区块链简介

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

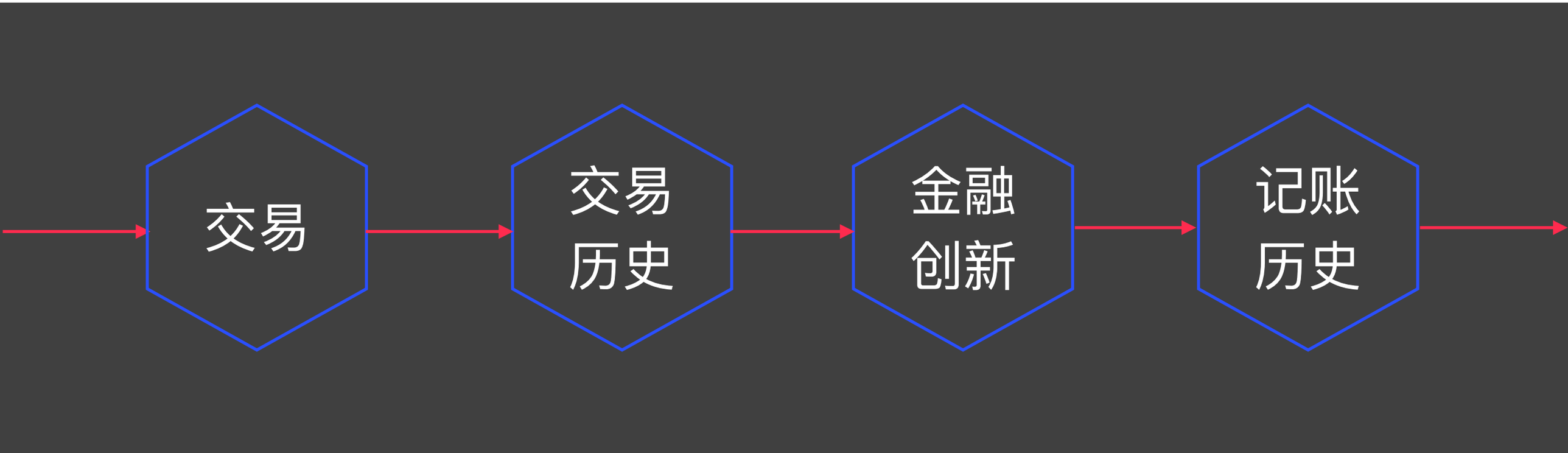
Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

Course Overview

上次课程内容

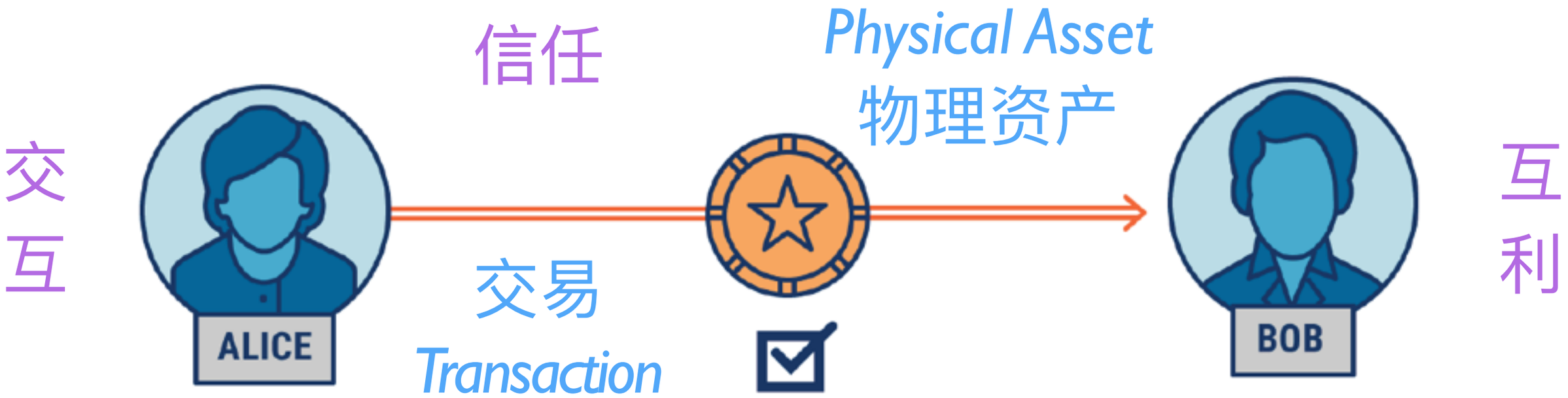
1 简介	2 系统	3 类型	4 挑战
• 定义 • 历史&现状 • 优缺点 • 应用&挑战	• 生物特征 • 注册&模版 • 匹配 • 指标	• 指纹&脸型 • 手型&语音 • 虹膜视网膜 • 签名&击键	• 唯一性 • 持久性 • 欺骗&攻击 • 验活&隐私

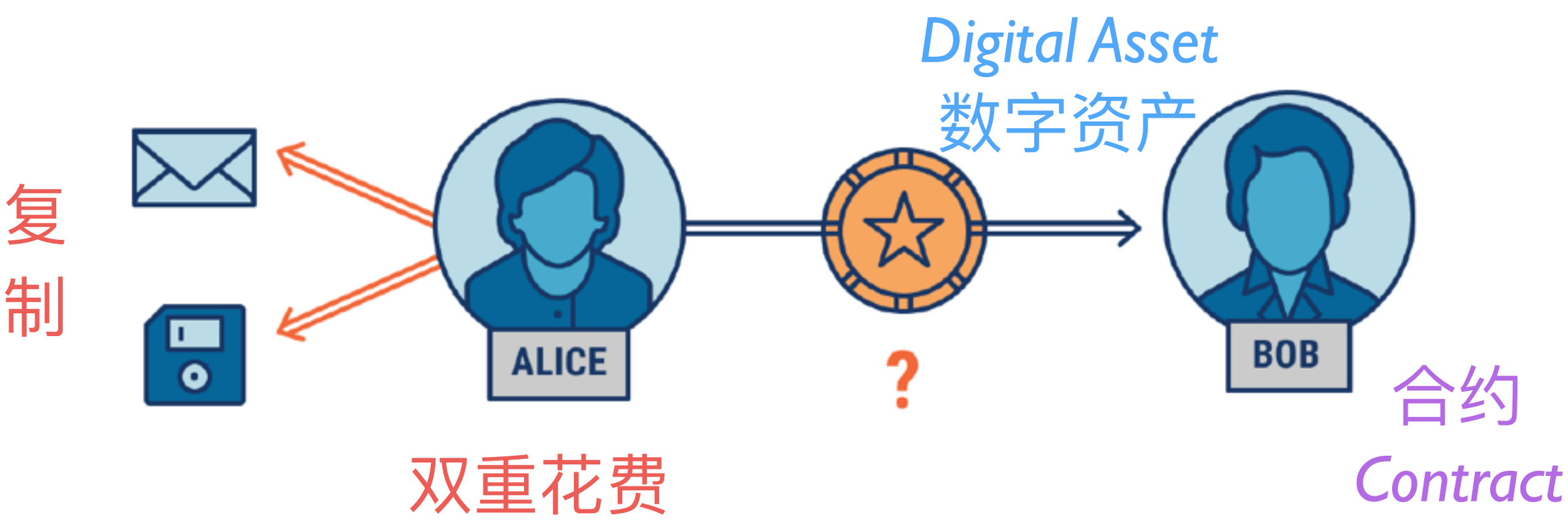
史前



交易：物理 vs. 数字

What is Blockchain Technology @ CBSInsights





交易历史

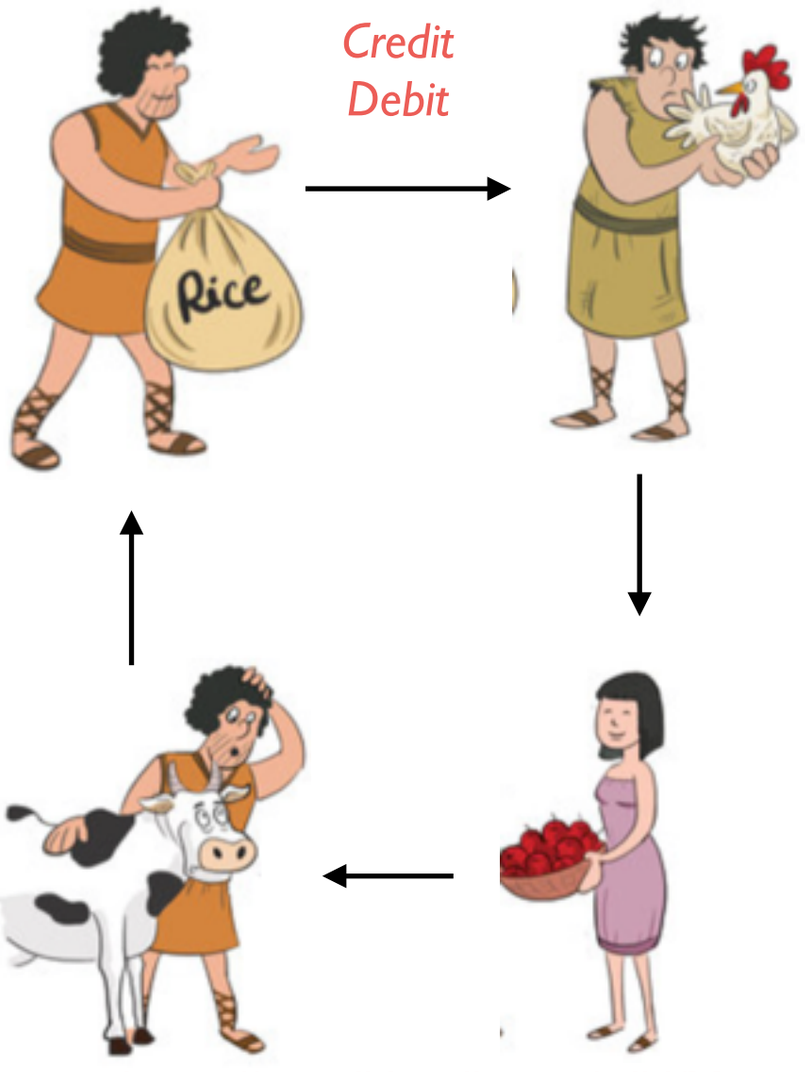
Barter

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

Money

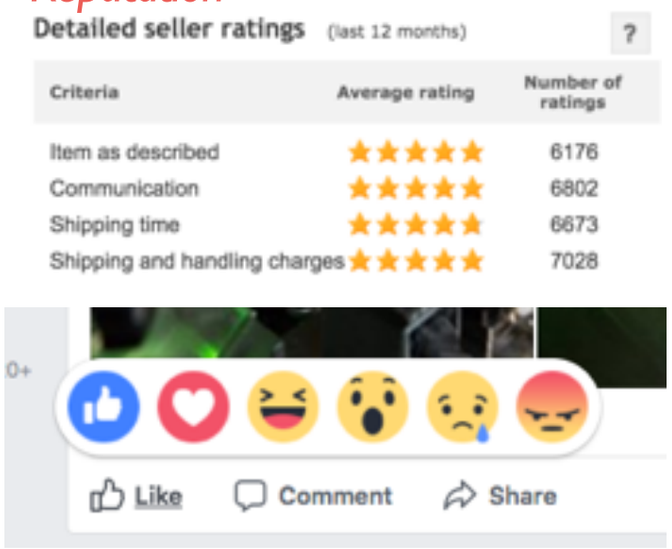
https://en.wikipedia.org/wiki/Credit

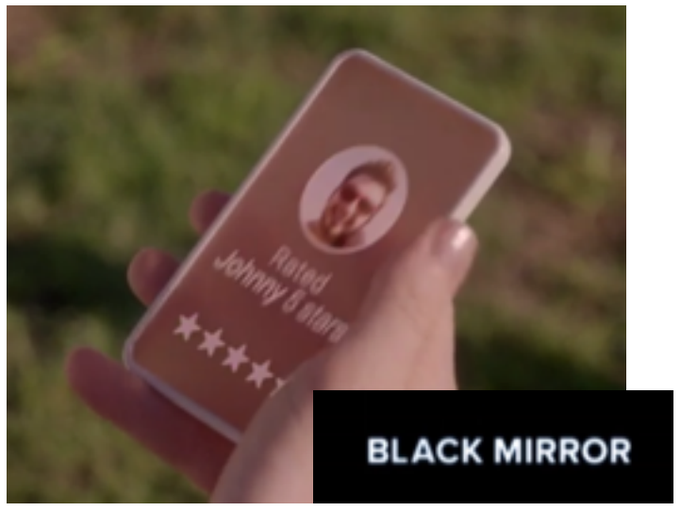
Credit
Debit

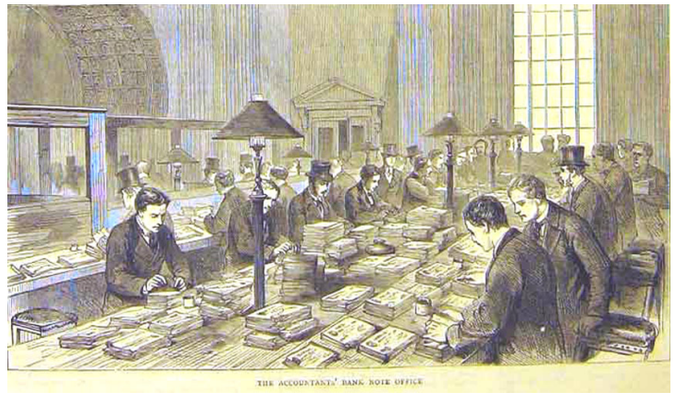


https://en.wikipedia.org/wiki/Money

Reputation





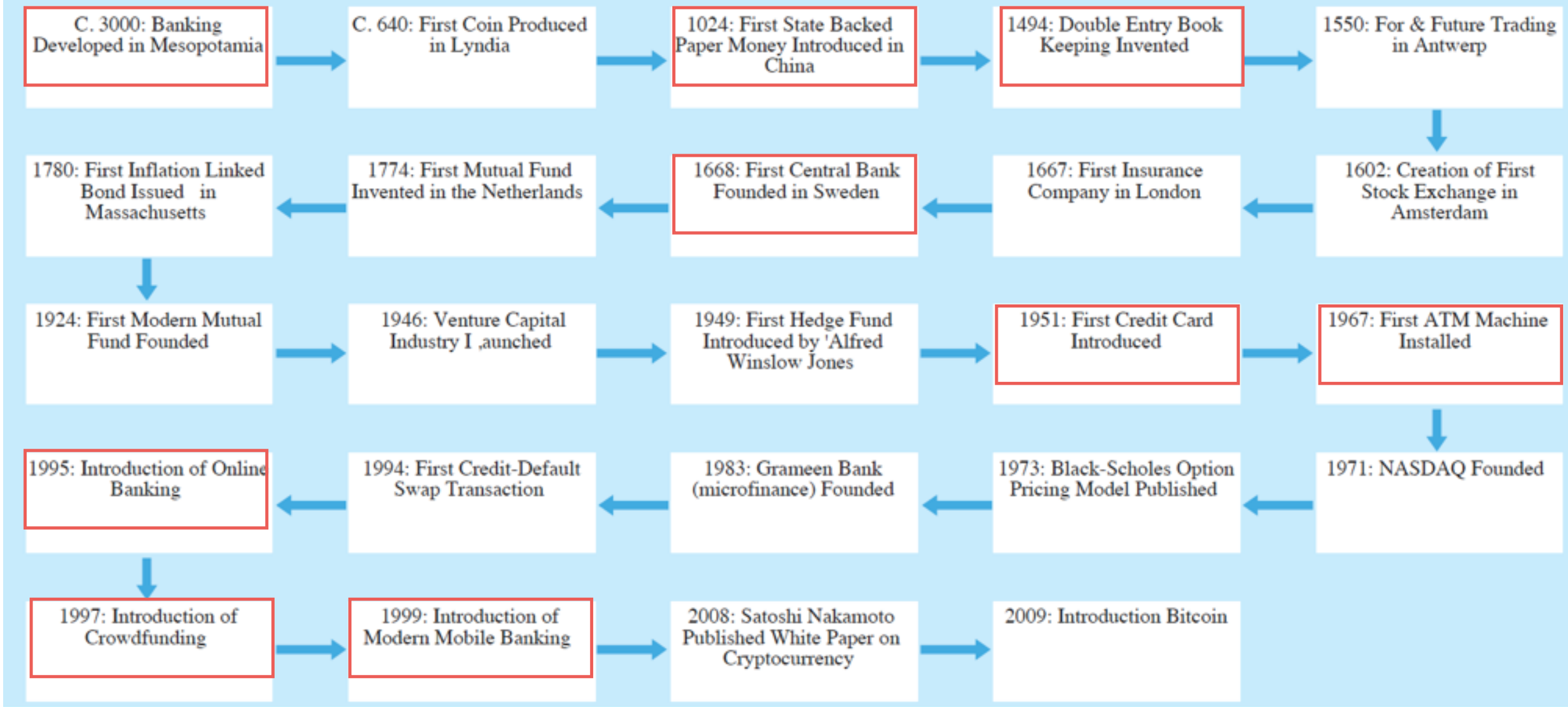


Bank

Credit Card

金融创新

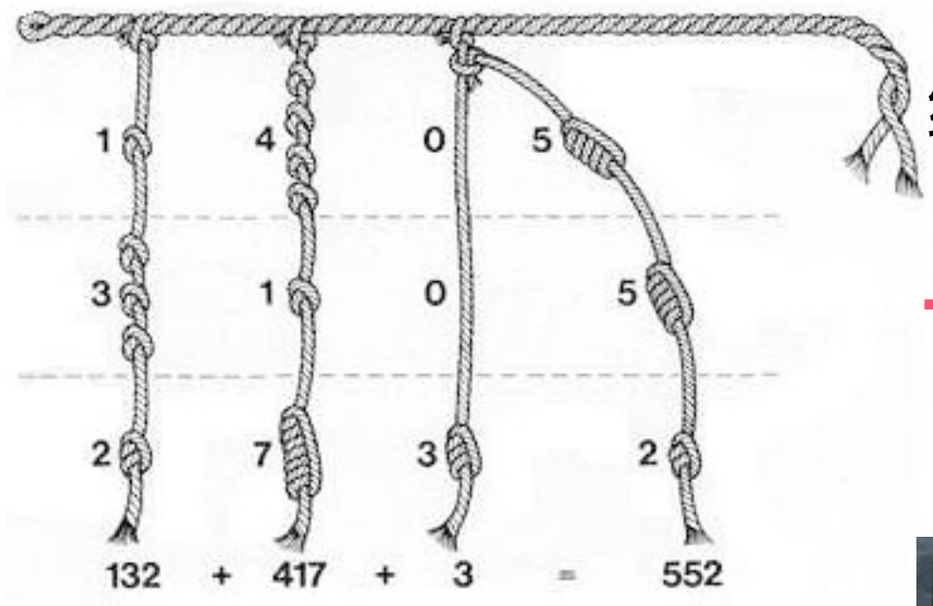
→ 金钱 → 纸币 → 复式记账 → 银行 → 信用卡 → ATM →



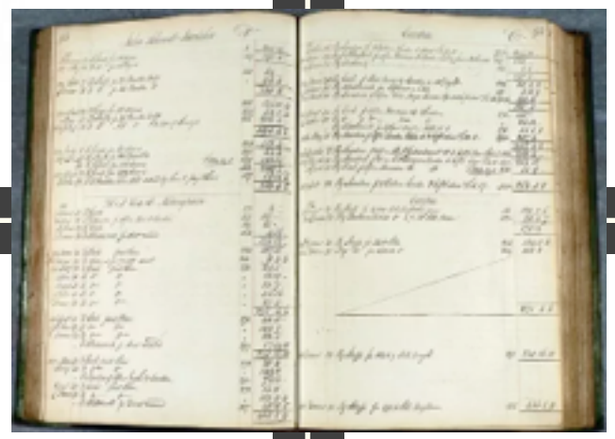
→ 在线银行 → 众筹 → 移动支付 → Bitcoin → 区块链 →

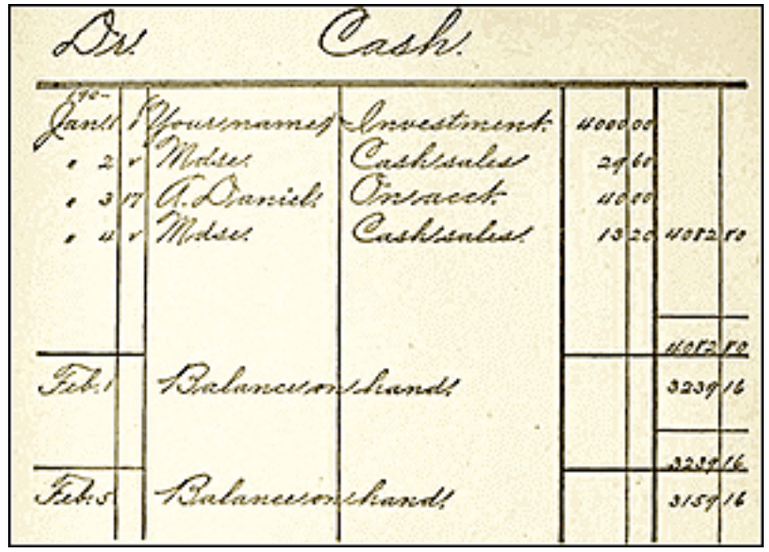
记账历史

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



结绳





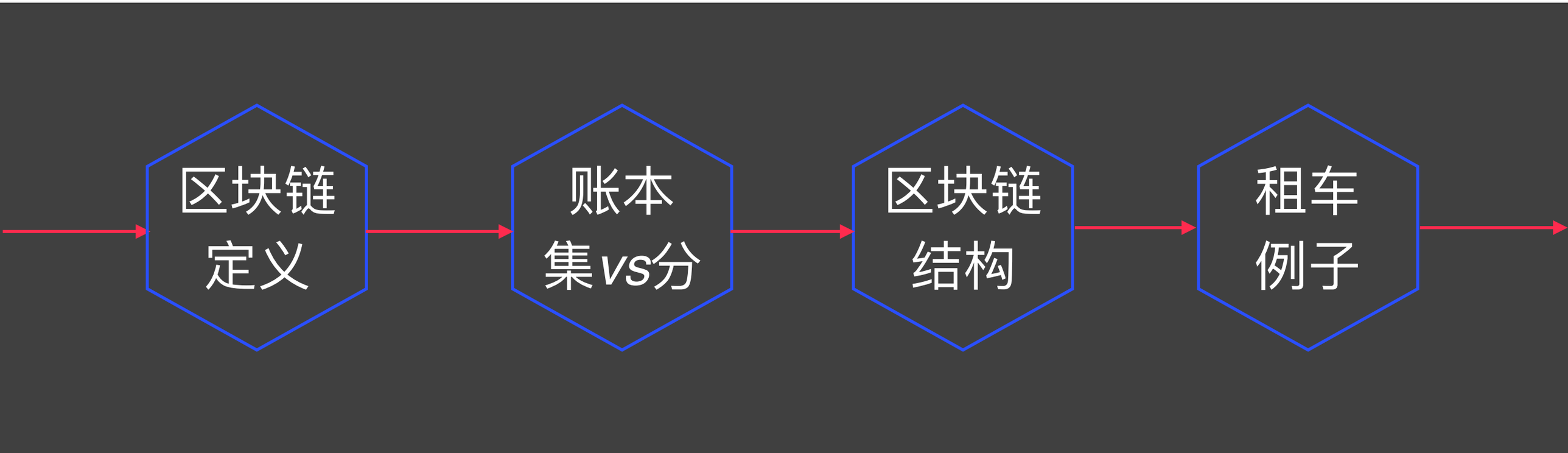
单式

复式

电子

物理

初识



Blockchain
Overview

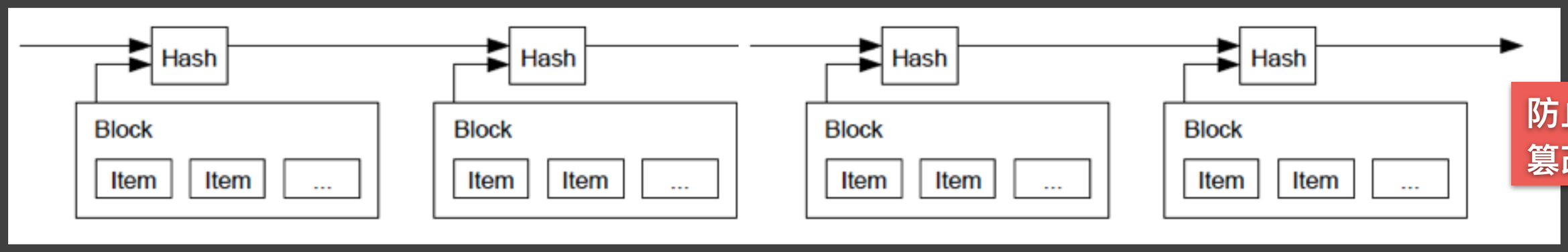
区块链定义

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

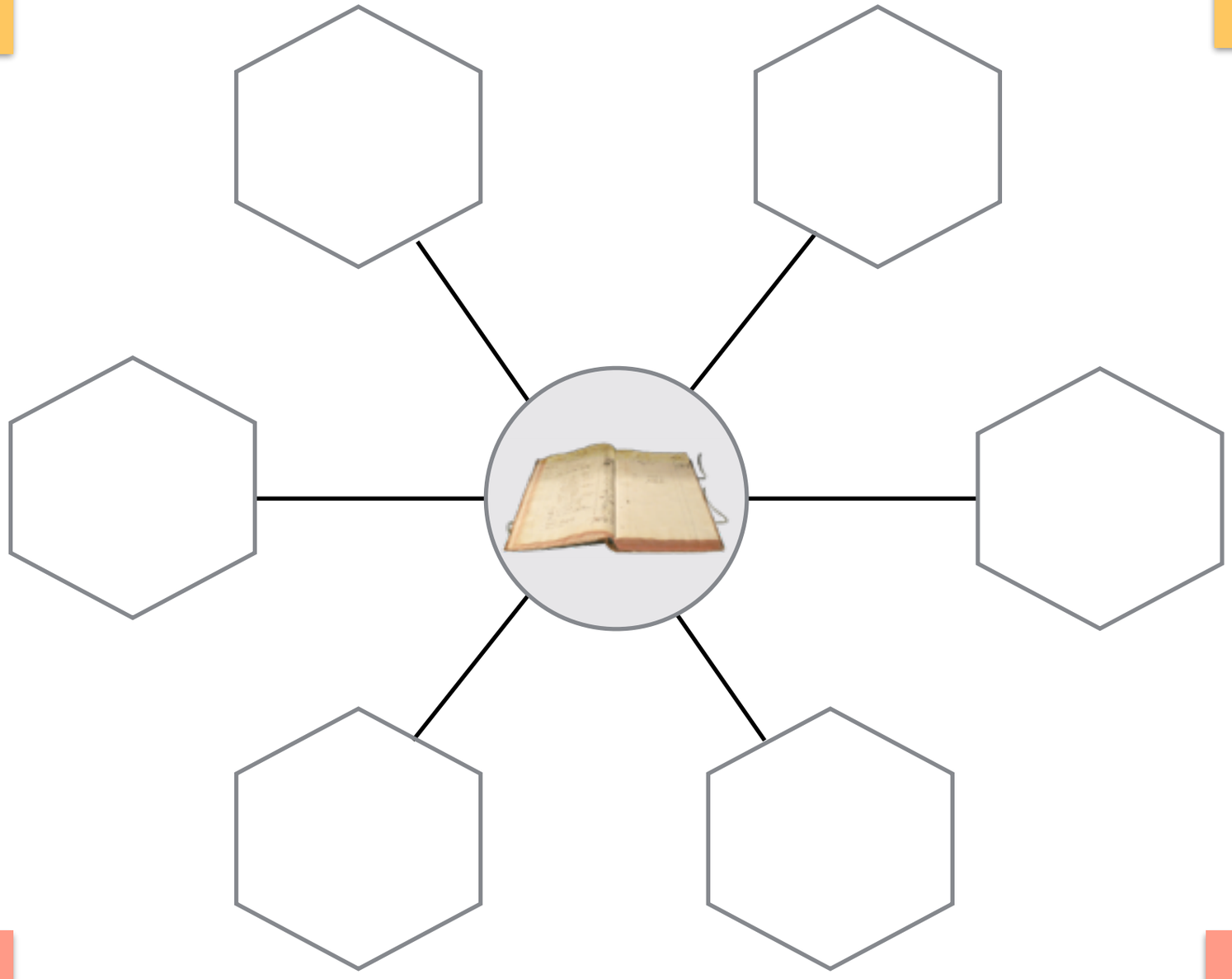
中心

P2P

集中式账本的优缺点

中心化

第三方



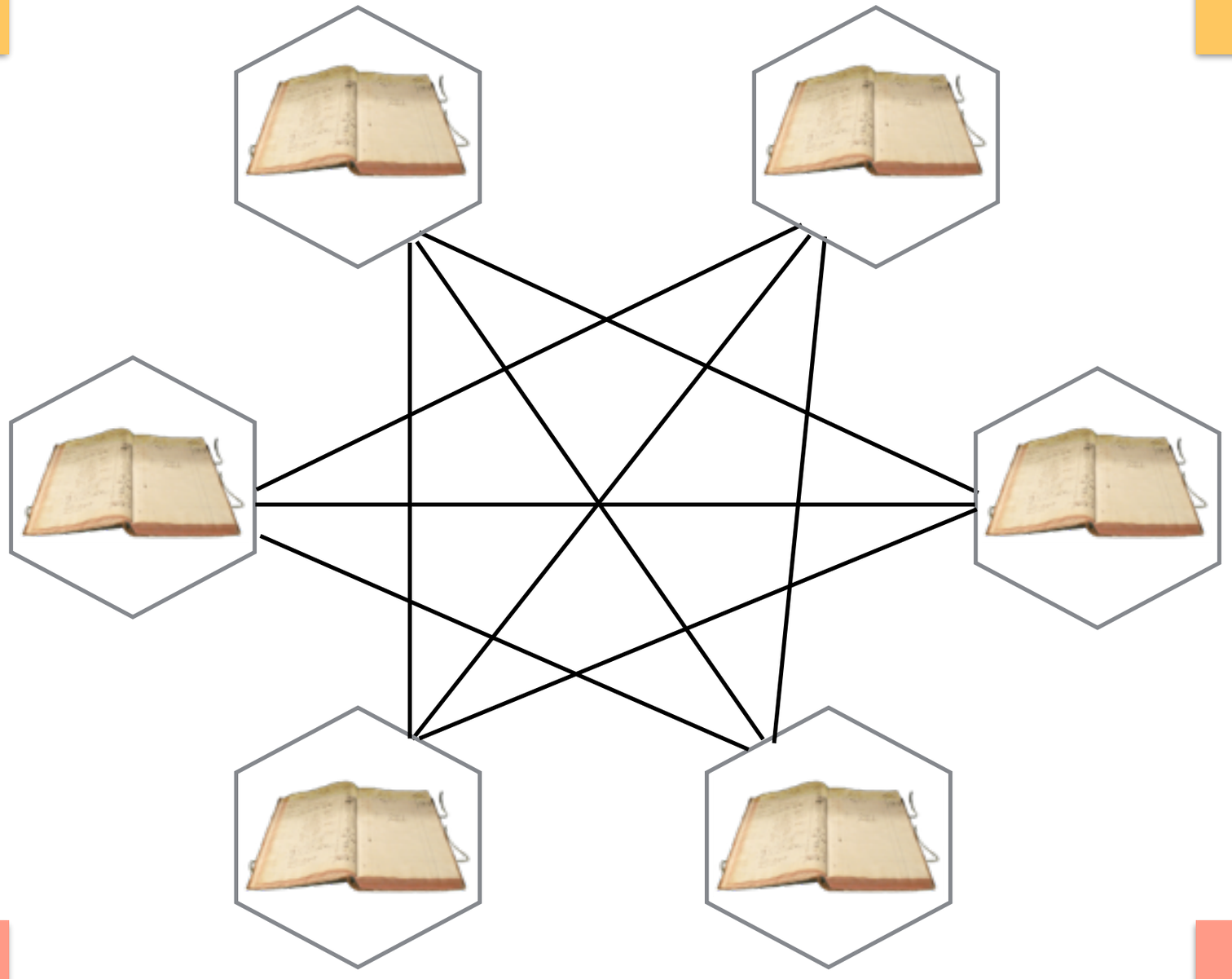
脆弱

信任

分布式账本的优缺点

一致性

完整性



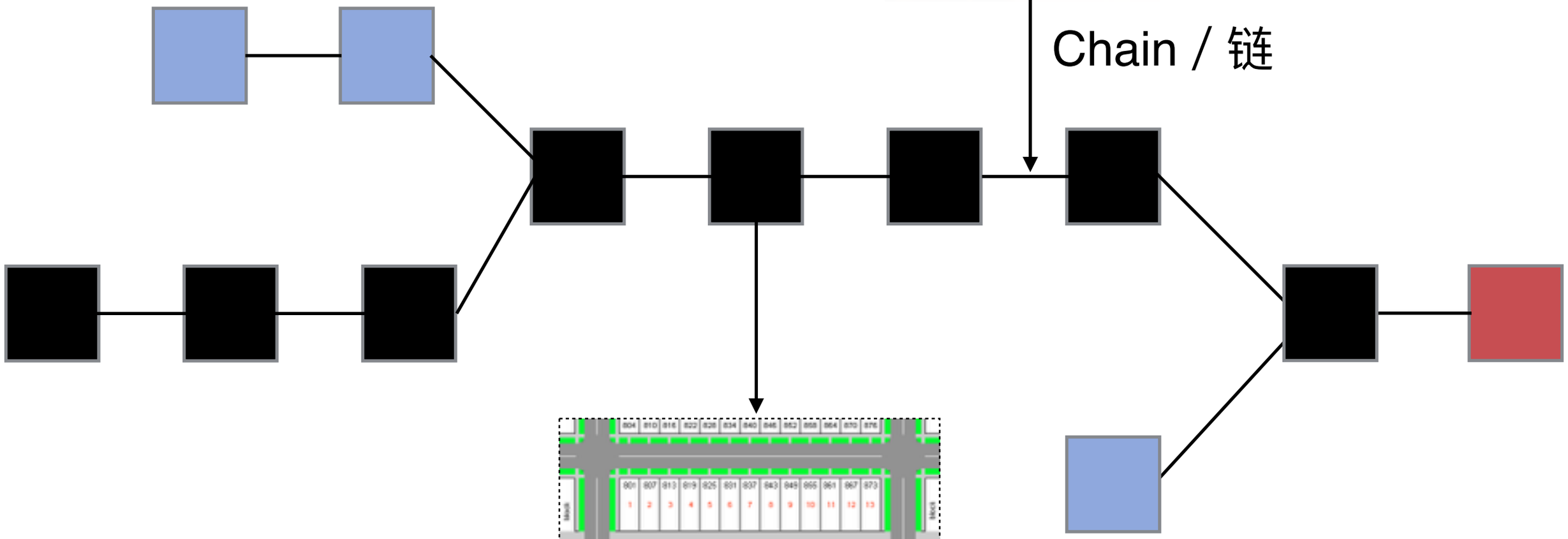
效率

花费

区块链结构

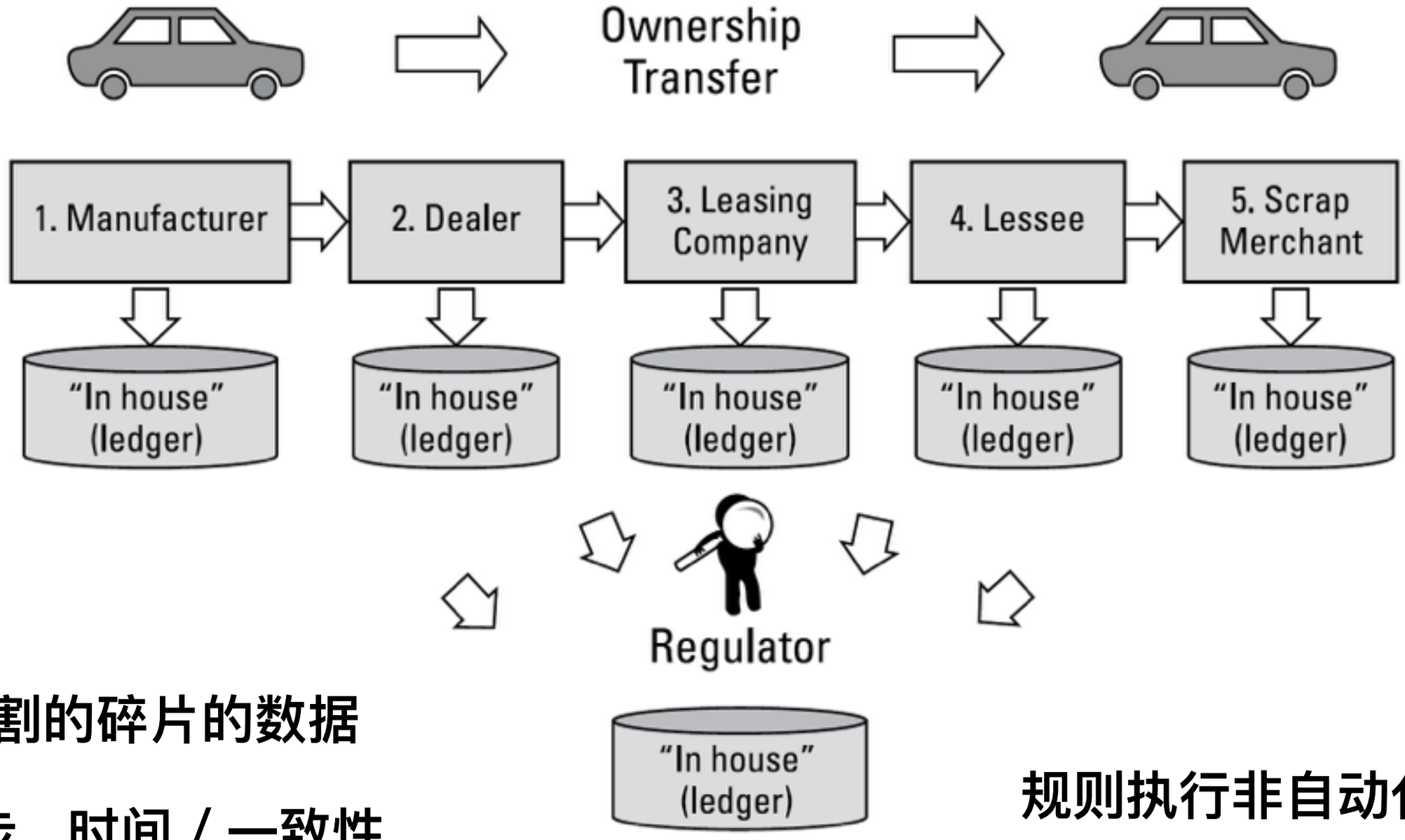
https://en.wikipedia.org/wiki/Blockchain

Chain / 链



Block / 区块

租车例子：没有区块链



分割的碎片的数据

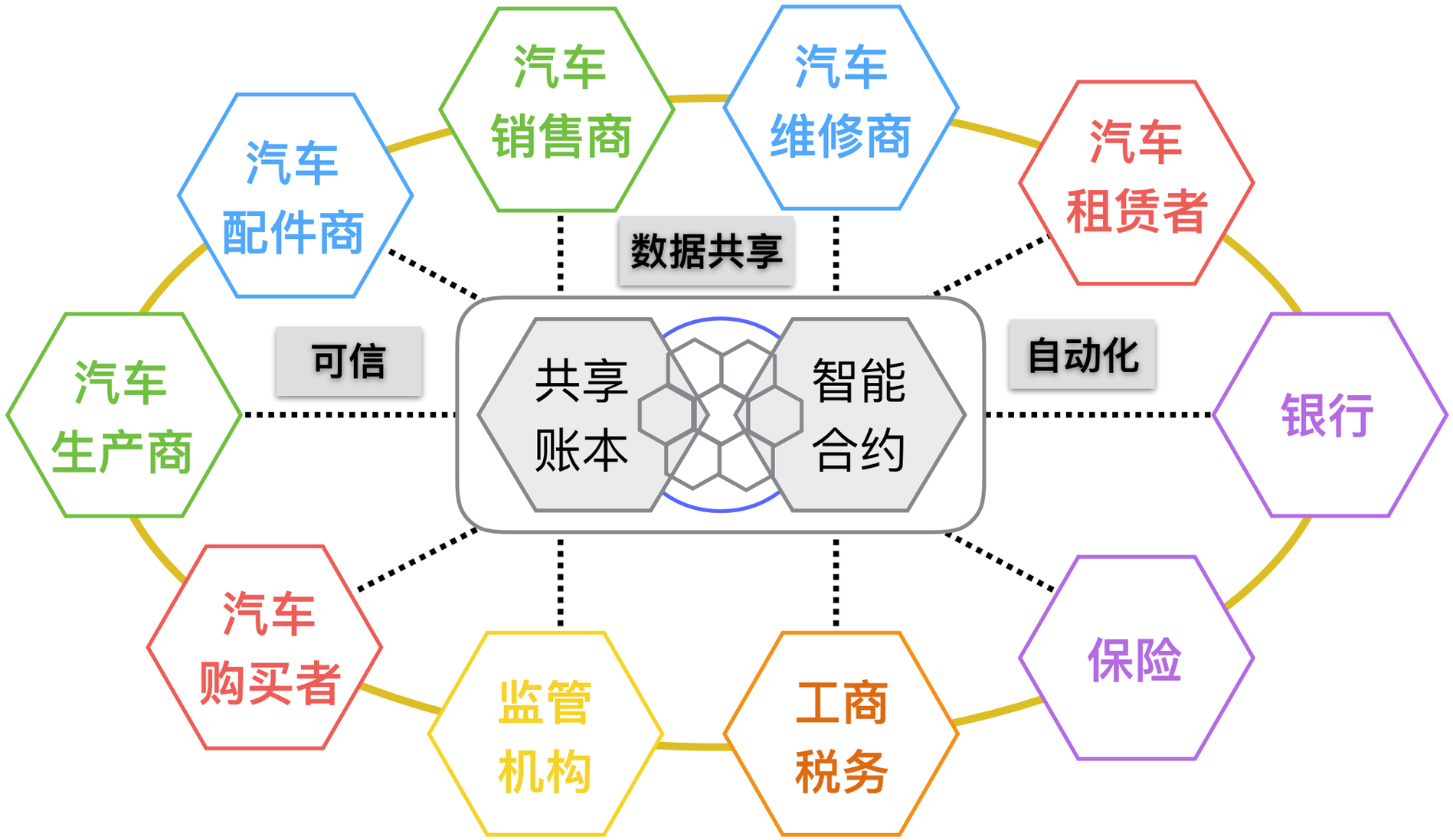
同步　时间 / 一致性

规则执行非自动化

区块链应用场景

数据一致性

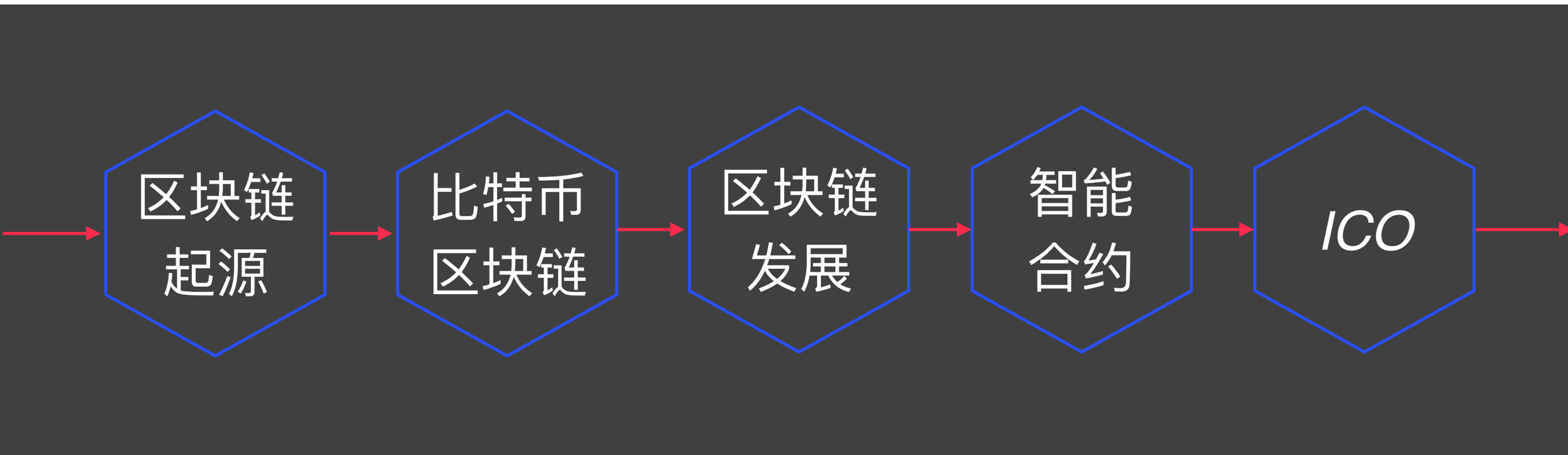
全生命周期管理



多中心

区块链增信

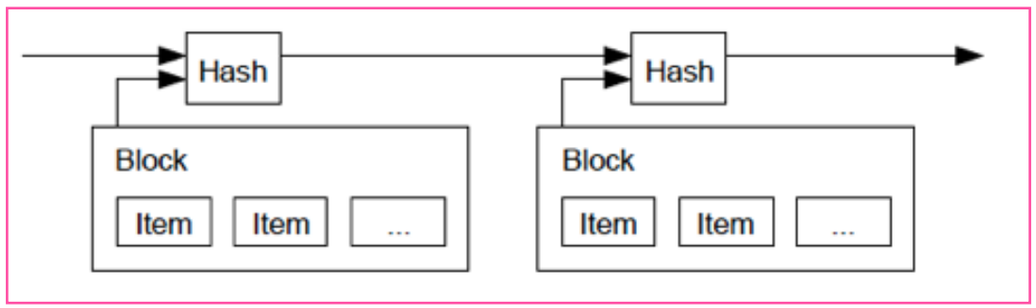
回顾



区块链起源

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System



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

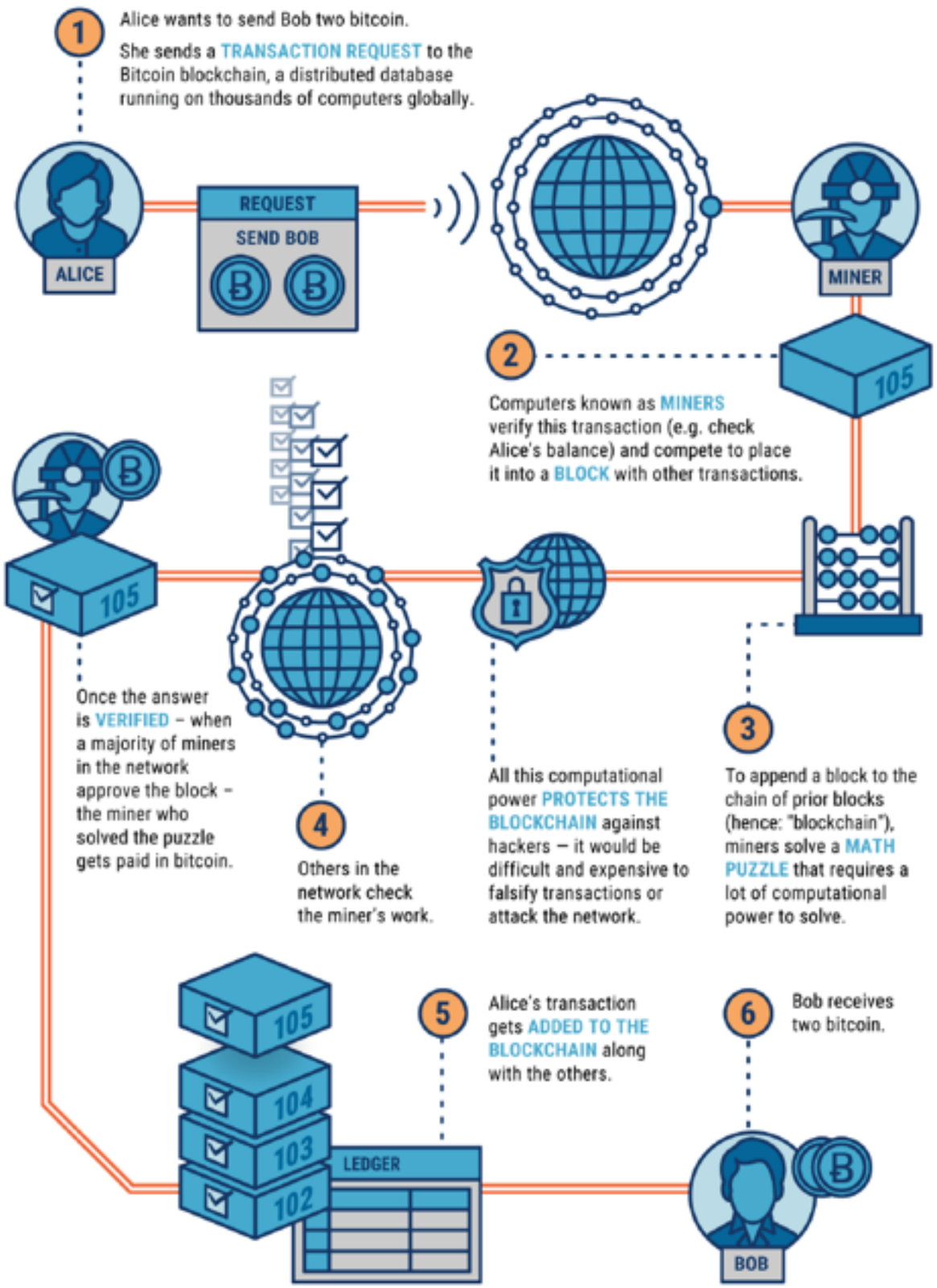
2008

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.

Blockchain Overview

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

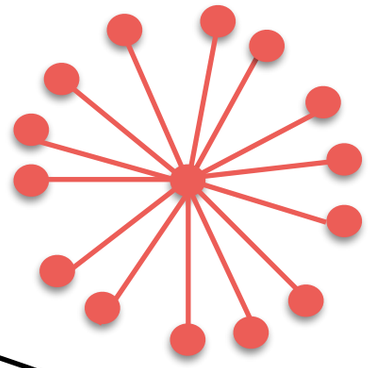
EOS ... ...

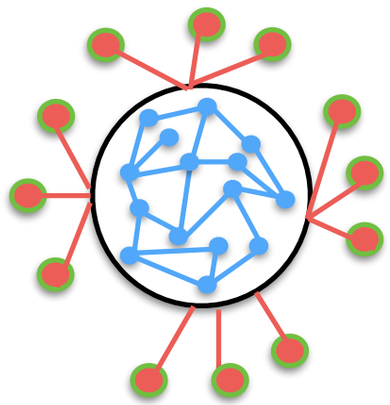
区块链

区块链发展现状

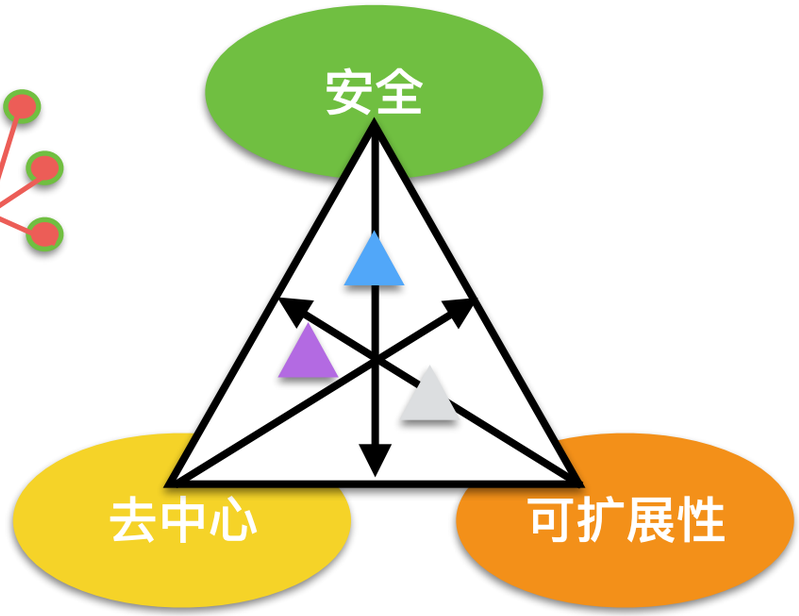
安全 信任 隐私

增加信任

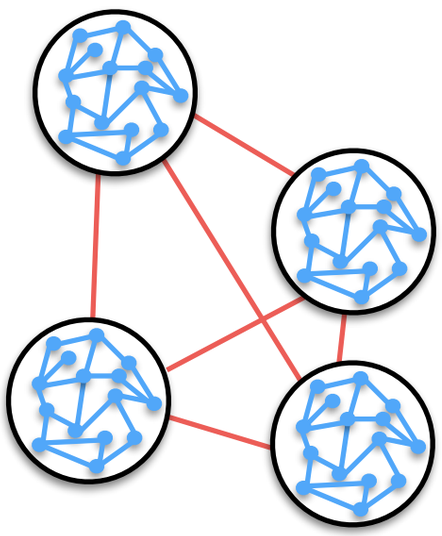


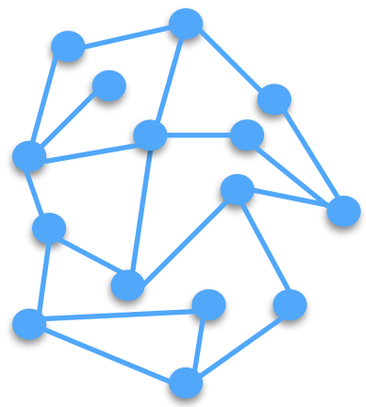


数据上链



适度去中心





2009

公链

智能合约

货币

ICO

私有区块链

1.0

2.0

Block chain

3.0

区块链＋

企业区块链

智能合约

交易各方确定合约条款 → 合约被编码成代码 → 合约代码存储在区块链上 → 合约条款满足时智能合约自动执行

传统合约

- 需要大量的文书
- 严重依赖第三方来执行
- 执行不力需要仲裁和司法

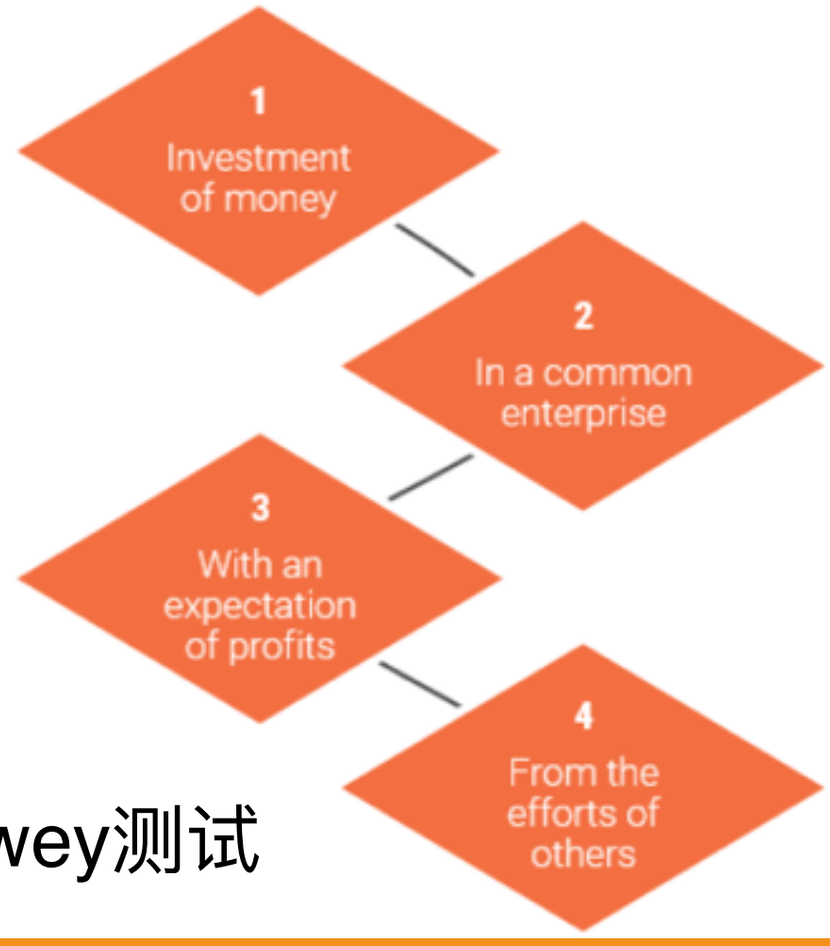
智能合约

- 完全数字化
- 自动执行
- 代码定义规则

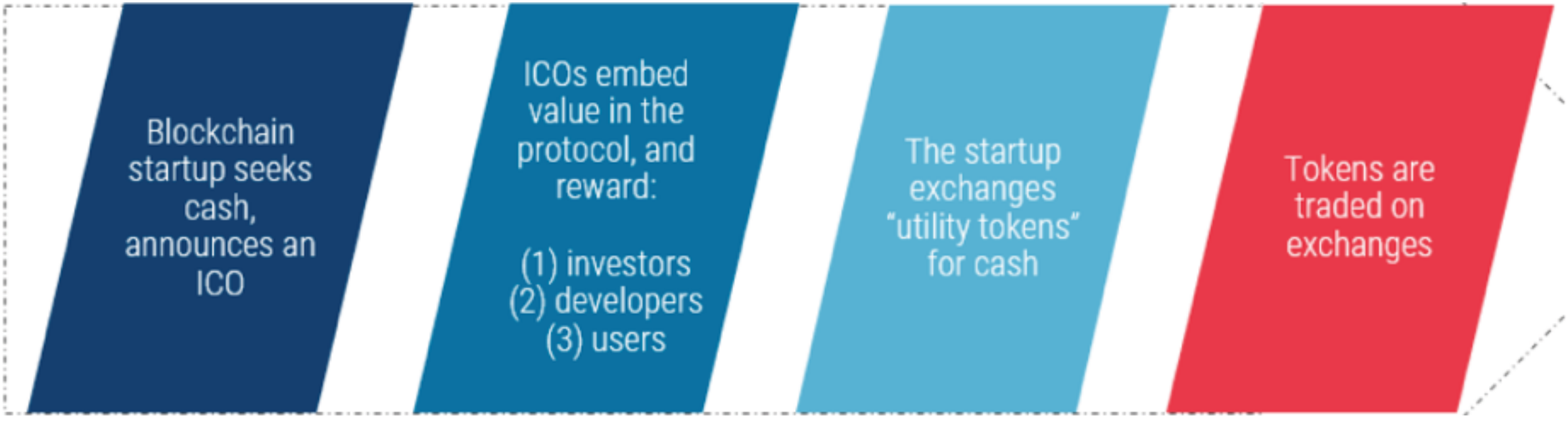
ICO

- Initial Coin Offering
- Token
- SEC：证券
- 空气币
- 2017年：ICO年

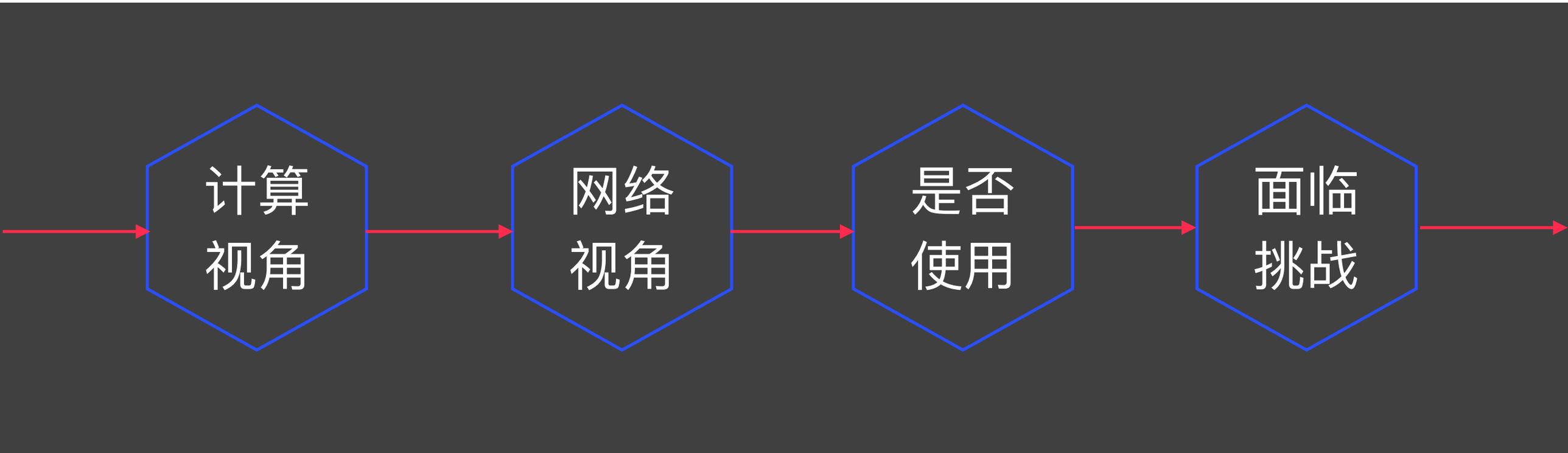
What is Blockchain Technology @ CBSInsights



Howey测试



剖析



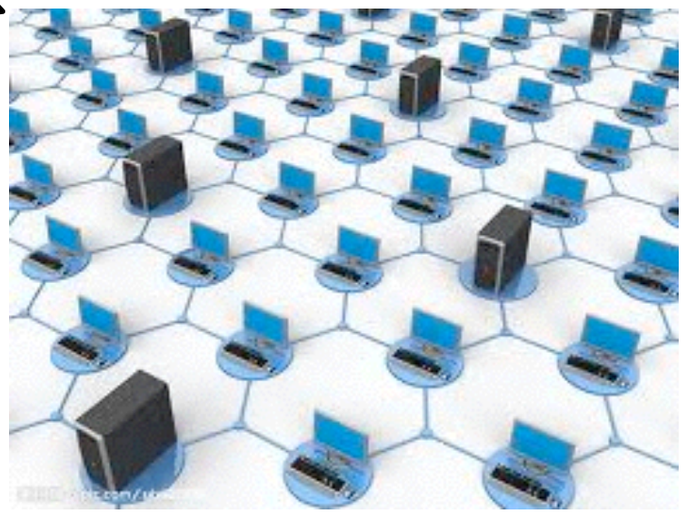
计算视角看区块链

?

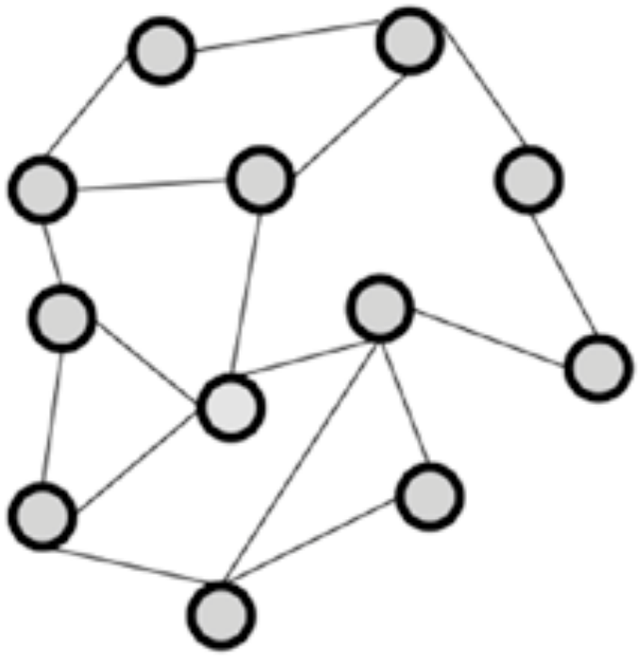
P2P

区块链

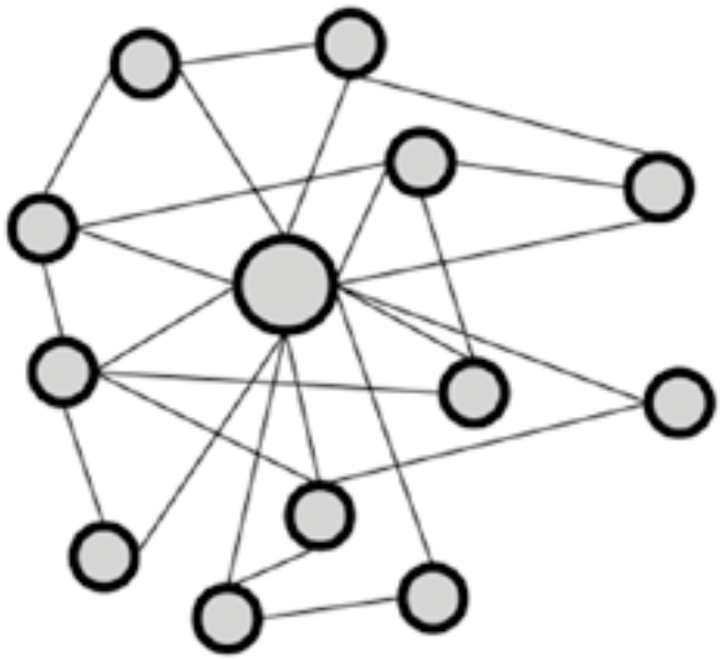
Client-Server

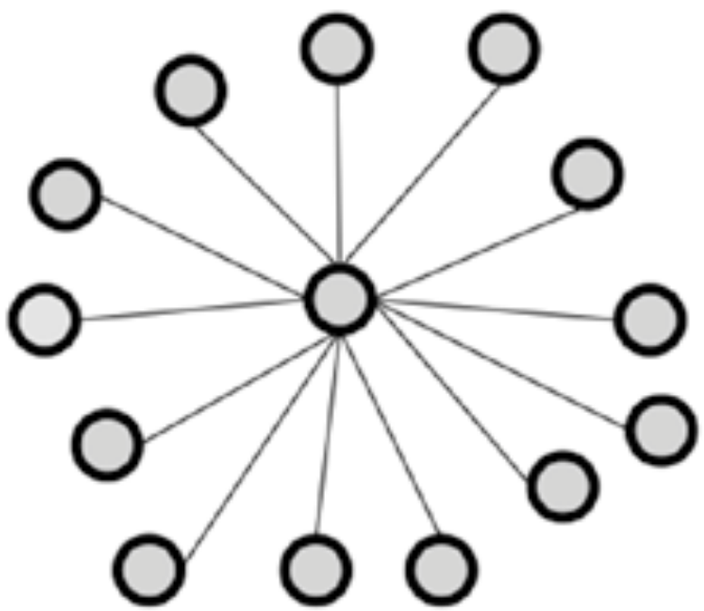


网络视角看区块链

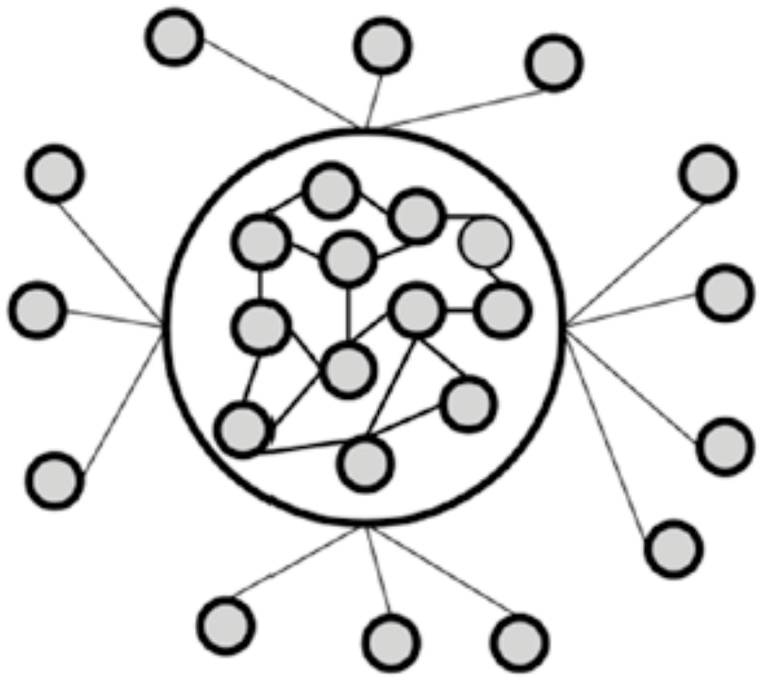


没有纯粹的
中心化系统
或者
分布式系统

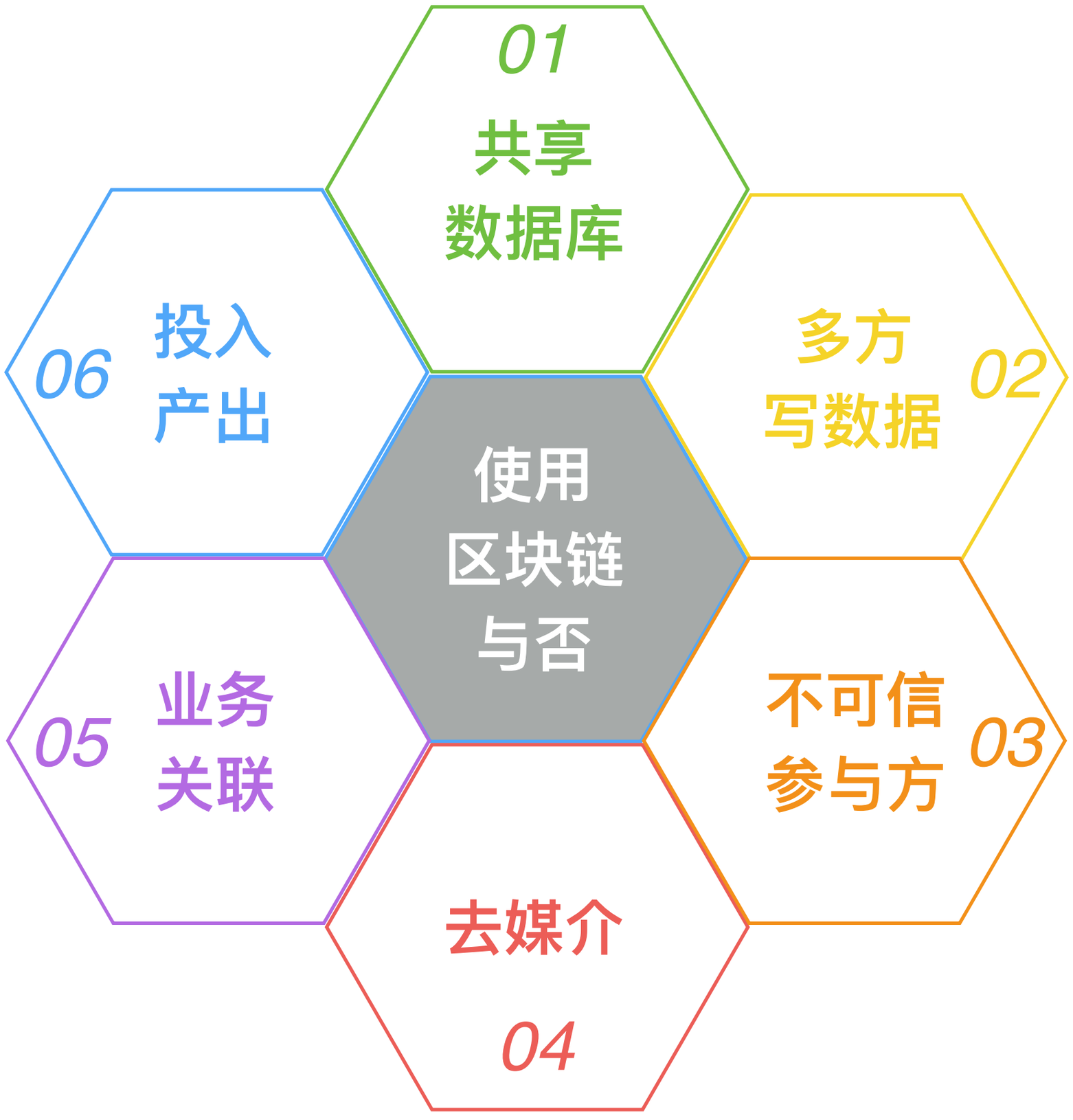




Internet
Email
IM
SNS



是否需要使用区块链



区块链面临挑战

隐私保护

匿名 ↔ 真实身份

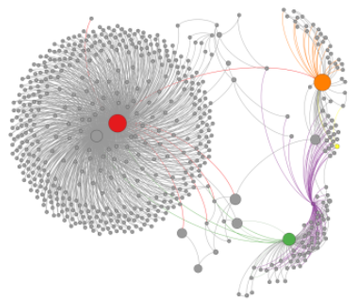
交易内容 ↔ 交易地址

内容隐私

访问控制

旁路攻击

聚类分析



上链数据

上链是有成本

链下数据如何保证真实性

性能扩展

PayPal 450

VISA 56000

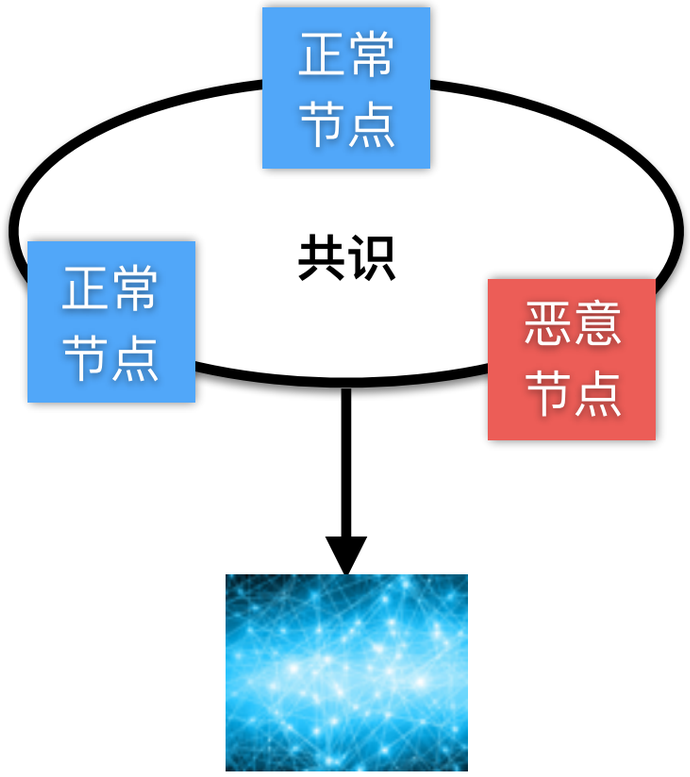
3

是否需要追求高的TPS

高TPS应用是否适合区块链

高不一定好，适合最好

安全是一种权衡

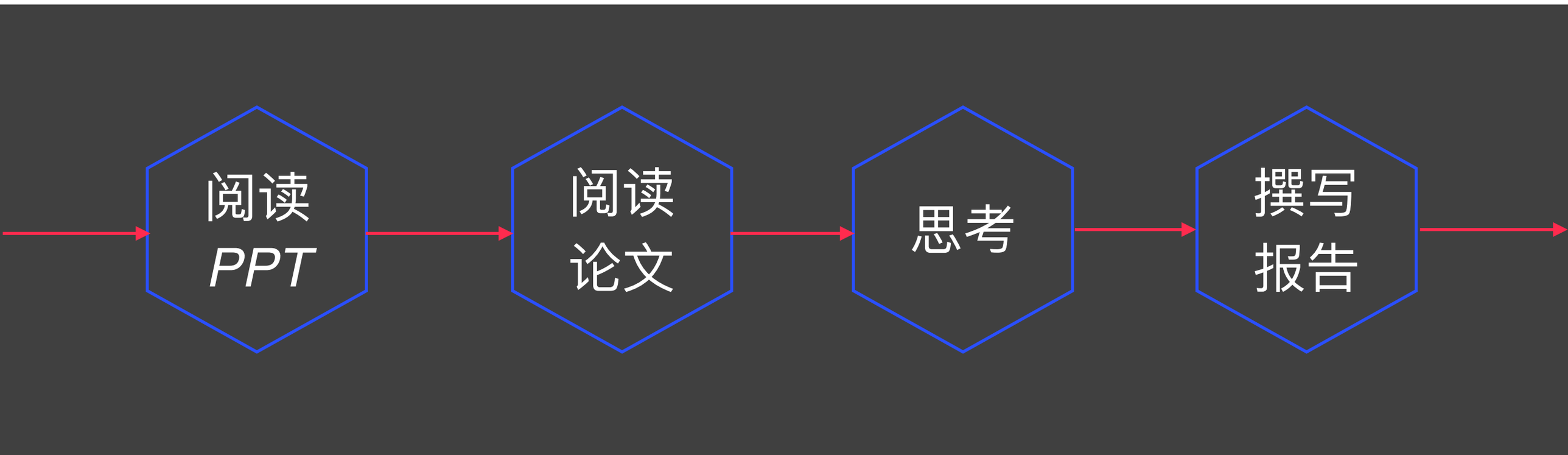


51%攻击

33.3%比例

安全攻击

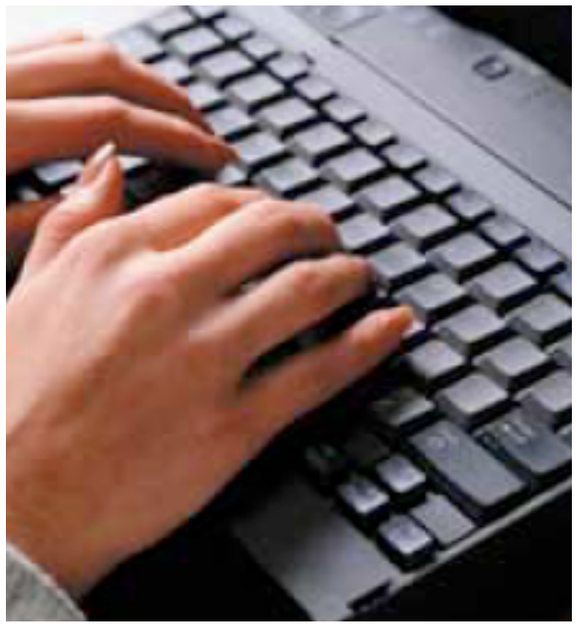
课后作业



Homework

课后作业

完成一个Demo



击键认证、*Keystroke*

1、算法描述

2、实现效果

3、存在问题

4、主要收获

5、改进空间

提交文档、PPT和代码

11月8日晚上
12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io