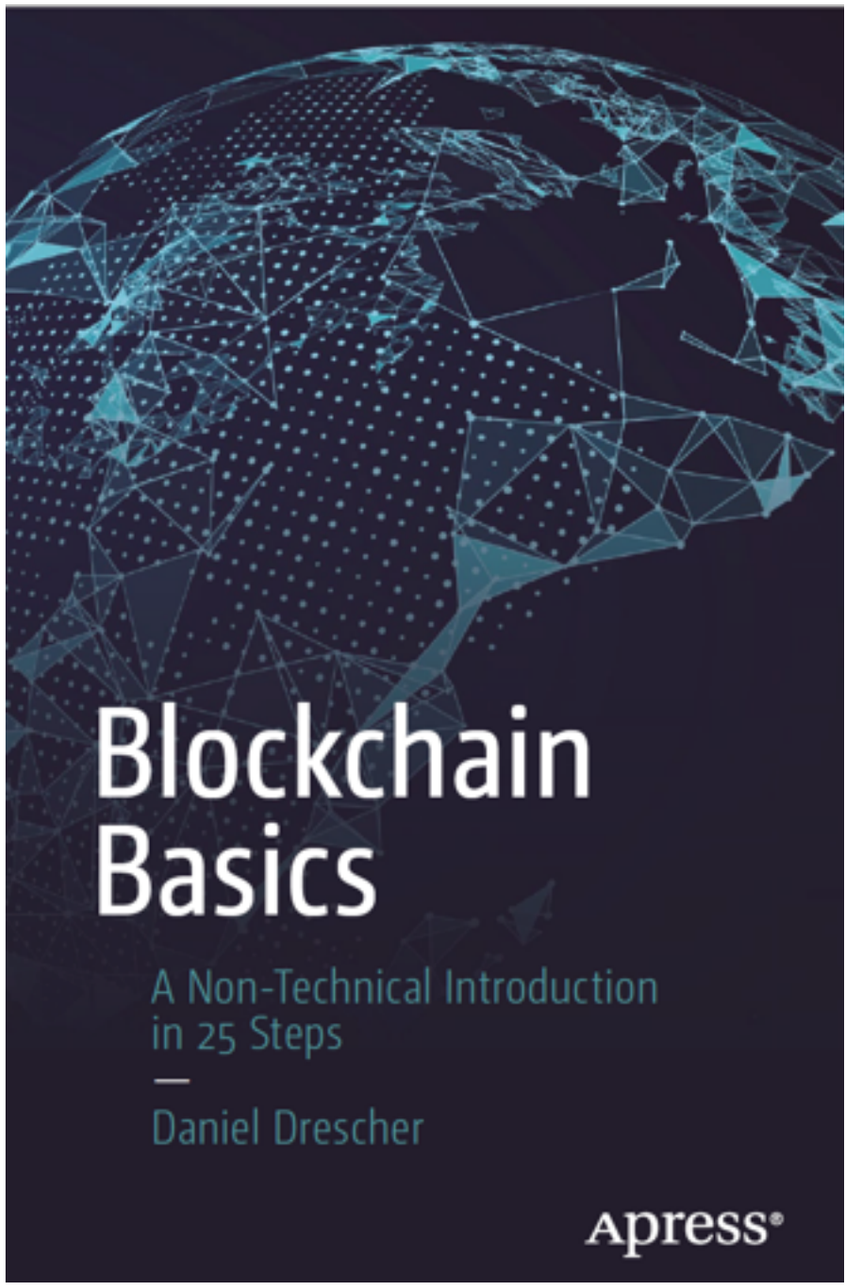
区块链

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

参考书 - 傻瓜书

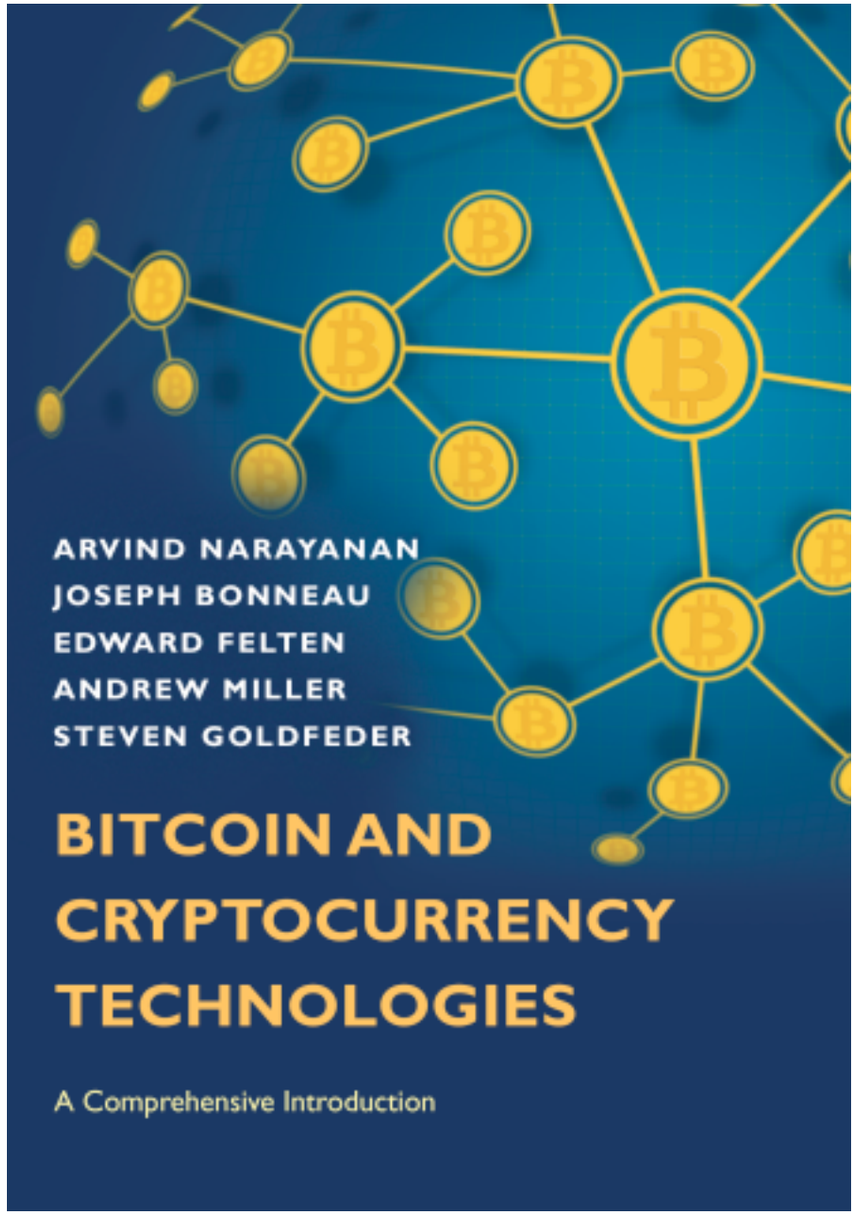

Blockchain
Basics
A Non-Technical Introduction
in 25 Steps
—
Daniel Drescher
Apress®


Apress®
区块链
基础知识 25 讲
Blockchain
Basics
A Non-Technical Introduction
in 25 Steps
—
[美] 丹尼尔 · 德雷舍 (Daniel Drescher) 著
马丹 王铁柔 张初阳 译
中国工信出版集团
人民邮电出版社

参考书 - 比特币

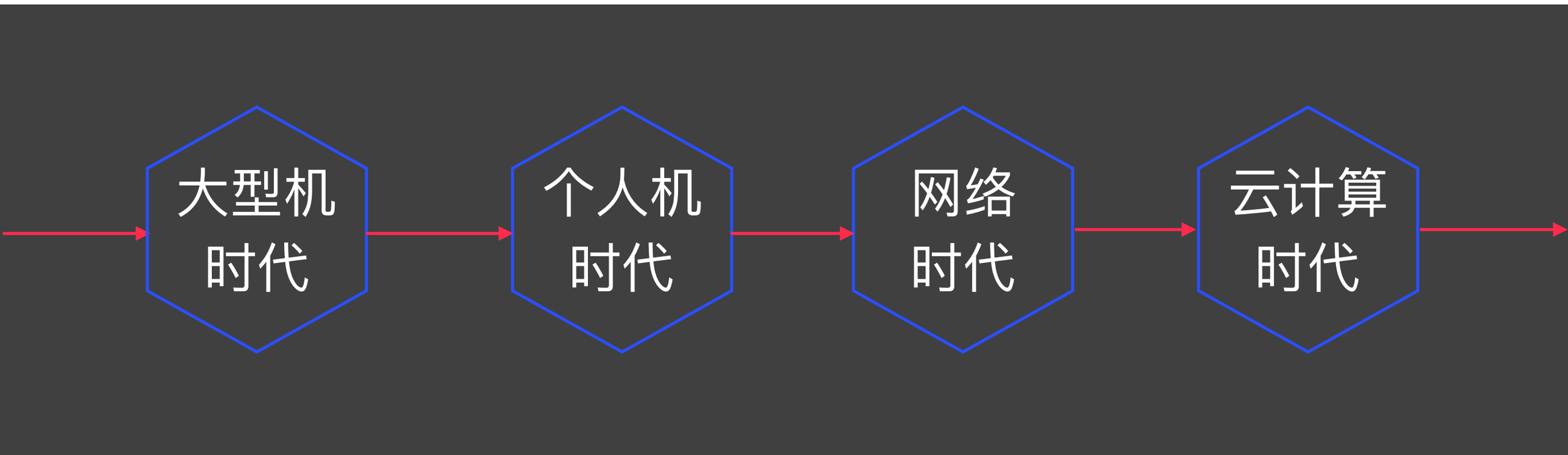

O'REILLY
第2版
Mastering
Bitcoin
精通比特币（影印版）
Andreas M. Antonopoulos 著
东南大学出版社
REILLY
原书第2版
精通区块链编程
加密货币原理、方法和应用开发
Mastering Bitcoin: Programming the Open Blockchain
[希] Andreas M. Antonopoulos 著
郭理靖 李国鹏 李卓 译
乔延宏 邵周 Higer 审校
机械工业出版社
China Machine Press

参考书 - 教材


ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER
BITCOIN AND
CRYPTOCURRENCY
TECHNOLOGIES
A Comprehensive Introduction

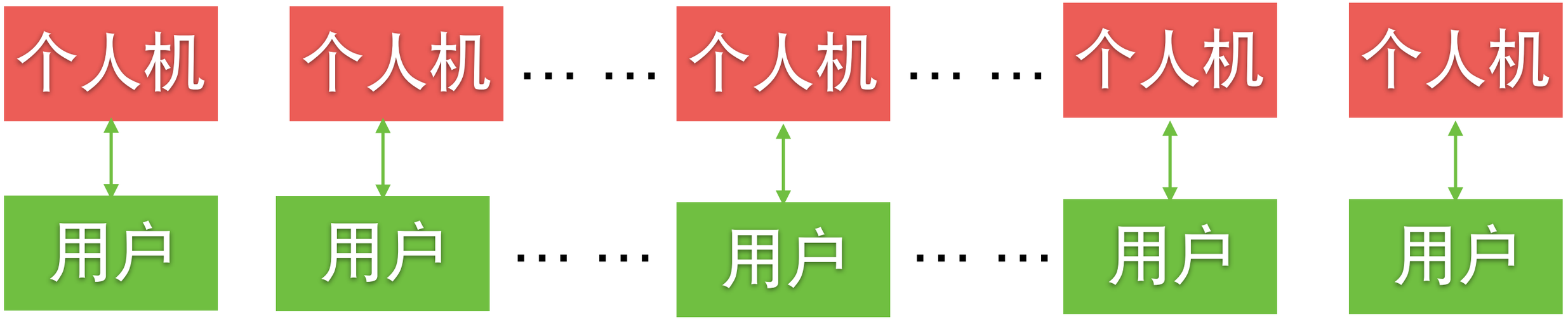

区块链
技术驱动金融
数字货币与智能合约技术
解密区块链，用技术重构金融世界
BITCOIN
AND
CRYPTOCURRENCY
TECHNOLOGIES

计算机视角

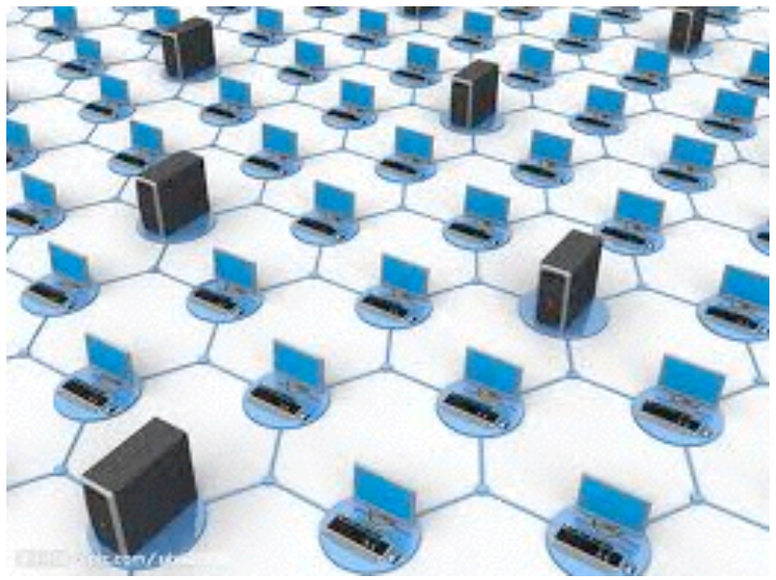


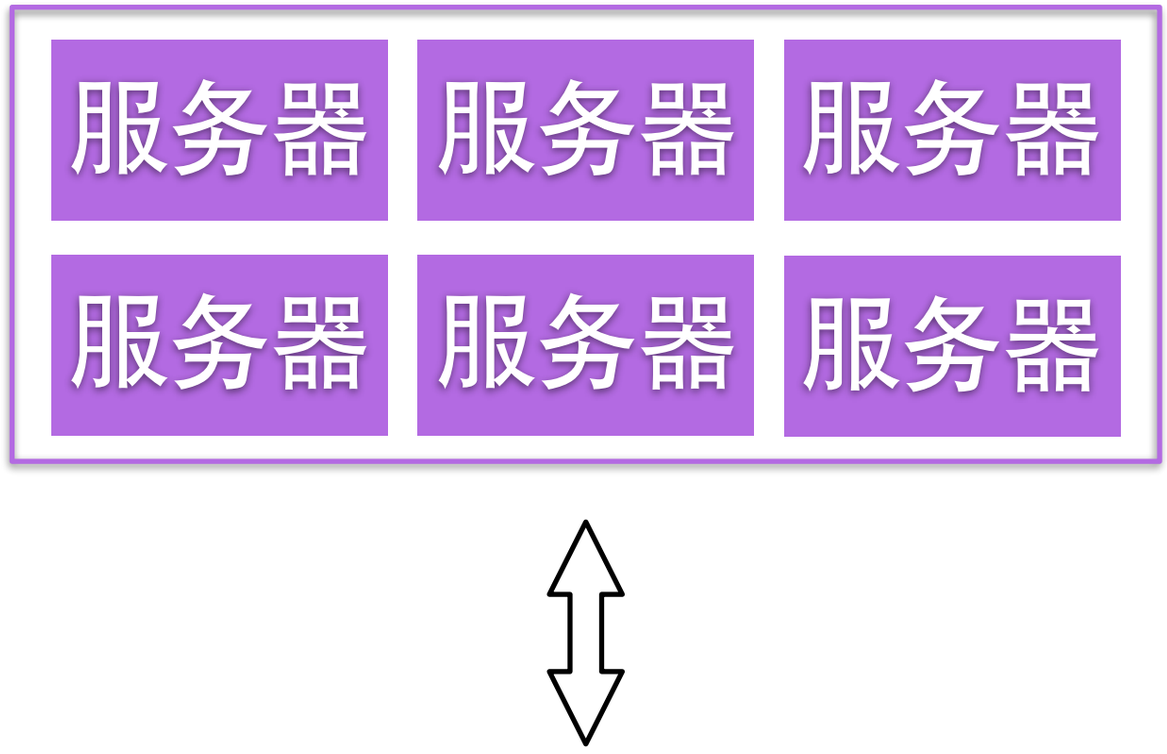
大型机时代

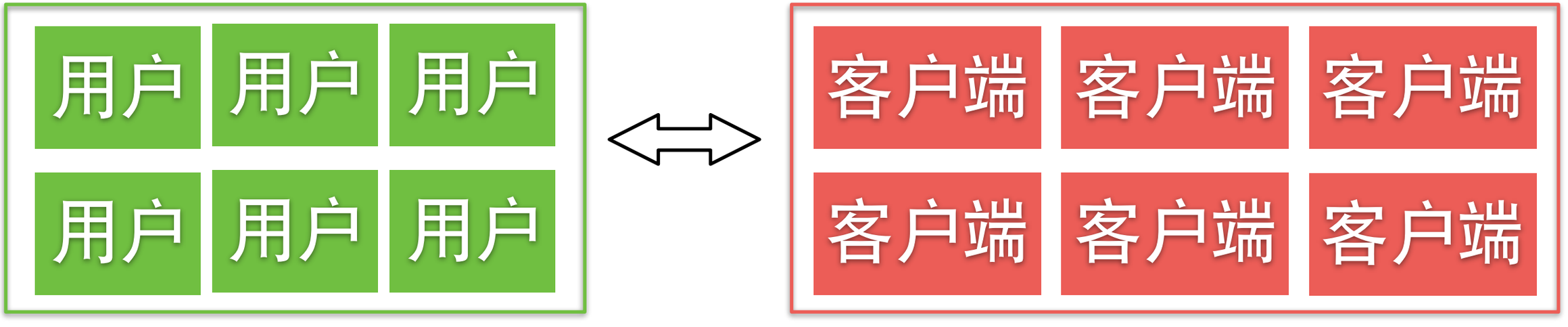
个人机时代



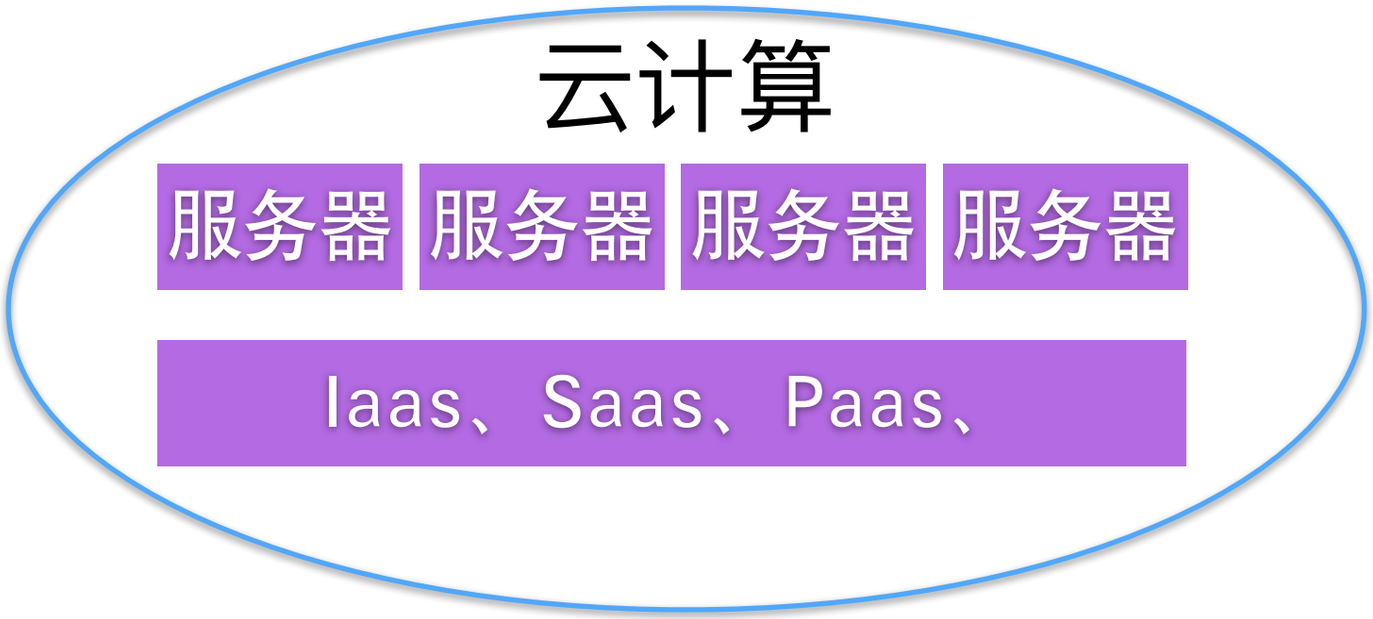
网络时代

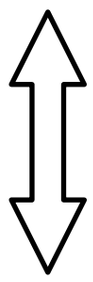


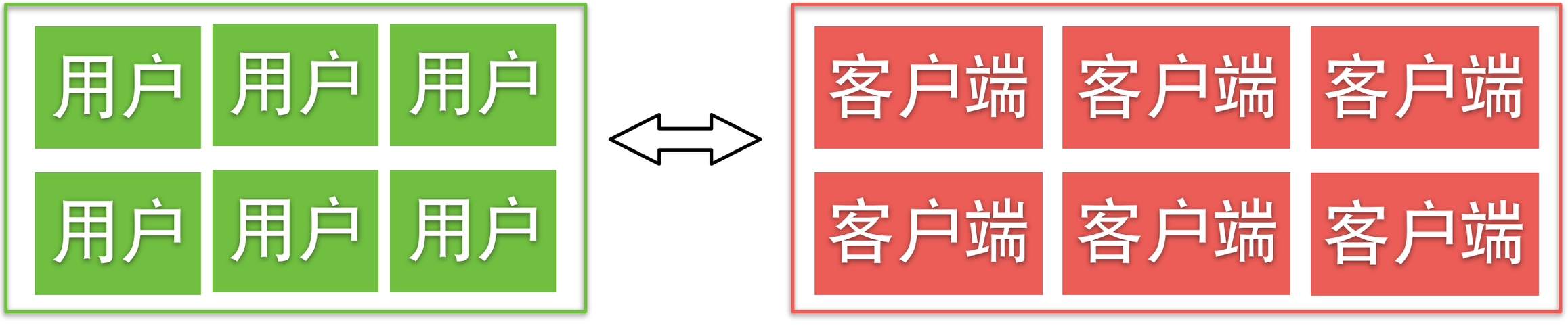




云计算时代


云计算
服务器
服务器
服务器
服务器
Iaas、Saas、Paas、




用户
用户
用户
用户
用户
用户
客户端
客户端
客户端
客户端
客户端
客户端

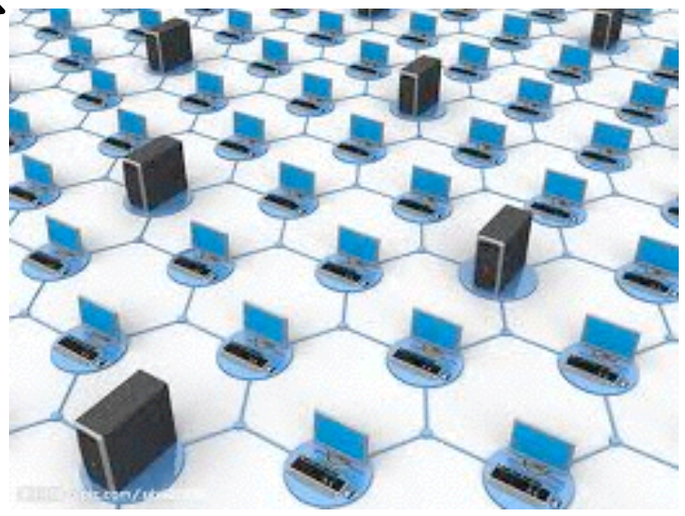
区块链

?

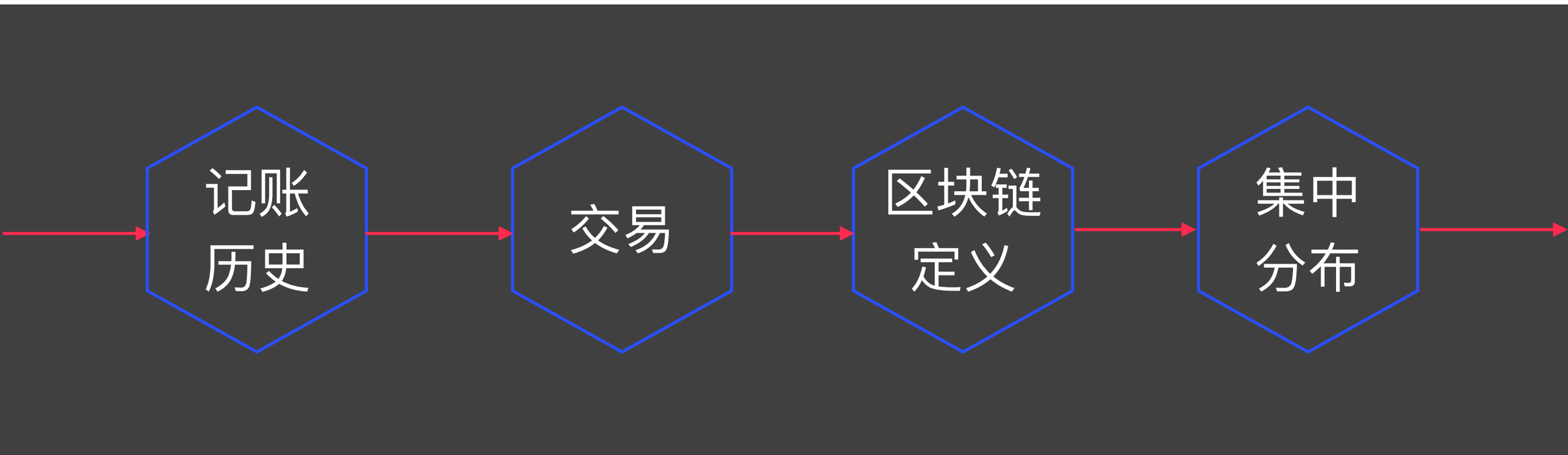
P2P

区块链

Client-Server

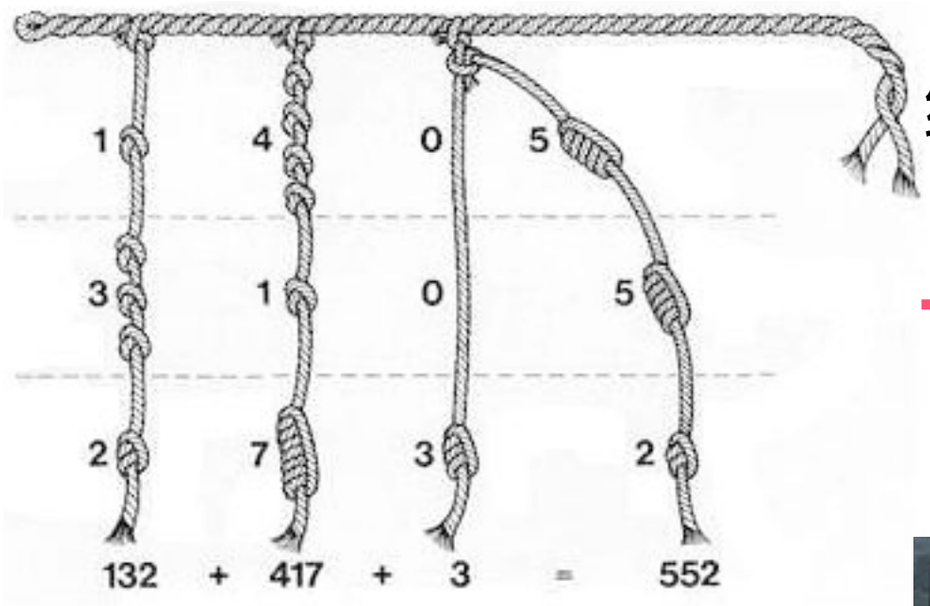


会计视角

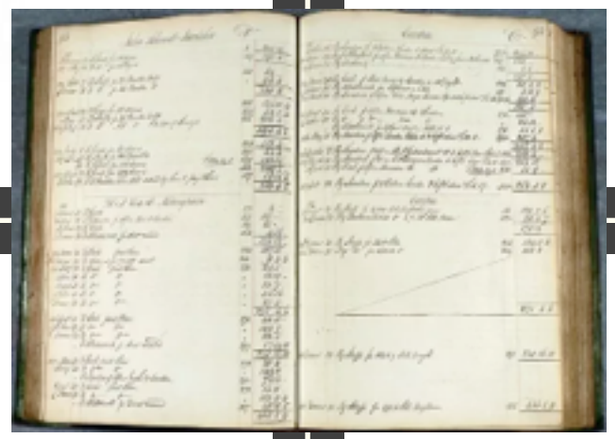


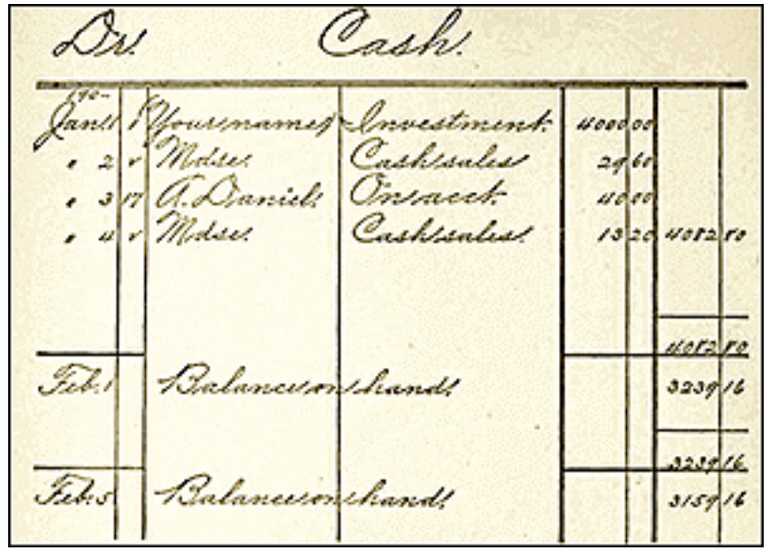
记账历史

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



结绳





单式

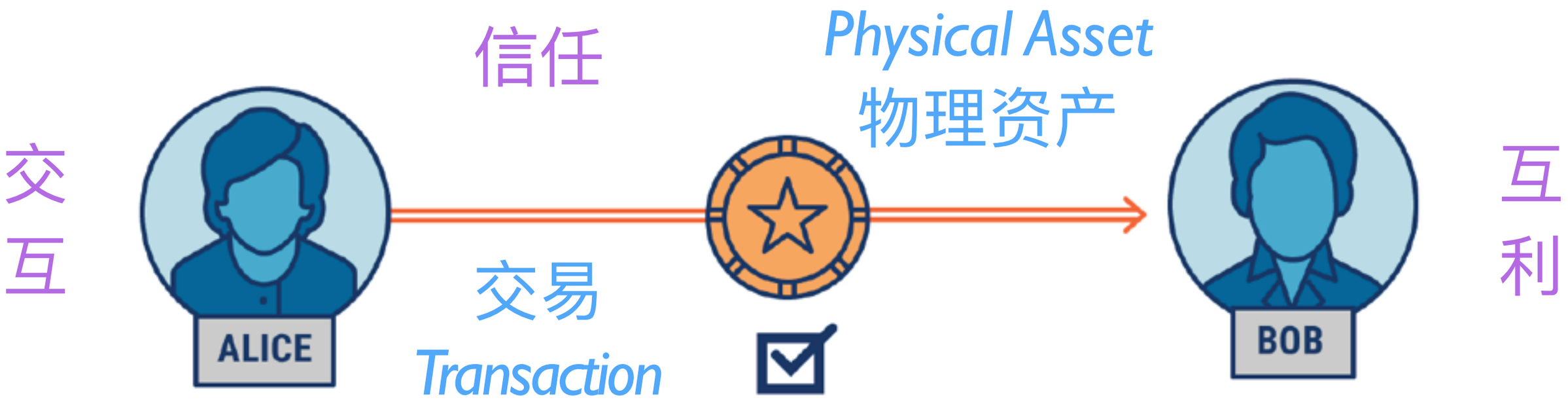
复式

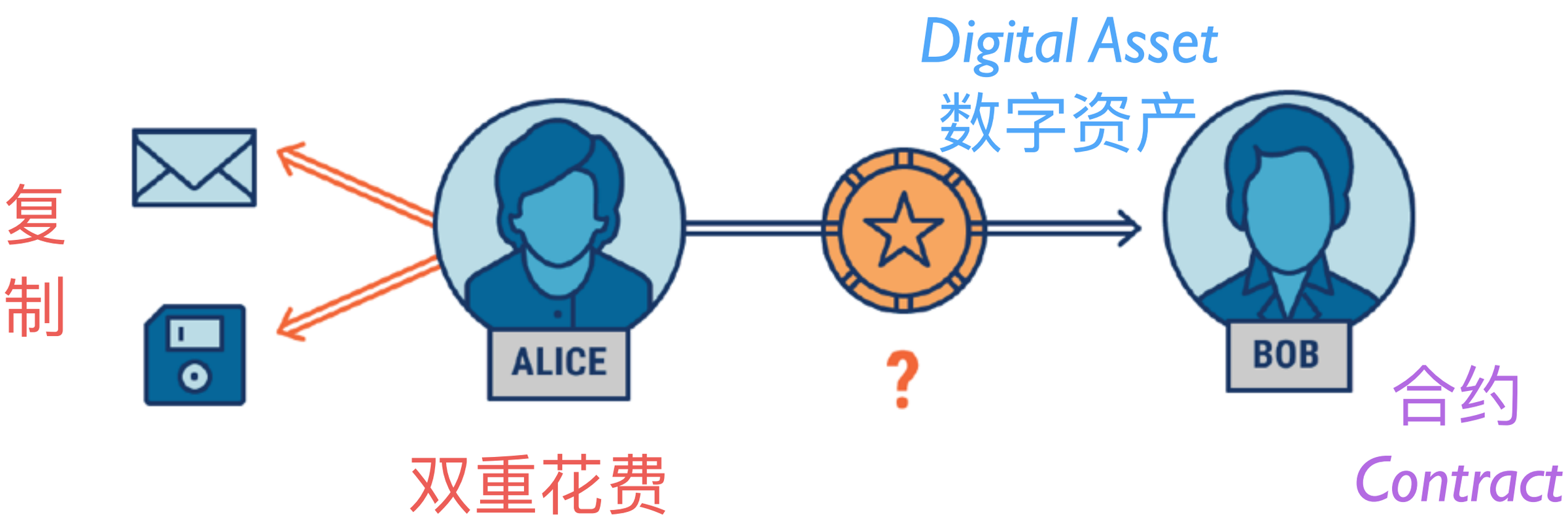
电子

物理

交易：物理 vs. 数字

What is Blockchain Technology @ CBSInsights





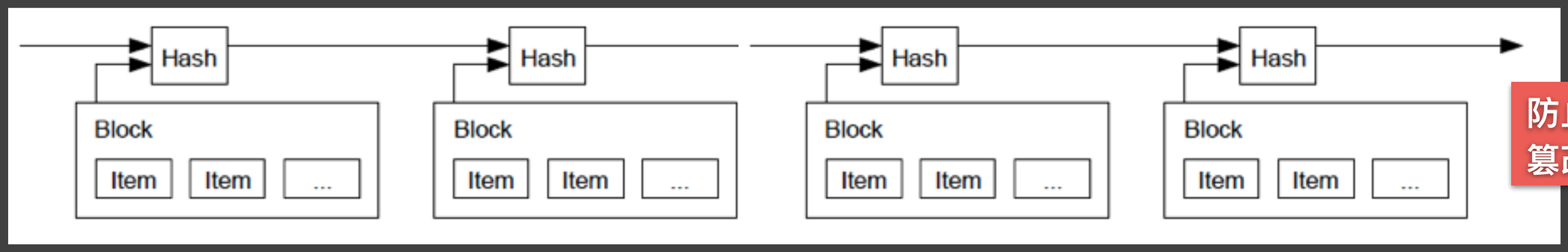
区块链定义

一个共享的分布式账本

公开

用于在商业网络中
促进交易记录和资产跟踪

可验证



防止篡改

账本：集中 vs. 分布

What is Blockchain Technology @ CBSInsights

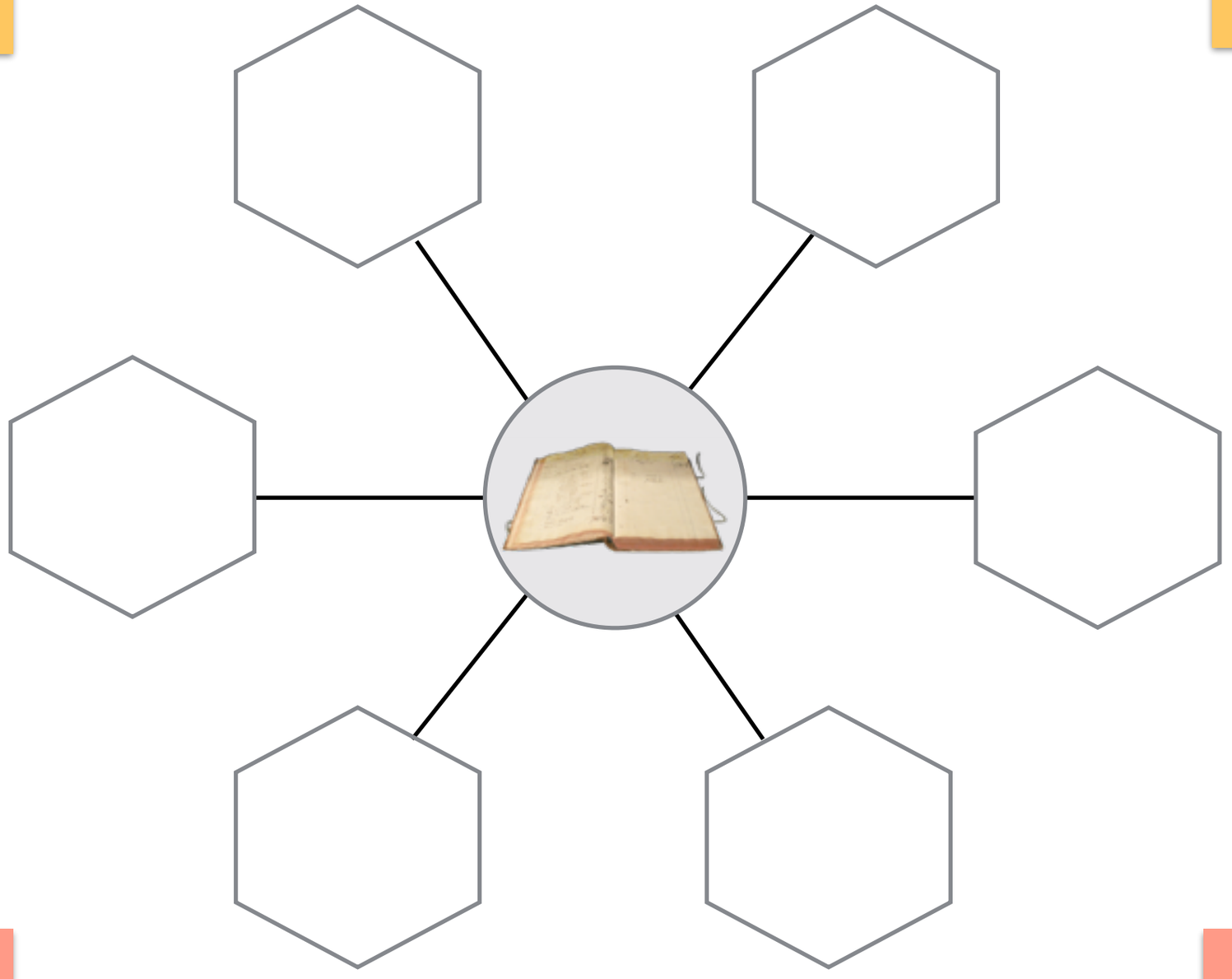
中心

P2P

集中式账本的优缺点

中心化

第三方



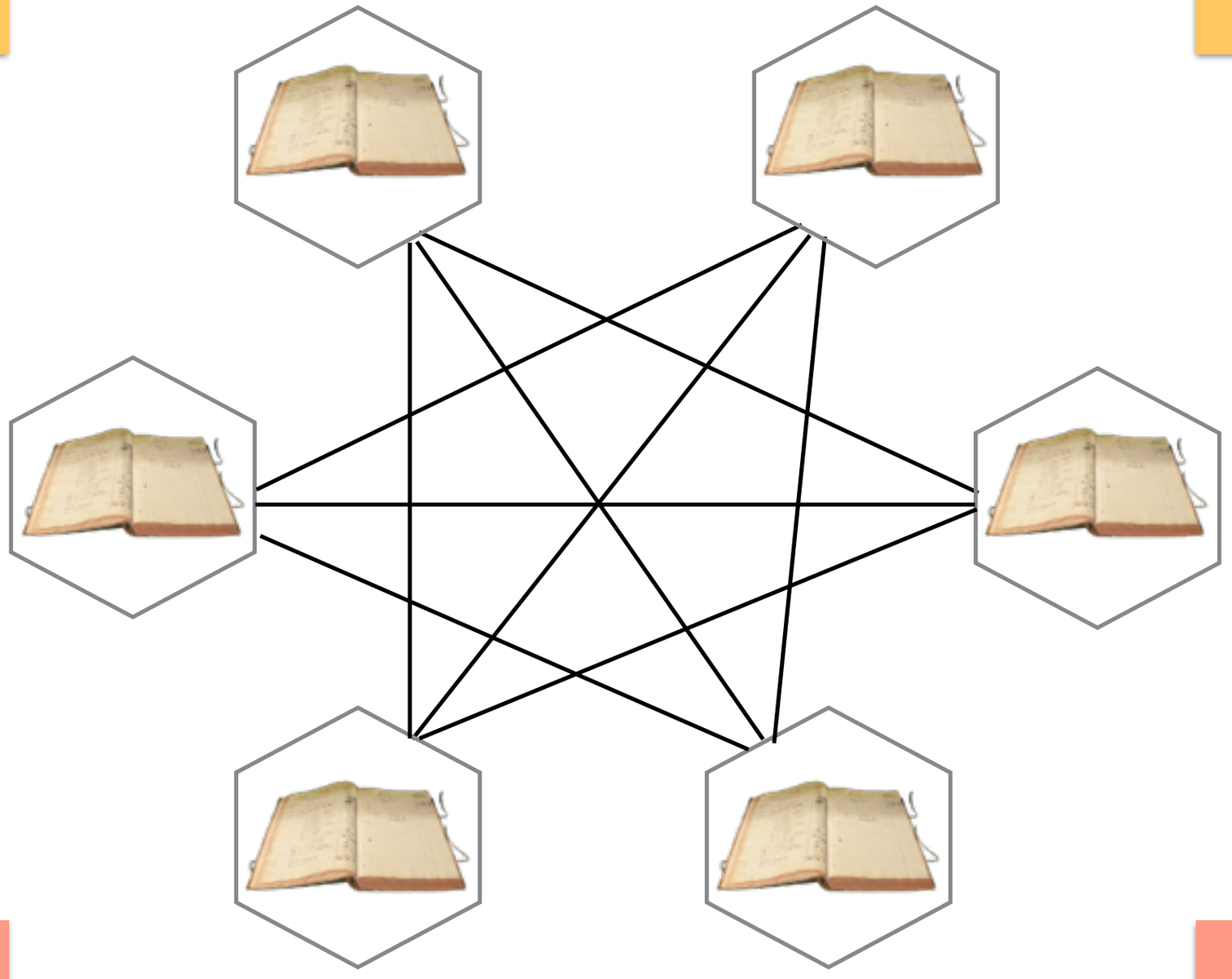
脆弱

信任

分布式账本的优缺点

一致性

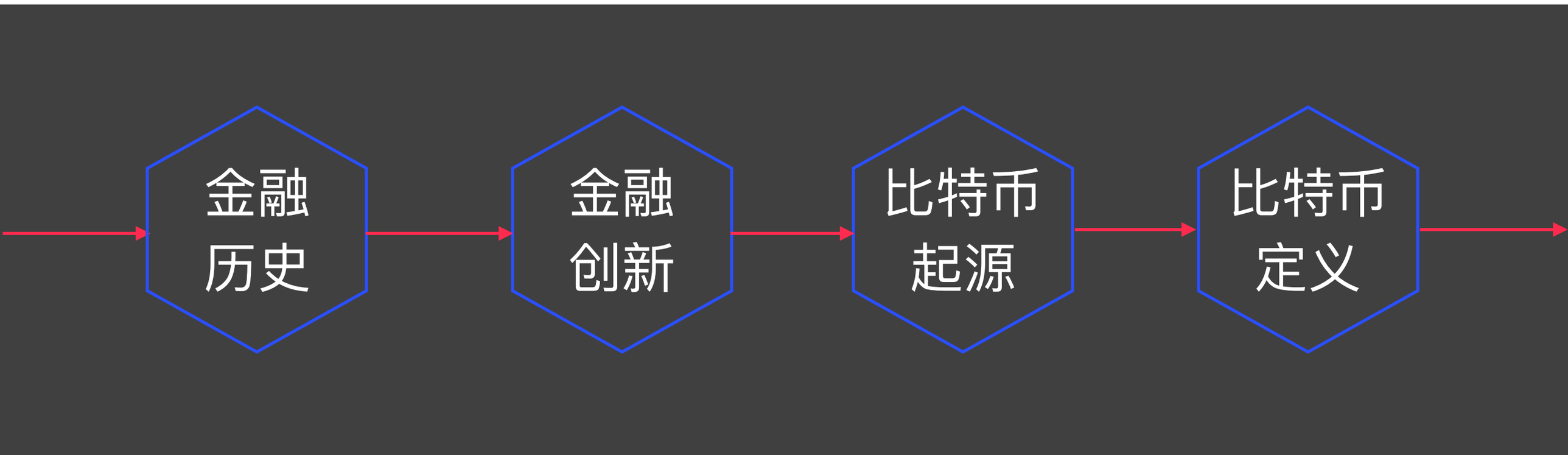
完整性



效率

花费

金融视角



金融历史

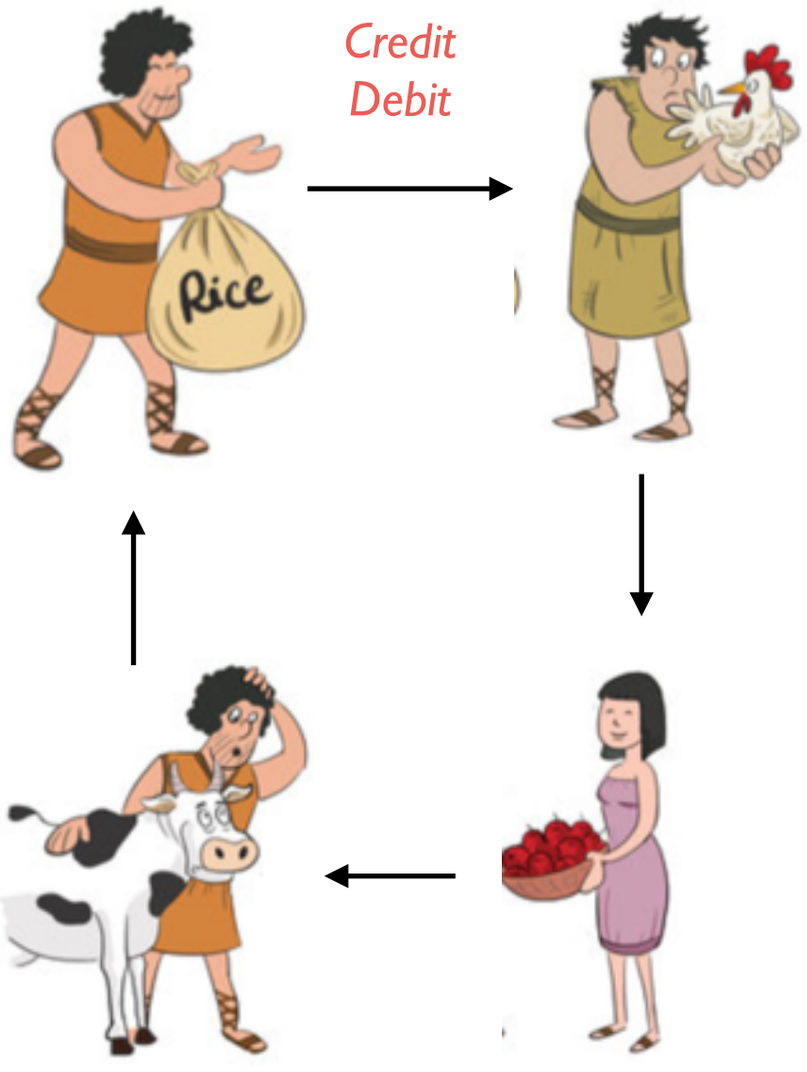
Barter

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

Money

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

Credit Debit

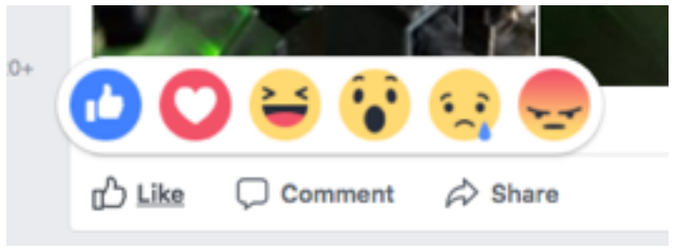


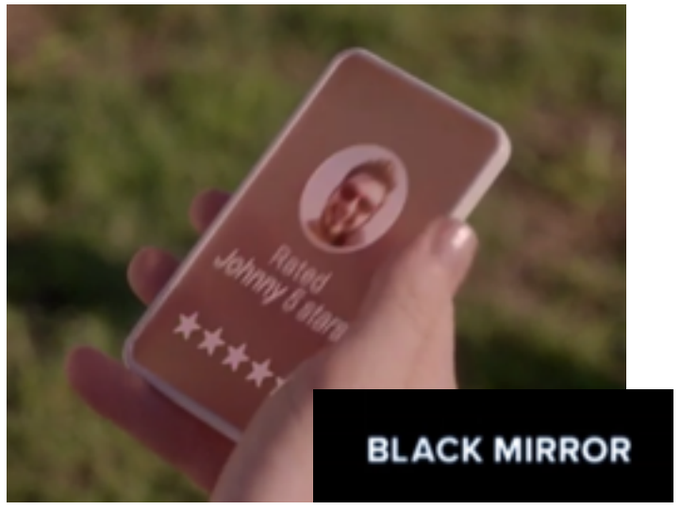
https://en.wikipedia.org/wiki/Money

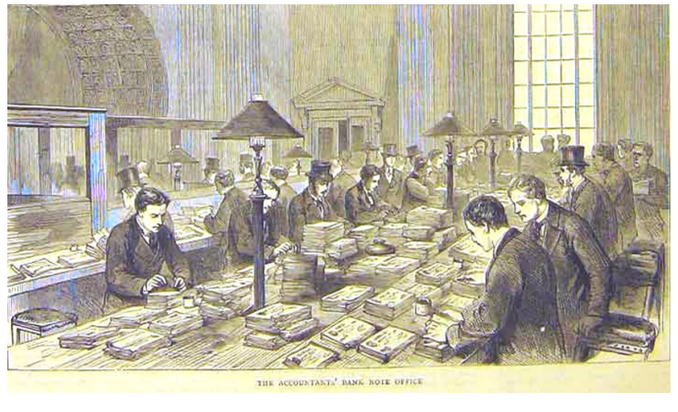
Reputation

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





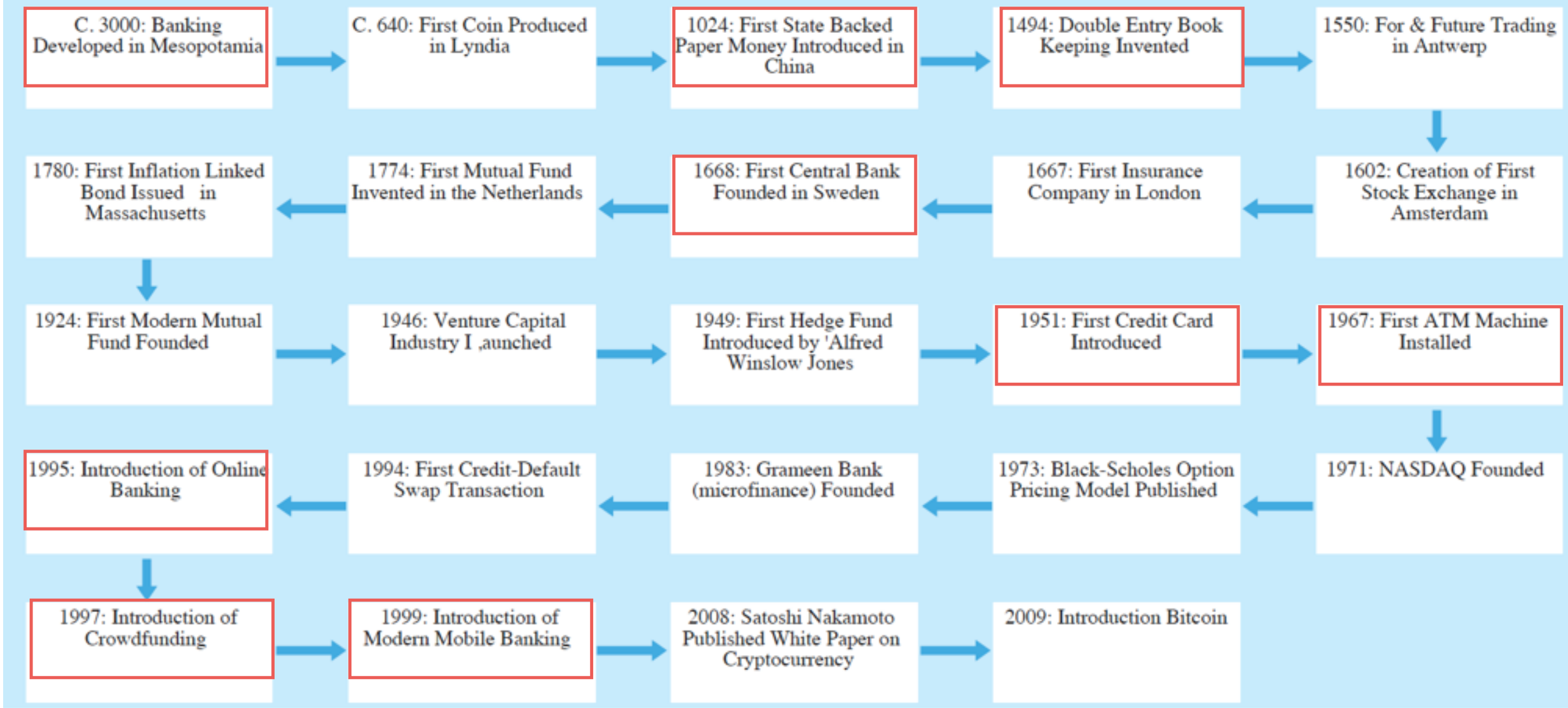


Bank

Credit Card

金融创新

→ 金钱 → 纸币 → 复式记账 → 银行 → 信用卡 → ATM →



→ 在线银行 → 众筹 → 移动支付 → Bitcoin → 区块链 →

法币

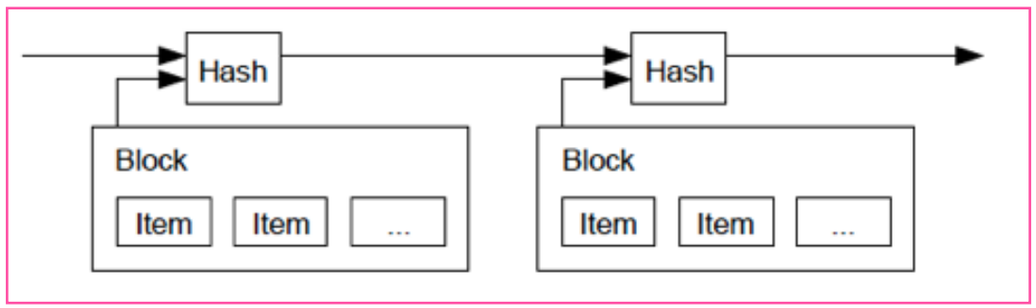

新版
2015年版 第5套
人民币
那些事...
中国人民银行
100
壹佰圆
样币
AA00000000
钞票正面
钞票背面
ZHONGGUO RENMIN YINHANG
100
YUAN
2015年
样币禁止流通
多一份金融了解
多一份财富保障
2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。
光变镂空开窗安全线
雕刻凹印
胶印对印图案
光彩光变数字
白水印
人像水印
横竖双号码
广发银行
CGB

比特币产生

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

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



2008

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.

比特币概念定义

构成数字货币生态系统基础概念和技术的总称

比特币网络中参与者存储和传输的货币单位

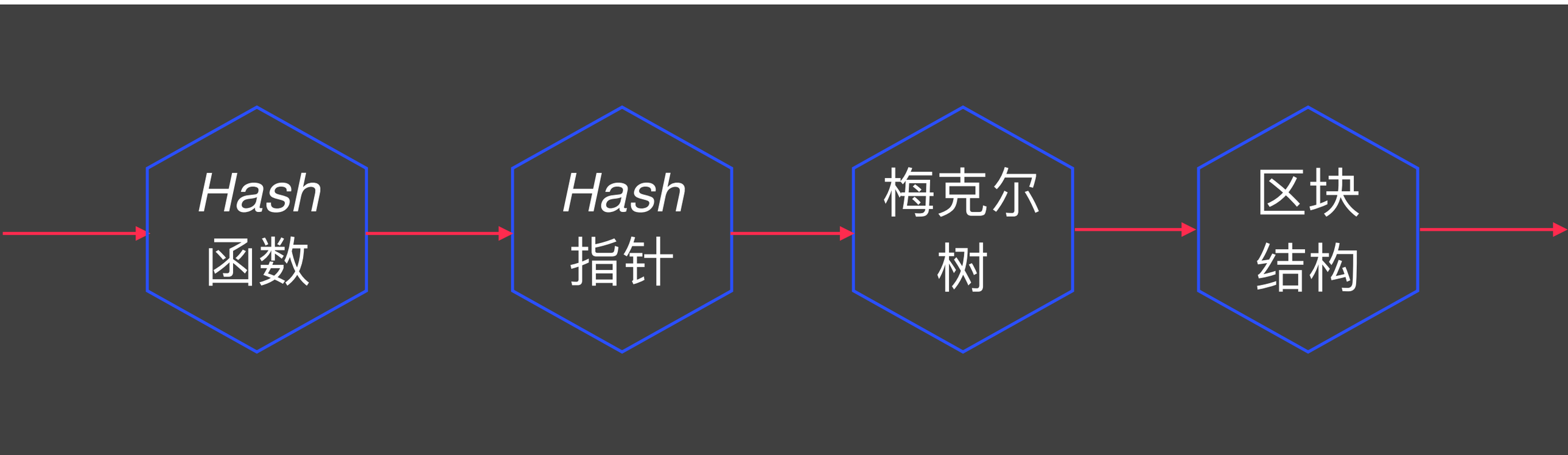
比特币是虚拟的，本身也不是简单数据化的

用户通过网络进行比特币进行转账和可以做到和传统货币一样的事情

比特币隐含在汇款方到收款方的转账交易中，用户用自己私钥来证明

传统银行依靠发行和结算，比特币依靠挖矿

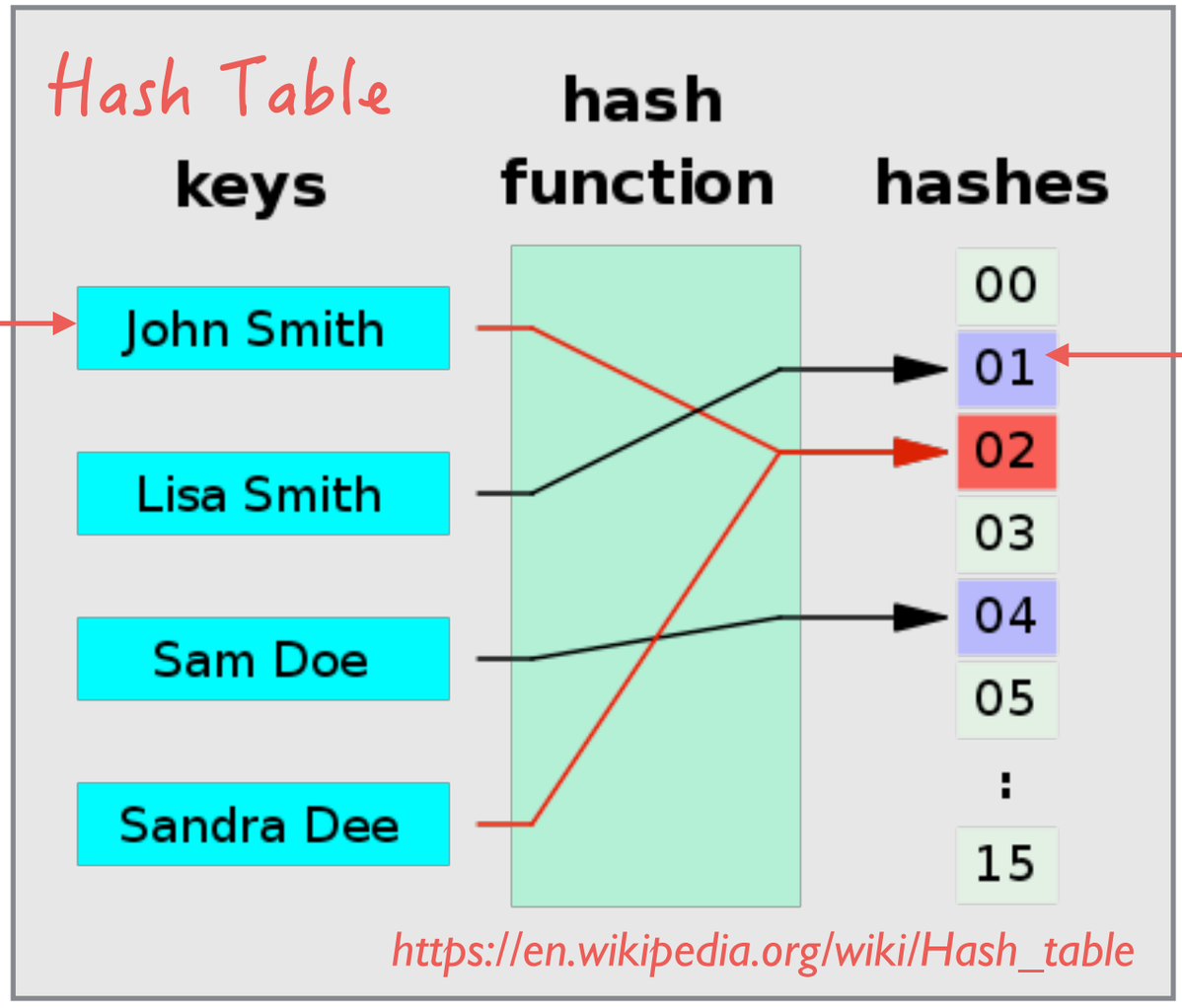
区块基础



Hash函数

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

输入为任意大小的字符串



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

输出为固定大小，例如256位

可以进行有效计算：例如O(n)

同样的输入产生同样的输出

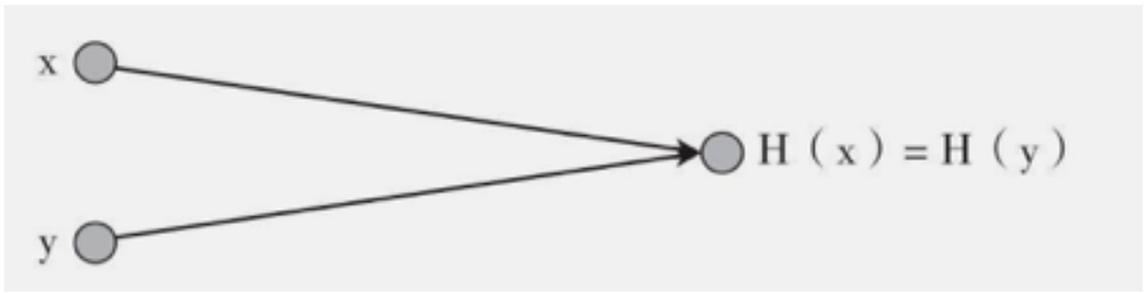
MEM2018 → SHA256 → 547d71f91fec62c23dee84cf2a5dcfd4bdc46a05b2ddd3253555c1b76be433e5

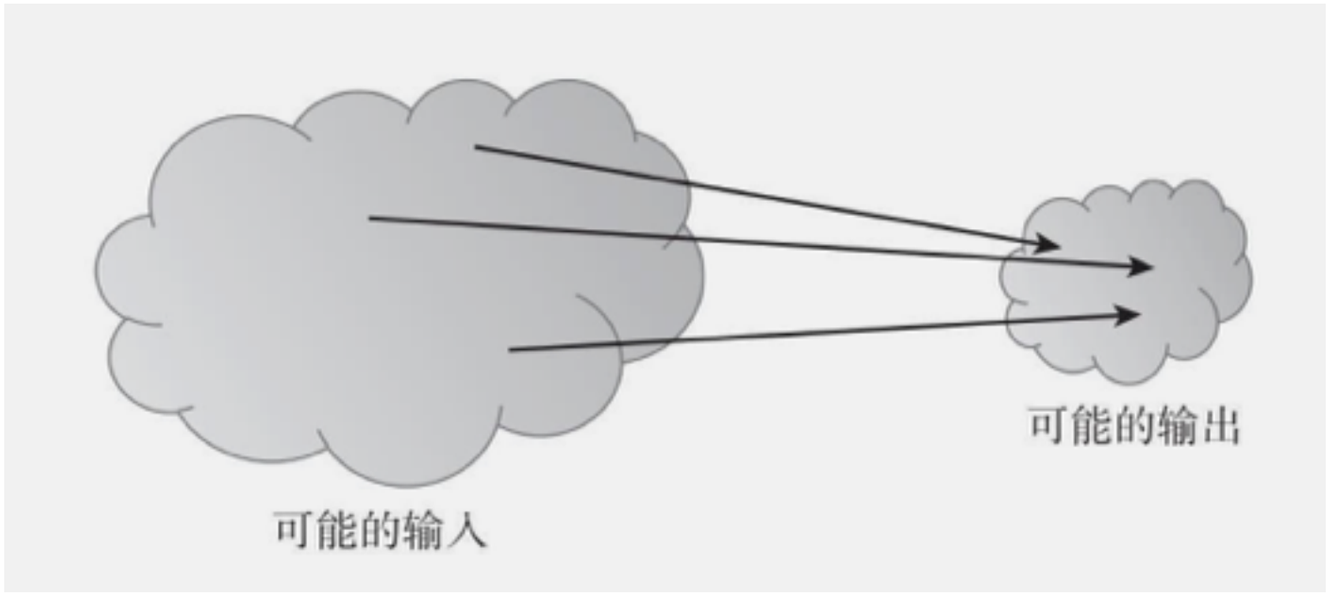
单向性

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

Hash函数

抗碰撞





隐匿性

H(“heads”)

H(“tails”)

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

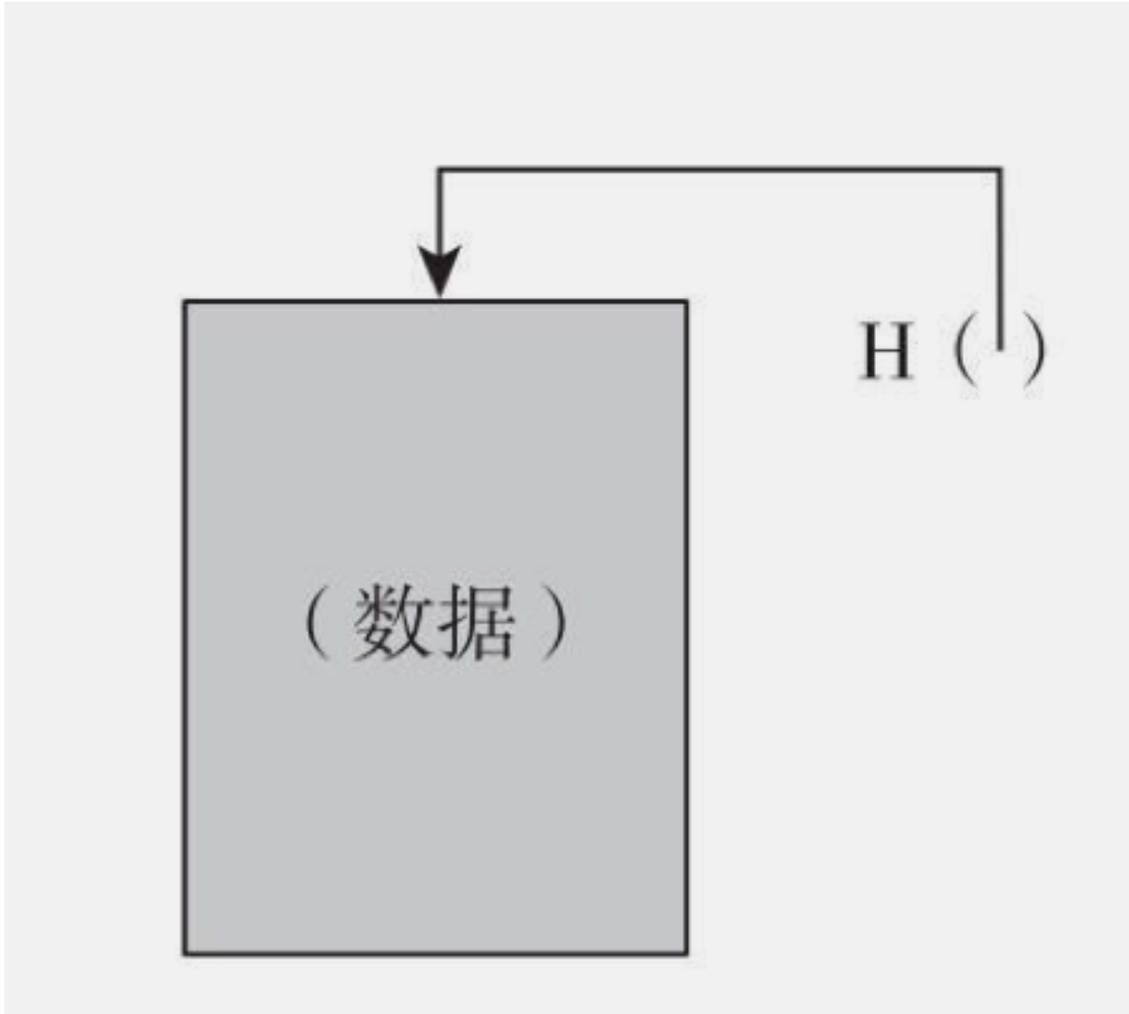
难题友好

Hash指针

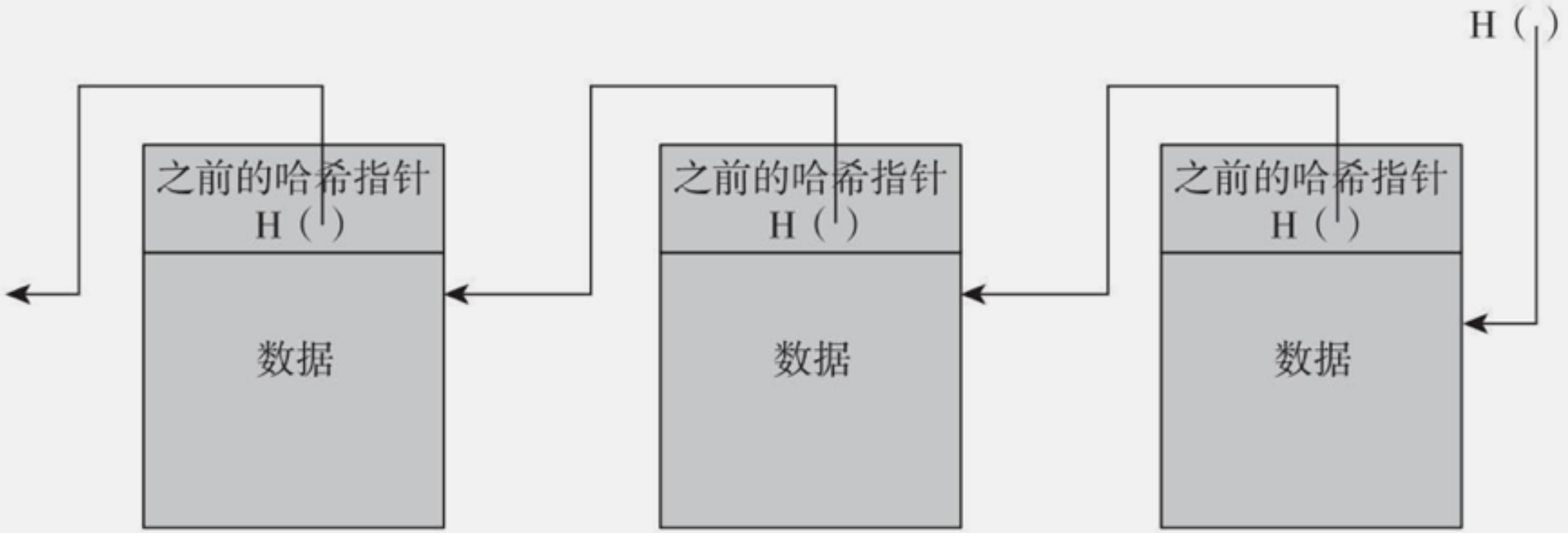
Hash指针：
是一个指向存储数据
及其数据Hash的指针

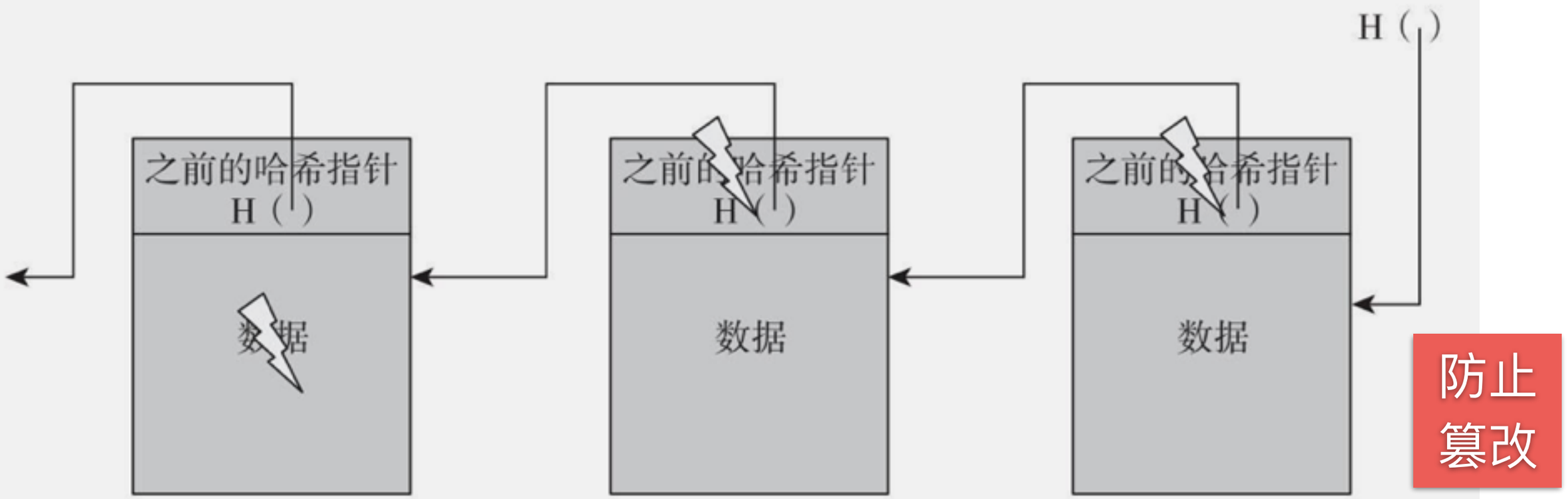
取回数据
验证数据是否改变

区块链的关键思想



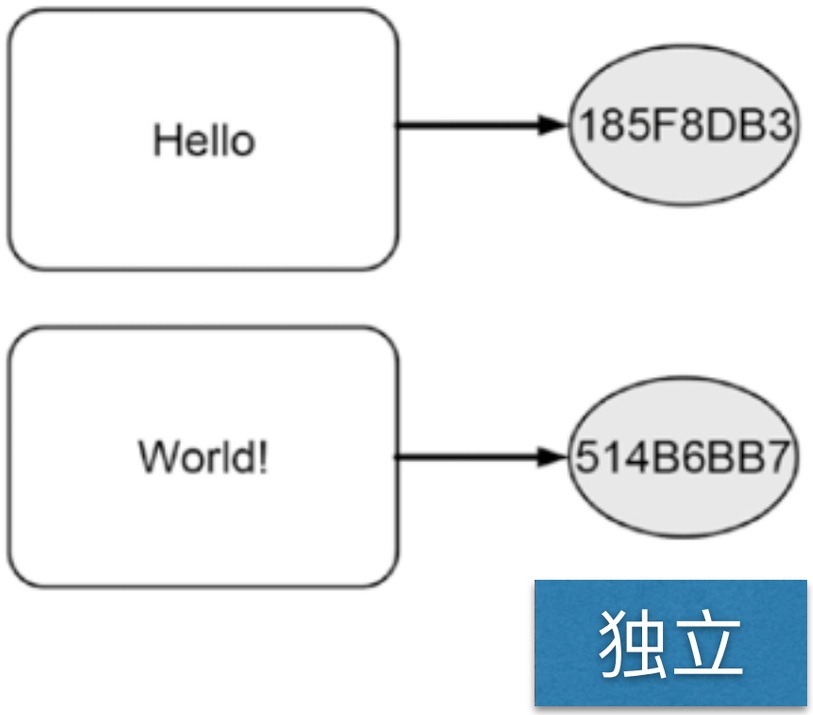
区块链

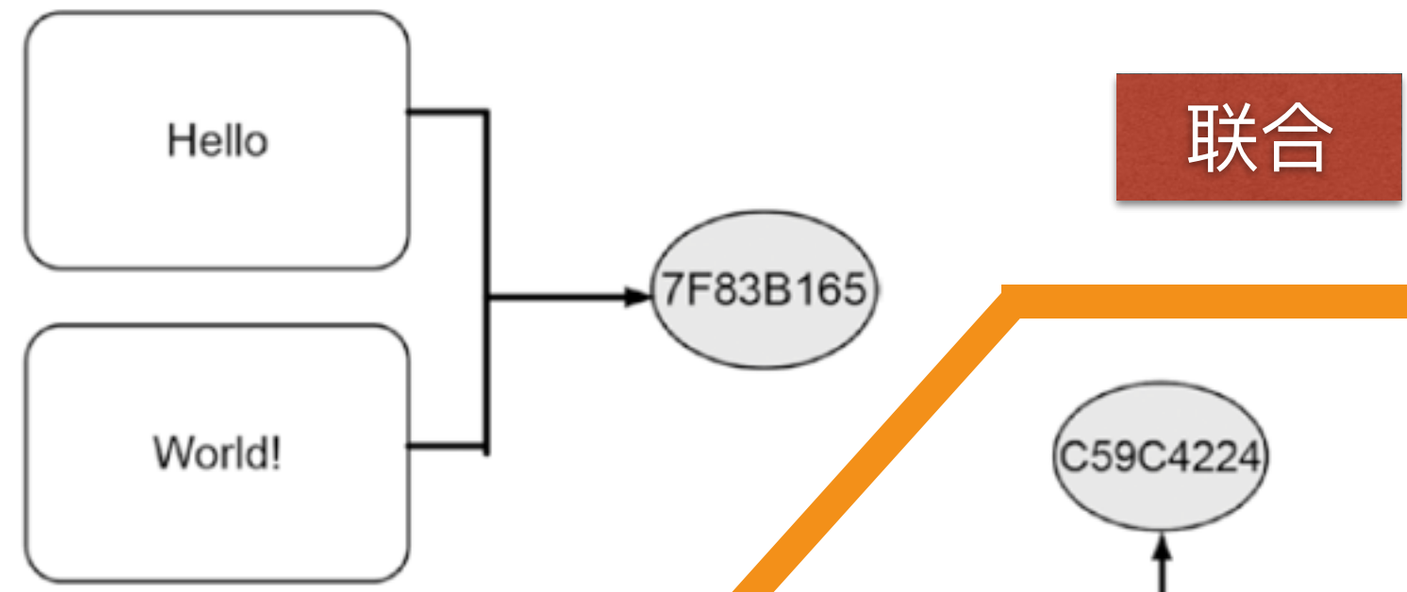

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据

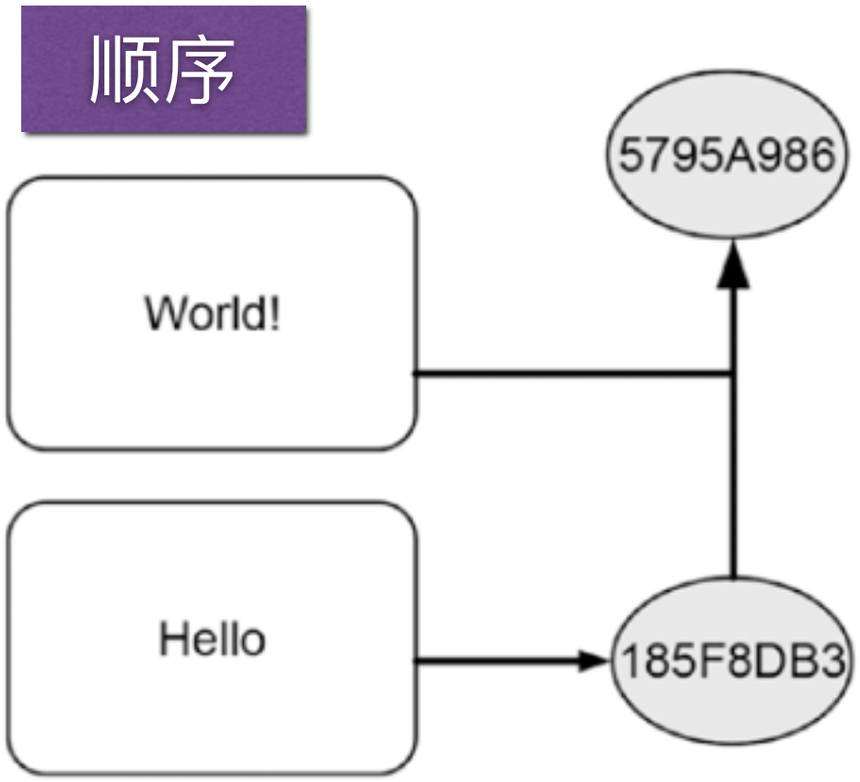

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
防止
篡改

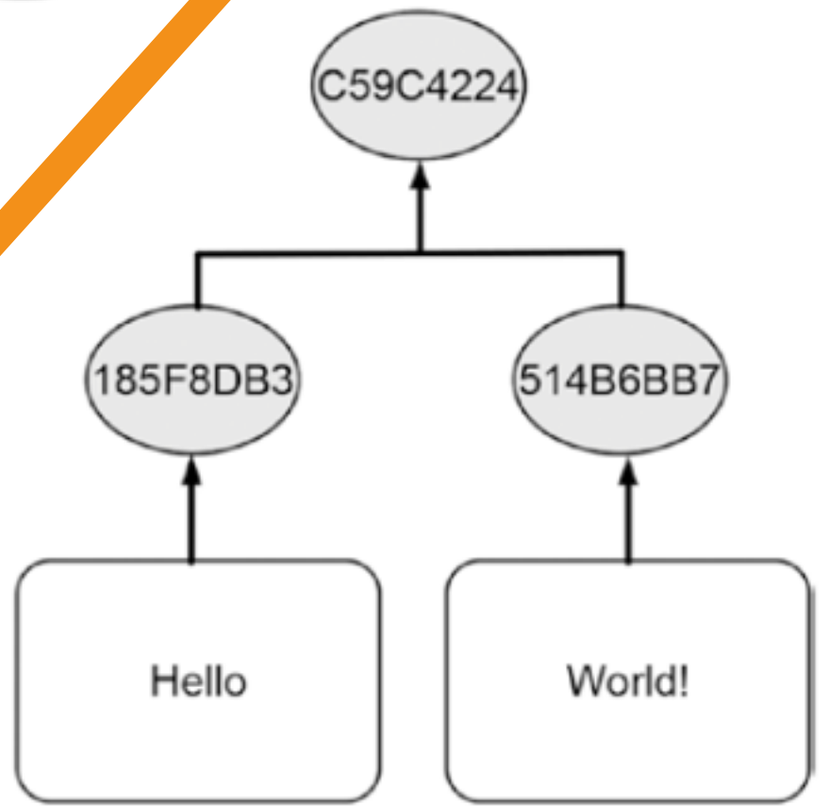
Hash数据模式

Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS

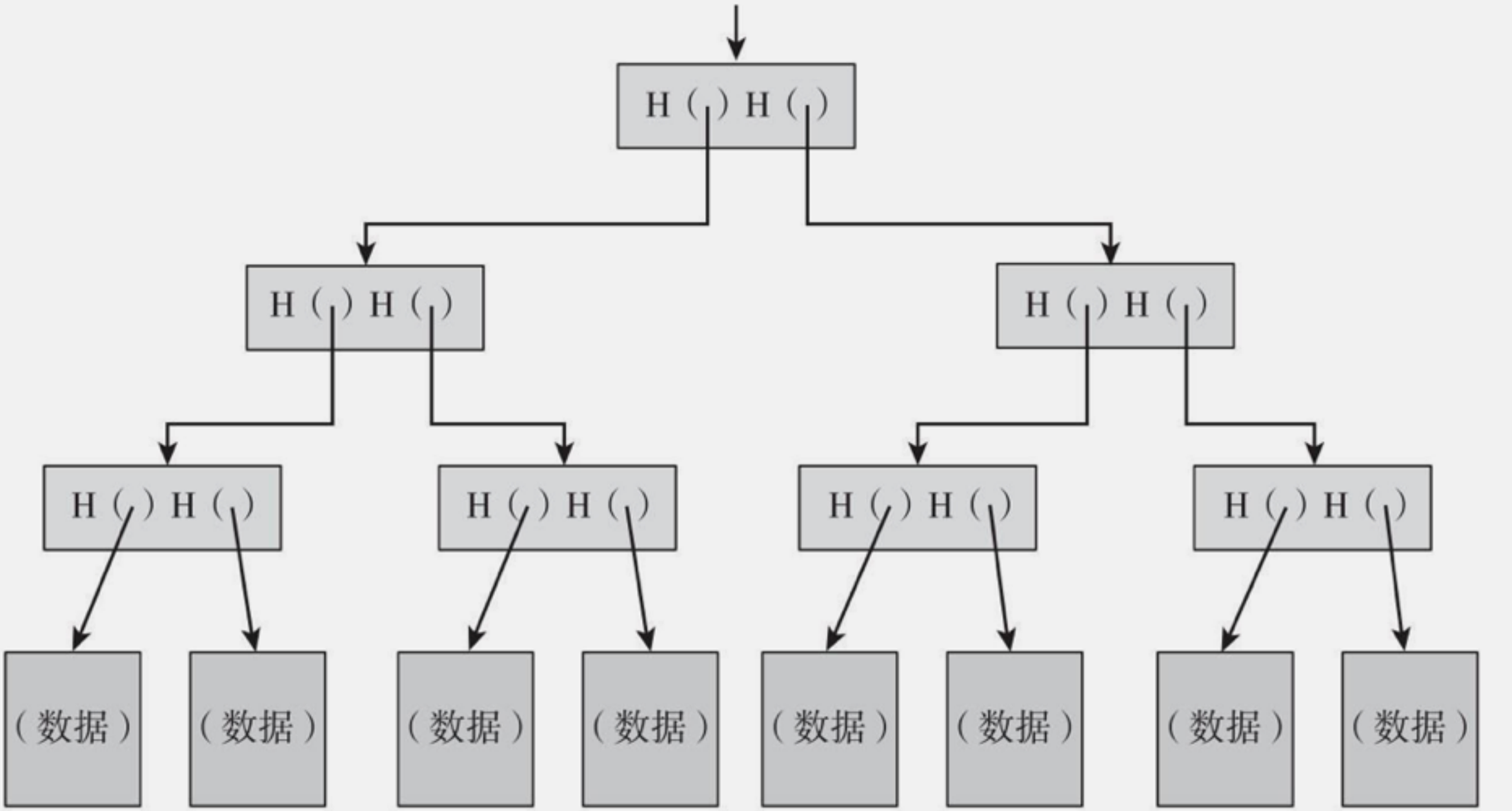




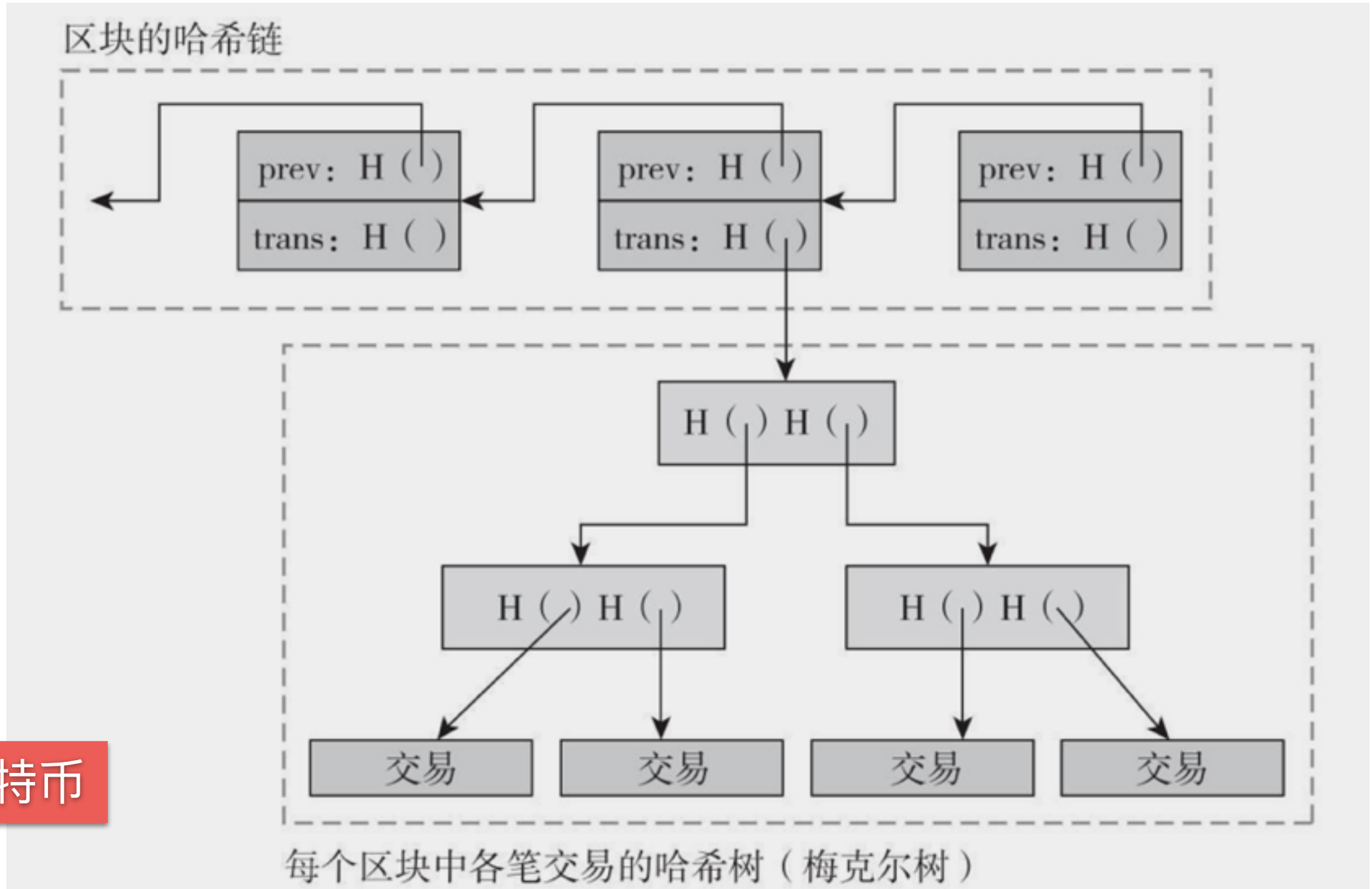




梅克尔树



区块结构



比特币

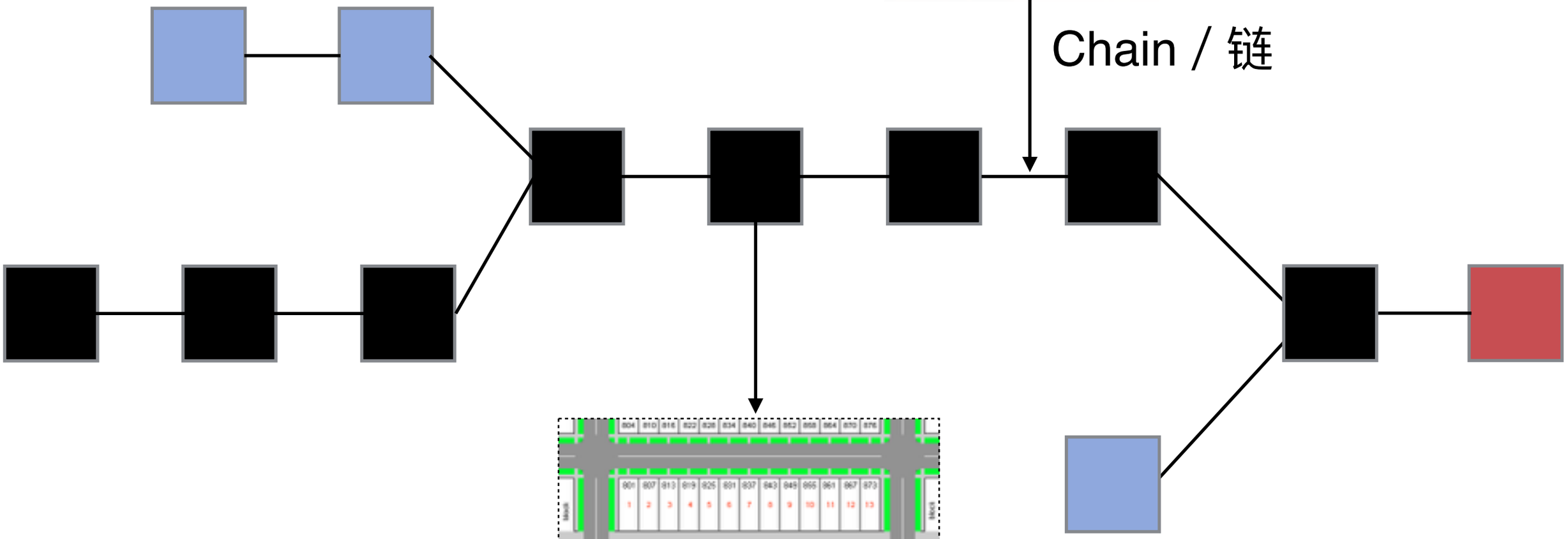
图3.7 比特币的区块链有两个哈希结构

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。

区块链结构

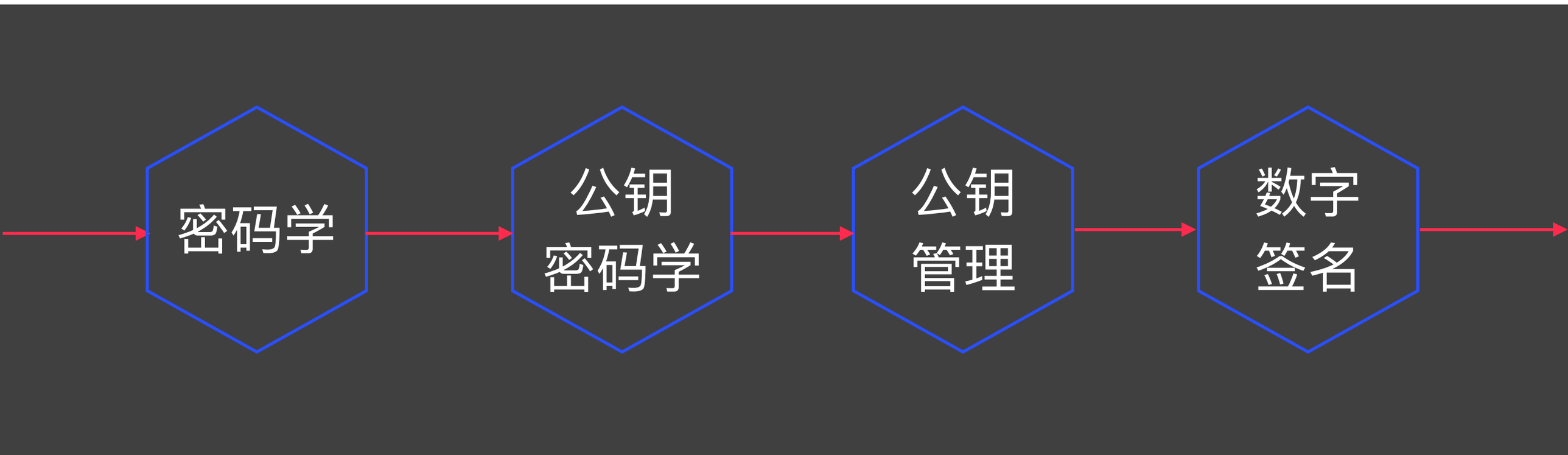
https://en.wikipedia.org/wiki/Blockchain

Chain / 链



Block / 区块

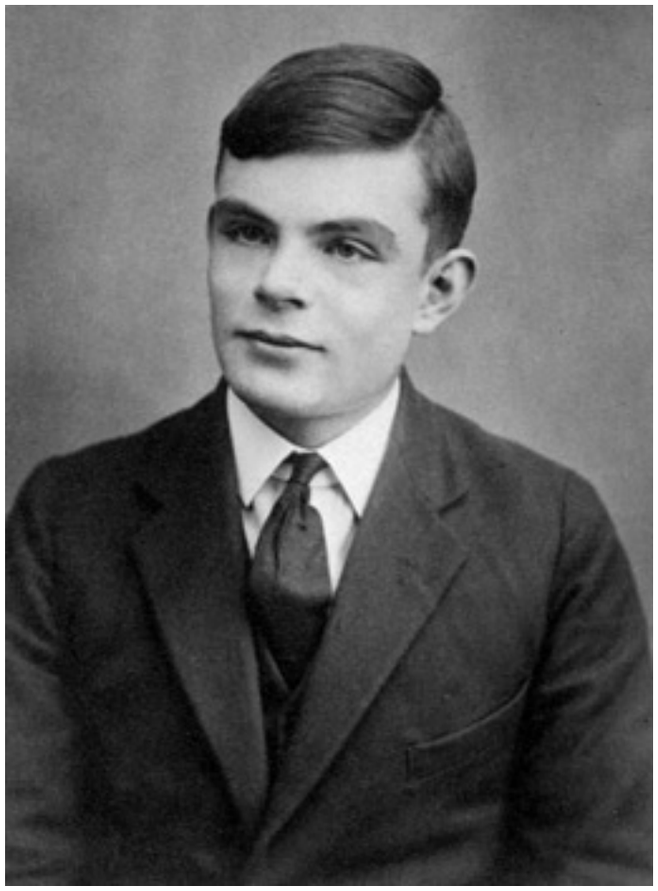
密码学基础



密码学

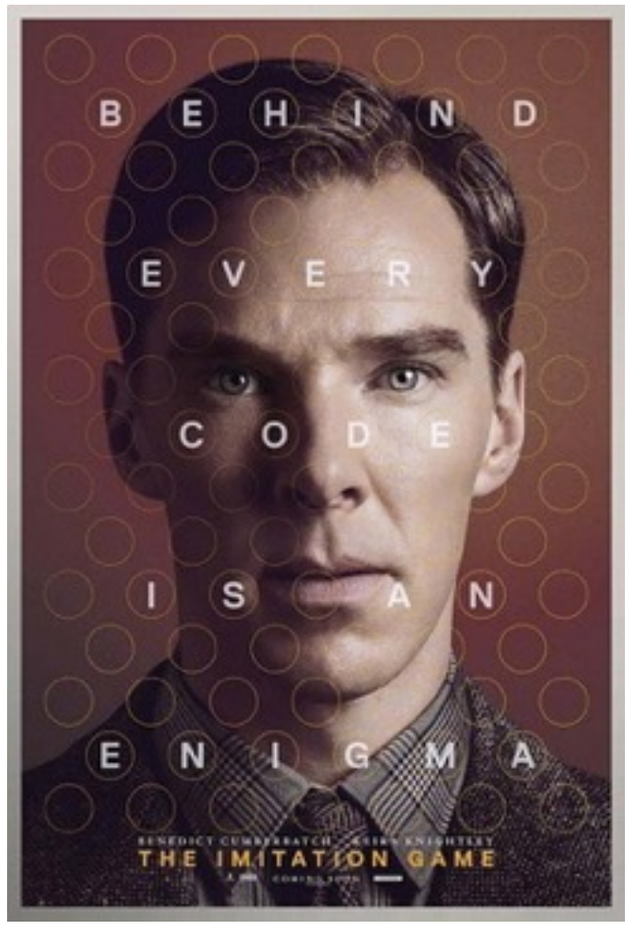
https://en.wikipedia.org/wiki/Alan_Turing

图灵

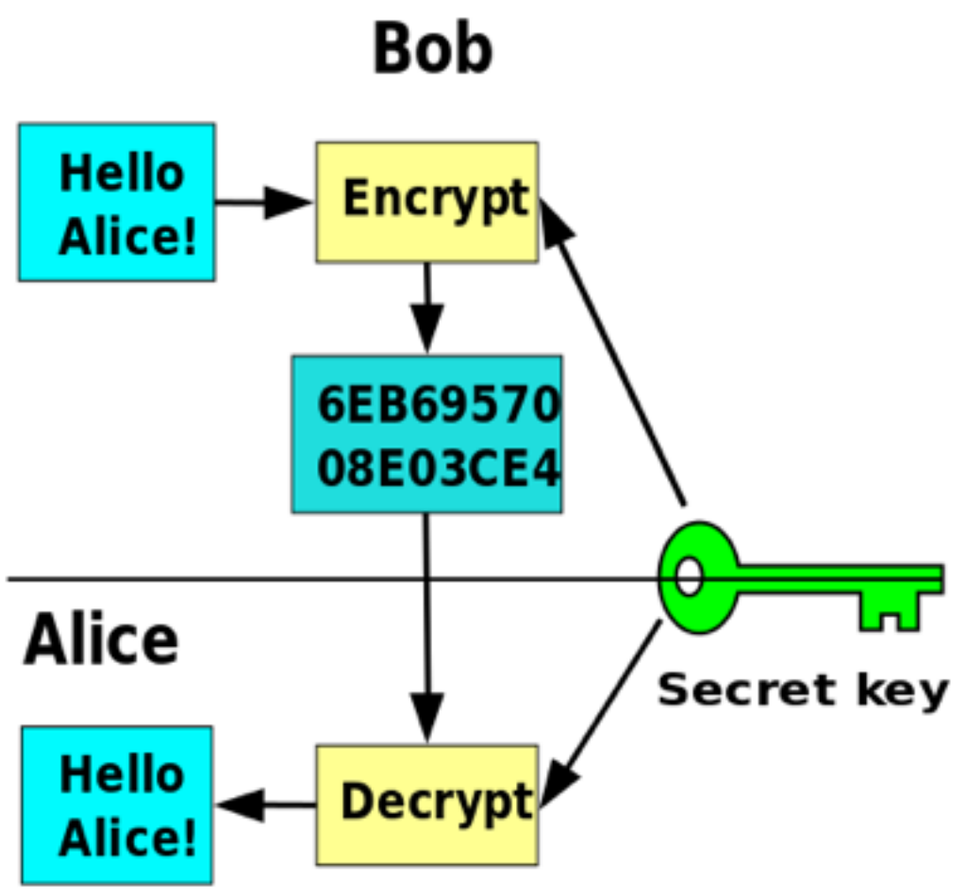


恩尼格玛密码机

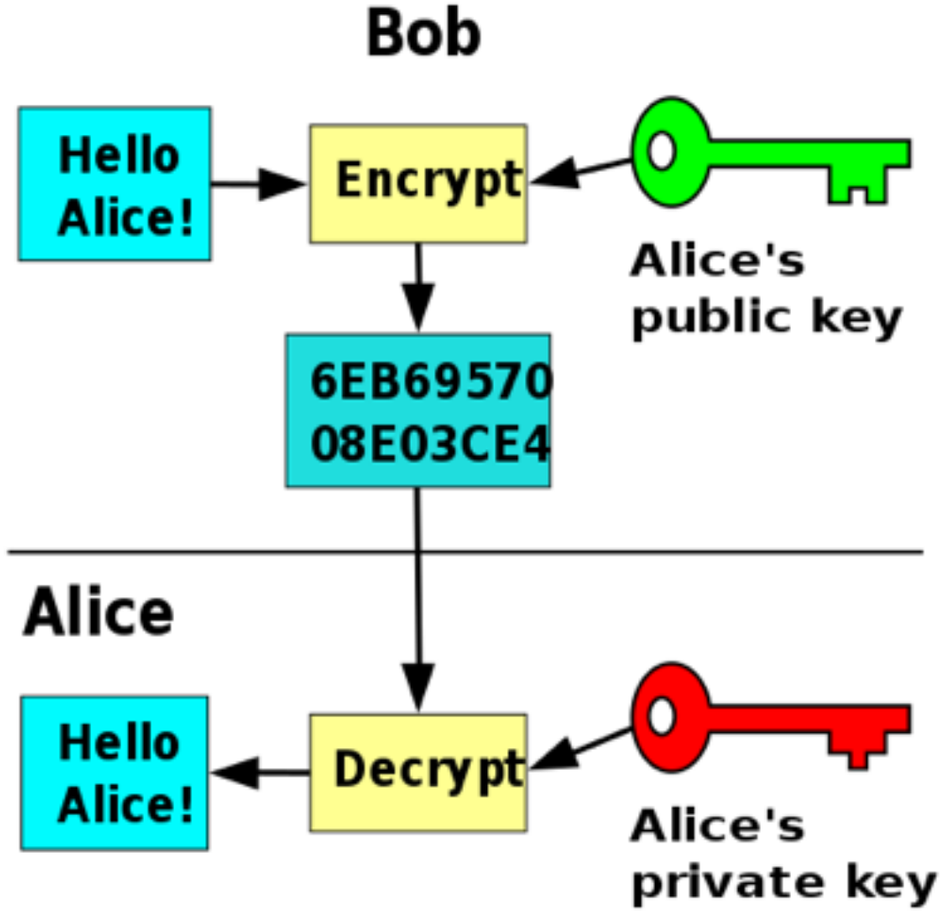
模仿游戏



对称密码学 vs. 非对称密码学



对称密码学



非对称密码学

DH vs. RSA

2015年
图灵奖

Whitfield Diffie

Martin Hellman

Ralph Merkle

1976

1978

2002年
图灵奖

Ronald L. Rivest

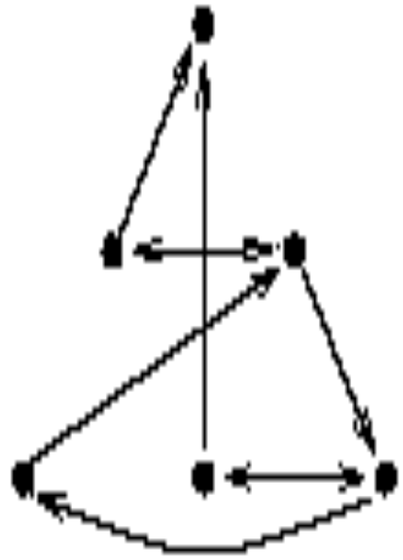
Adi Shamir

Leonard Max Adleman

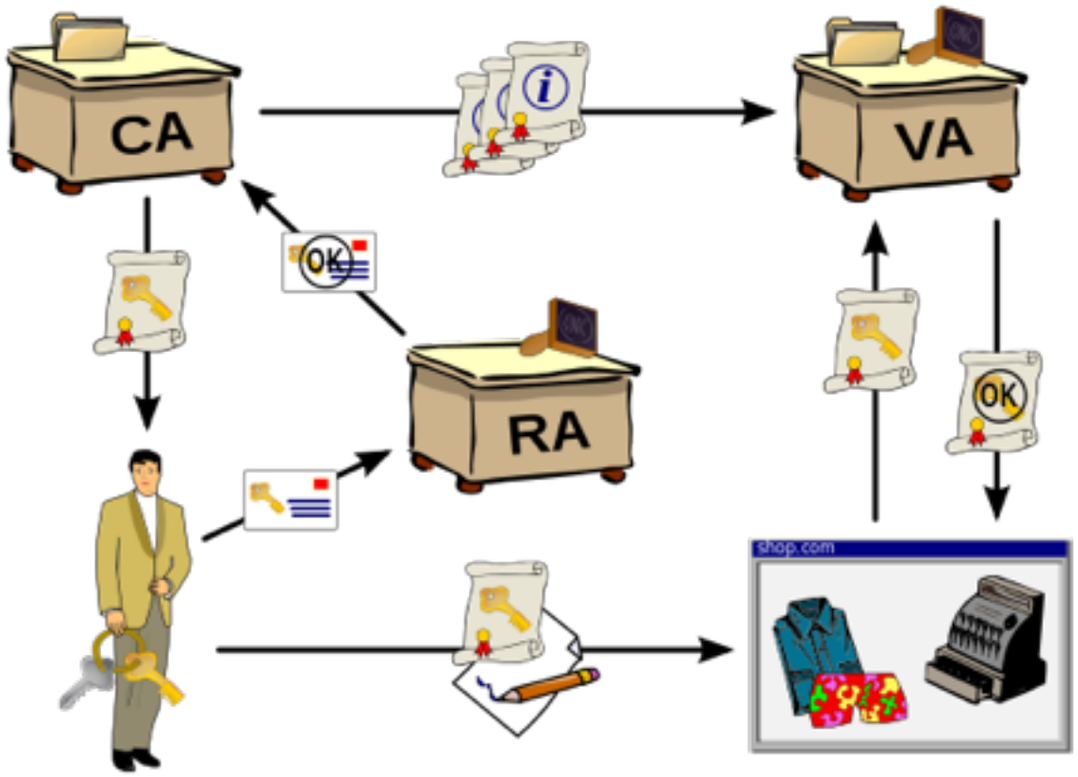
公钥管理: PKI vs. PGP

RSA

VERISIGN™



公钥管理的P2P版本



PGP®

1991

GnuPG

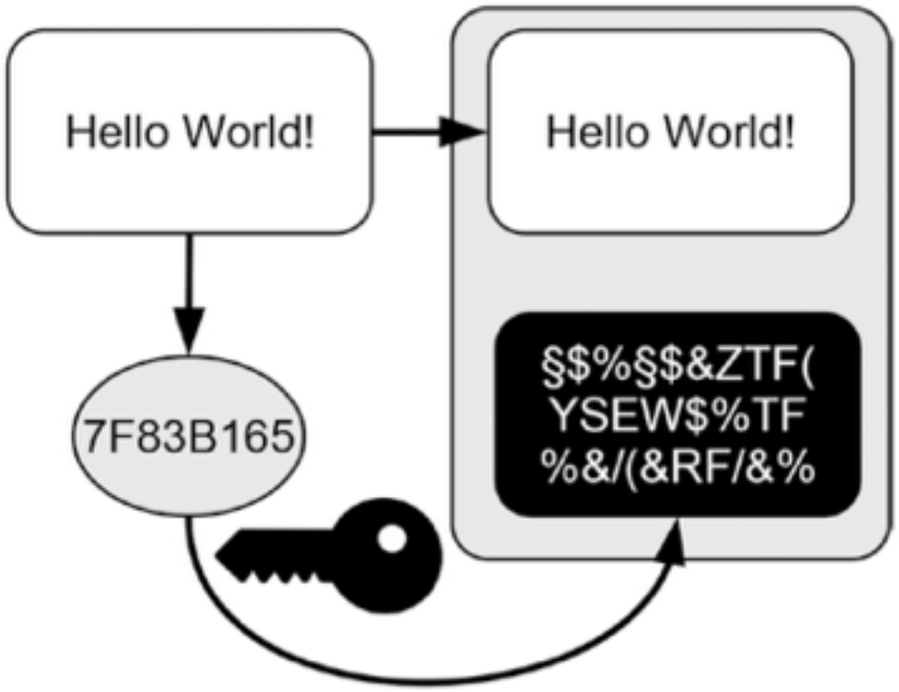
1999

Phil Zimmermann

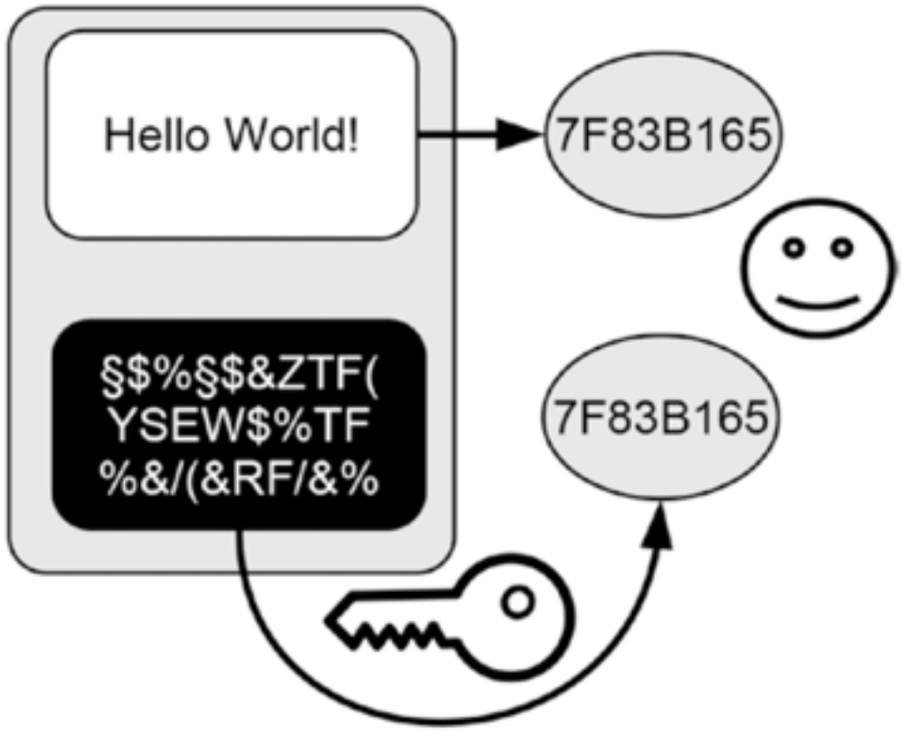
数字签名

Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS

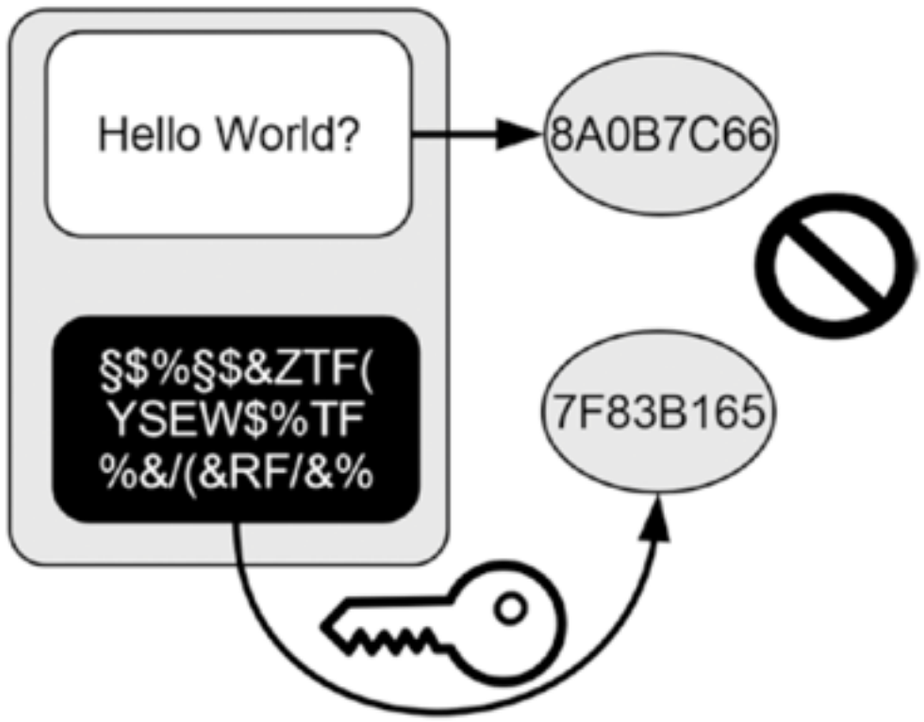
产生签名



验证签名



发现欺骗

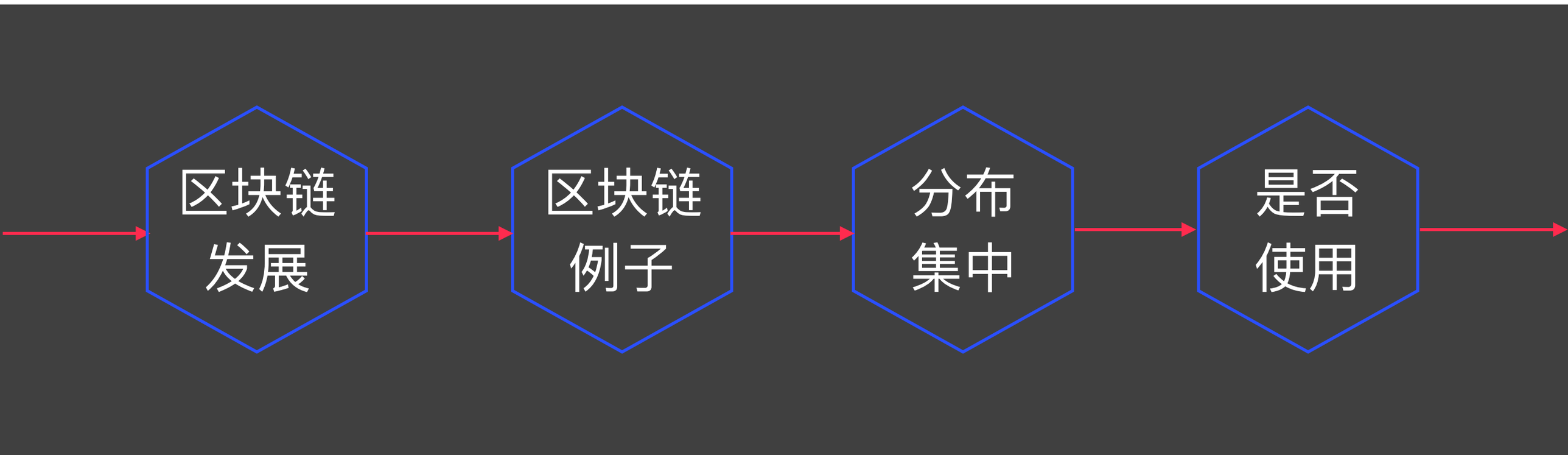


自己签名，任何人都可以验证（公钥分发）

不可伪造，公钥私钥

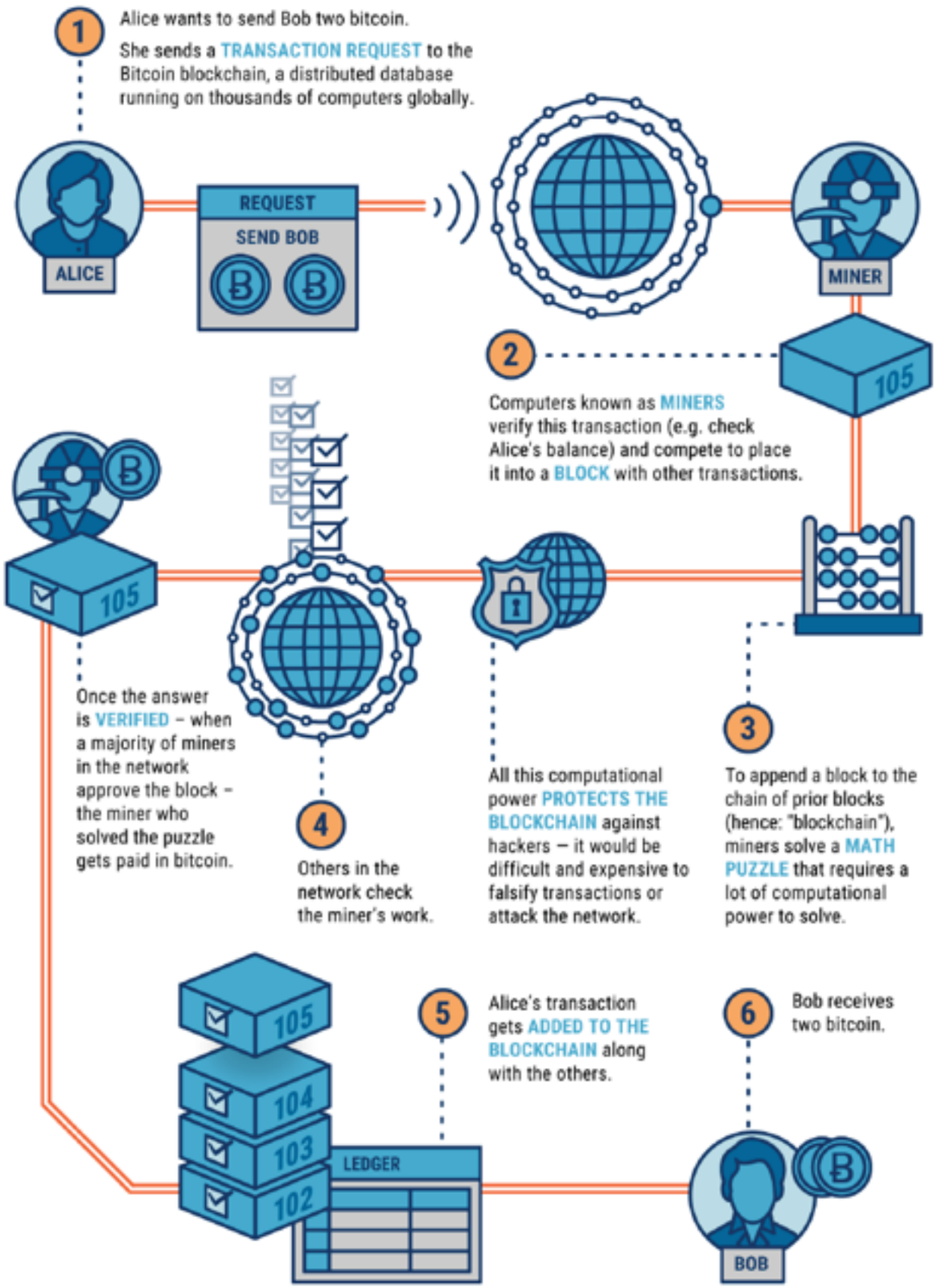
签名信息的大小

区块链应用



比特币和区块链

What is Blockchain Technology @ CBSInsights



比特币 …… 超级账本

区块链

比特币 超级账本

以太坊 R3 Corda

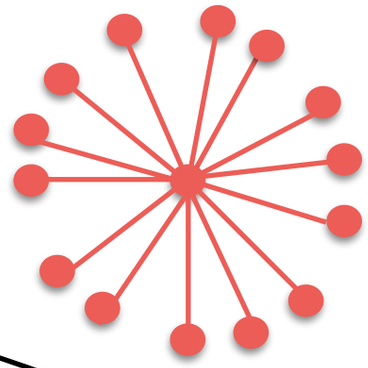
EOS ……

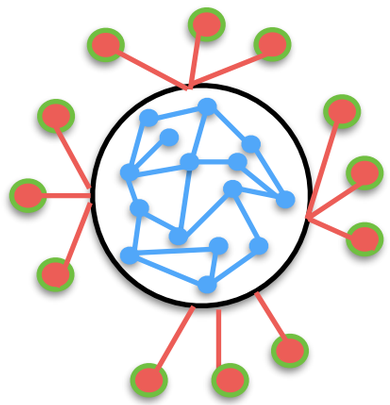
区块链

区块链发展现状

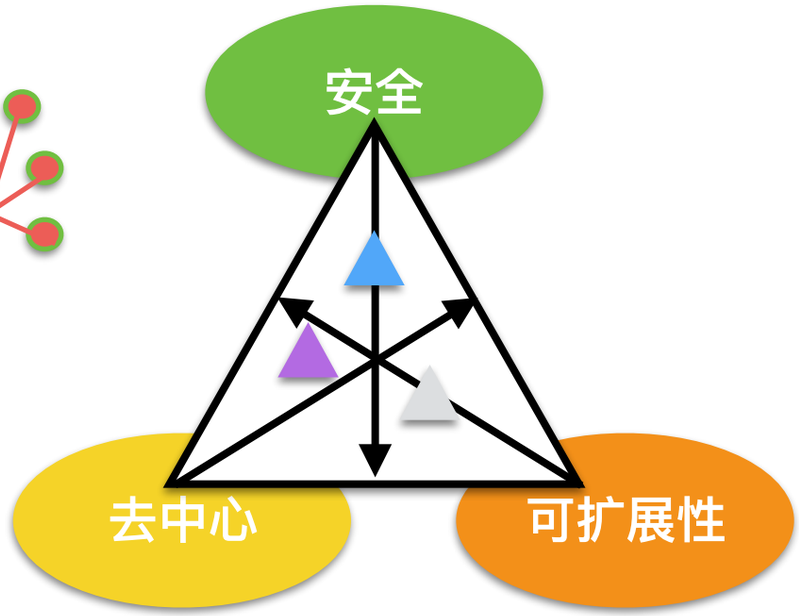
安全 信任 隐私

增加信任





数据上链

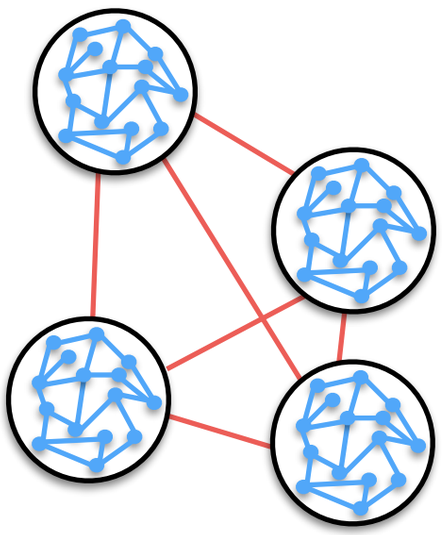


2009

公链

智能合约

适度去中心



货币

ICO

私有区块链

1.0

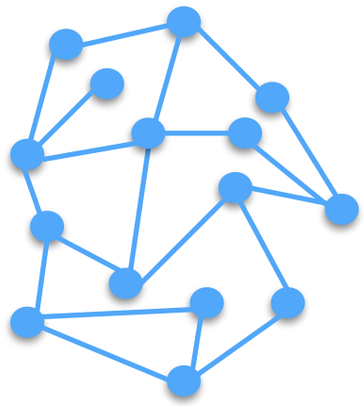
2.0

Block chain

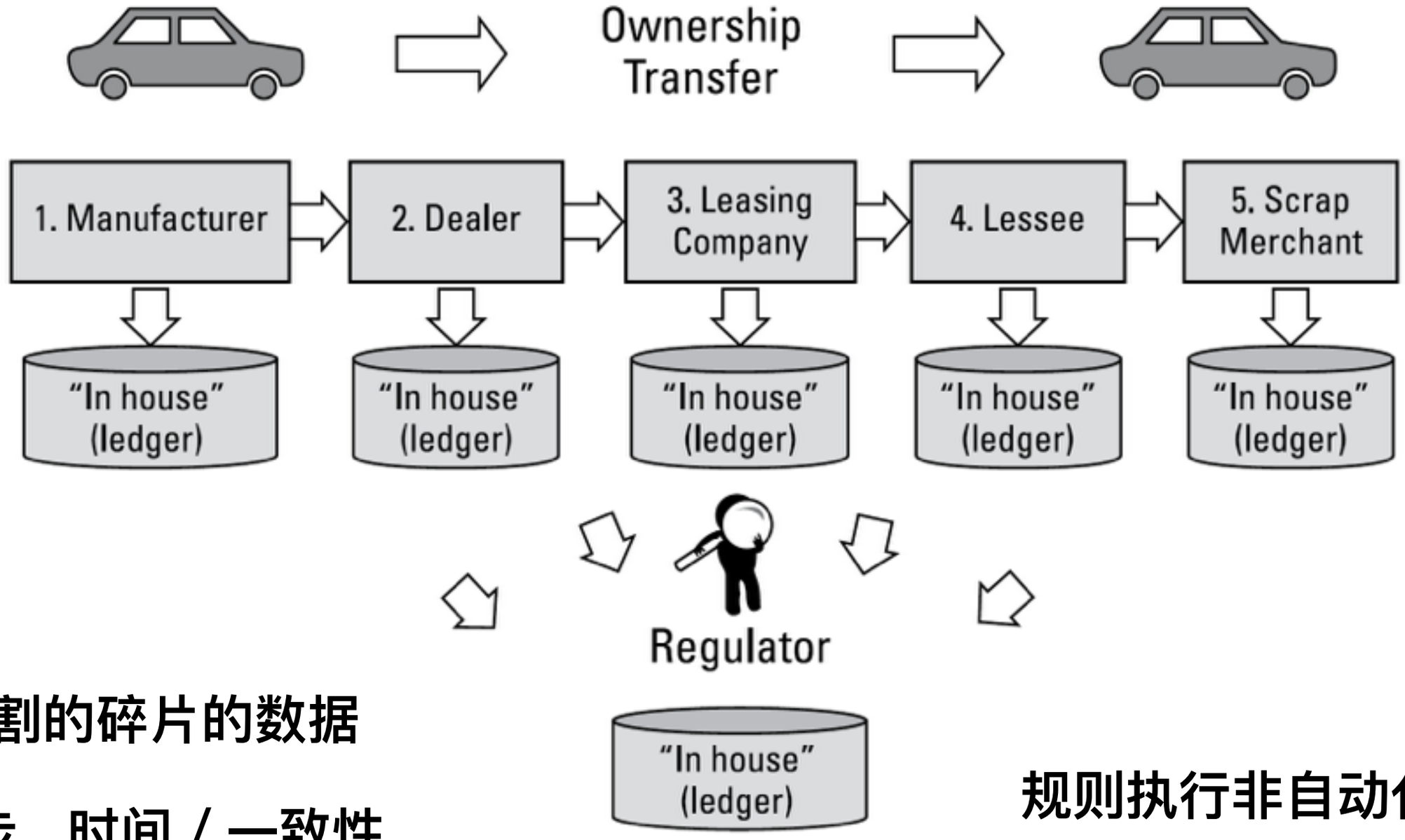
3.0

区块链＋

企业区块链



租车例子：没有区块链



分割的碎片的数据

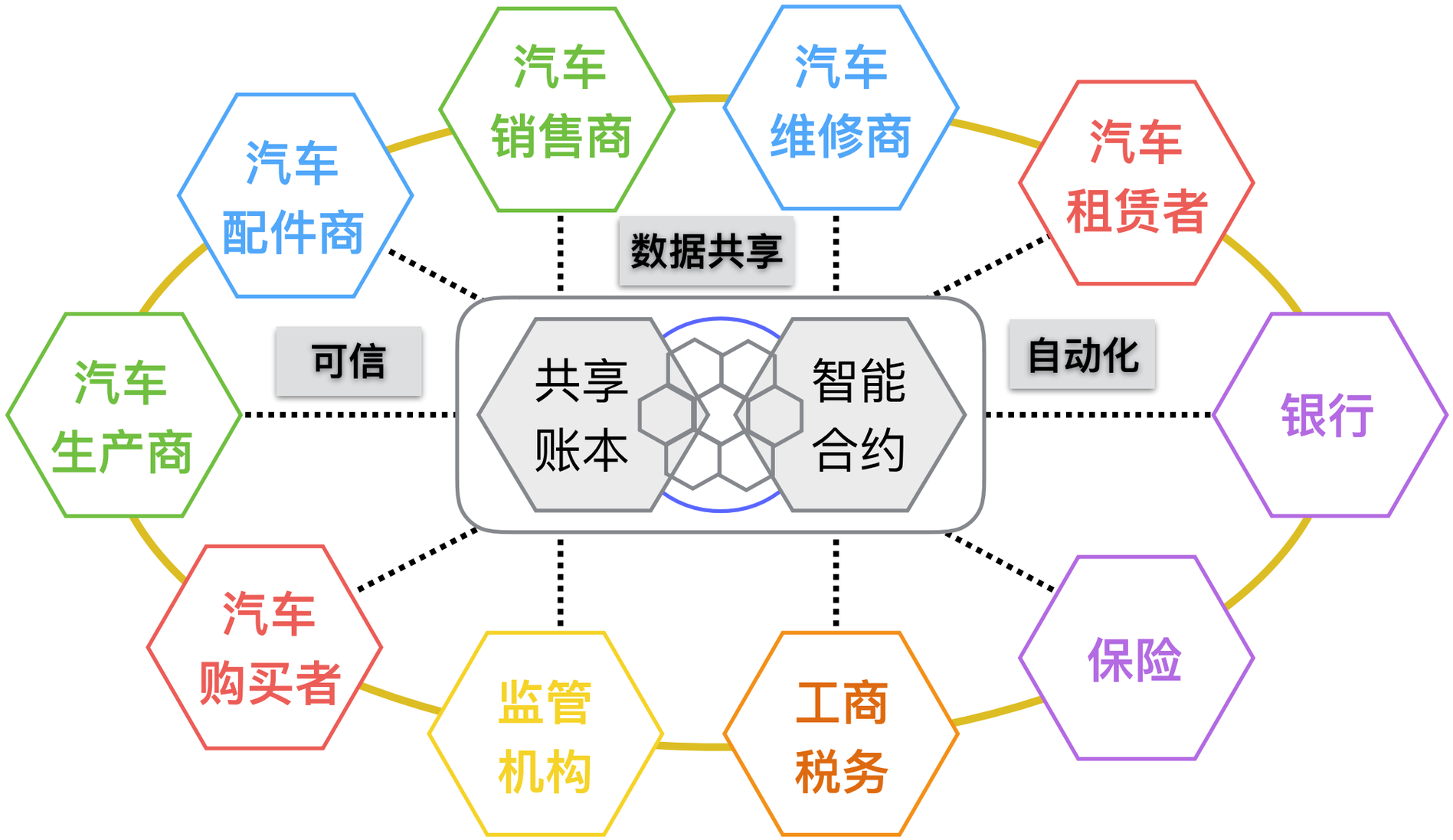
同步　时间 / 一致性

规则执行非自动化

区块链应用场景

数据一致性

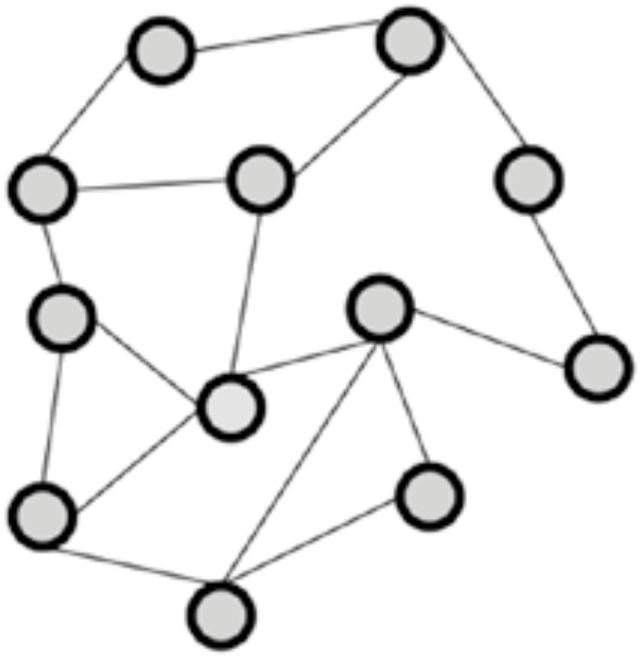
全生命周期管理



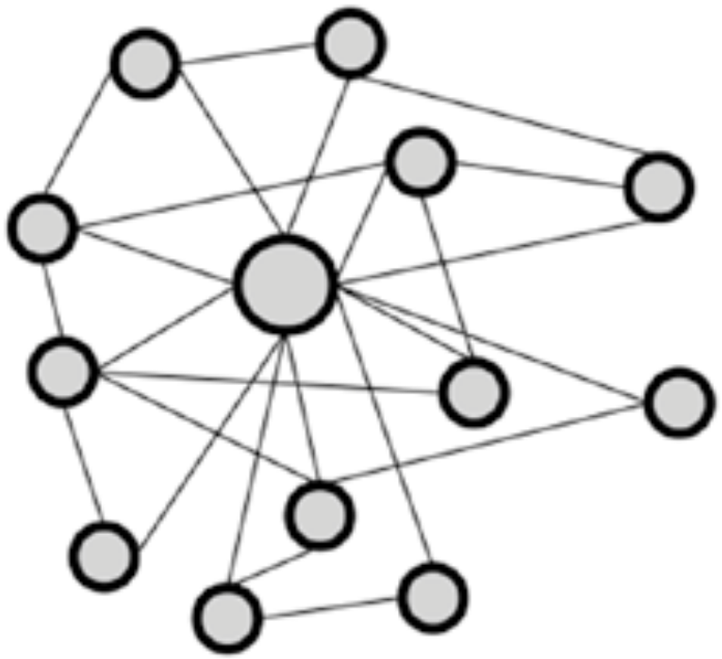
多中心

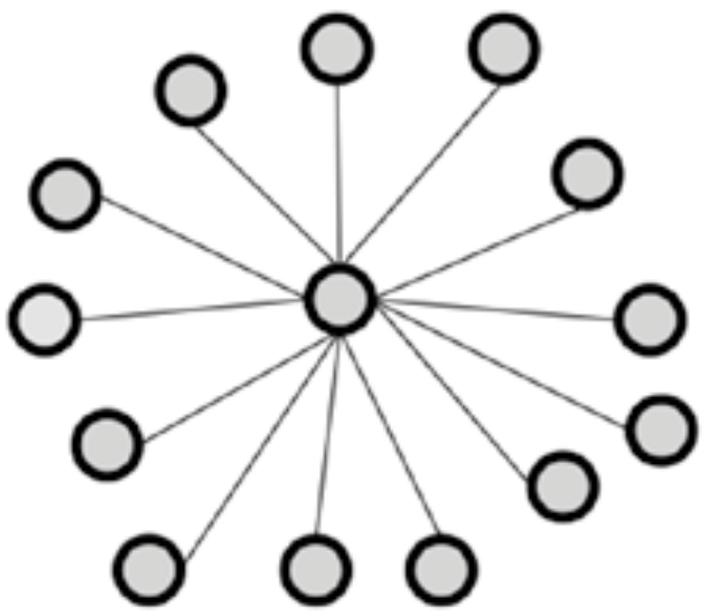
区块链增信

分布还是集中

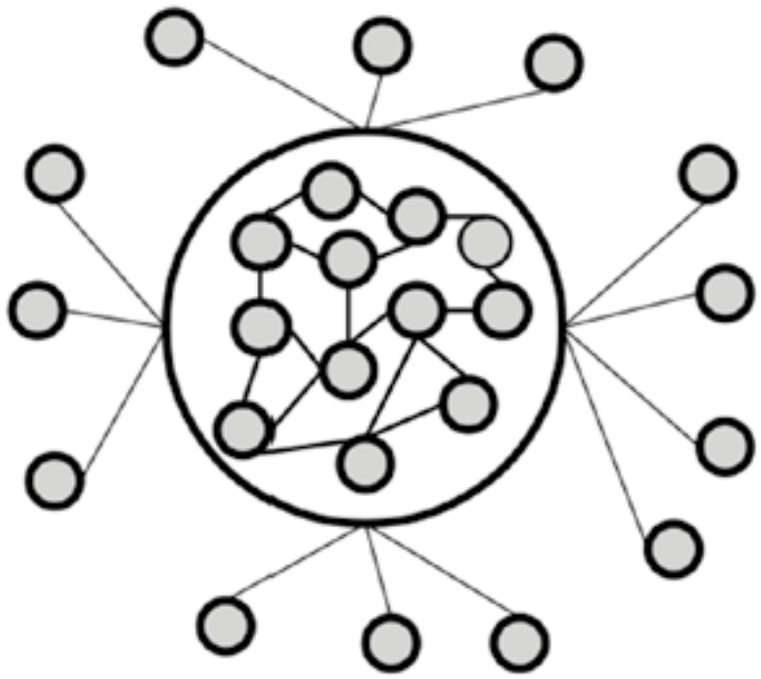


没有纯粹的
中心化系统
或者
分布式系统

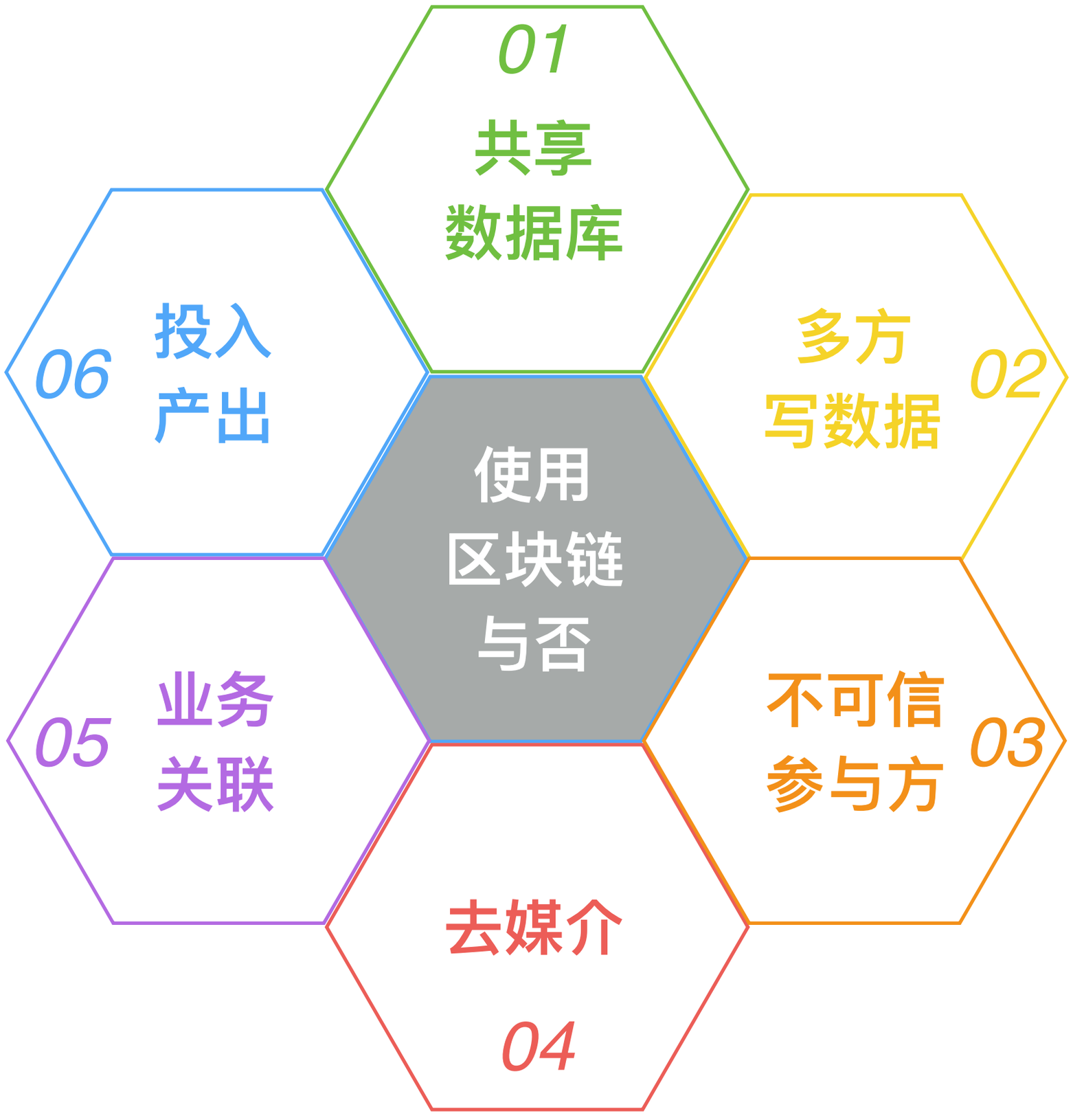




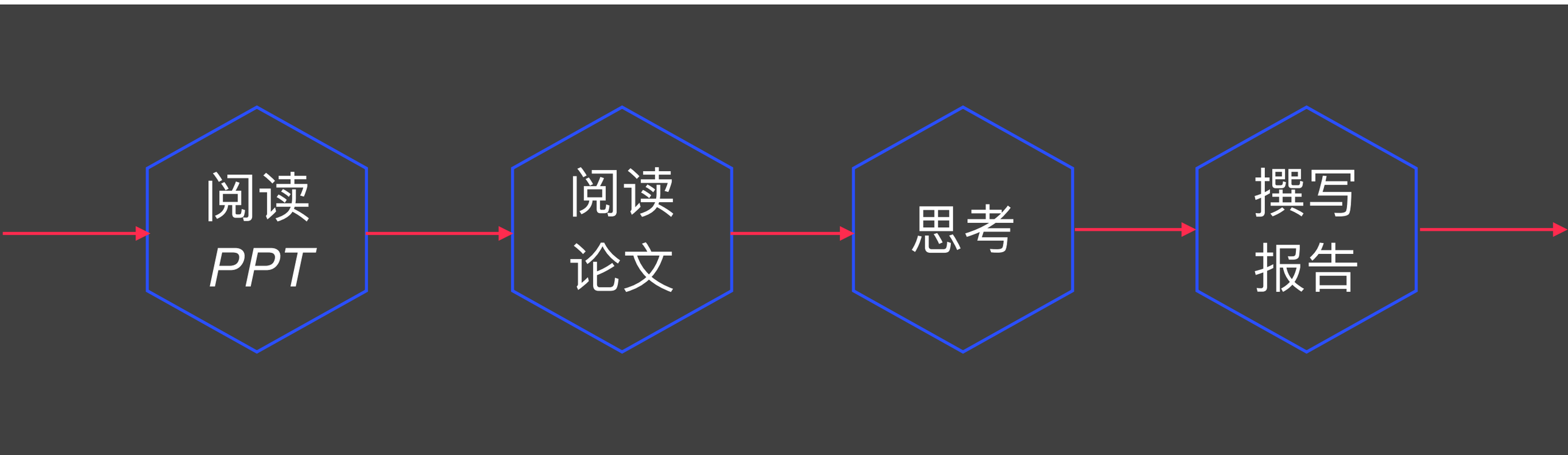
Internet
Email
IM
SNS



是否需要使用区块链



课后作业



Homework

课后作业

要求阅读如下论文，写论文阅读报告

In IEEE SP 2015

2015 IEEE Symposium on Security and Privacy

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies

Joseph Bonneau*†‡, Andrew Miller§, Jeremy Clark¶, Arvind Narayanan*, Joshua A. Kroll*, Edward W. Felten*
*Princeton University, †Stanford University, ‡Electronic Frontier Foundation, §University of Maryland, ¶Concordia University

https://ieeexplore.ieee.org/document/7163021

选择一篇引用该文的论文，阅读该论文
并在论文阅读报告中简单介绍

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

12月20日晚上
12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io