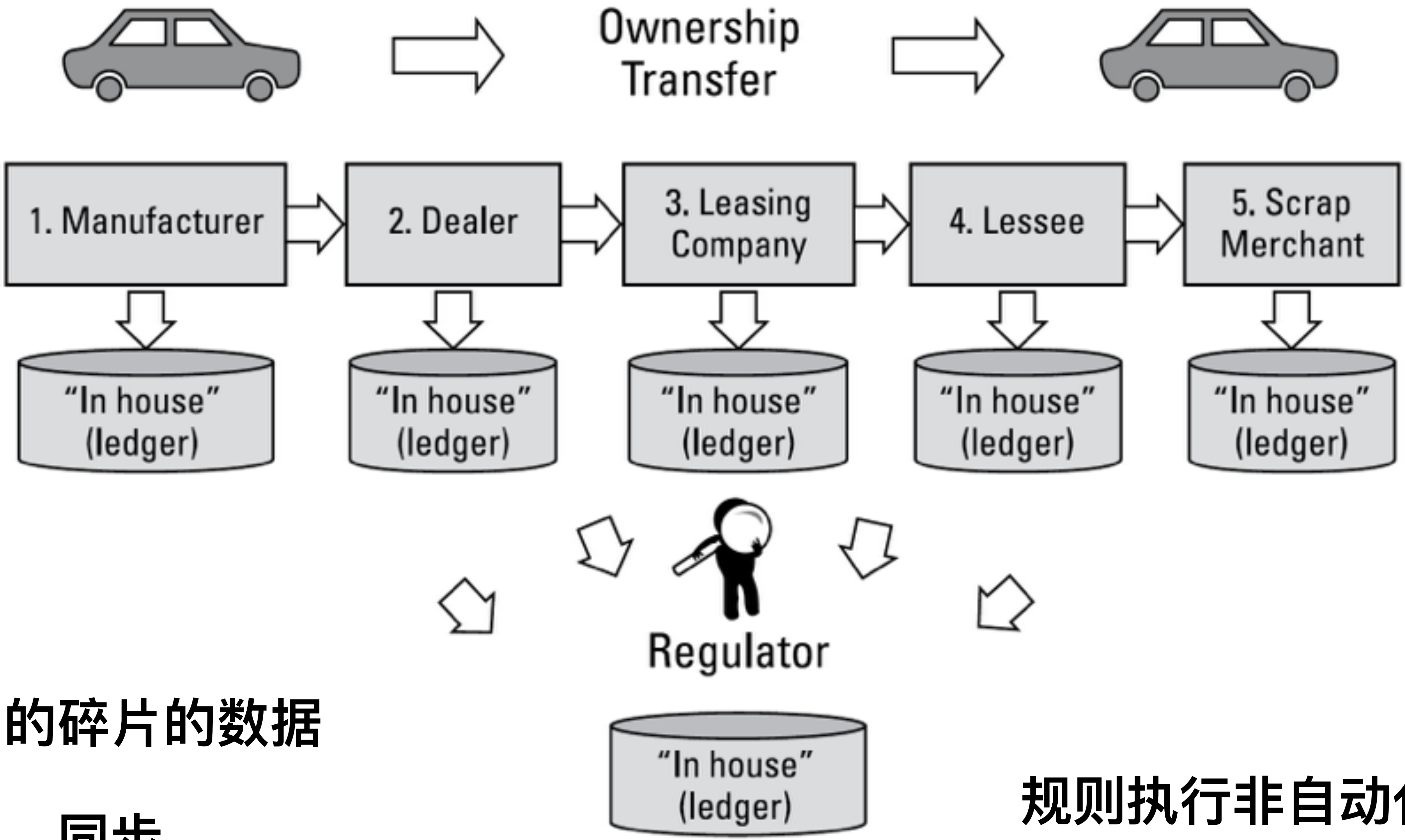
区块链之后的商业网络

- 无第三方
  - ✳ 经济
- 共识
  - ✳ 高效
- 无中心
  - ✳ 安全


Auditor
Digitally signed/encrypted transactions and ledger
Party A
Party B
All parties have same replica of the ledger
Bank

记录不可更改　　对等网络

没有使用区块链的租车应用



分割的碎片的数据

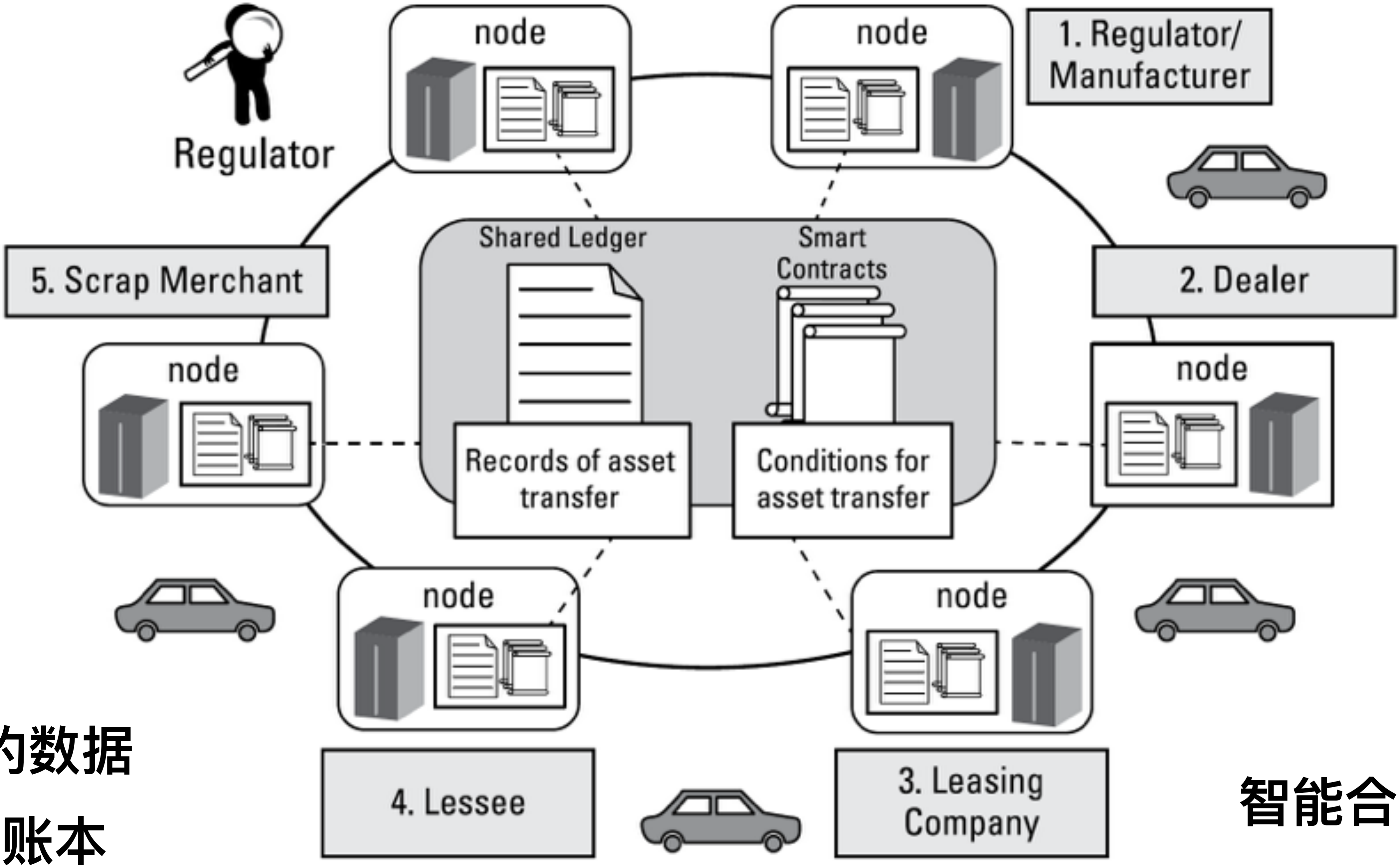
同步

时间 / 一致性

规则执行非自动化

Why use Blockchain

使用区块链的租车应用



一致的数据

共享账本

智能合约

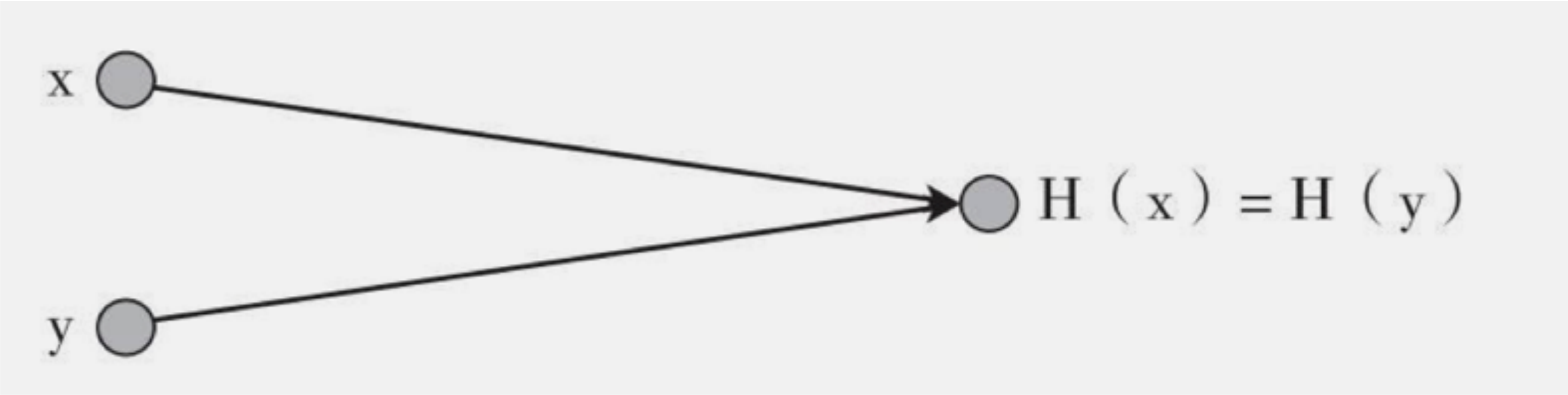
How Blockchain Work

Hash函数

- 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：$O(n)$

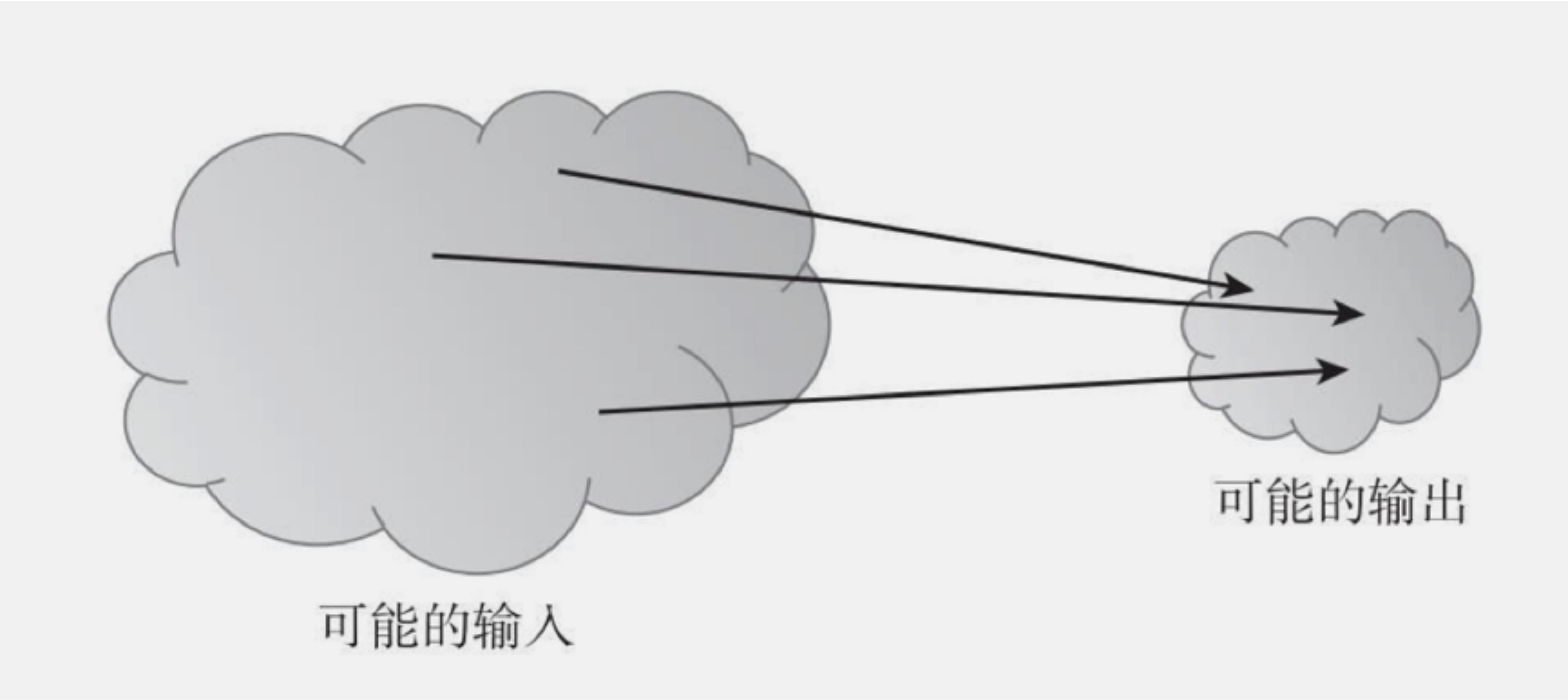
- 抗碰撞
- 隐匿性
- 难题友好

抗碰撞



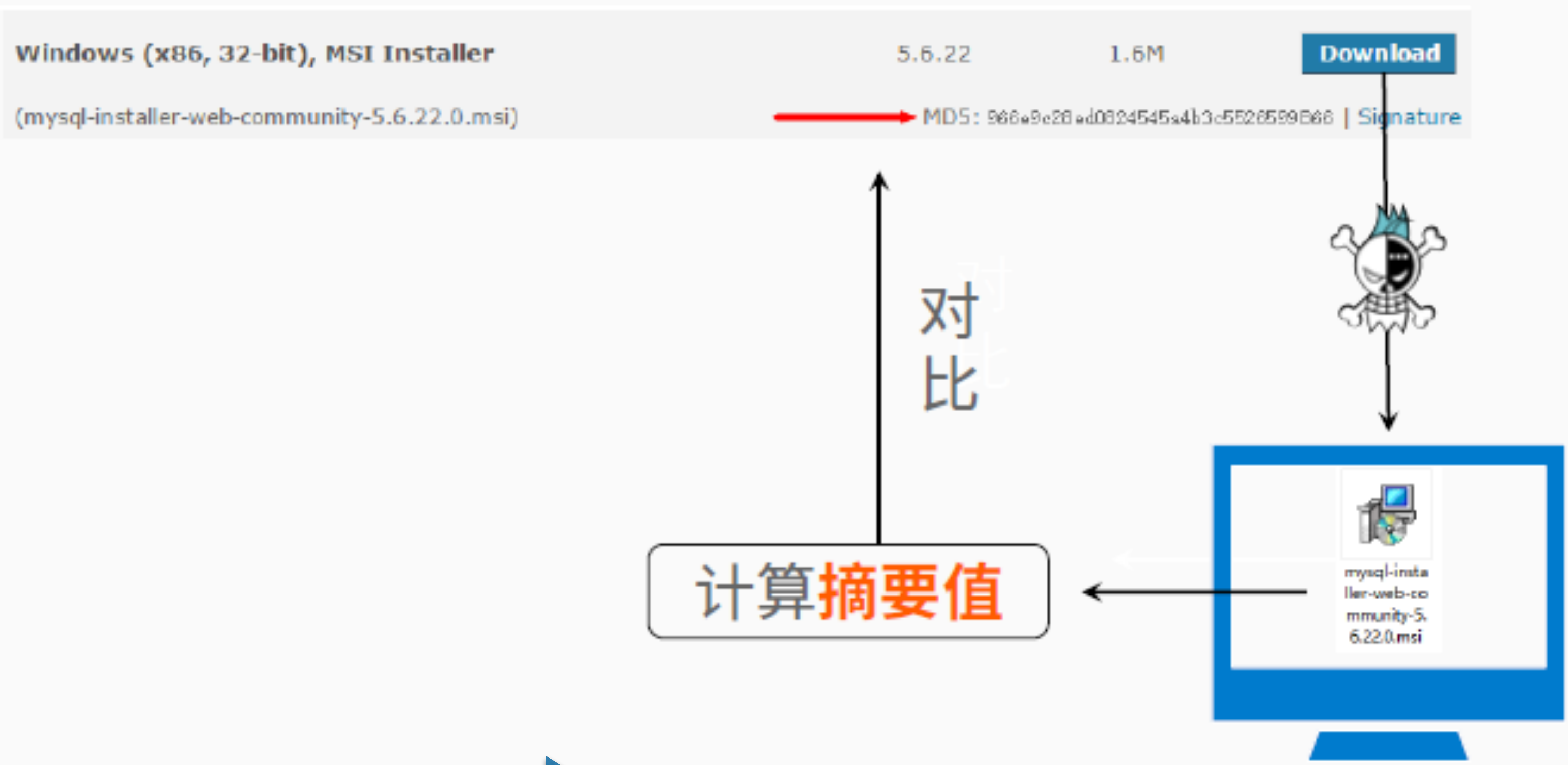
2^{130}

99.8%



应用：Hash作为消息摘要

hash足够小



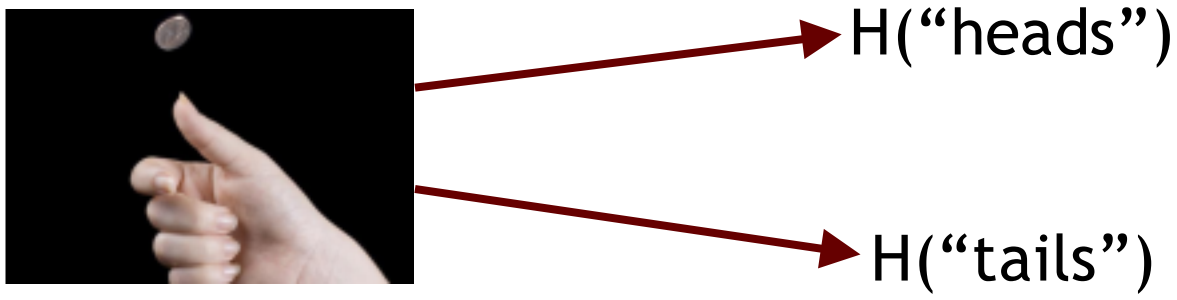
Windows (x86, 32-bit), MSI Installer 5.6.22 1.6M Download

(mysql-installer-web-community-5.6.22.0.msi) MD5: 966a9e28ad0824545a4b3c5526599866 | Signature

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

隐匿性

- 给出*H*(*x*)，不能找到*x*



H(“heads”)

H(“tails”)

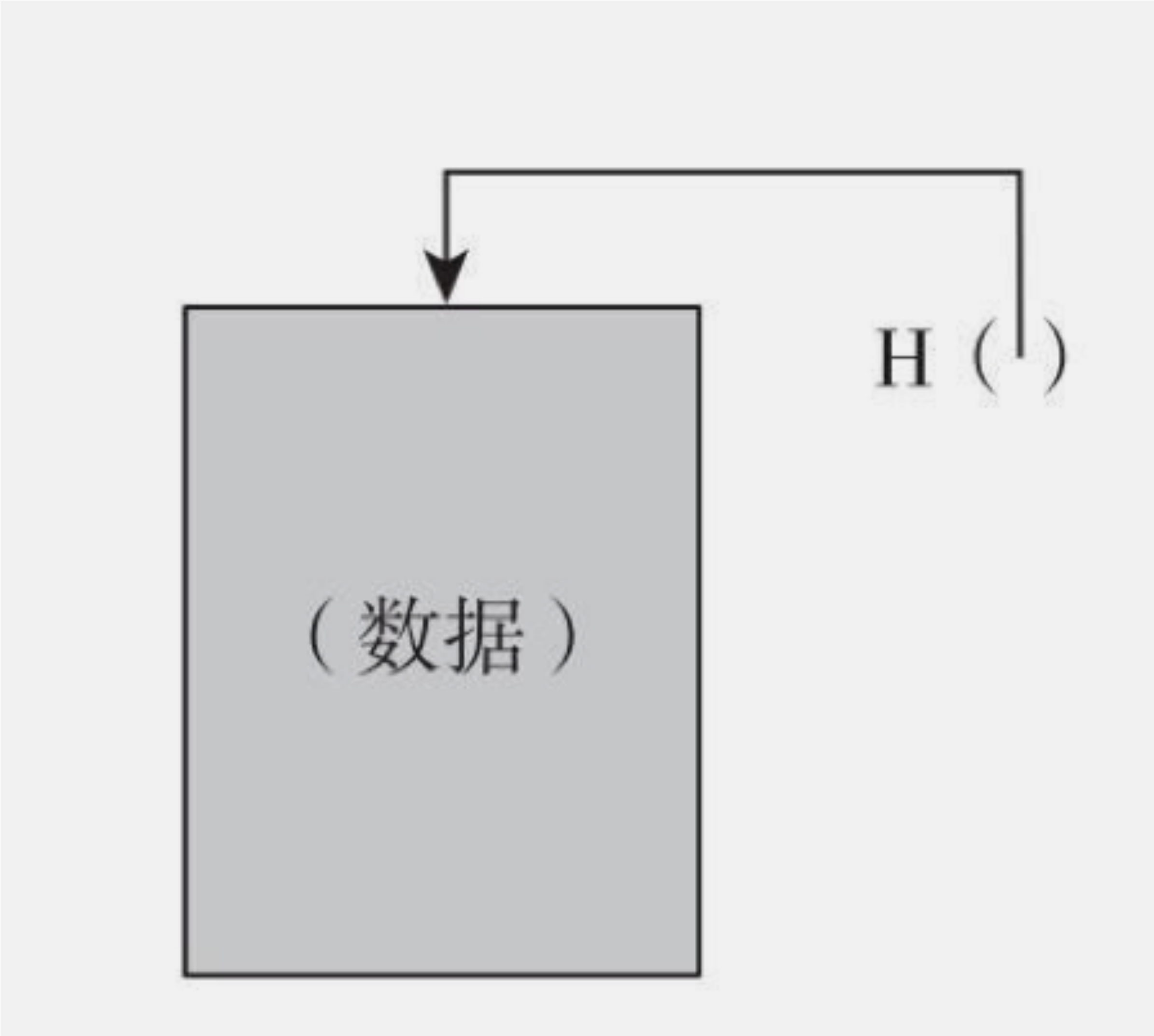
- 如果概率分布有高的最小熵，非常分散，则具有隐匿性

Hash指针

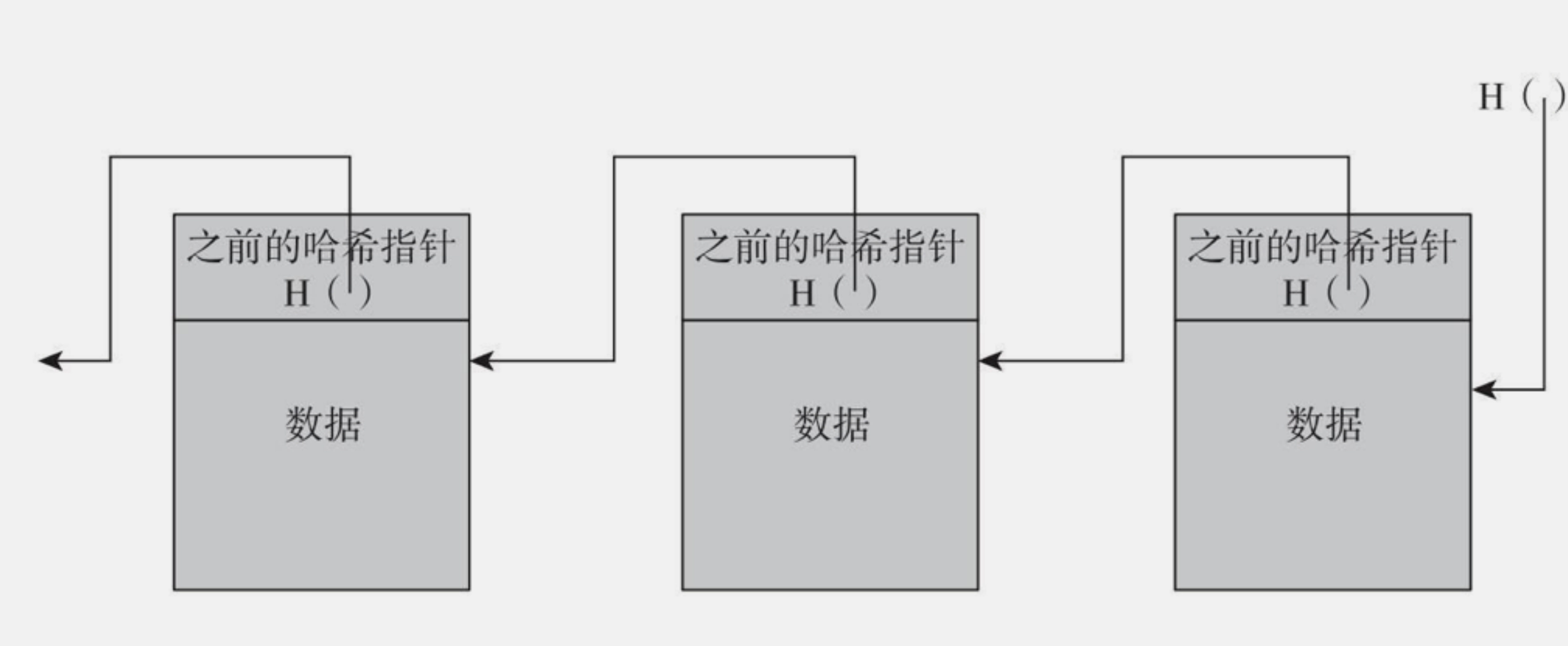
- *Hash*指针是一个指向存储数据及其数据*Hash*的指针

- 取回数据
- 验证数据是否改变

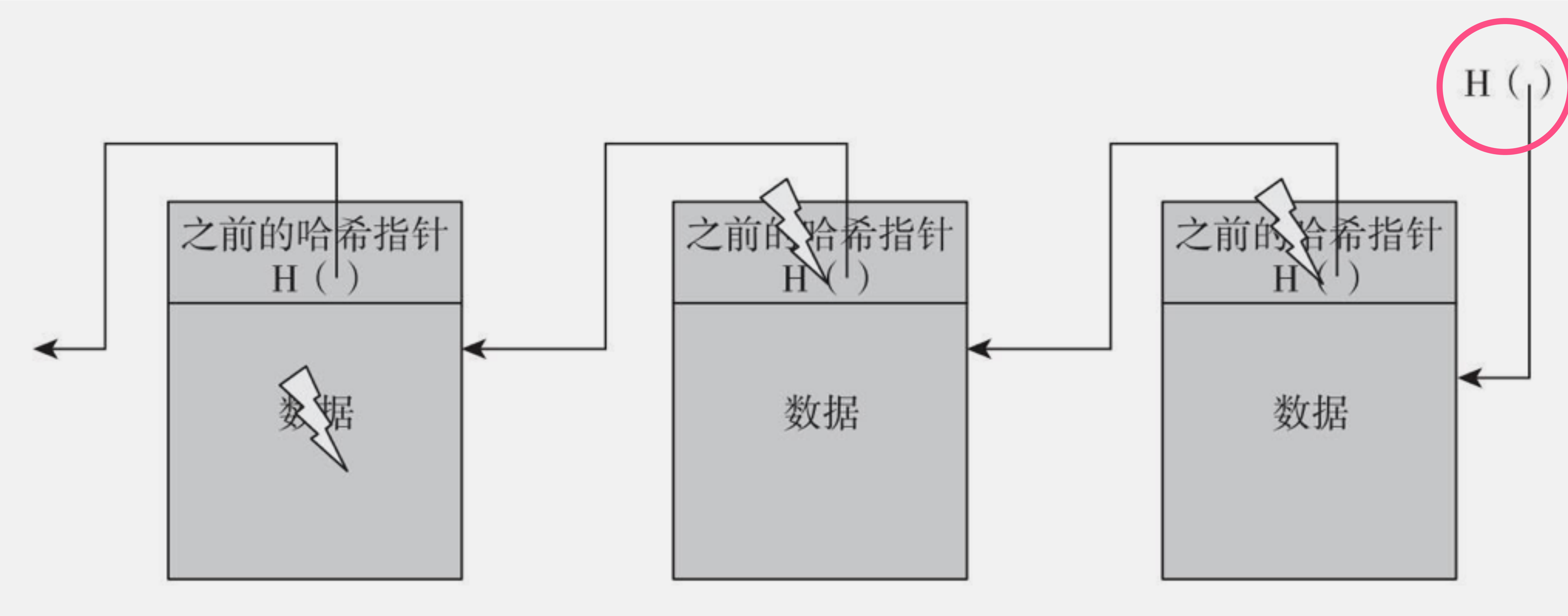
- 区块链的关键思想



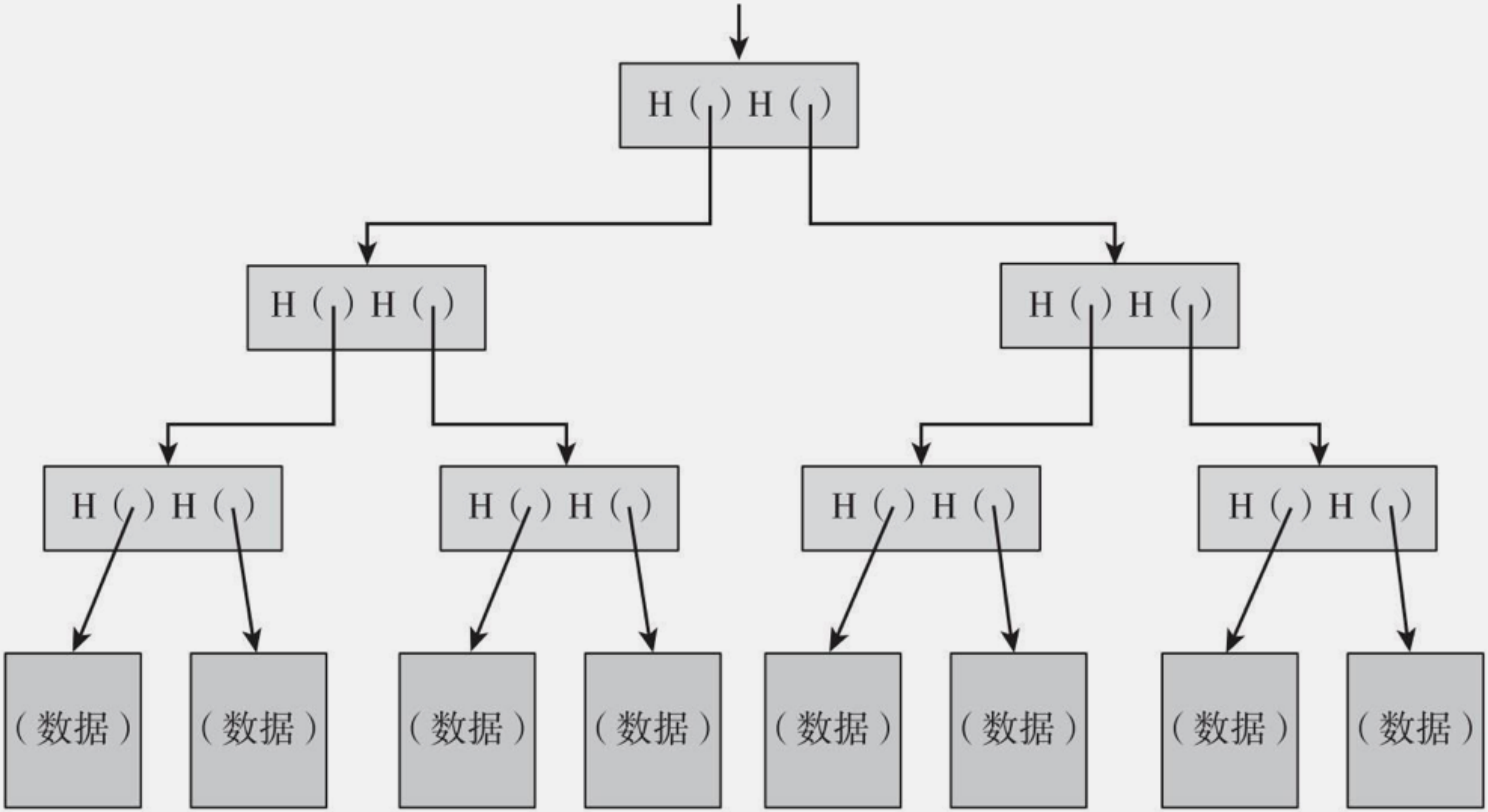
区块链



防止篡改



梅克尔树

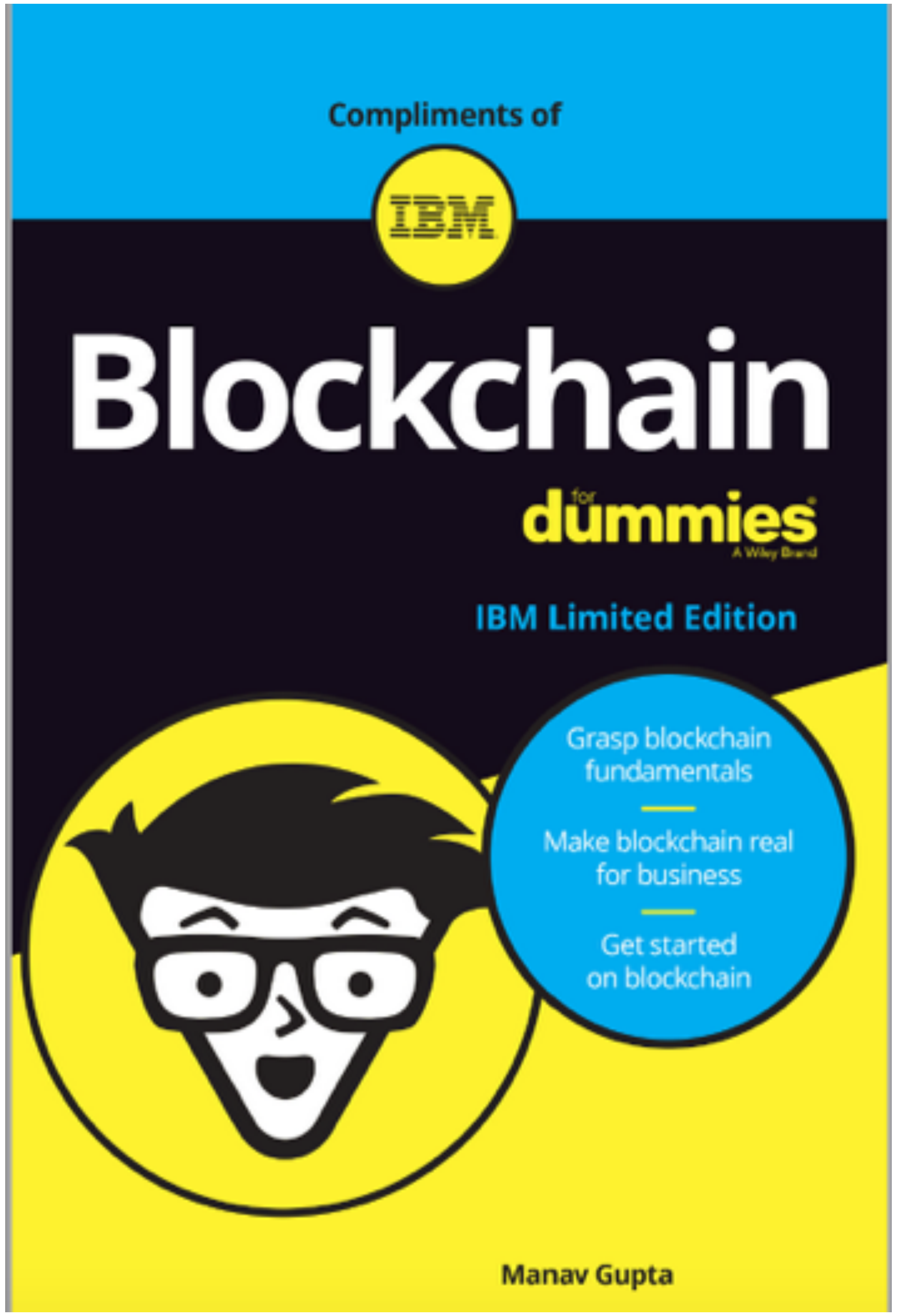


提问时间！

Home work

Homework

课后作业


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES
A Comprehensive Introduction
区块链
技术驱动金融
数字货币与智能合约技术
解密区块链，用技术重构金融世界

序言、第1章

Homework

课后作业

- 要求阅读如下论文，写论文阅读报告：

➡ *In IEEE Computer Maganize 2017.*

COVER FEATURE **BLOCKCHAIN TECHNOLOGY IN FINANCE**

Blockchain Technologies: The Foreseeable Impact on Society and Industry

谢谢！

孙惠平

sunhp@ss.pku.edu.cn