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

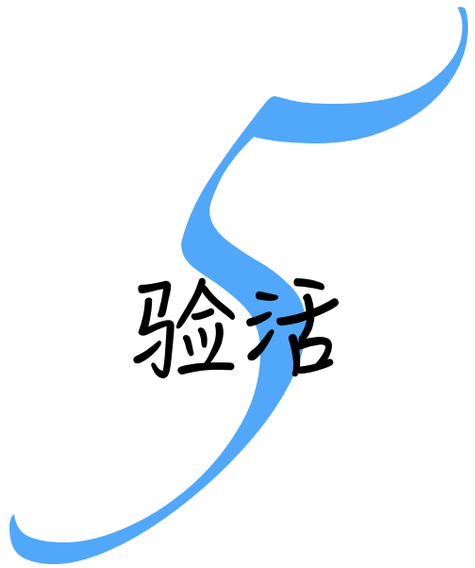
论文讲解

第二组

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

上次课程内容

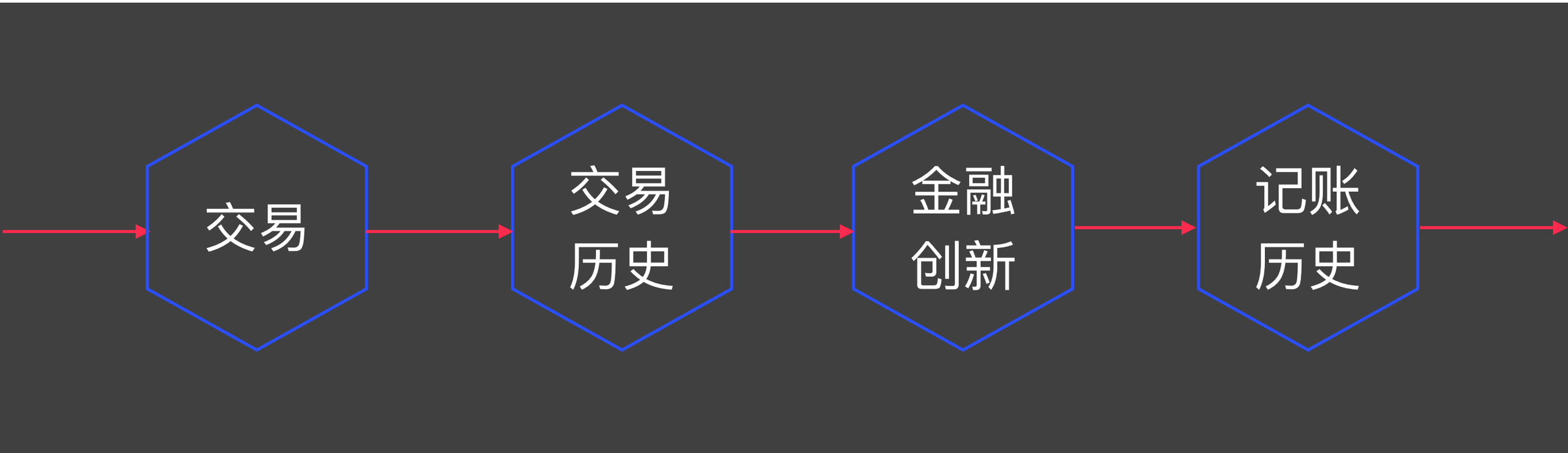


- 攻击分类
- 物理攻击
- 人工替代物
- 活体检测

- 验活分类
- 传感器特性
- 眨眼检测
- 挑战响应

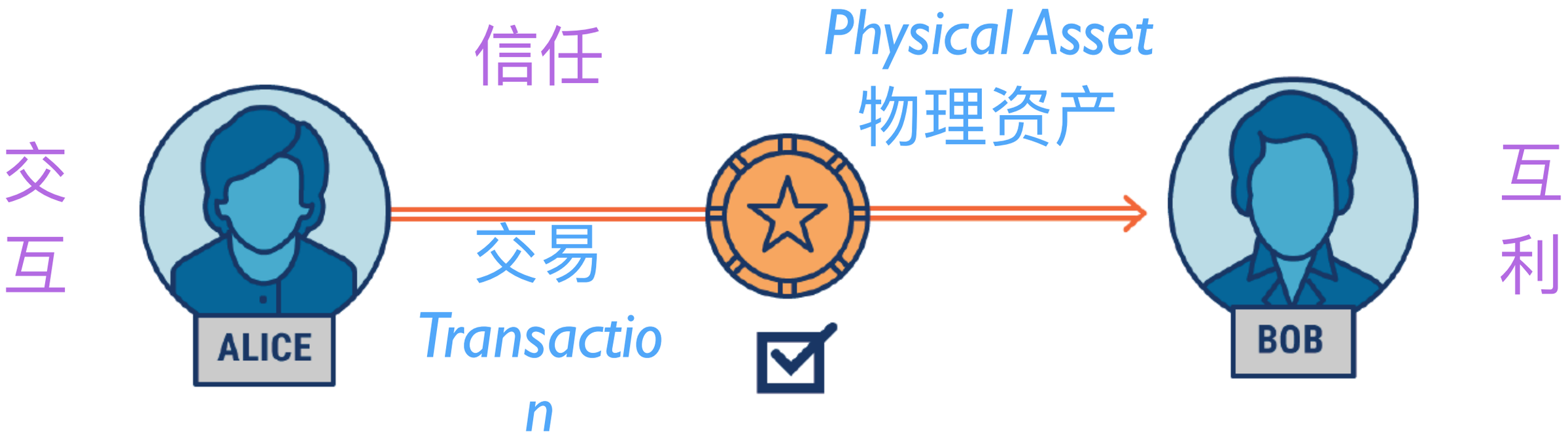
- 纹理分析
- 频率分析
- 混合
- 静态 动态

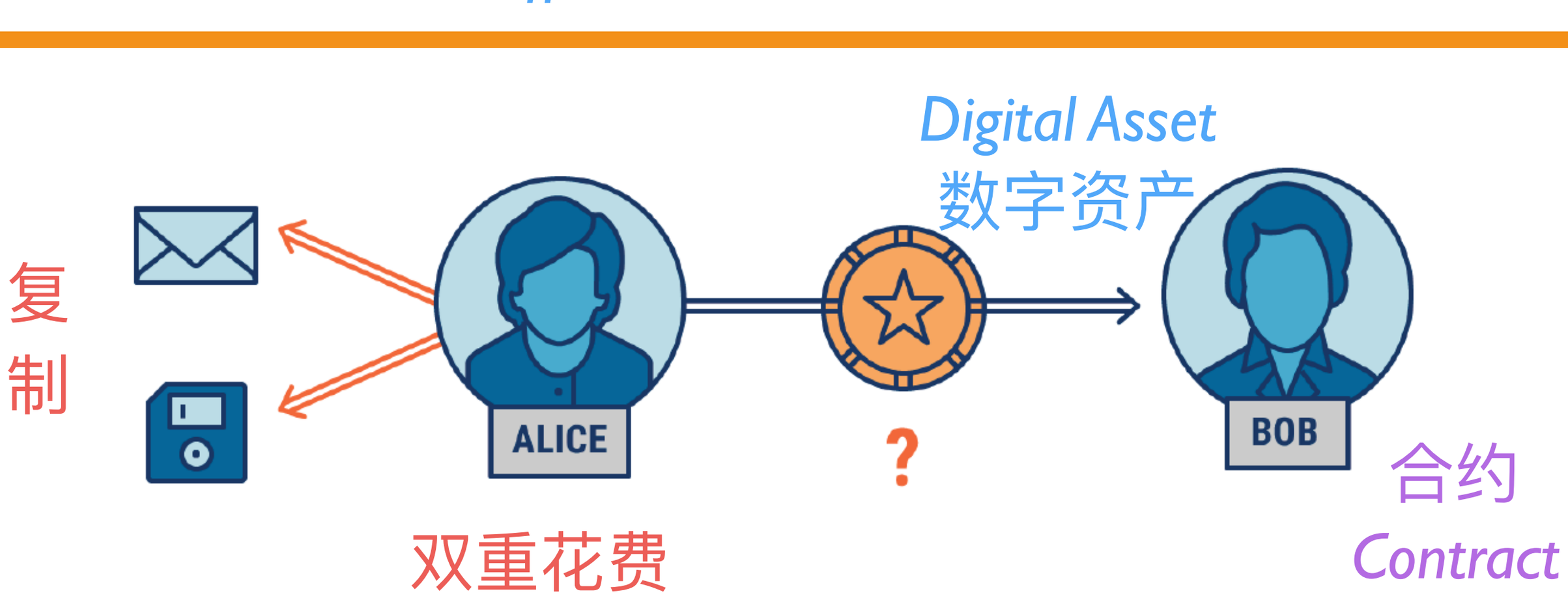
史前



交易：物理 vs. 数字

What is Blockchain Technology @ CBSInsights





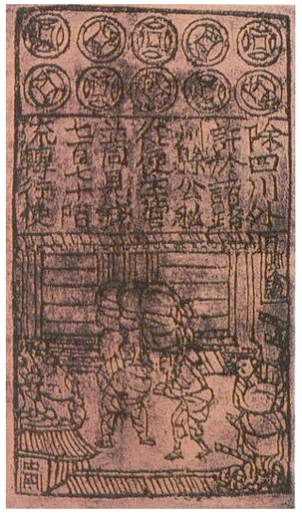
Blockchain Overview

交易历史

Barter

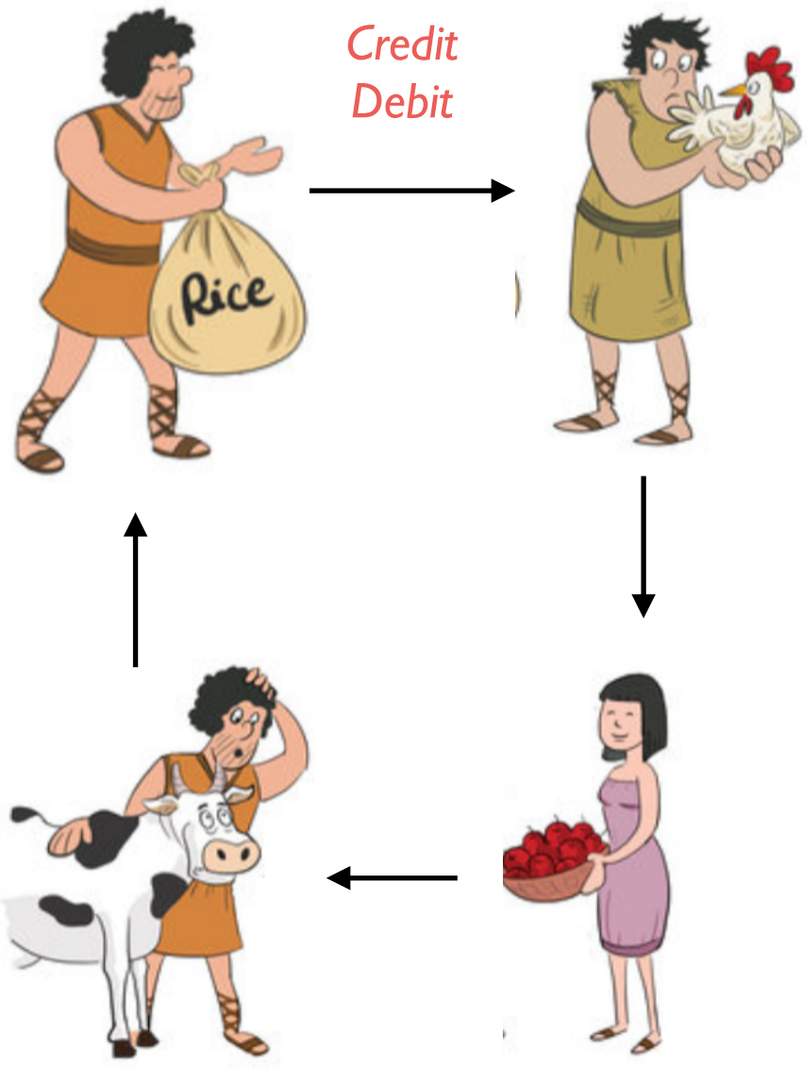
https://en.wikipedia.org/wiki/Barter

Money



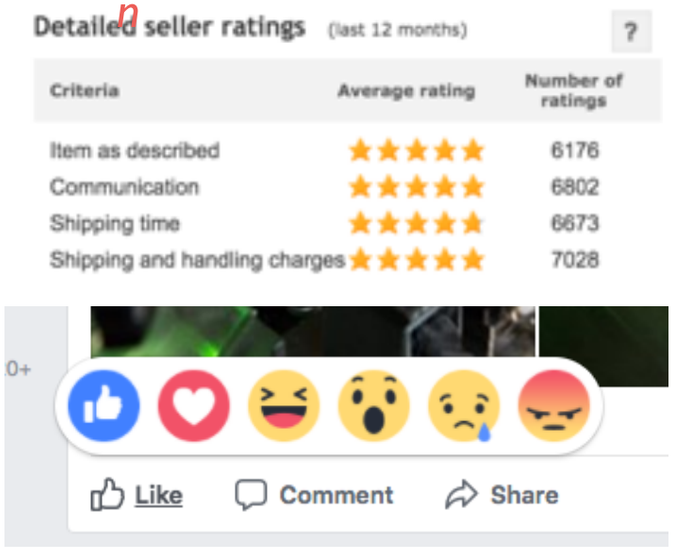
https://en.wikipedia.org/wiki/Credit

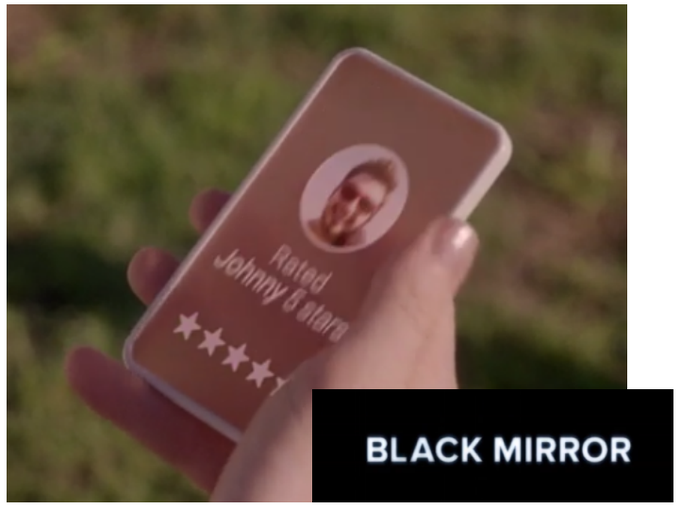
Credit Debit



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

Reputation





Bank

Credit Card

金融创新

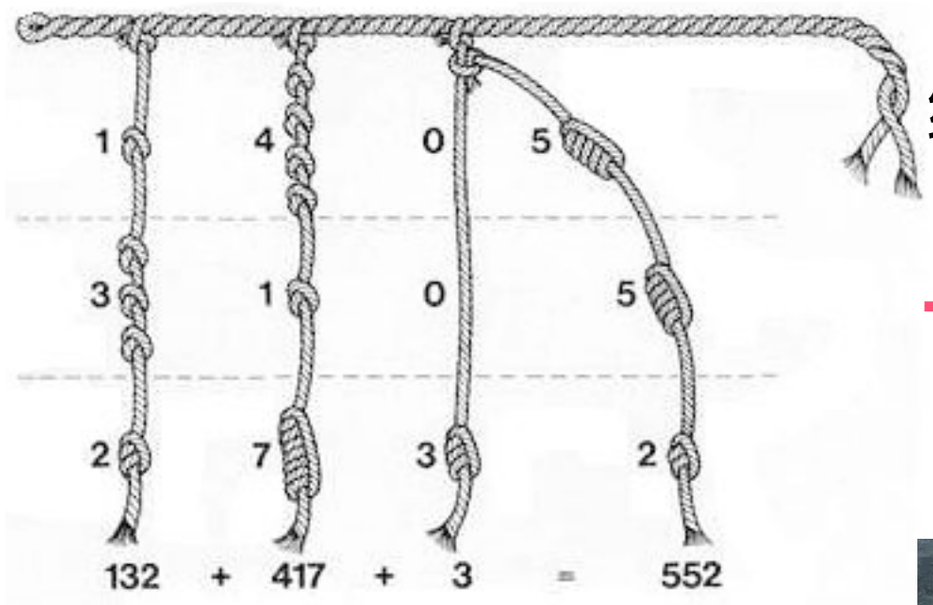
→ 金钱 → 纸币 → 复式记账 → 银行 → 信用卡 → ATM →

C. 3000: Banking Developed in Mesopotamia → C. 640: First Coin Produced in Lyndia → 1024: First State Backed Paper Money Introduced in China → 1494: Double Entry Book Keeping Invented → 1550: For & Future Trading in Antwerp → 1602: Creation of First Stock Exchange in Amsterdam → 1667: First Insurance Company in London → 1668: First Central Bank Founded in Sweden → 1774: First Mutual Fund Invented in the Netherlands → 1780: First Inflation Linked Bond Issued in Massachusetts → 1924: First Modern Mutual Fund Founded → 1946: Venture Capital Industry I ,aunched → 1949: First Hedge Fund Introduced by 'Alfred Winslow Jones → 1951: First Credit Card Introduced → 1967: First ATM Machine Installed → 1971: NASDAQ Founded → 1973: Black-Scholes Option Pricing Model Published → 1983: Grameen Bank (microfinance) Founded → 1994: First Credit-Default Swap Transaction → 1995: Introduction of Online Banking → 1997: Introduction of Crowdfunding → 1999: Introduction of Modern Mobile Banking → 2008: Satoshi Nakamoto Published White Paper on Cryptocurrency → 2009: Introduction Bitcoin

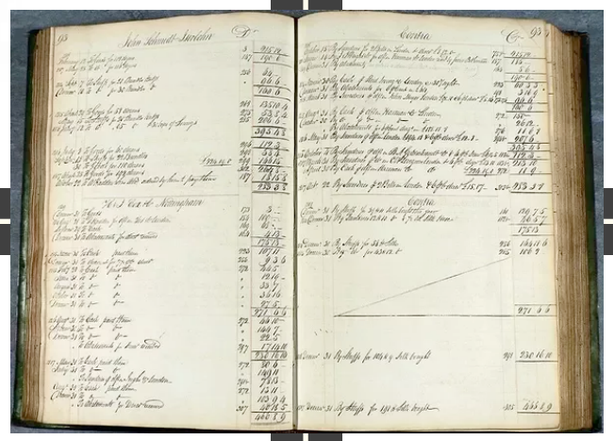
→ 在线银行 → 众筹 → 移动支付 → Bitcoin → 区块链 →

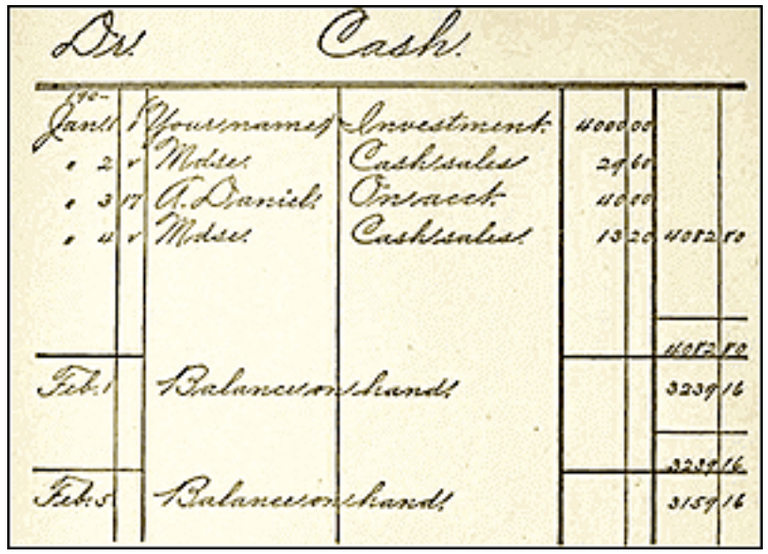
记账历史

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



结绳





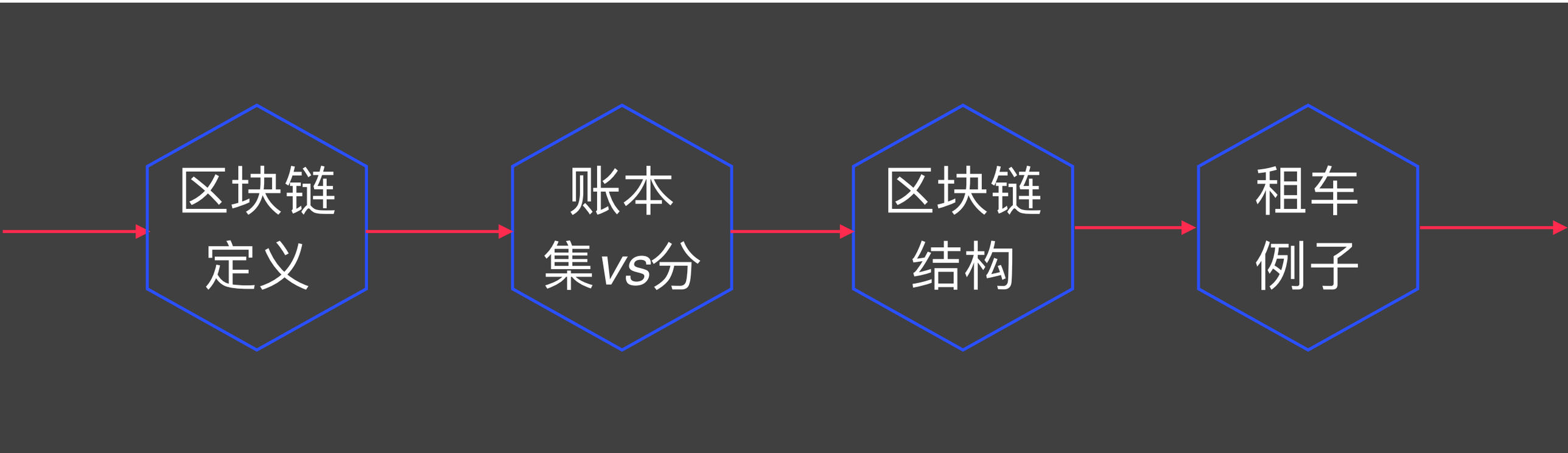
单式

复式

电子

物理

初识



Blockchain Overview

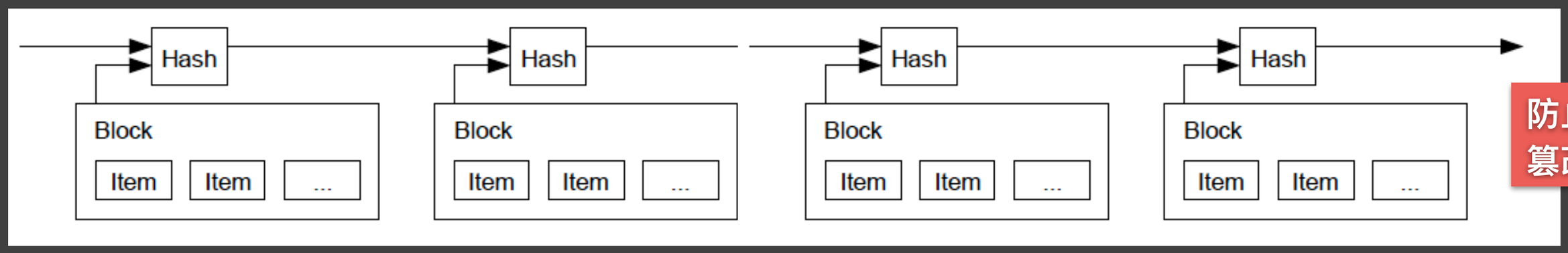
区块链定义

一个共享的分布式账本

公开

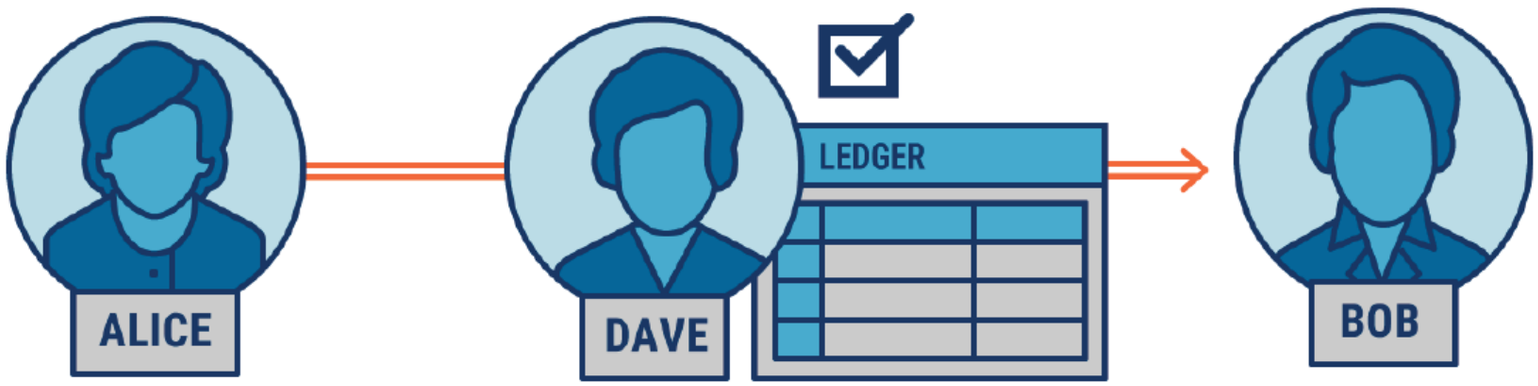
用于在商业网络中
促进交易记录和资产跟踪

可验证



账本: 集中 vs. 分布

What is Blockchain Technology @ CBSInsights



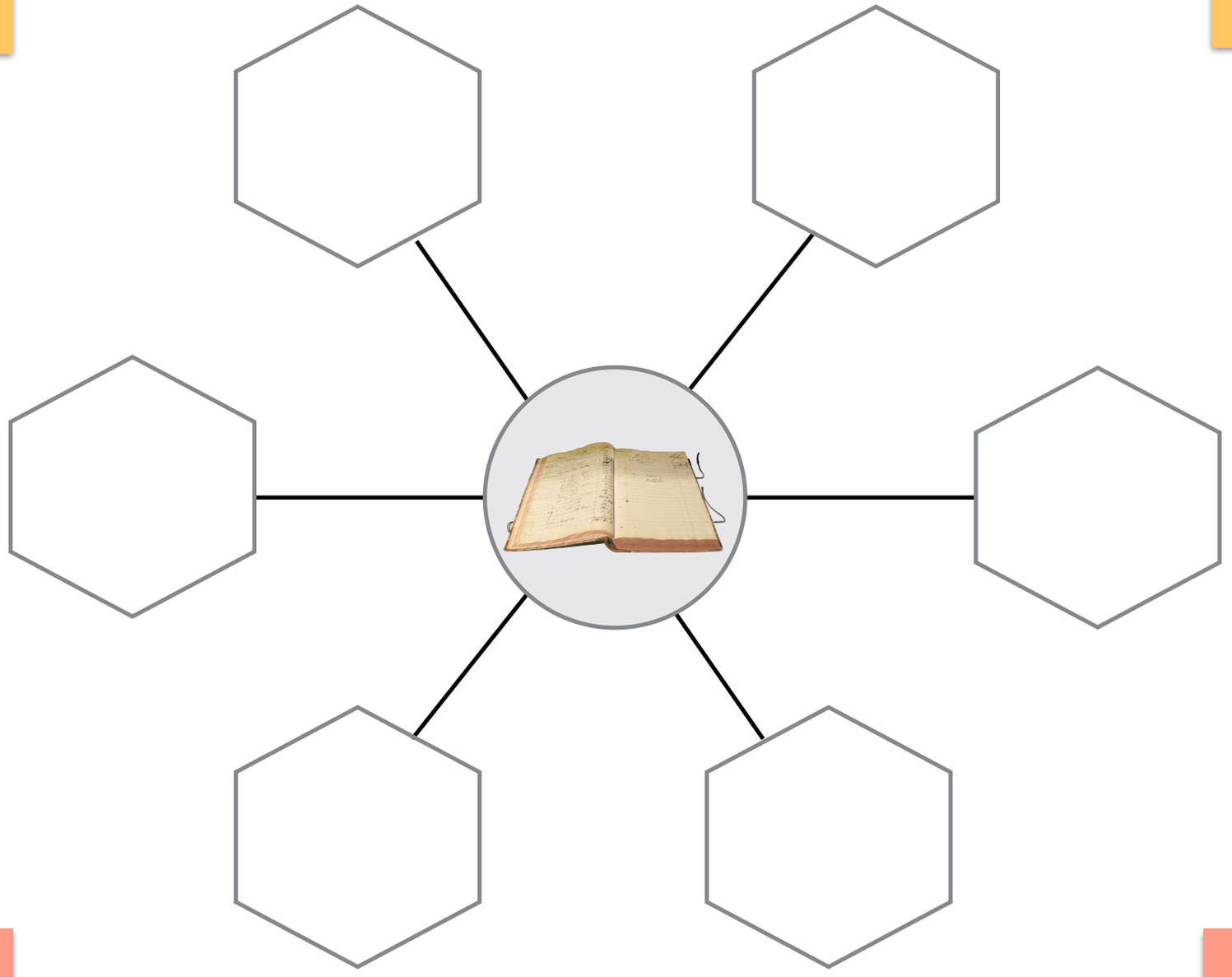
中心

P2P

集中式账本的优缺点

中心化

第三方



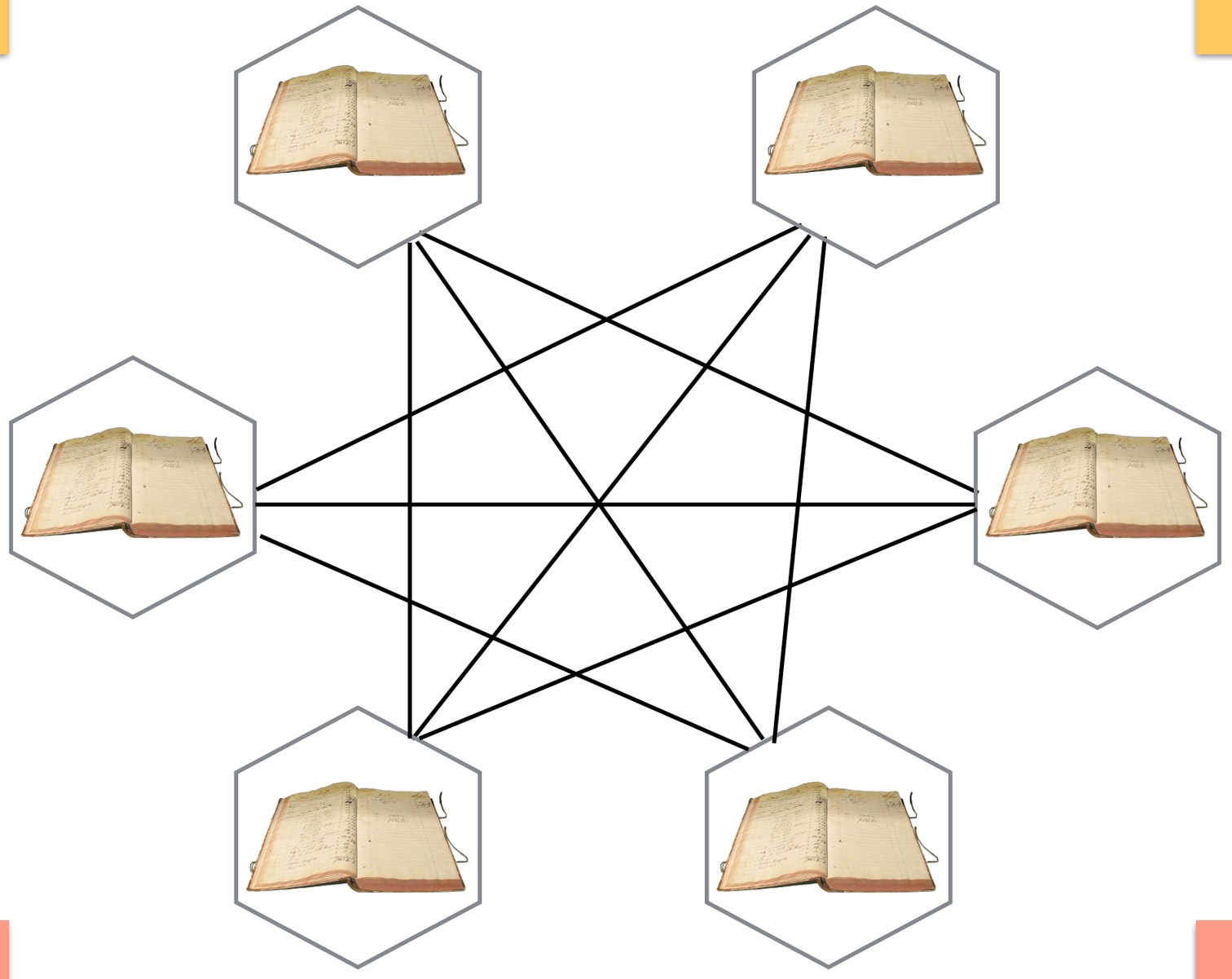
脆弱

信任

分布式账本的优缺点

一致性

完整性

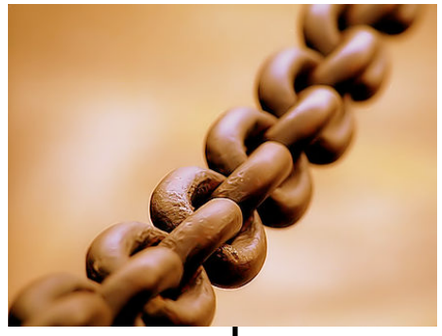


效率

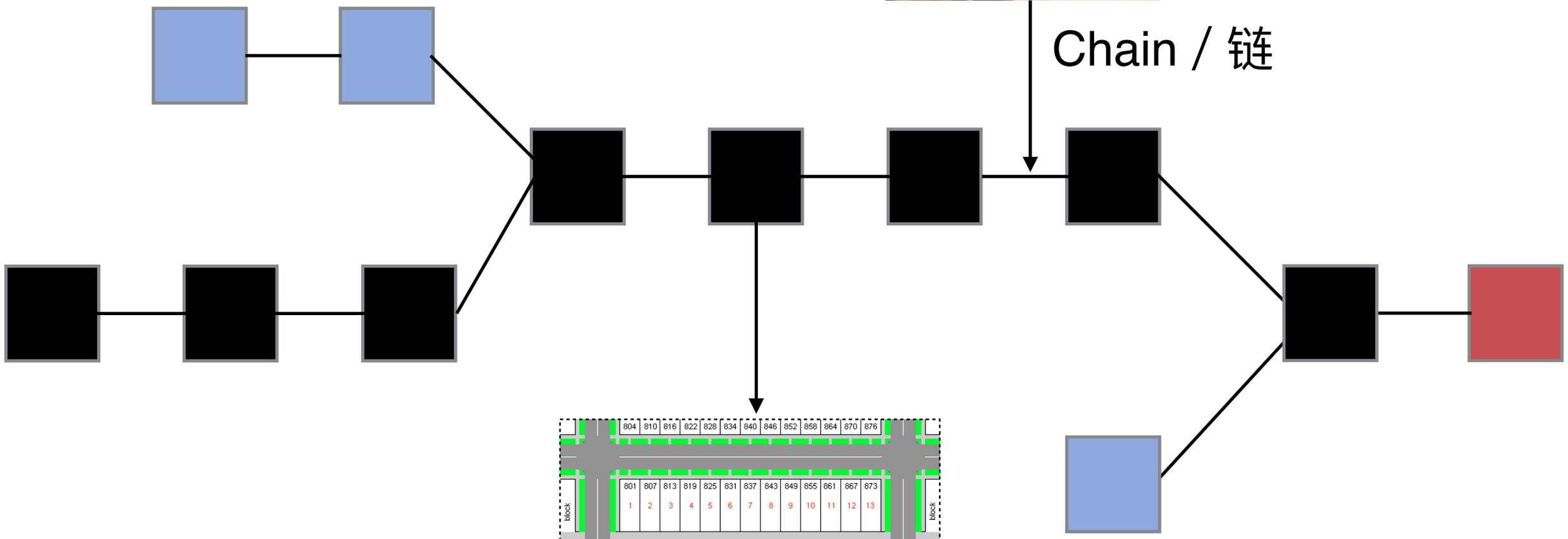
花费

区块链结构

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

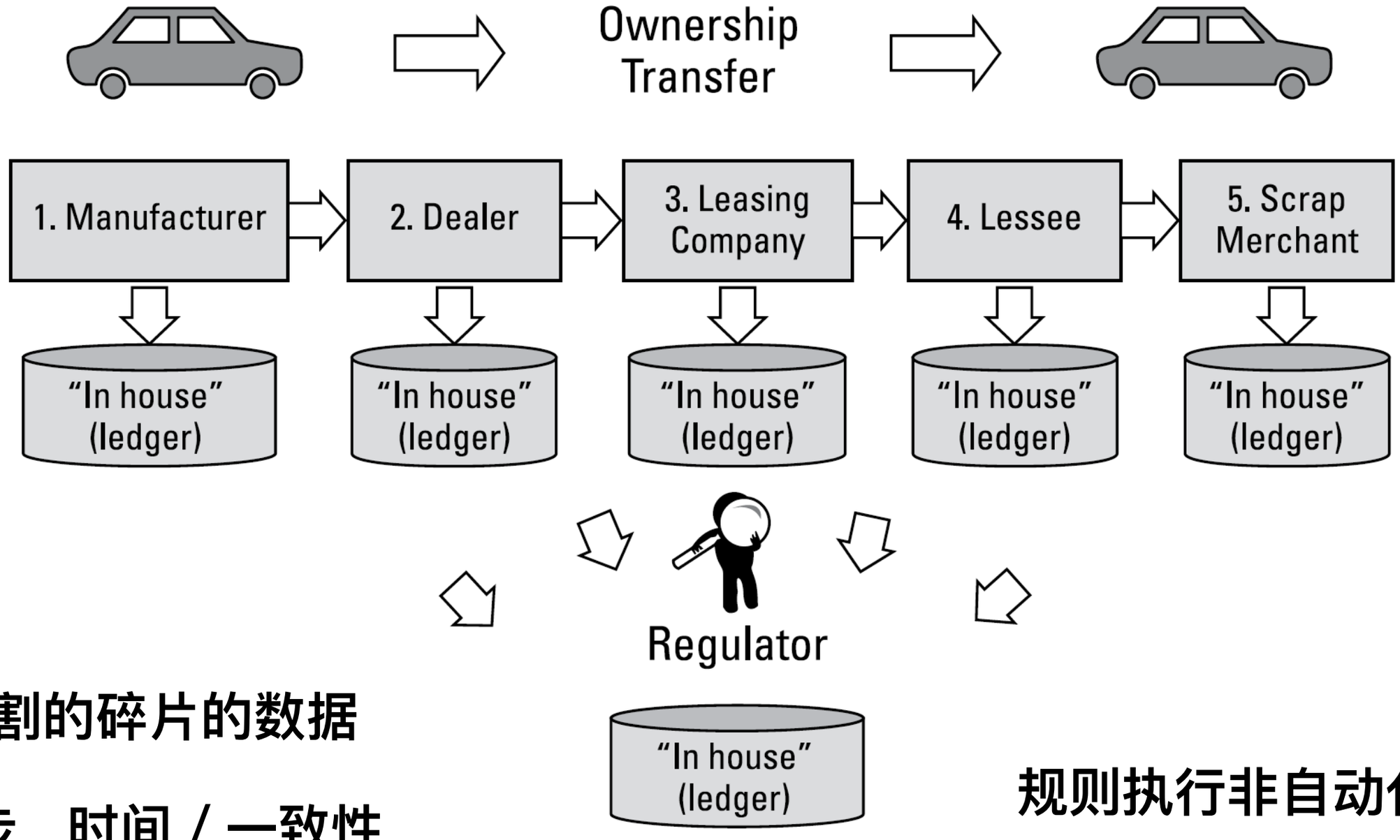


Chain / 链



Block / 区块

租车例子：没有区块链



分割的碎片的数据

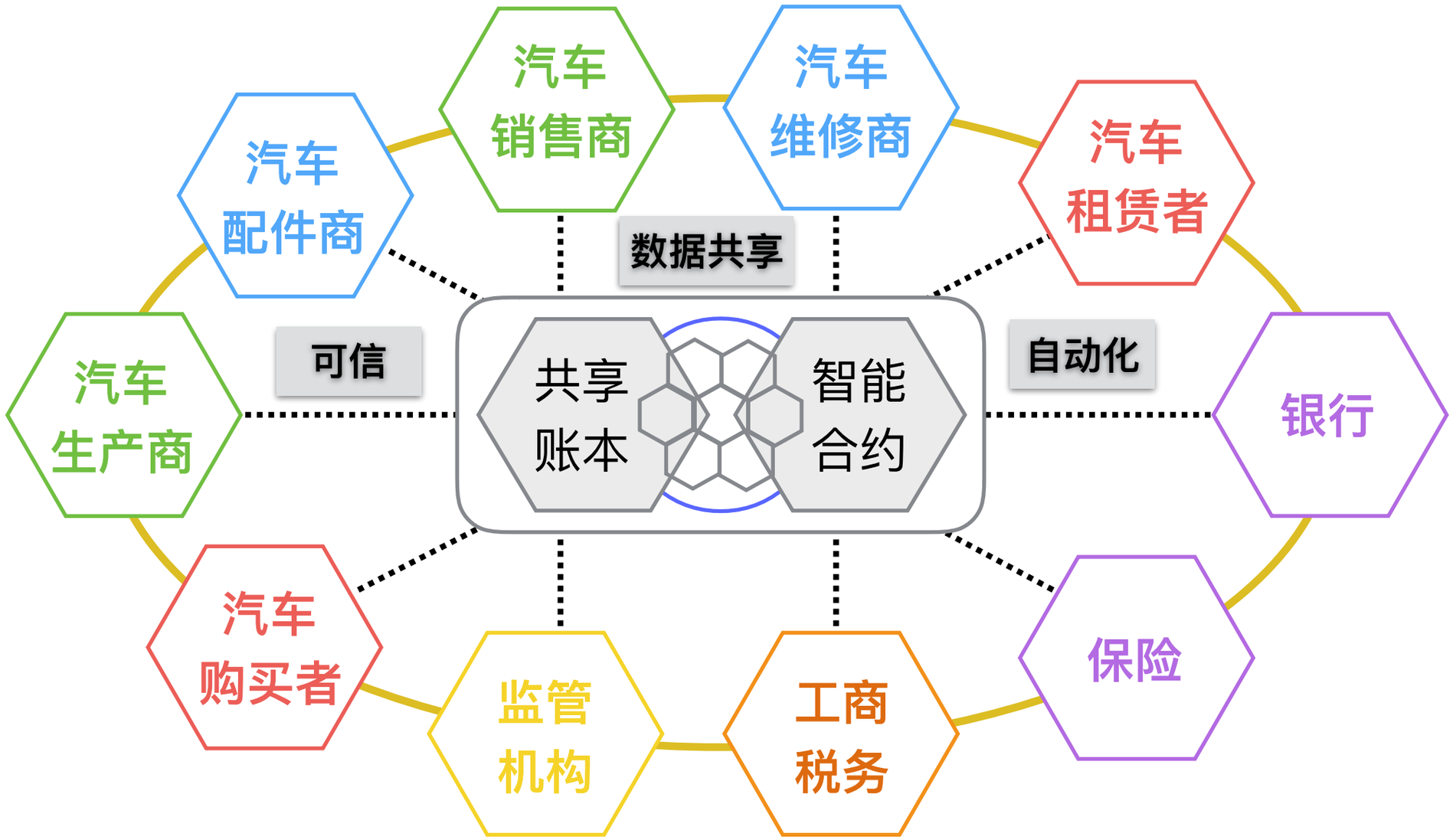
同步　时间 / 一致性

规则执行非自动化

区块链应用场景

数据一致性

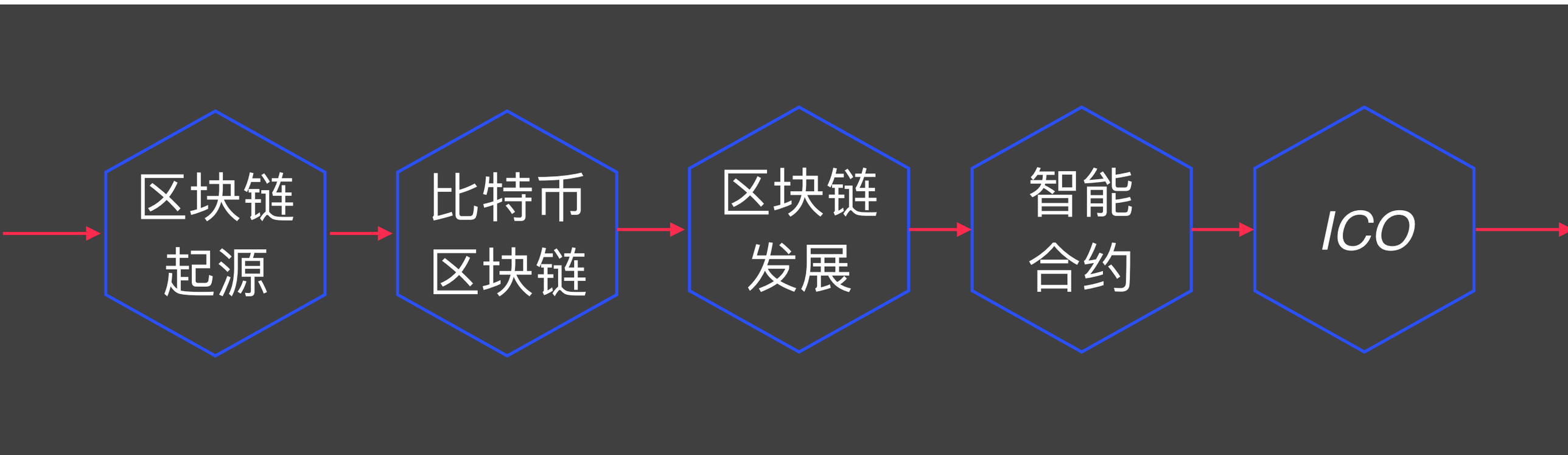
全生命周期管理



多中心

区块链增信

回顾

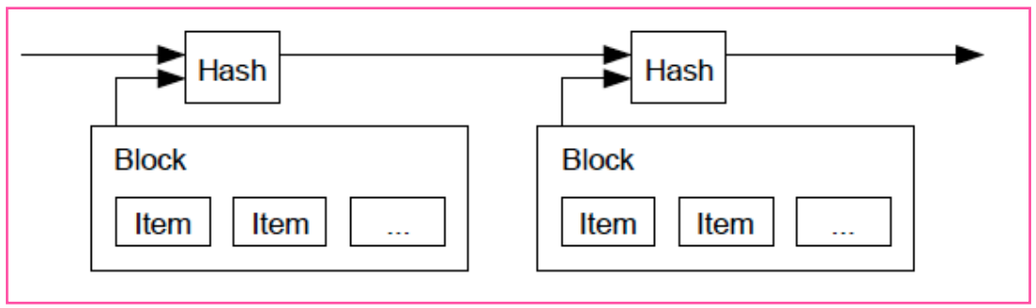


区块链起源

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

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



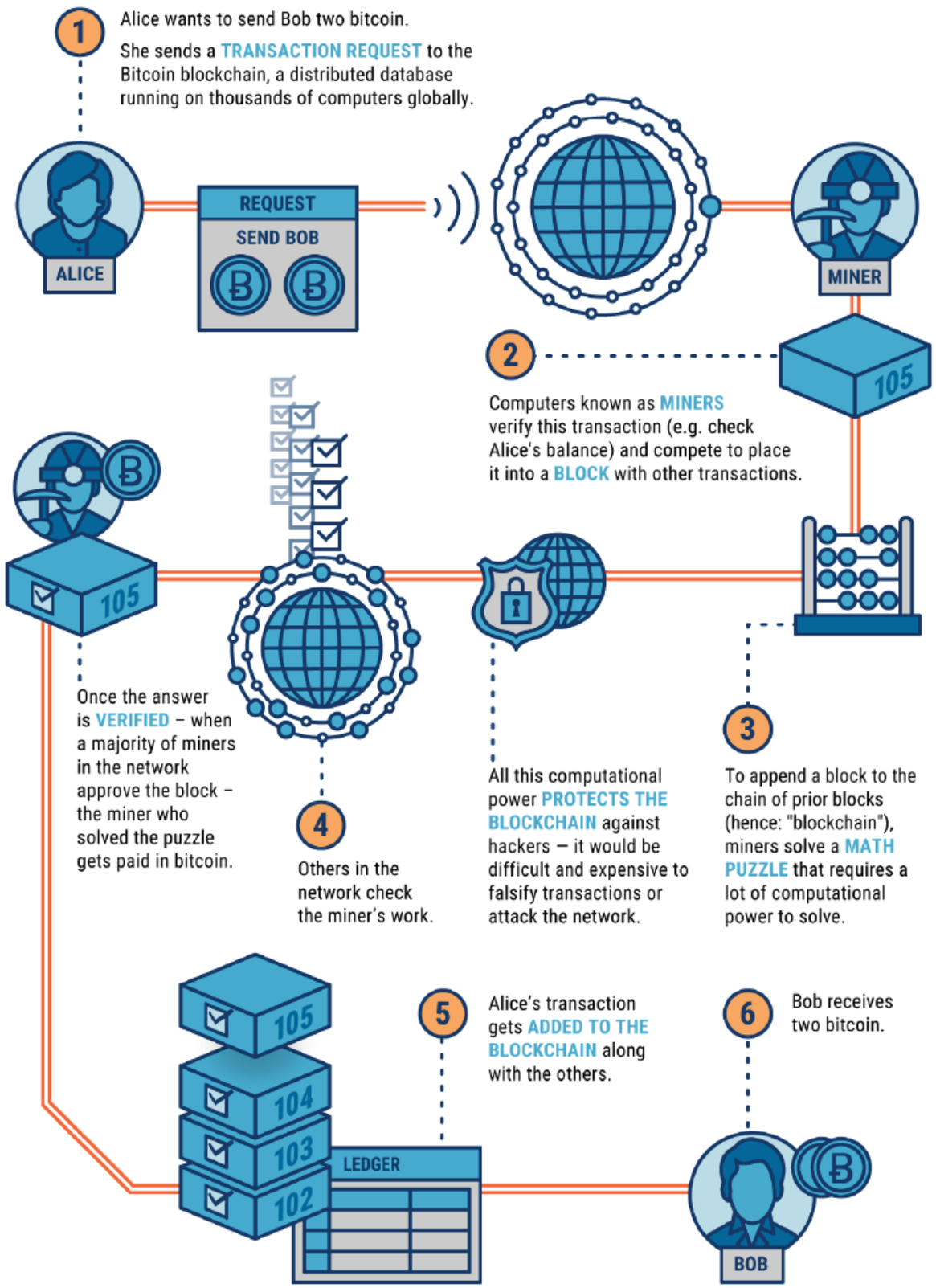
2008

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 … …

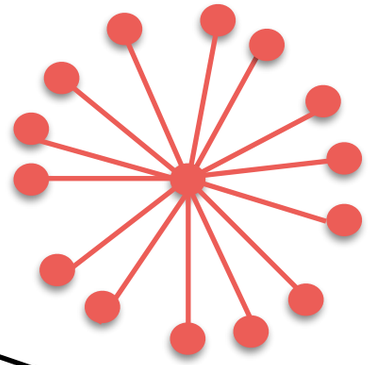
区块链

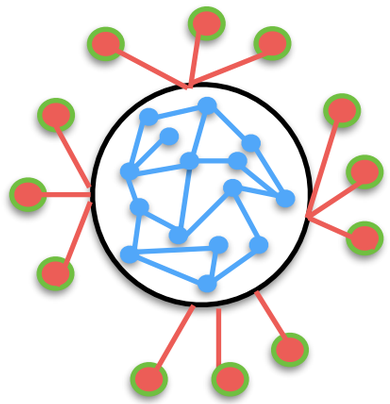
Blockchain Overview

区块链发展现状

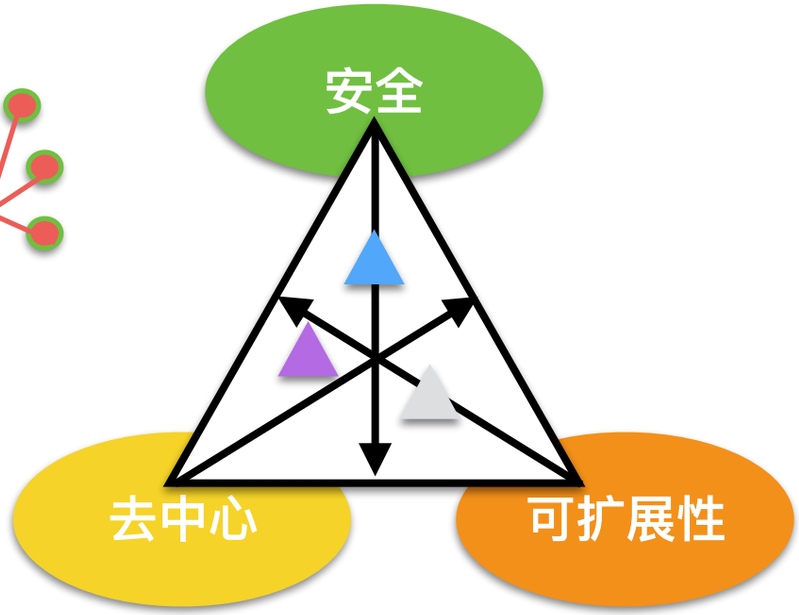
安全 信任 隐私

增加信任





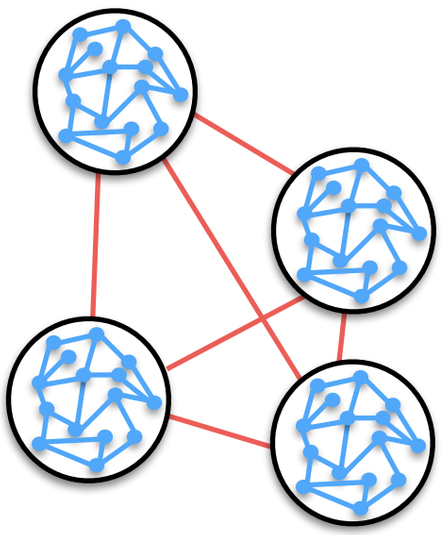
数据上链



2009

公链

适度去中心



货币

智能合约

ICO

私有区块链

1.0

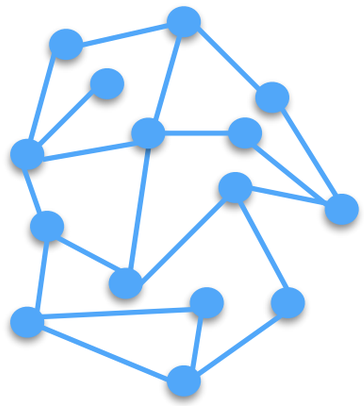
2.0

3.0

Block chain

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

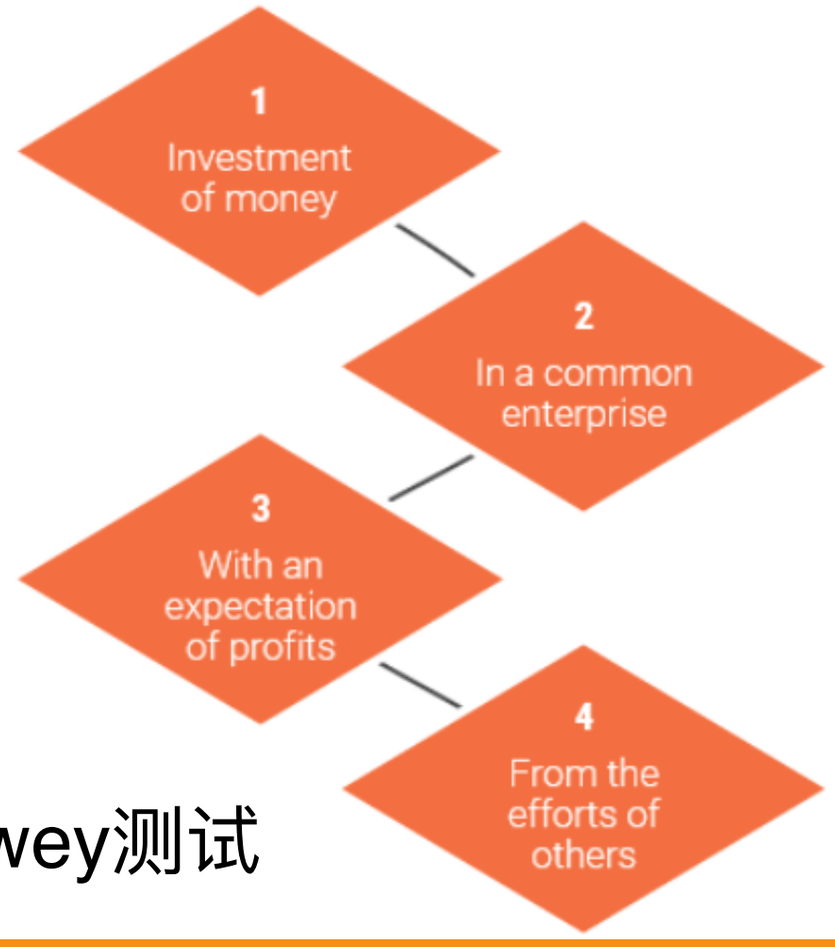
智能合约

- 完全数字化
- 自动执行
- 代码定义规则

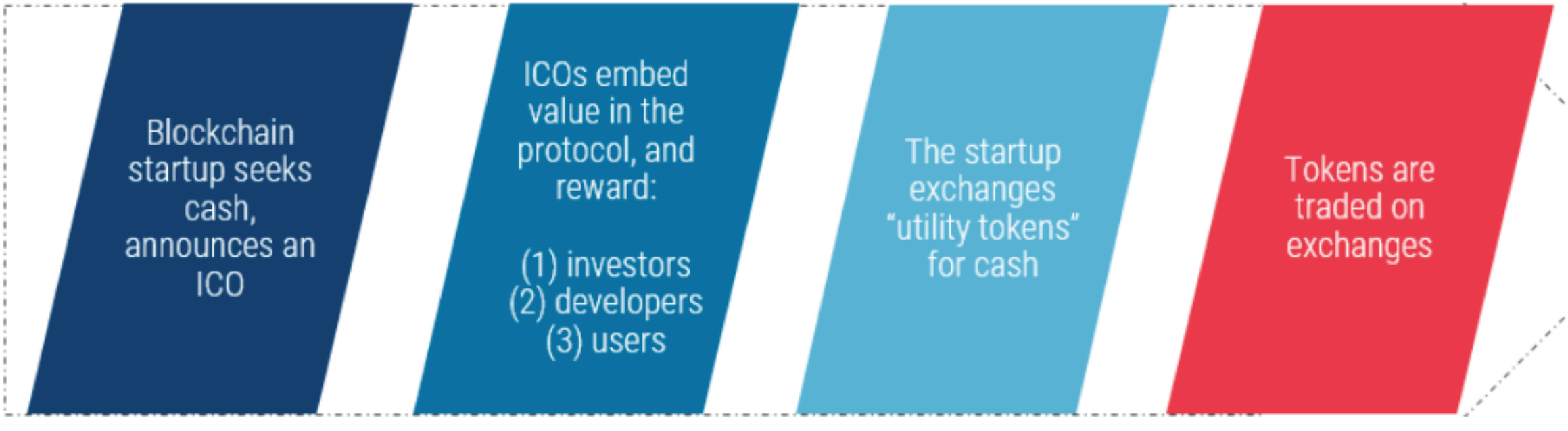
ICO

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

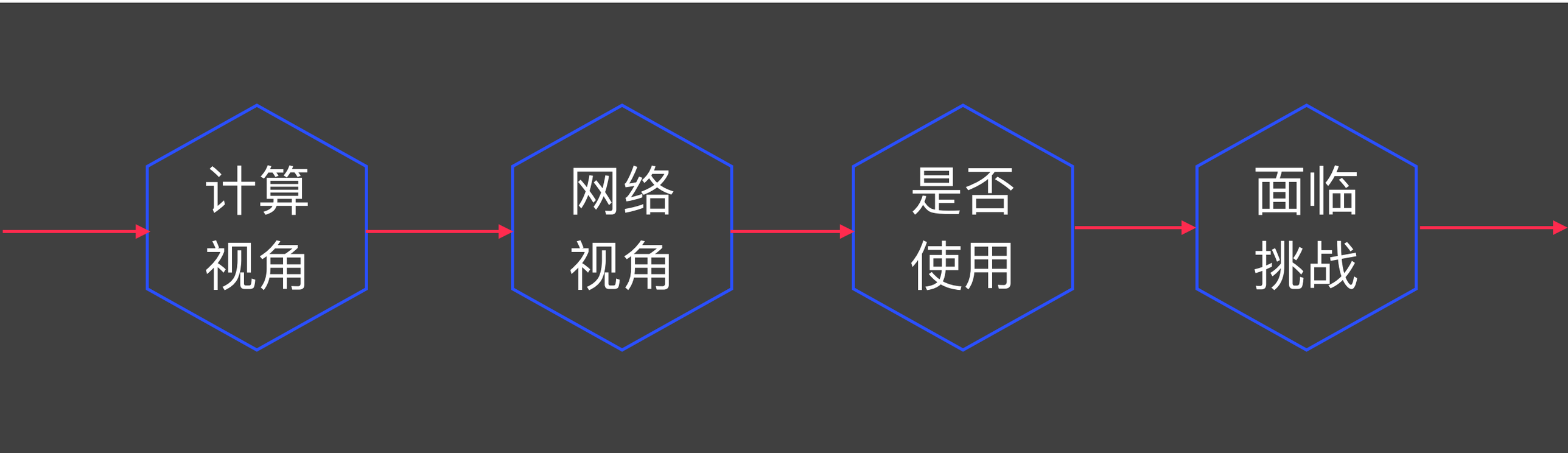
What is Blockchain Technology @ CBSInsights



Howey测试



剖析



Blockchain Overview

计算视角看区块链

?

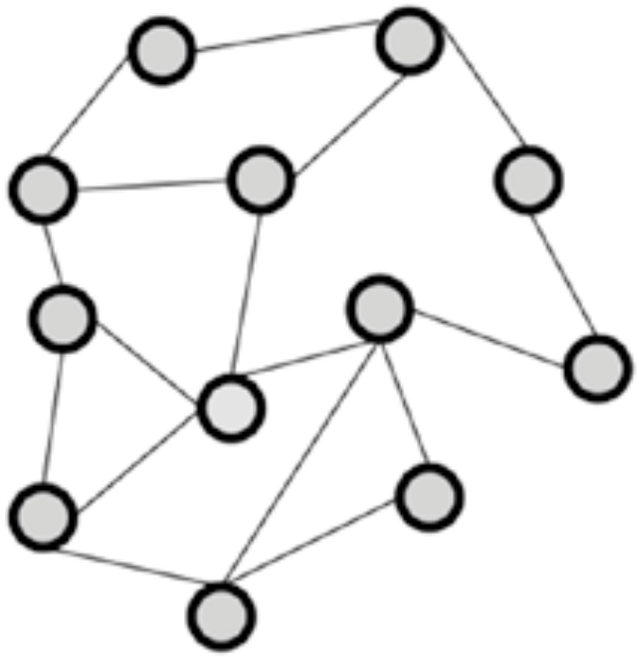
P2P

区块链

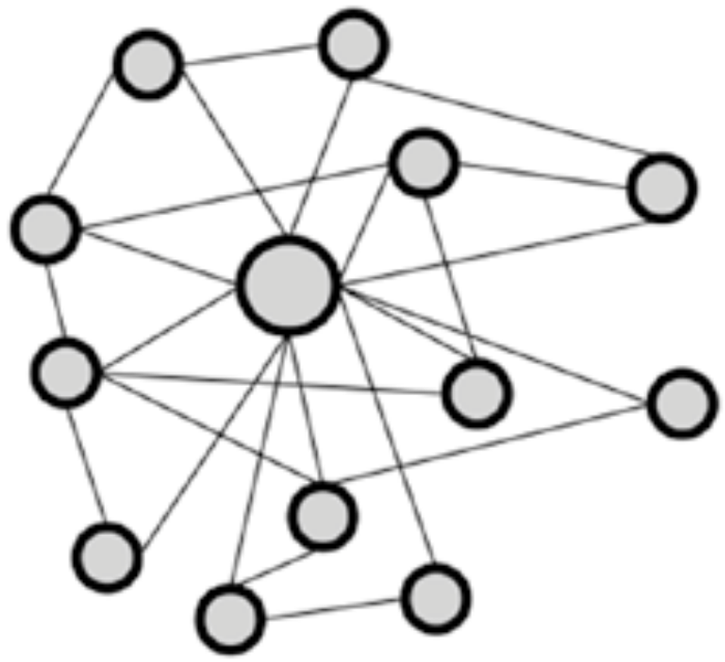
Client-Server

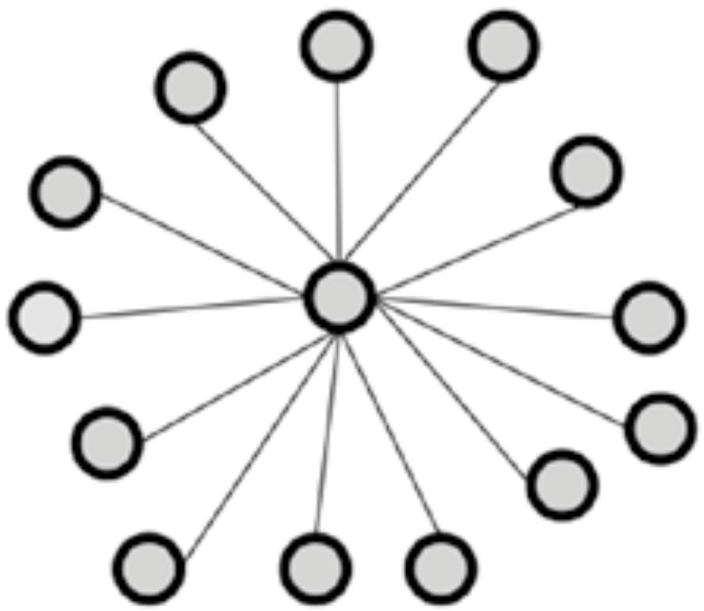
网络视角看区块链

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

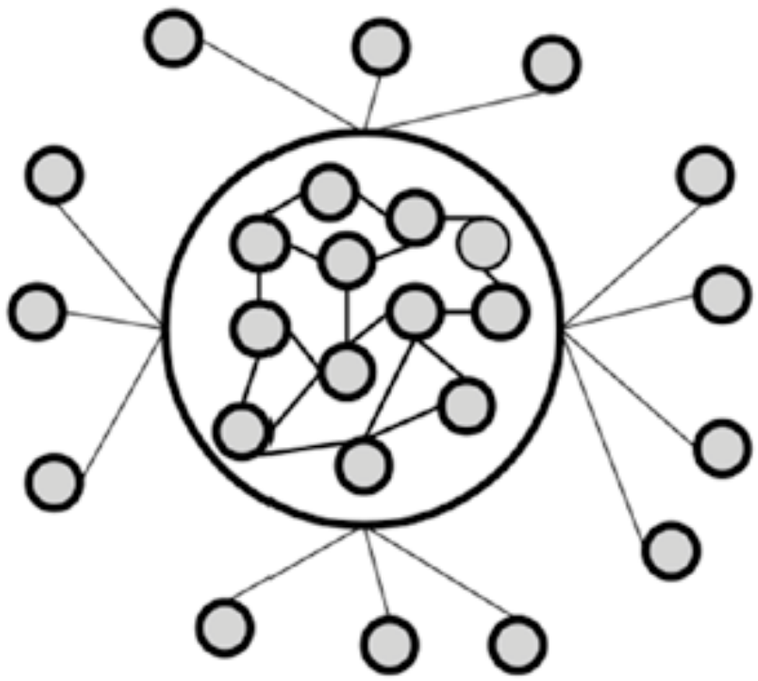


没有纯粹的
中心化系统
或者
分布式系统

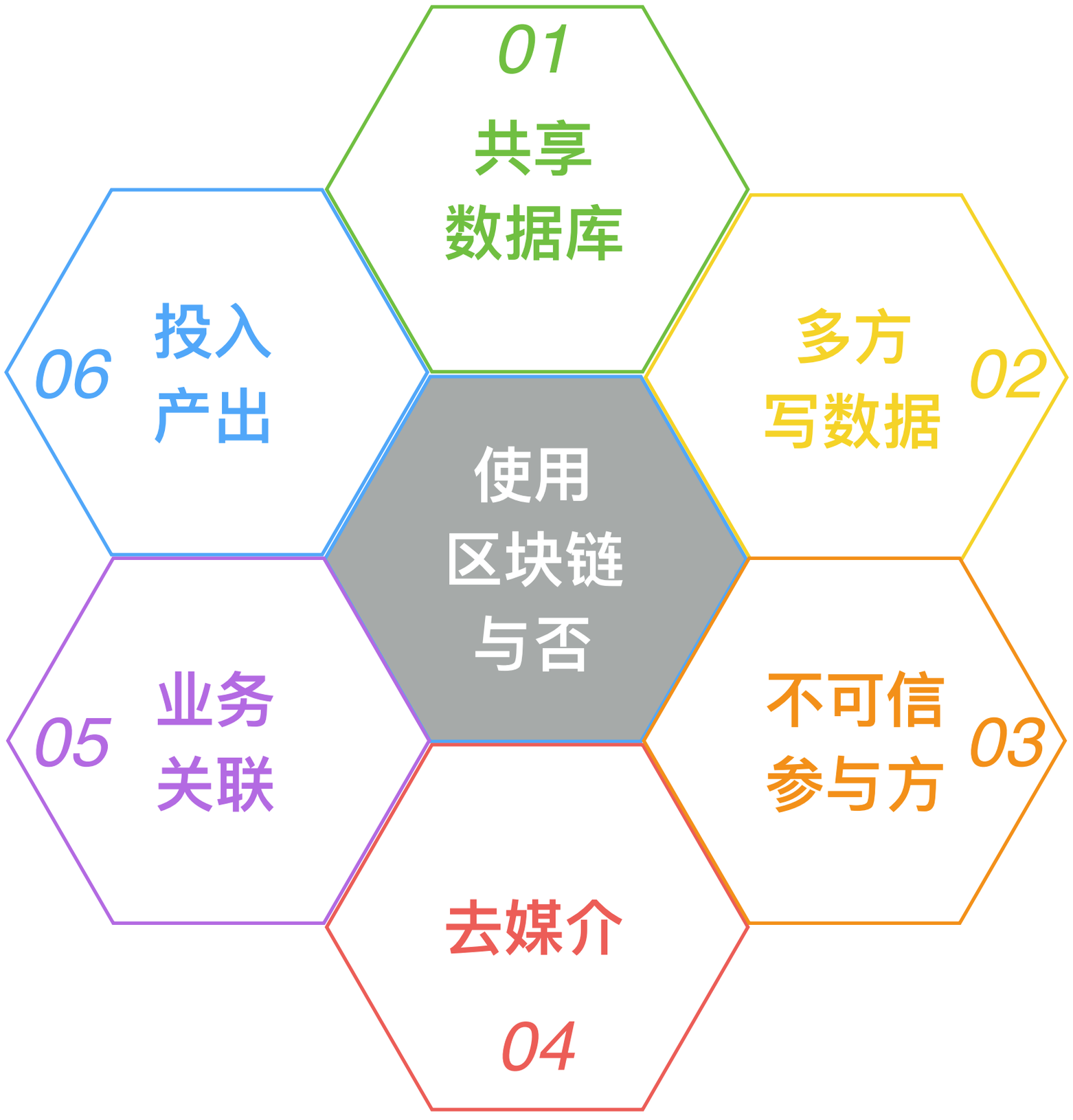




Internet
Email
IM
SNS



是否需要使用区块链



Blockchain Overview

区块链面临挑战

隐私保护

匿名 ↔ 真实身份

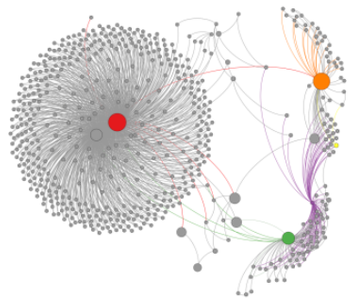
交易内容 ↔ 交易地址

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

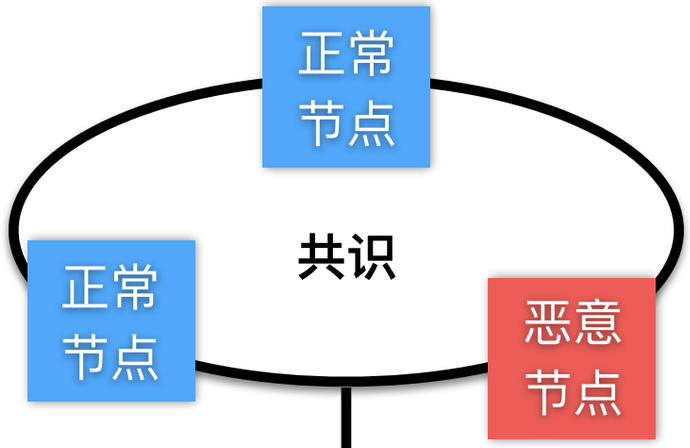
3

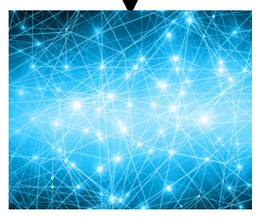
是否需要追求高的TPS

高TPS应用是否适合区块链

高不一定好，适合最好

安全攻击



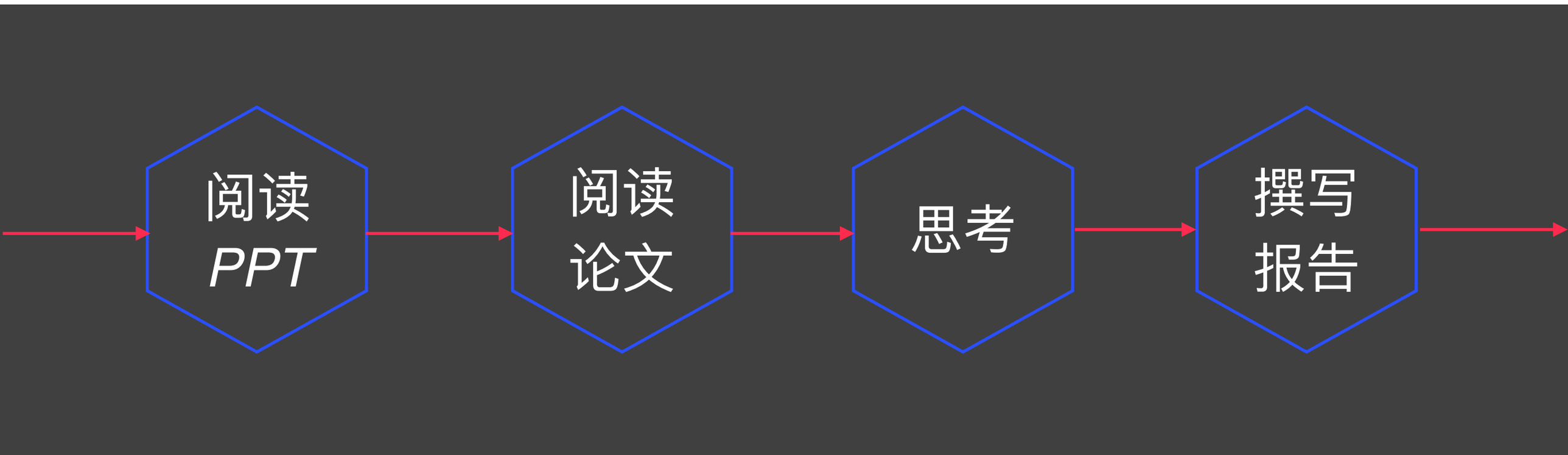


安全是一种权衡

51%攻击

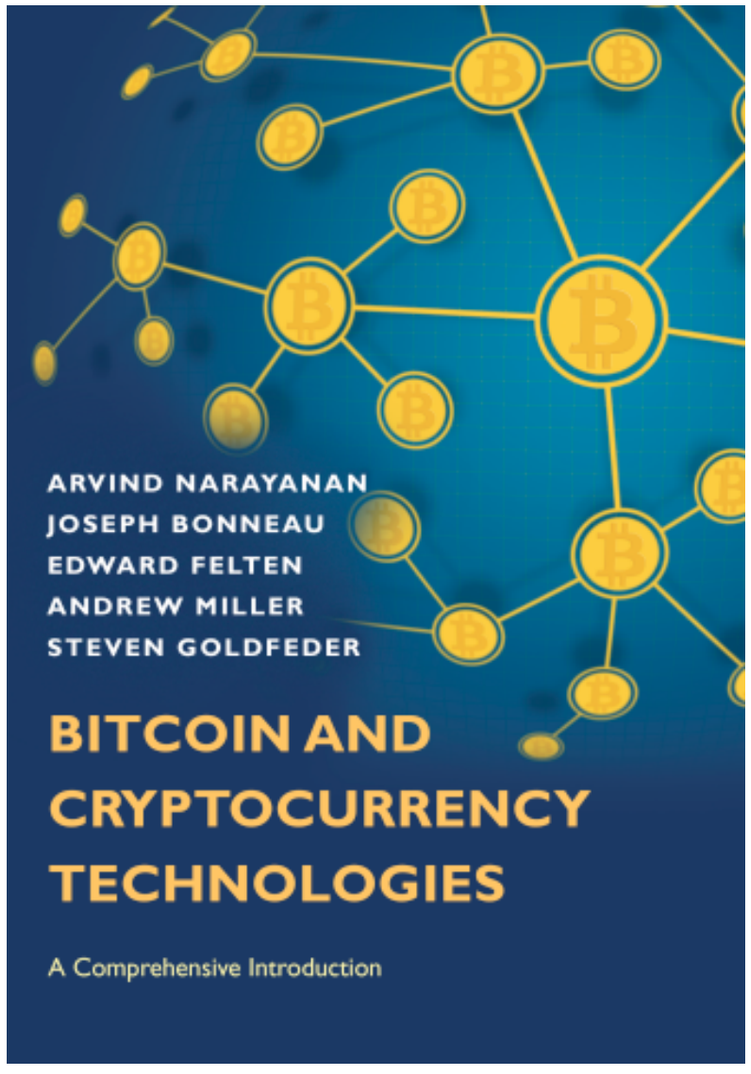
33.3%比例

课后作业



Homework

阅读教材



阅读引言

阅读第1-5章

Homework

课后作业

要求阅读如下资料，写阅读报告

Bitcoin Developer Guide

Find detailed information about the Bitcoin protocol and related specifications.

https://bitcoin.org/en/developer-guide#block-chain-overview

1、资料概述

2、主要收获

3、存在疑问

4、所思所感

周日晚上12点前
提交给助教

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io