

区块链简介



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
- 验证&隐私

本次课程内容

1
史前

2
初识

3
回顾

4
剖析

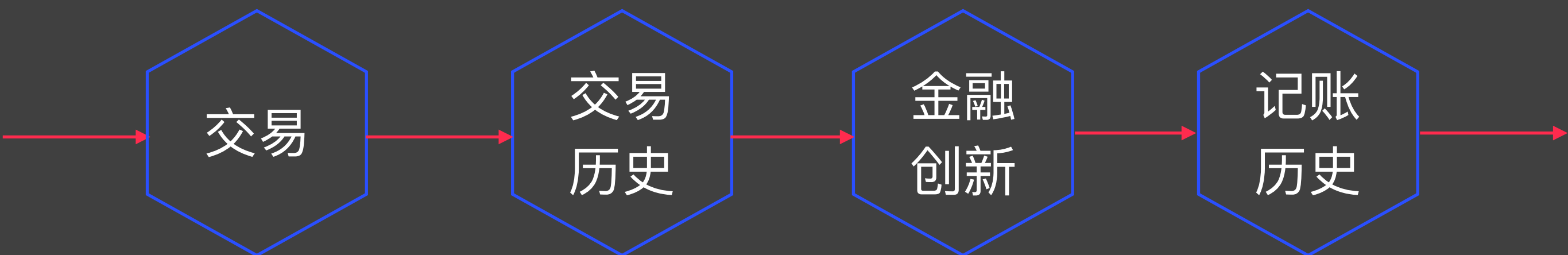
- 交易
- 交易历史
- 金融创新
- 记账历史

- 区块链定义
- 账本集vs.分
- 区块链结构
- 租车例子

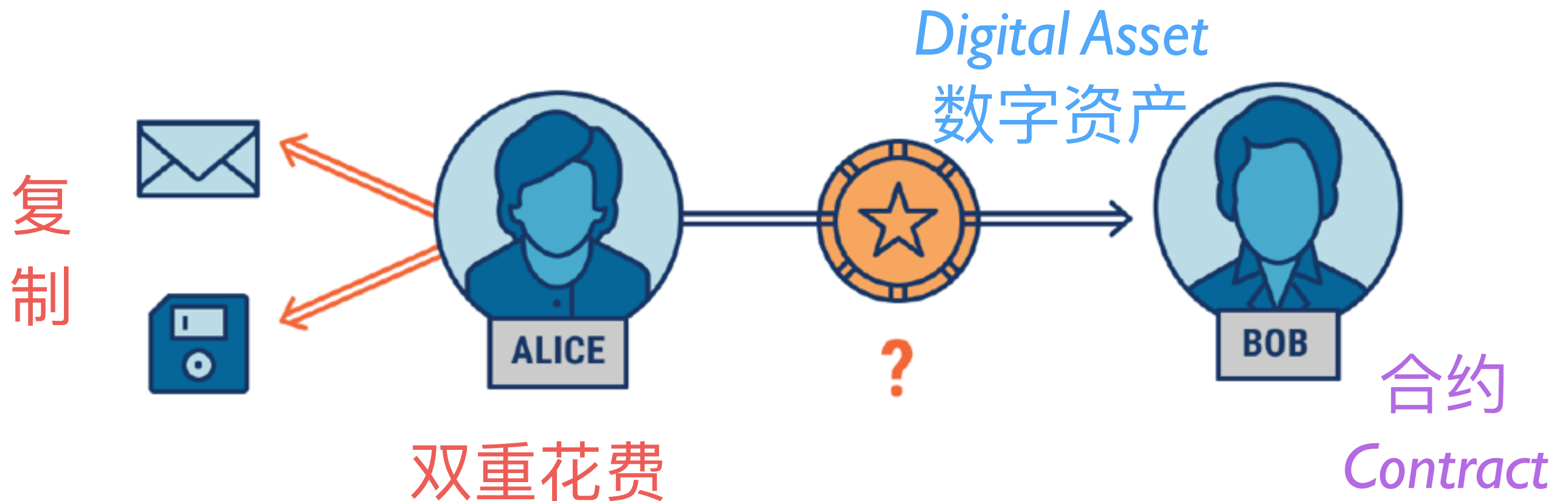
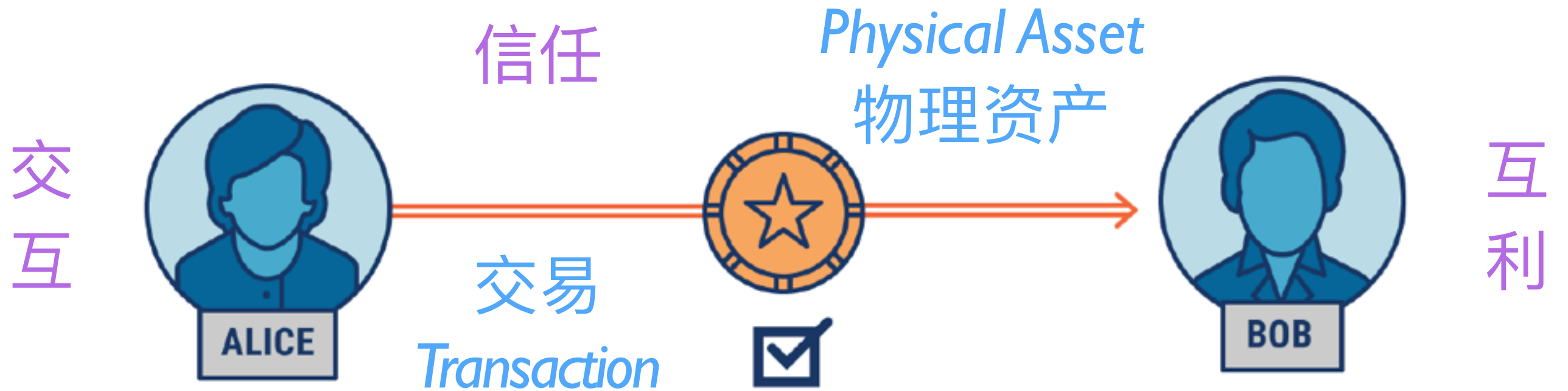
- 区块链起源
- 比特币
- 区块链发展
- 智能合约
- ICO

- 计算视角
- 网络视角
- 是否使用
- 面临挑战

史前



交易: 物理 vs. 数字



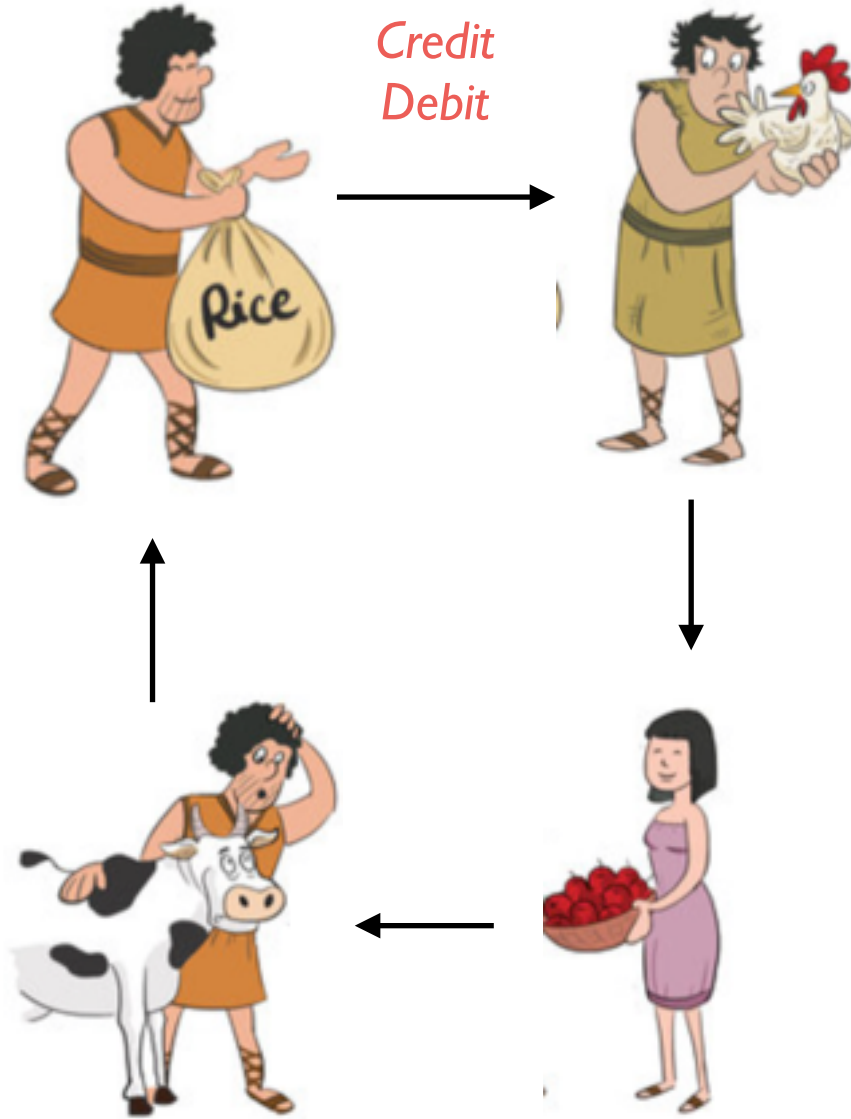
交易历史

Barter



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

Credit Debit

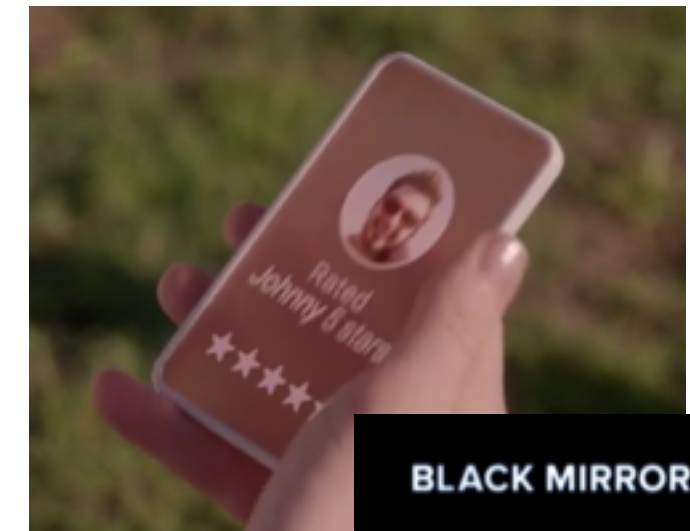
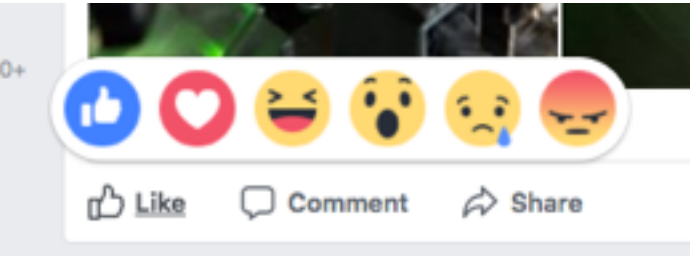


<https://en.wikipedia.org/wiki/Money>

Reputation

Detailed seller ratings (last 12 months) ?

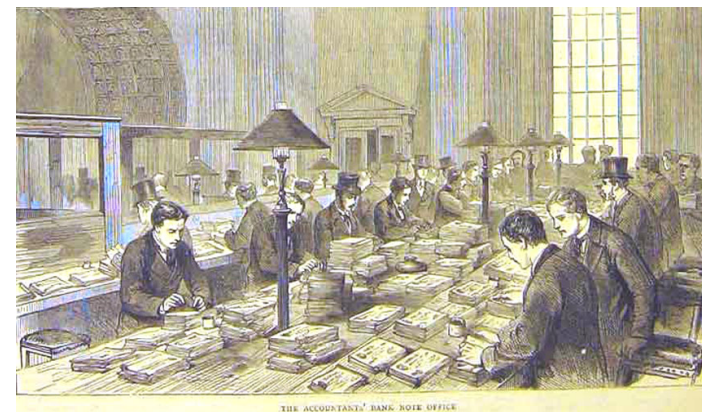
Criteria	Average rating	Number of ratings
Item as described	★★★★★	6176
Communication	★★★★★	6802
Shipping time	★★★★★	6673
Shipping and handling charges	★★★★★	7028



Money



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

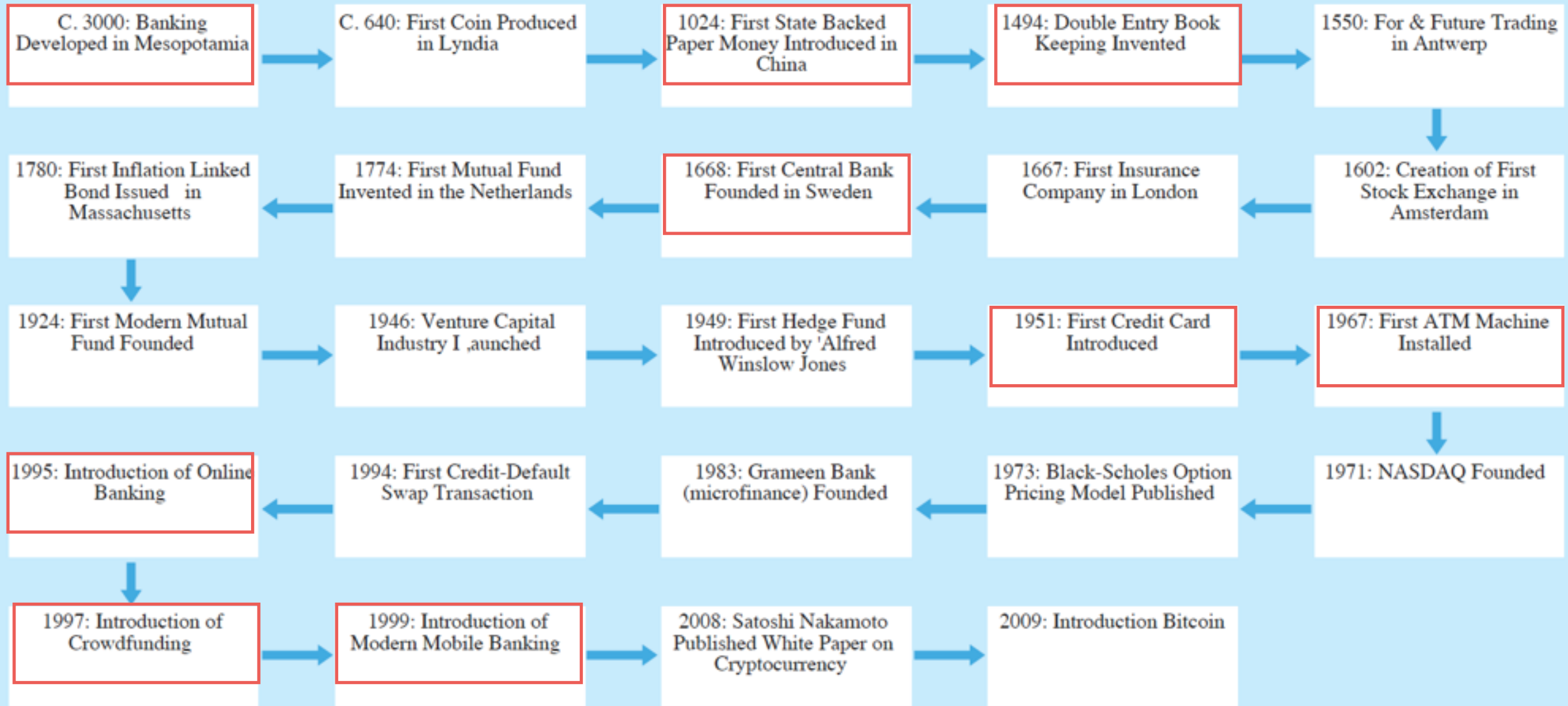


Bank



Credit Card

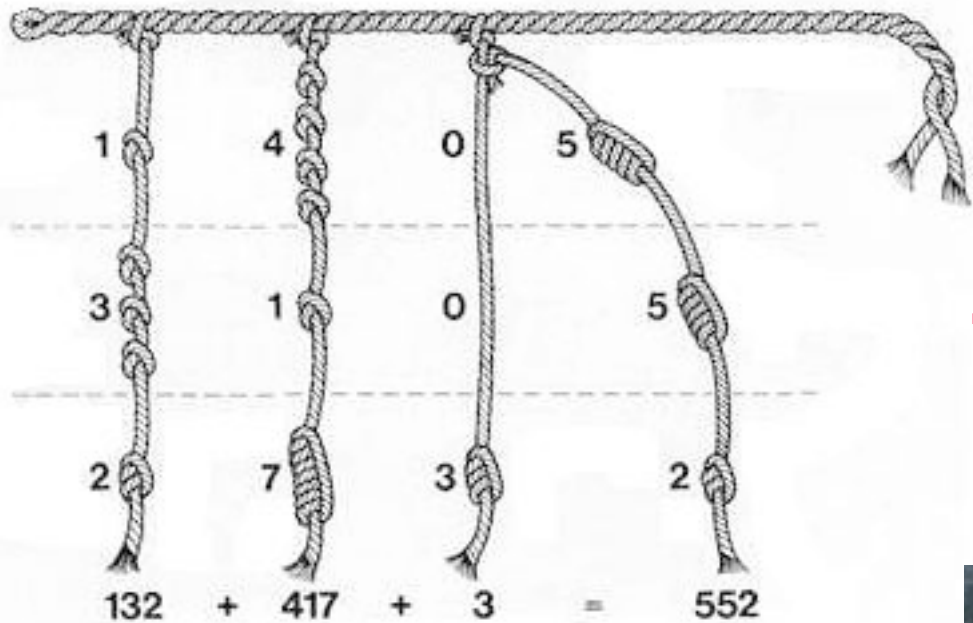
→ 金钱 → 纸币 → 复式记账 → 银行 → 信用卡 → ATM →



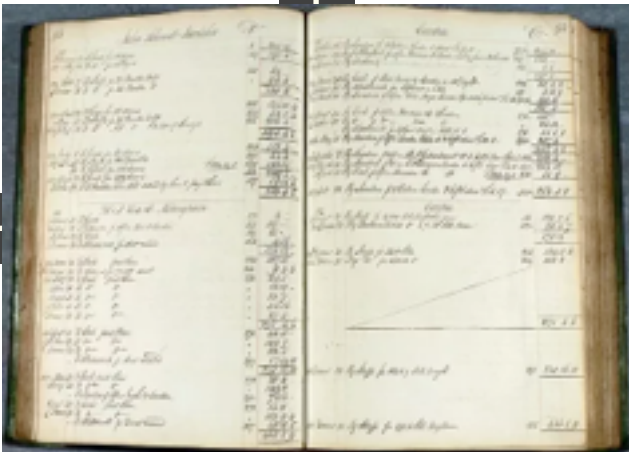
→ 在线银行 → 众筹 → 移动支付 → Bitcoin → 区块链 →

记账历史

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



结绳



Dr.		Cash.	
190-			
Jan 1	Your name's Investment	4000.00	
" 2	Mdse.	Cash sales	29.60
" 3	A. Daniels	On acct.	40.00
" 4	Mdse.	Cash sales	1320.40
			4072.00
Feb 1	Balance on hand		3239.16
			3239.16
Feb 5	Balance on hand		3159.16

单式

复式

1月家计簿				每日的记录	
本月收入				本月支出	
项目	金额	支出日	项目	金额	支出日
薪水(夫)			伙食费	50	
薪水(妻)			日用品		
奖金			交通费		
收入合计	0		累计余额	50	
			本月结余		

电子

物理



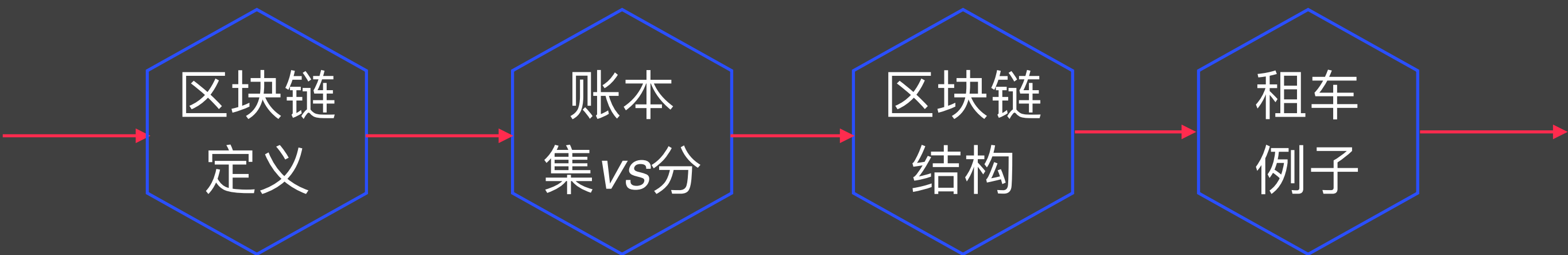
初识

区块链
定义

账本
集 vs 分

区块链
结构

租车
例子

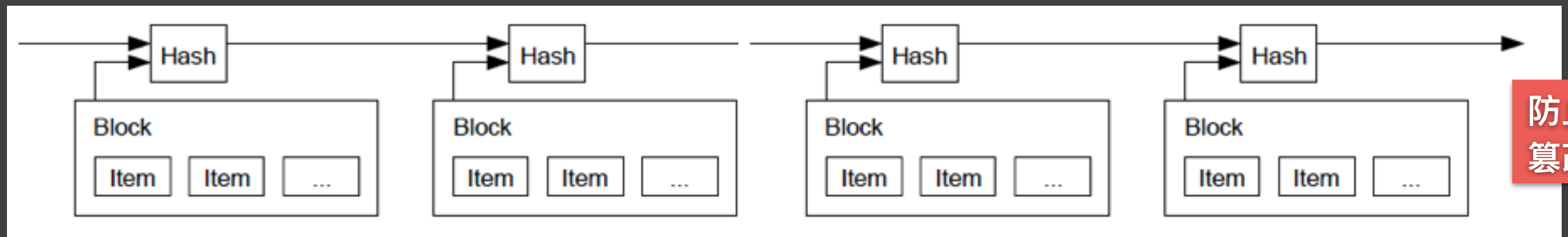


一个共享的分布式账本

公开

用于在商业网络中
促进交易记录和资产跟踪

可验证



账本: 集中 vs. 分布

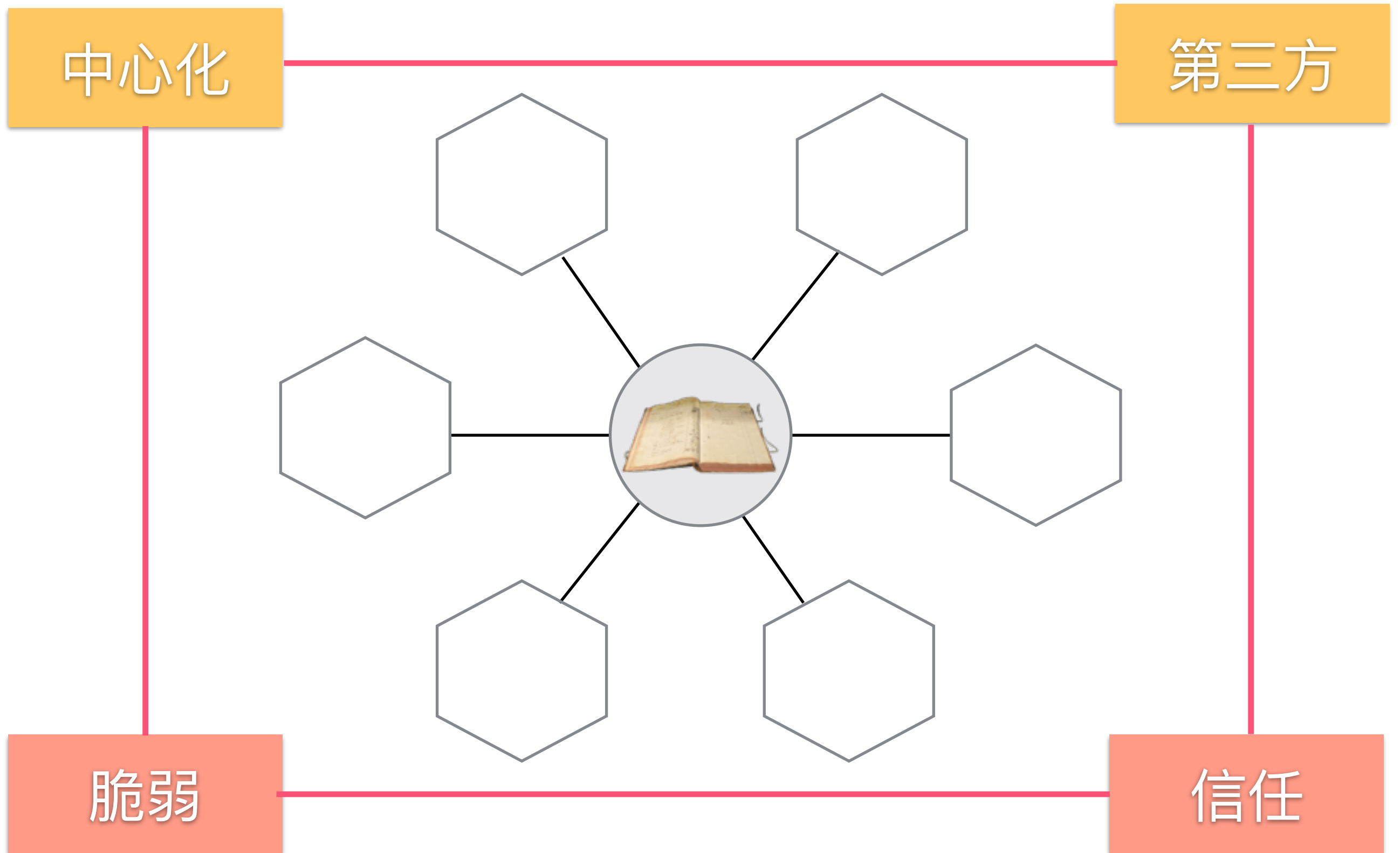


中心



P2P

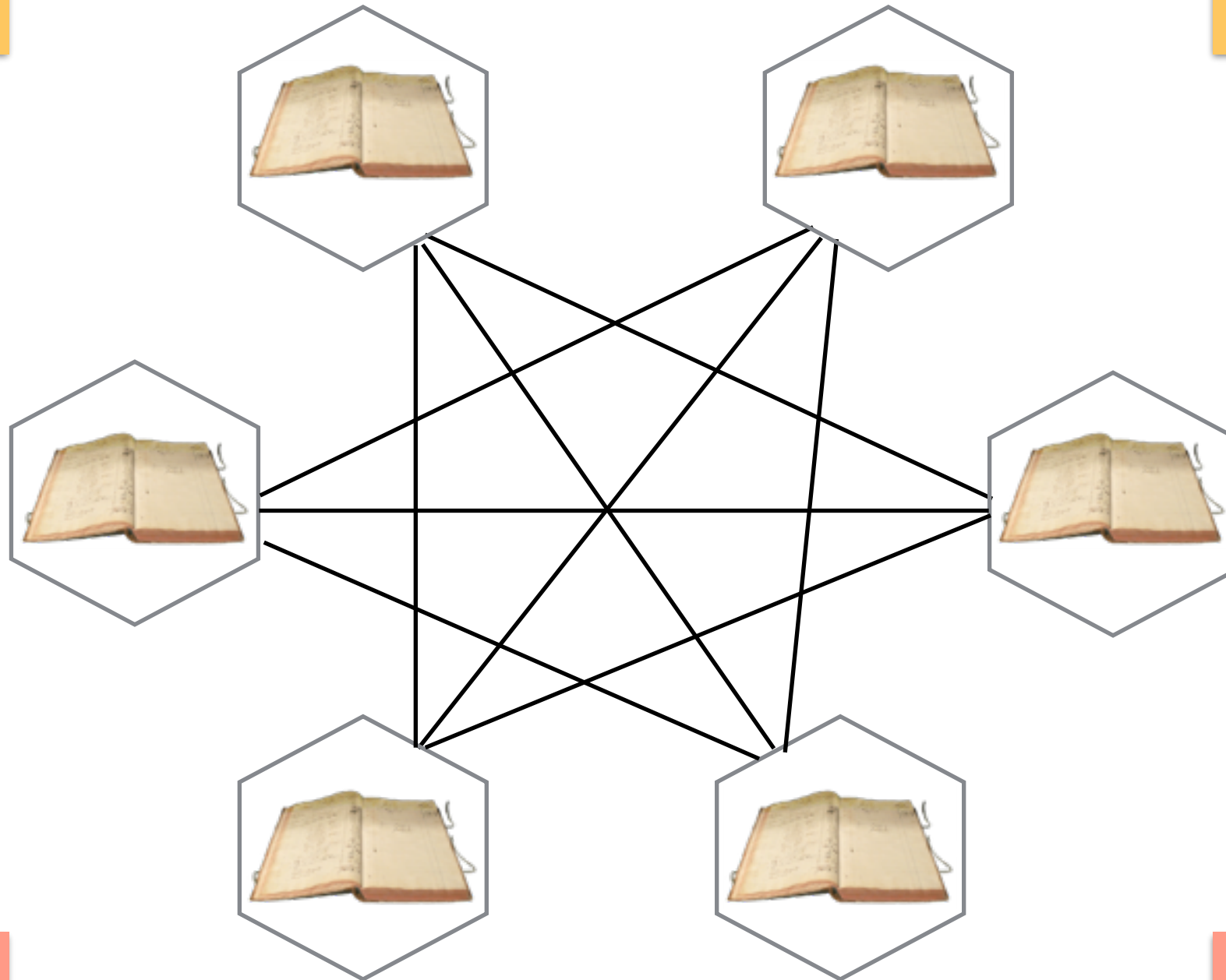
集中式账本的优缺点



分布式账本的优缺点

一致性

完整性



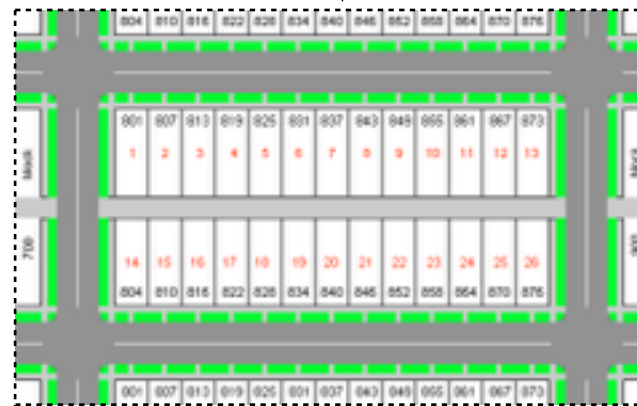
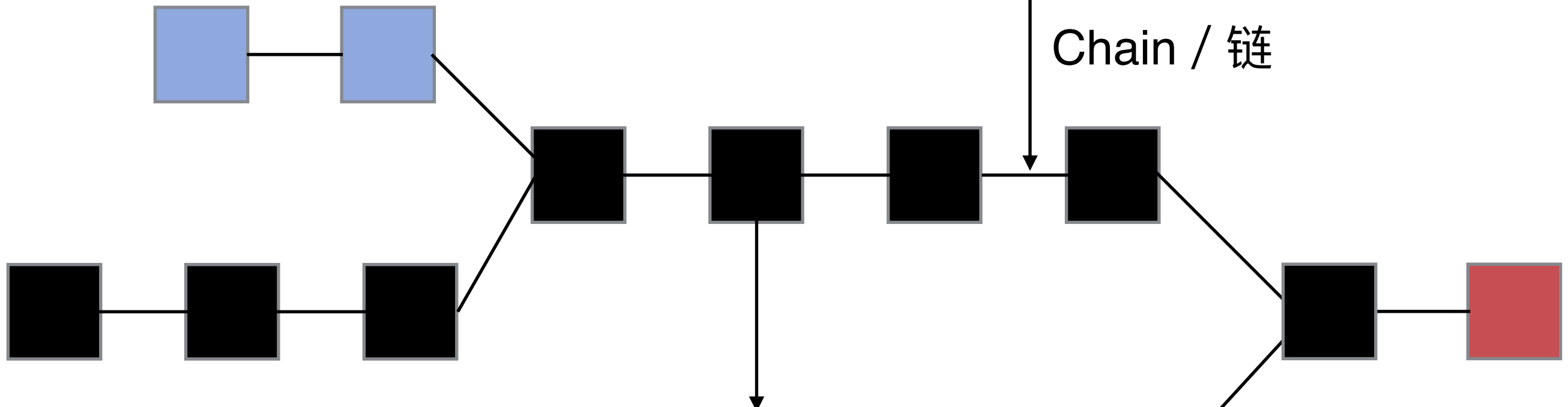
效率

花费

区块链结构

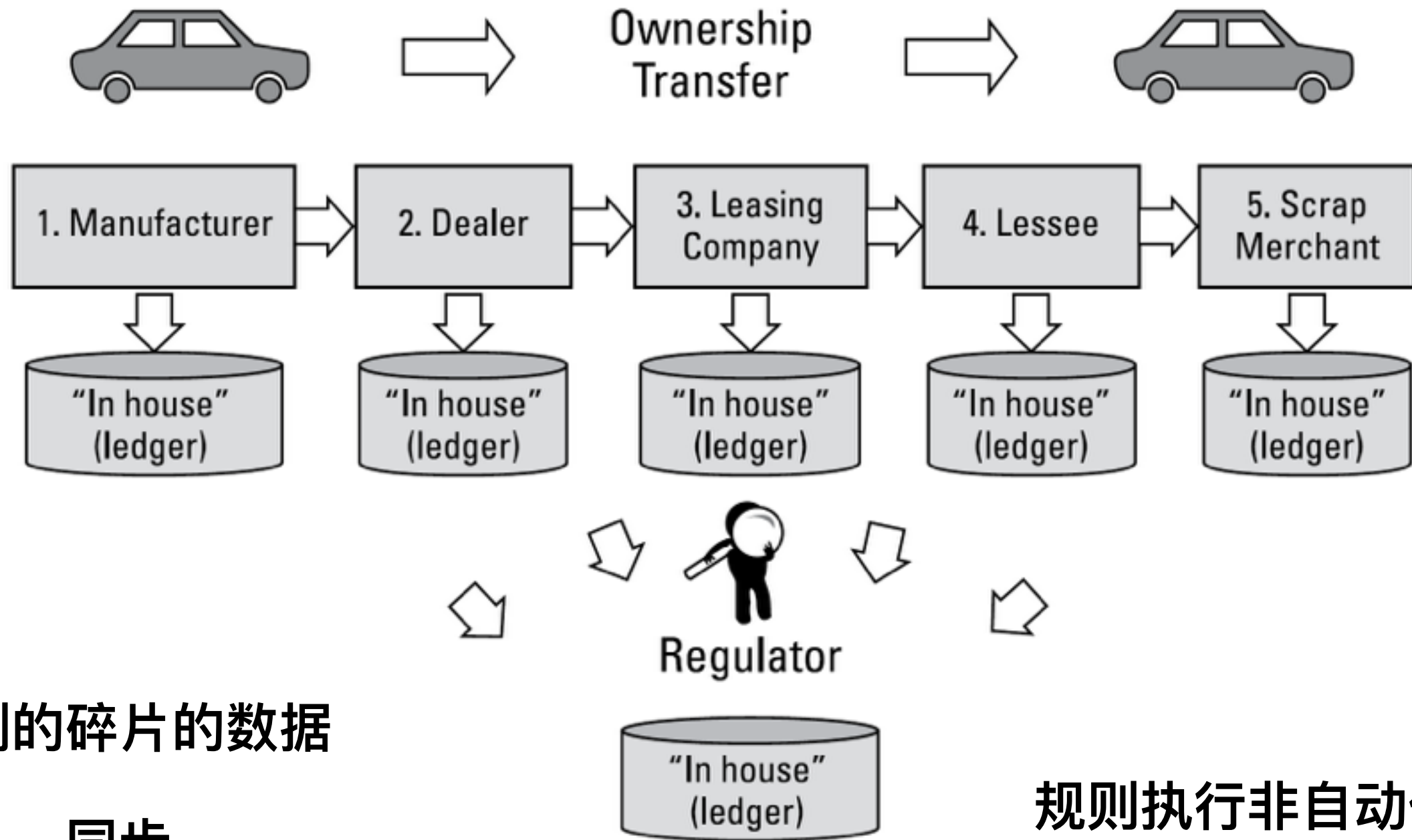


Chain / 链



Block / 区块

租车例子：没有区块链



分割的碎片的数据

同步

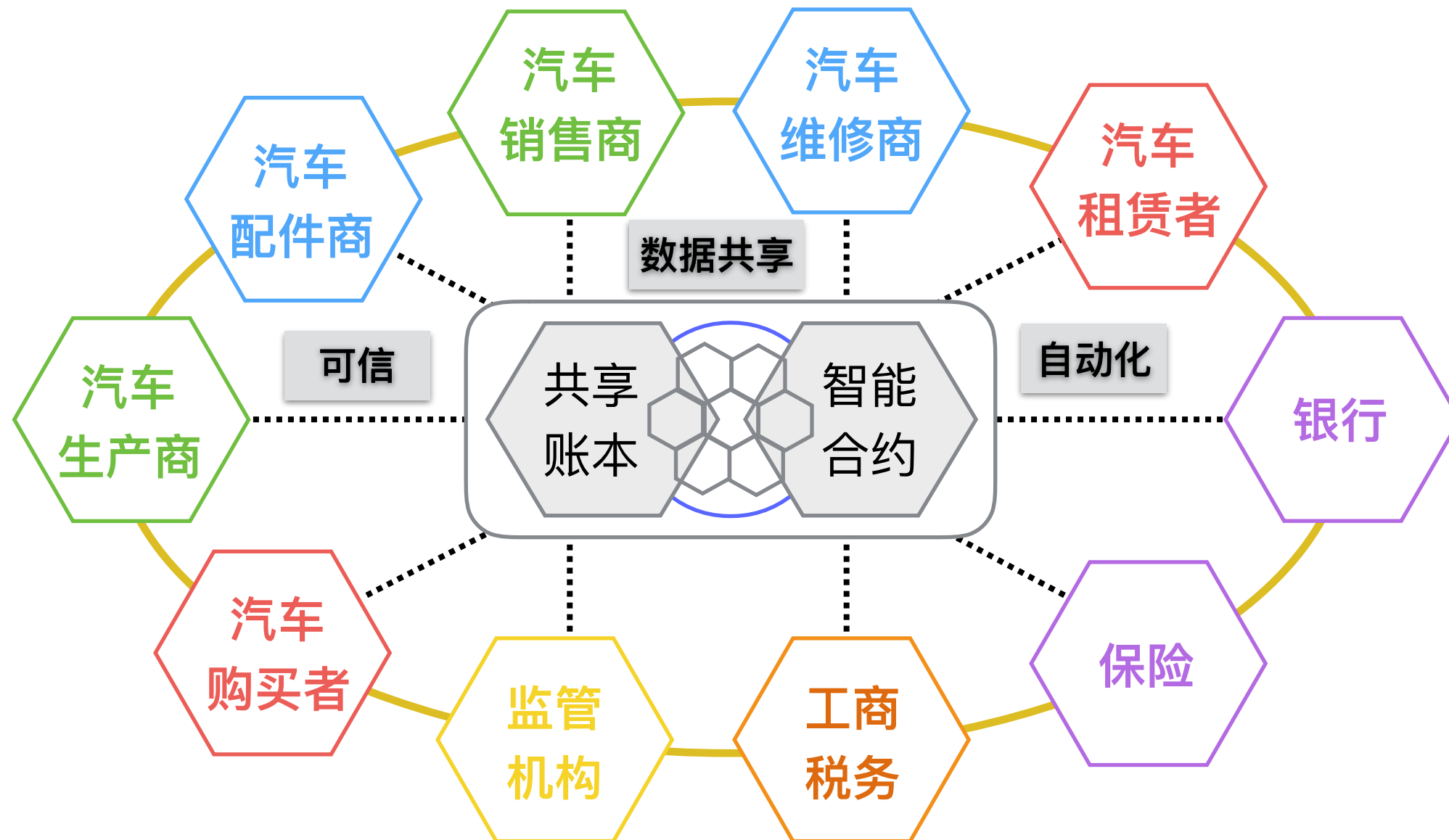
时间 / 一致性

规则执行非自动化

区块链应用场景

数据一致性

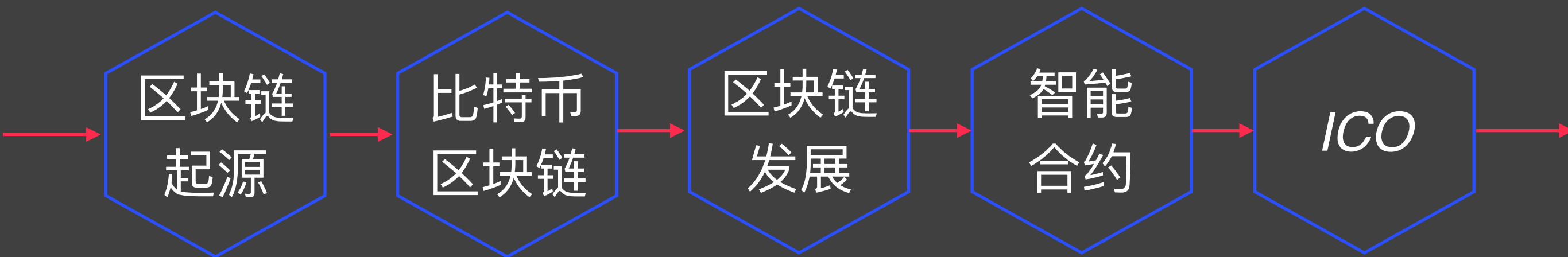
全生命周期管理



多中心

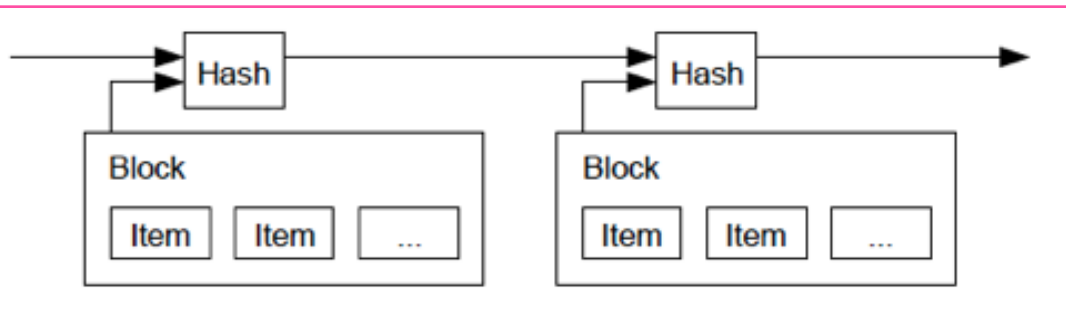
区块链增信

回顾



Bitcoin: A Peer-to-Peer Electronic Cash System

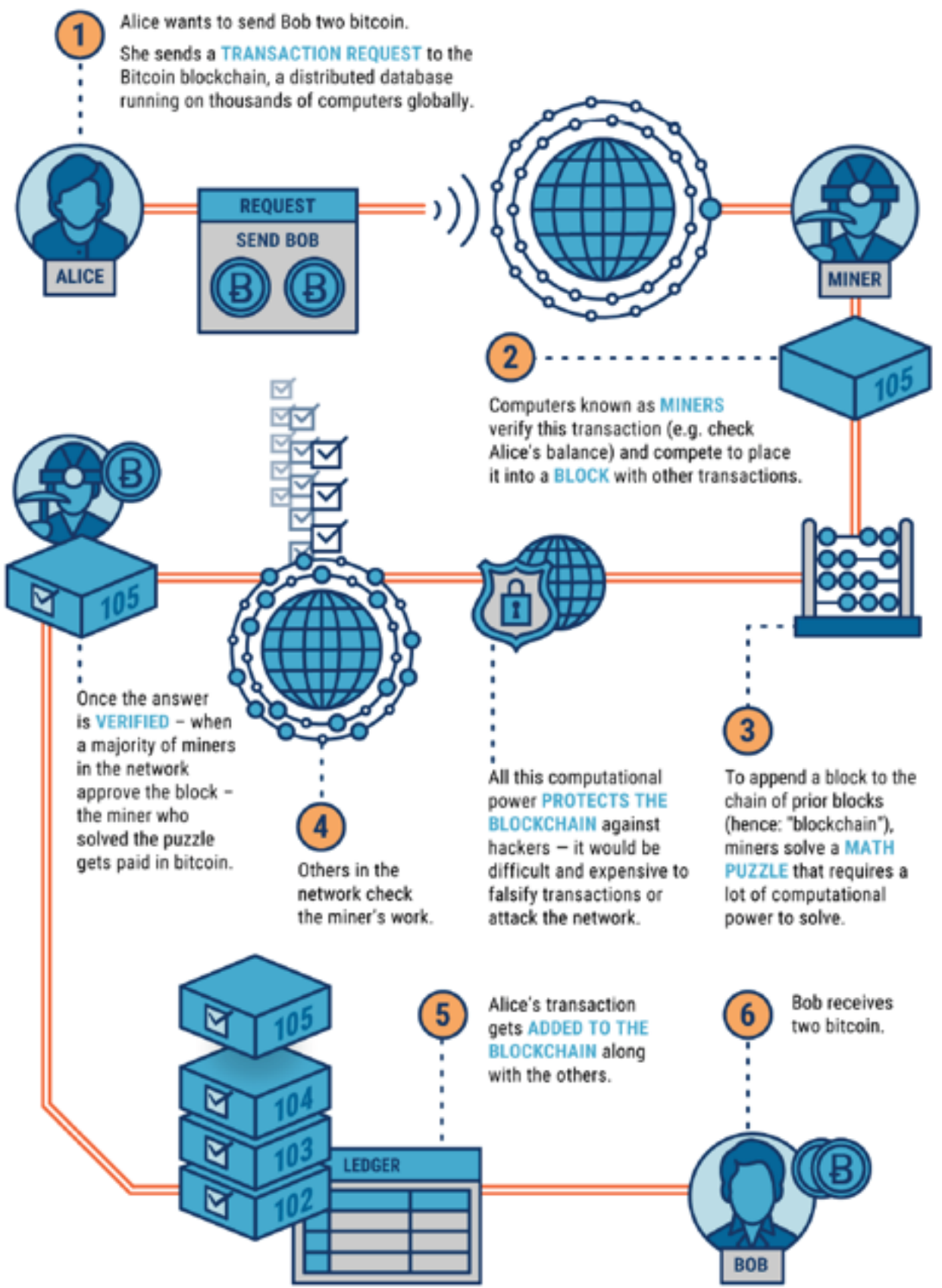
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



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 超级账本

区块链

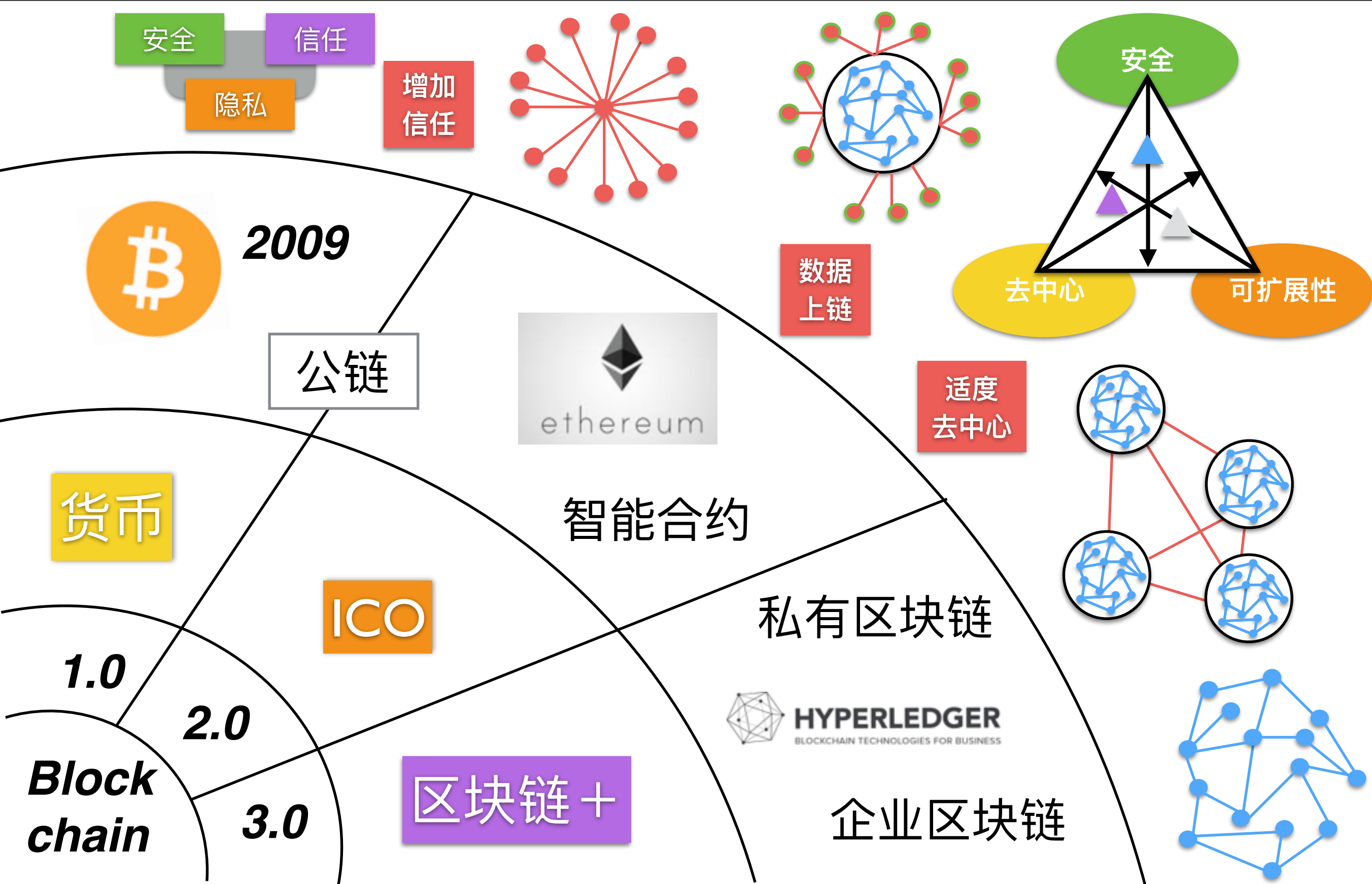
比特币 超级账本

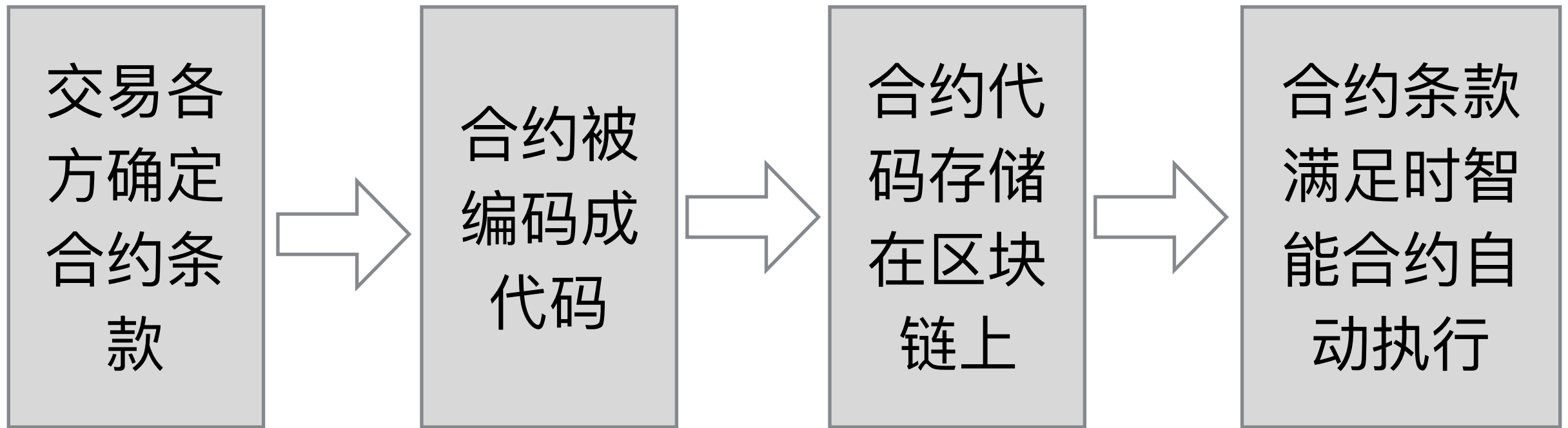
以太坊 R3 Corda

EOS

区块链

区块链发展现状





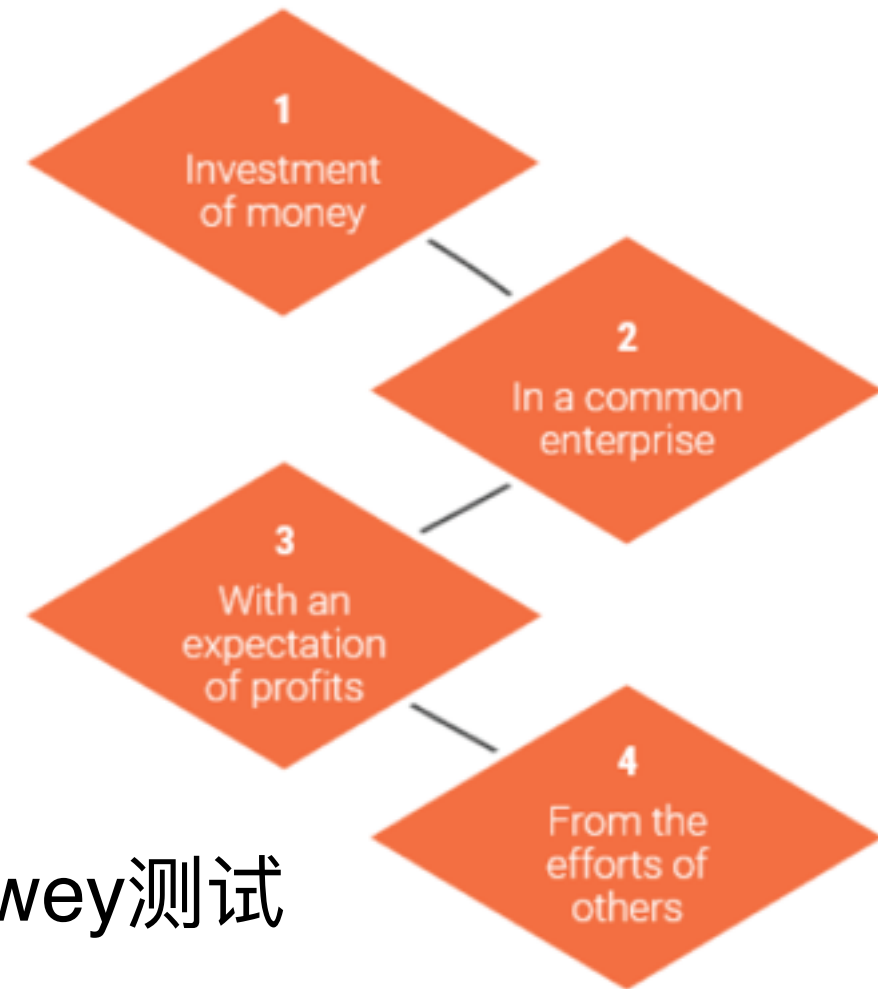
传统合约

- 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

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



Howey测试



剖析

```
graph LR; A[计算视角] --> B[网络视角]; B --> C[是否使用]; C --> D[面临挑战];
```

计算
视角

网络
视角

是否
使用

面临
挑战

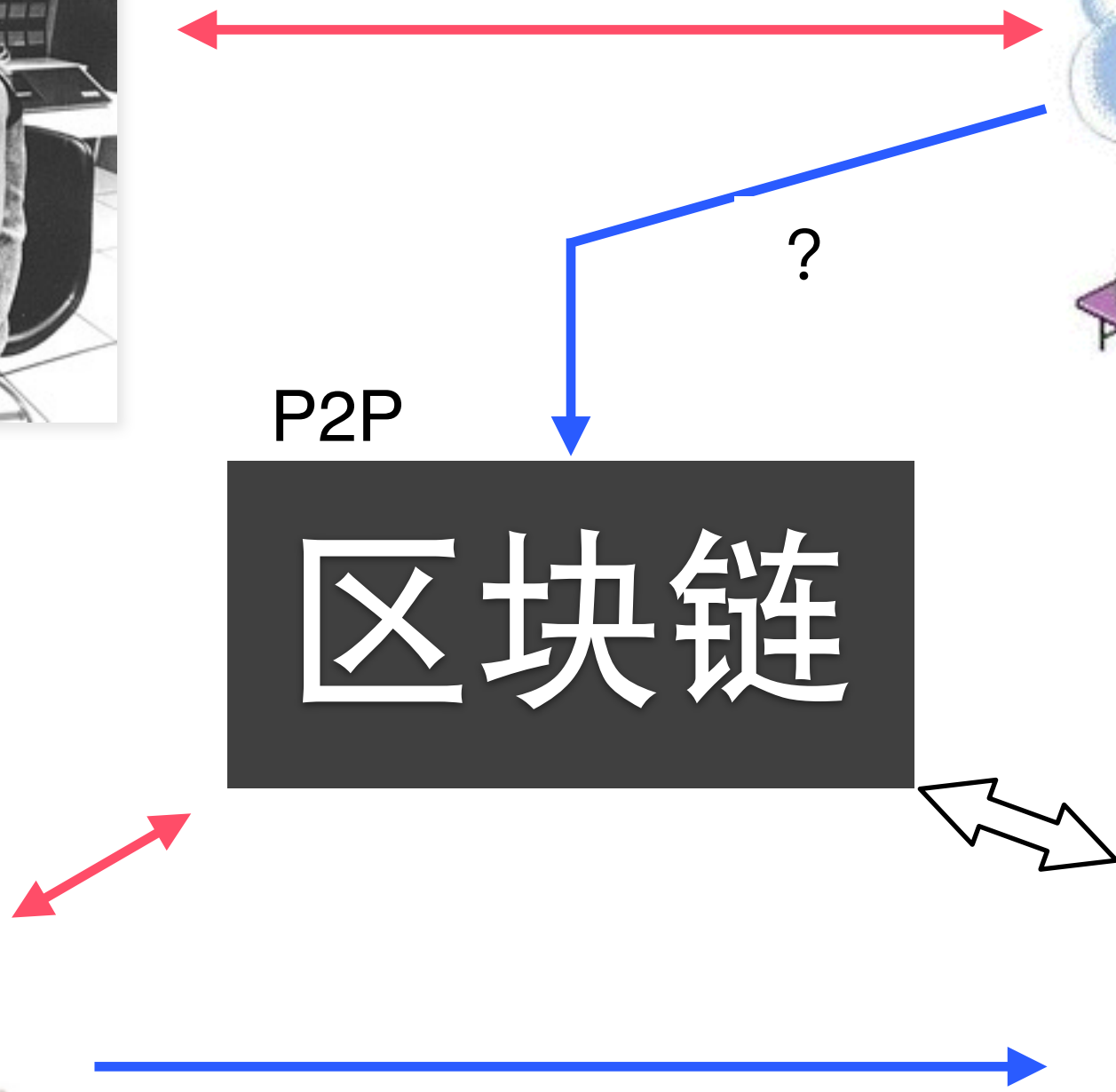
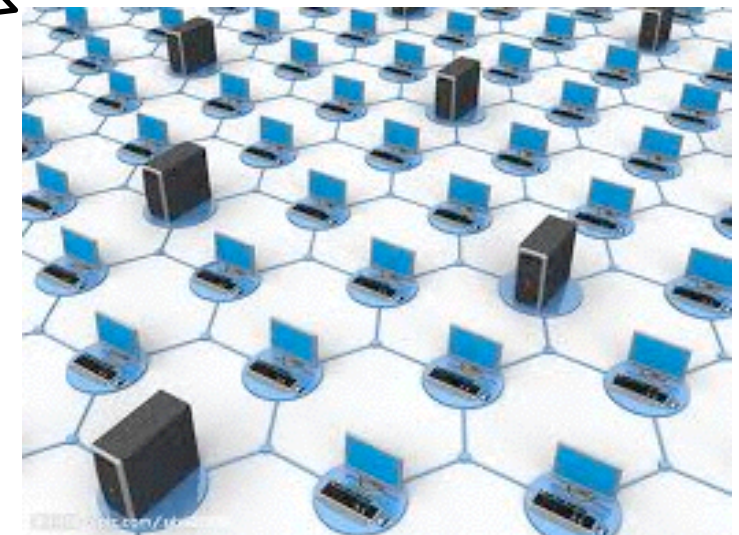
计算视角看区块链

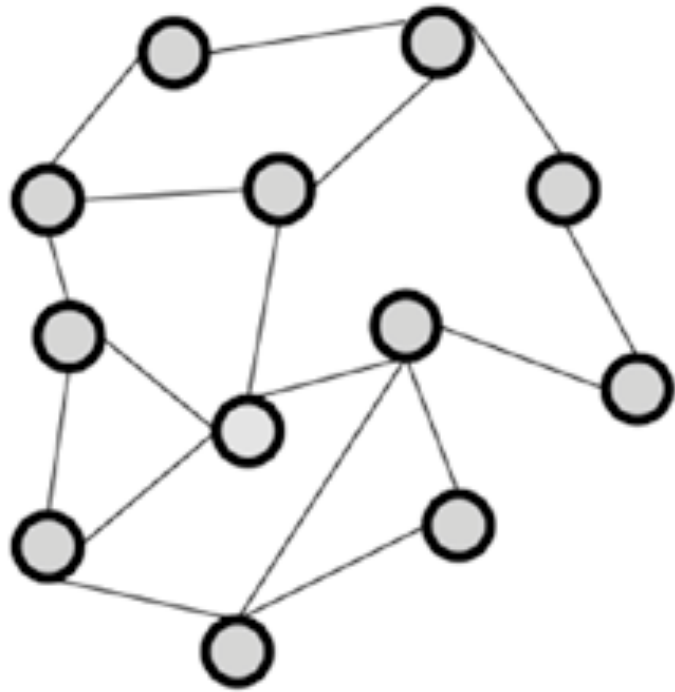


P2P

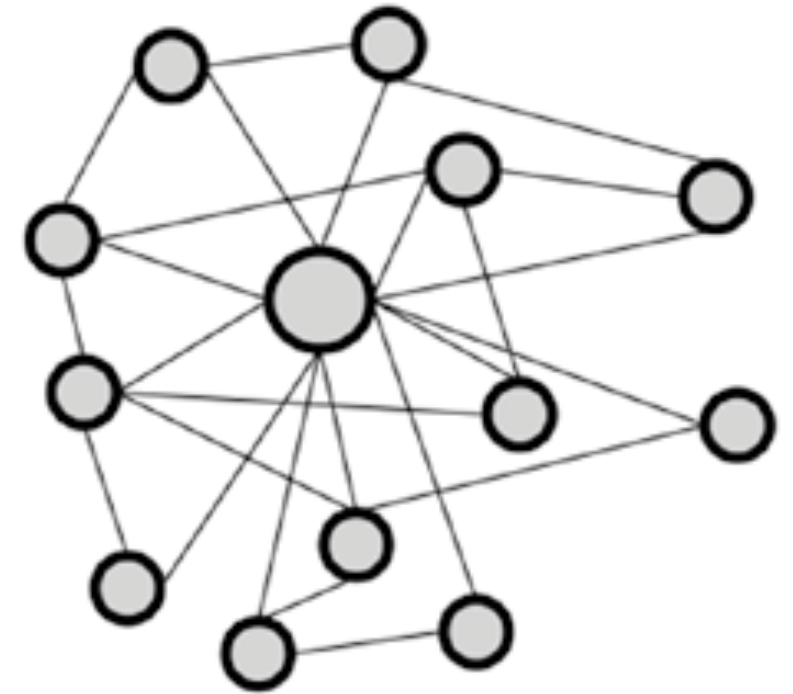
区块链

Client-Server

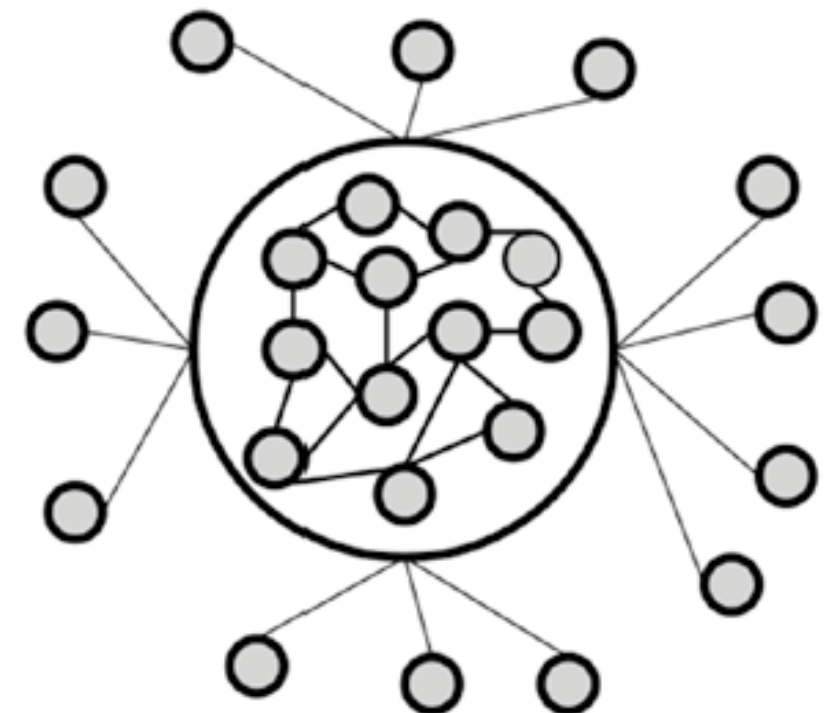




没有纯粹的
中心化系统
或者
分布式系统



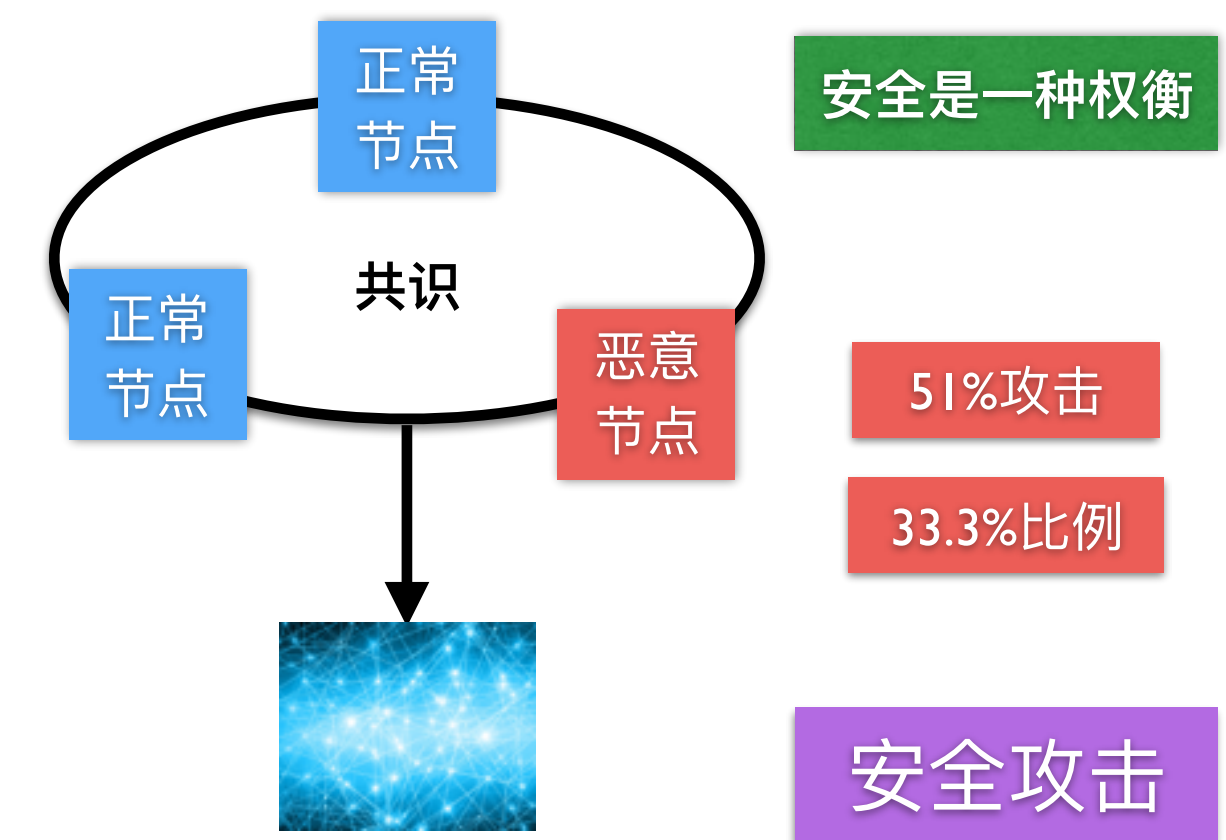
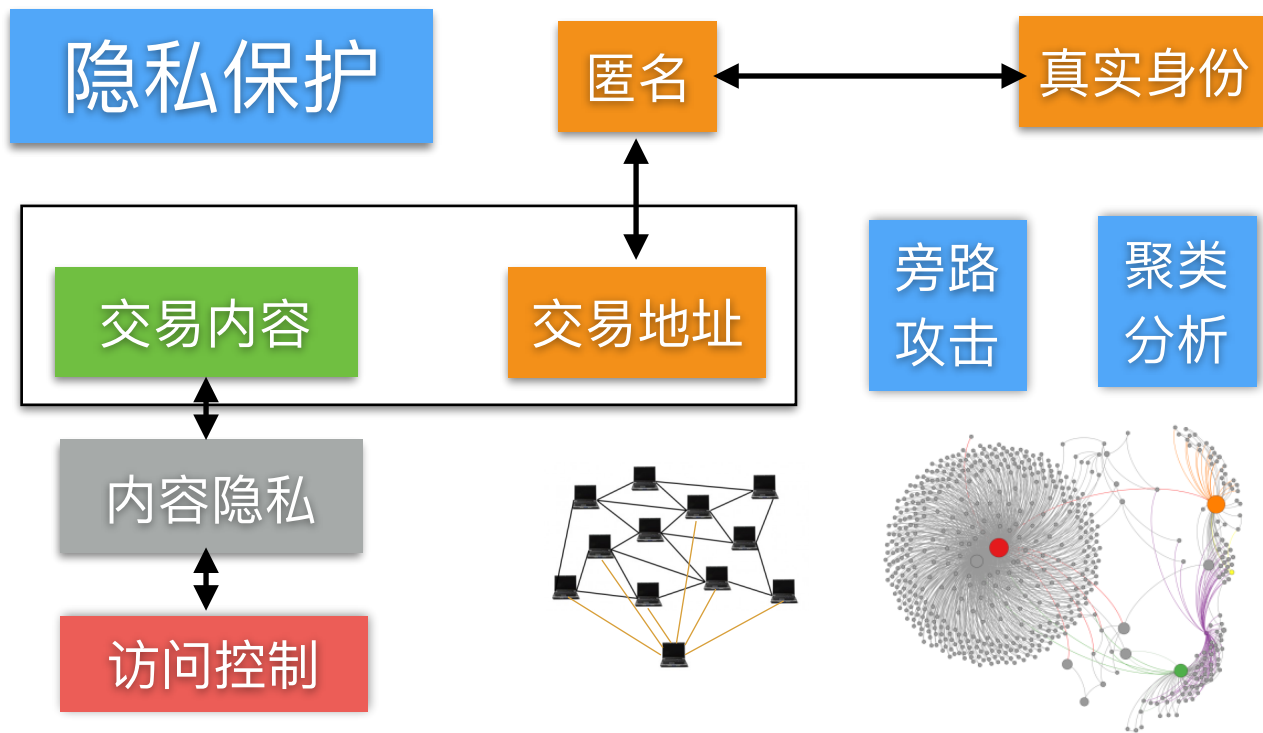
Internet
Email
IM
SNS



是否需要使用区块链



区块链面临挑战



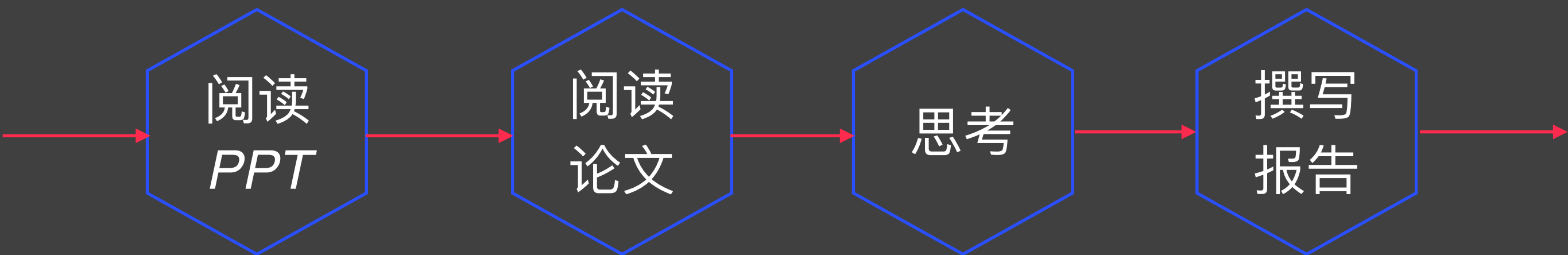
课后作业

阅读
PPT

阅读
论文

思考

撰写
报告



要求阅读如下论文，写论文阅读报告



In IEEE Computer Magazine 2017.

选择一篇介绍区块链应用的论文，2017-2018的最好，阅读该并在报告中简单介绍

- 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

周六晚上12点
前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

<https://huipingsun.github.io>