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

上次课程内容回顾

1 信息安全经济学

- 安全工程
- 经济视角
- 差别定价
- 信息价格

2 信任

- 外部性
- 柠檬市场
- 信息泄露
- 博弈

3 大数据

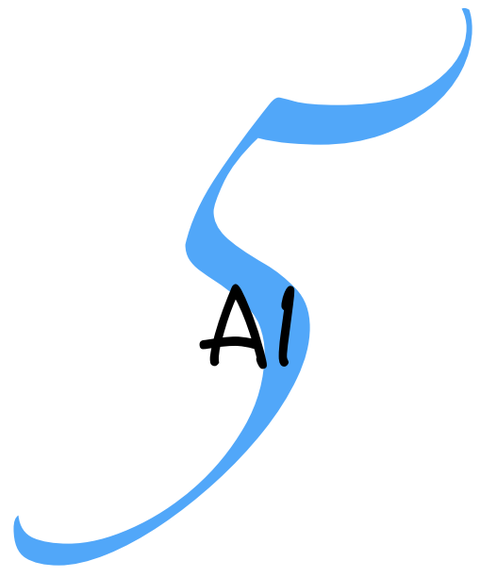
- 作用
- 信誉
- ebay等
- 信用评分

- 数字化
- 隐私
- 设备指纹
- 窃听

上次课程内容回顾

- 社会工程
- 网络钓鱼
- 安全选择
- 可用性

- 可用安全
- 挑战和目标
- 文本口令
- PassFaces等



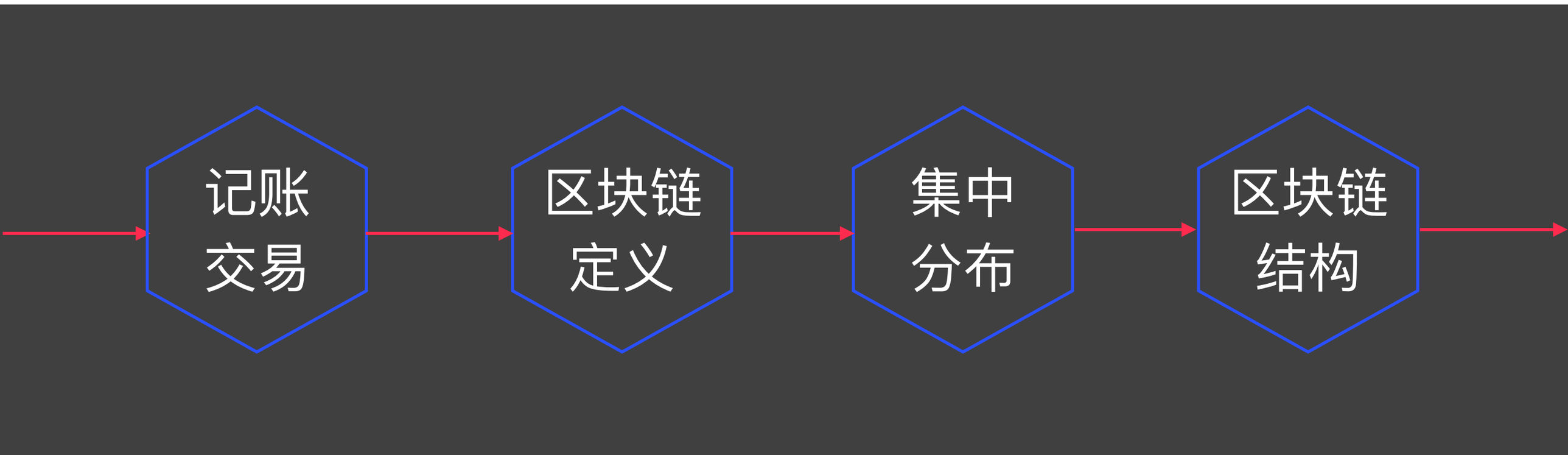
- CAPTCHA
- 人计算
- 人工智能
- 图像识别

- 算法正确性
- 结果汇聚
- ESP
- Turk

主要内容

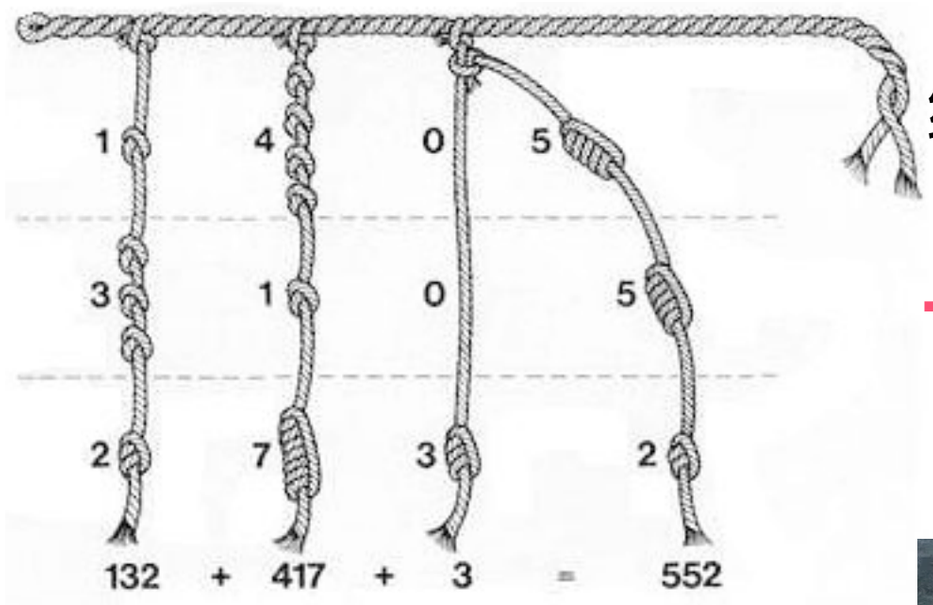

区块链定义与特性
会计视角
逻辑挑战
举例、面临挑战
数字货币
金融视角
区块链发展
1.0, 2.0, 3.0,
存证, DAPP
分布、集中、共识
网络视角
计算视角
基础设施、数字化

会计视角

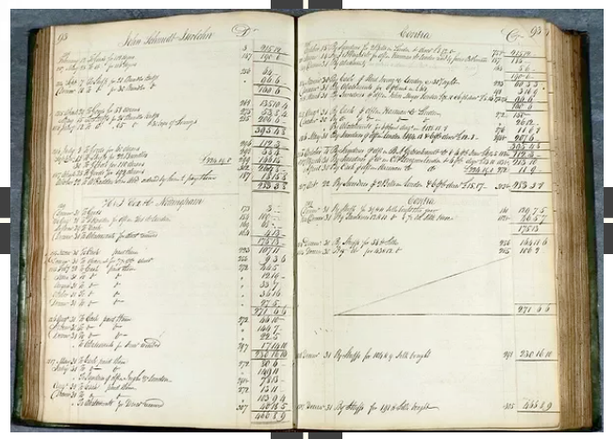


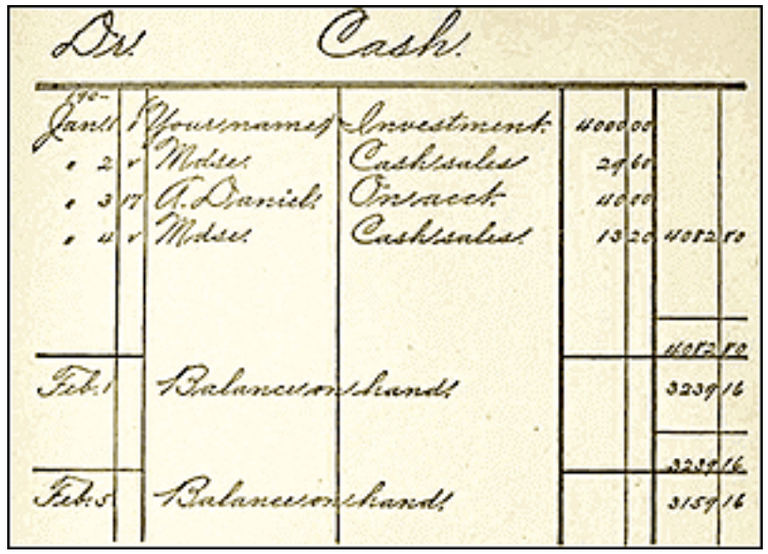
记账历史

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



结绳





单式

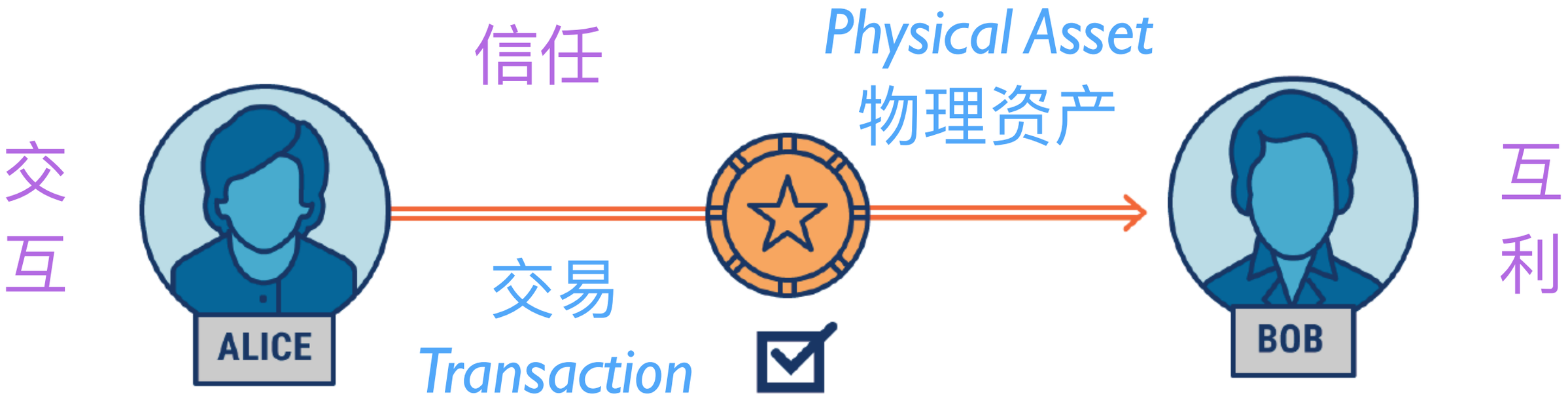
复式

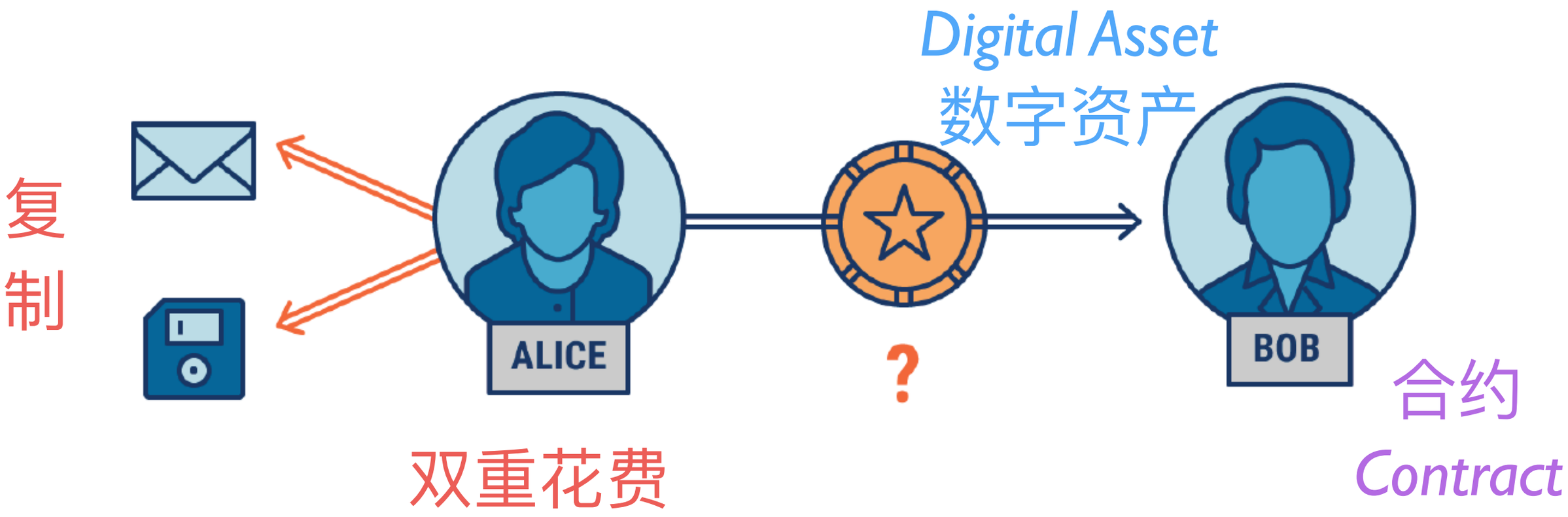
电子

物理

交易：物理 vs. 数字

What is Blockchain Technology @ CBSInsights





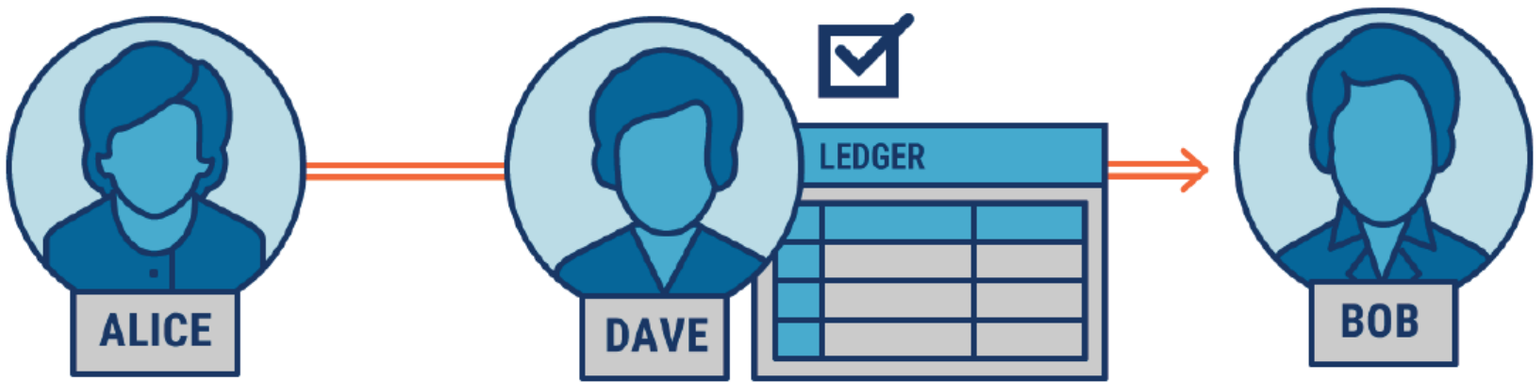
区块链定义

一个共享的分布式账本

用于在商业网络中
促进交易记录和资产跟踪

账本: 集中 vs. 分布

What is Blockchain Technology @ CBSInsights



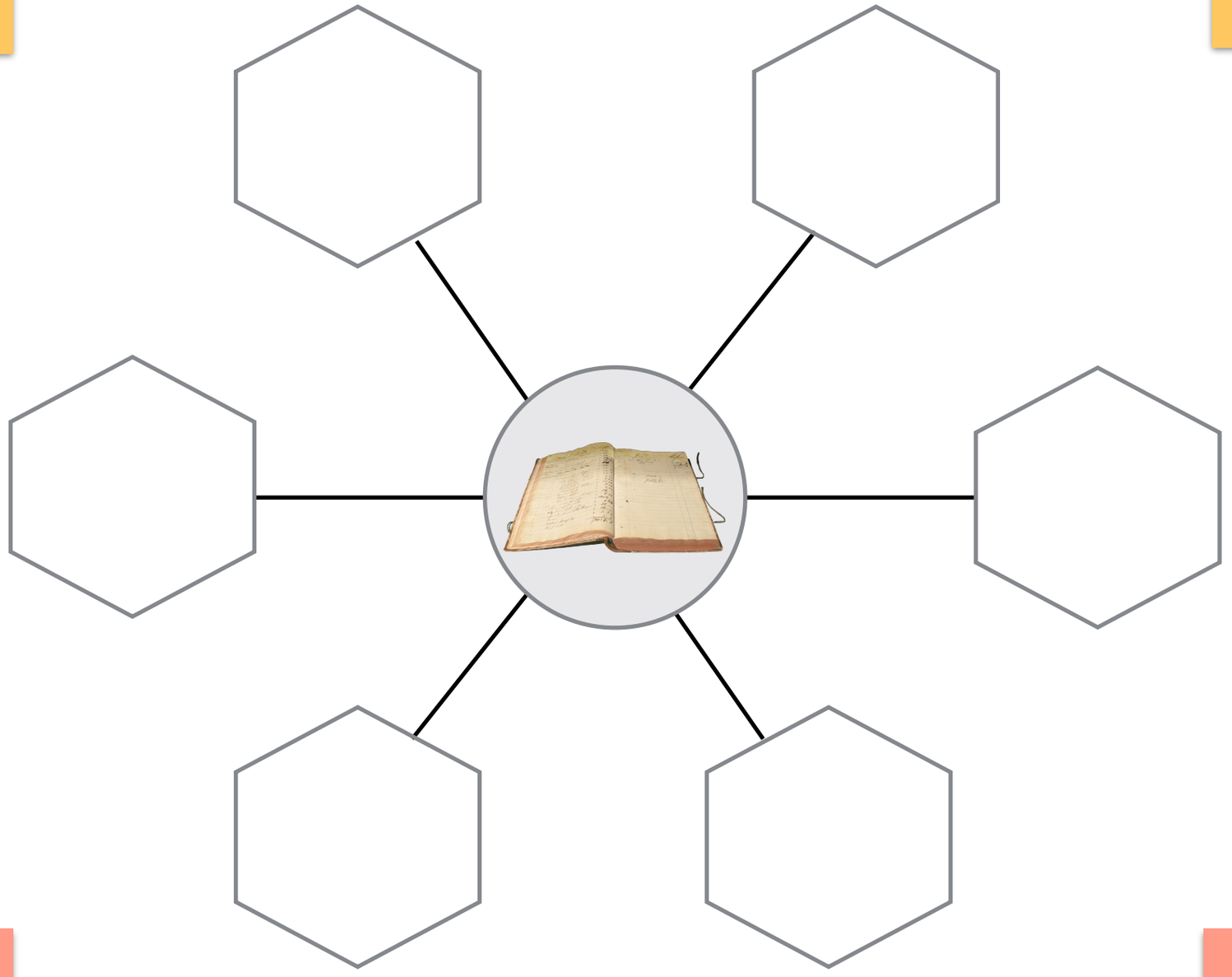
中心

P2P

集中式账本的优缺点

中心化

第三方



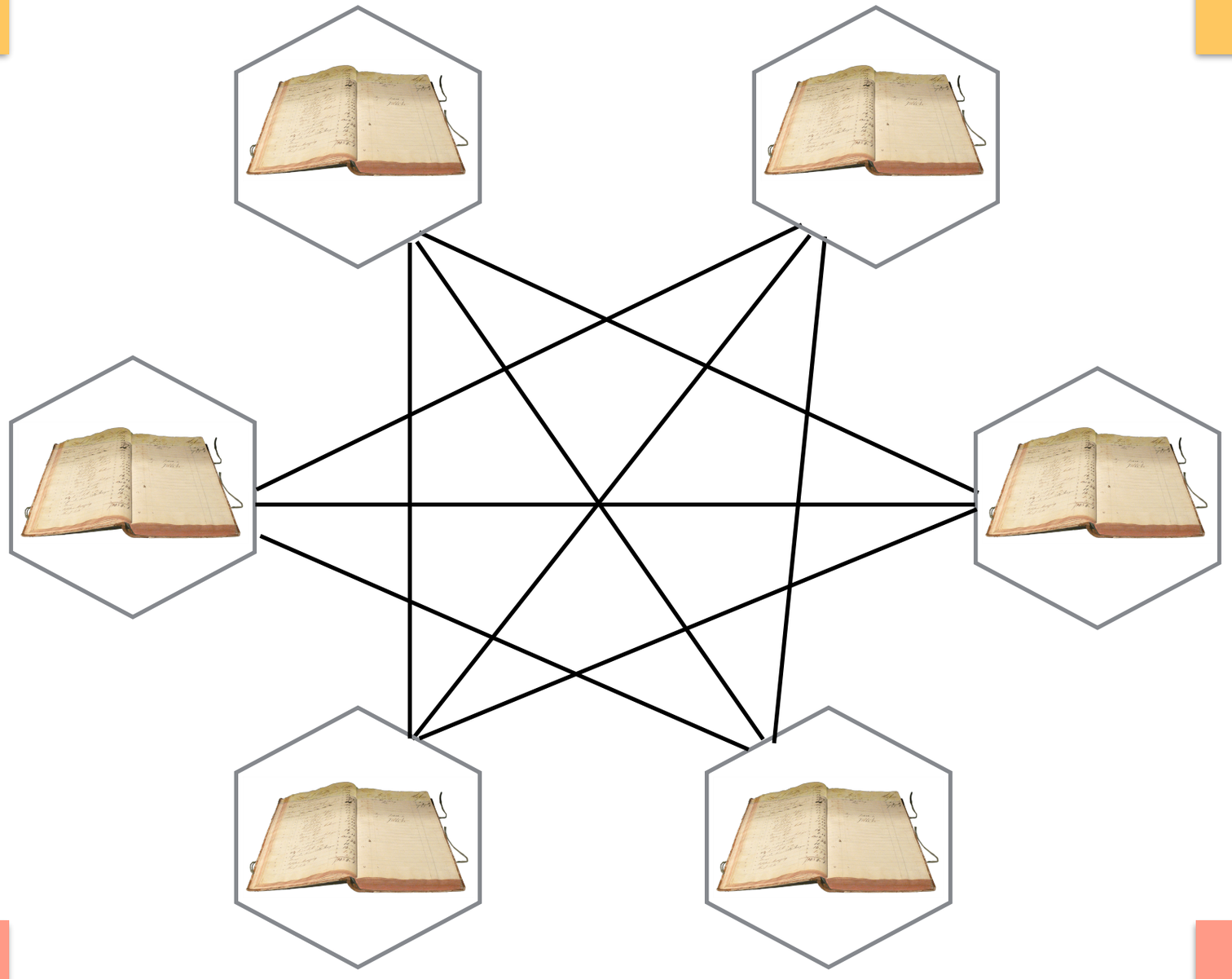
脆弱

信任

分布式账本的优缺点

一致性

完整性



效率

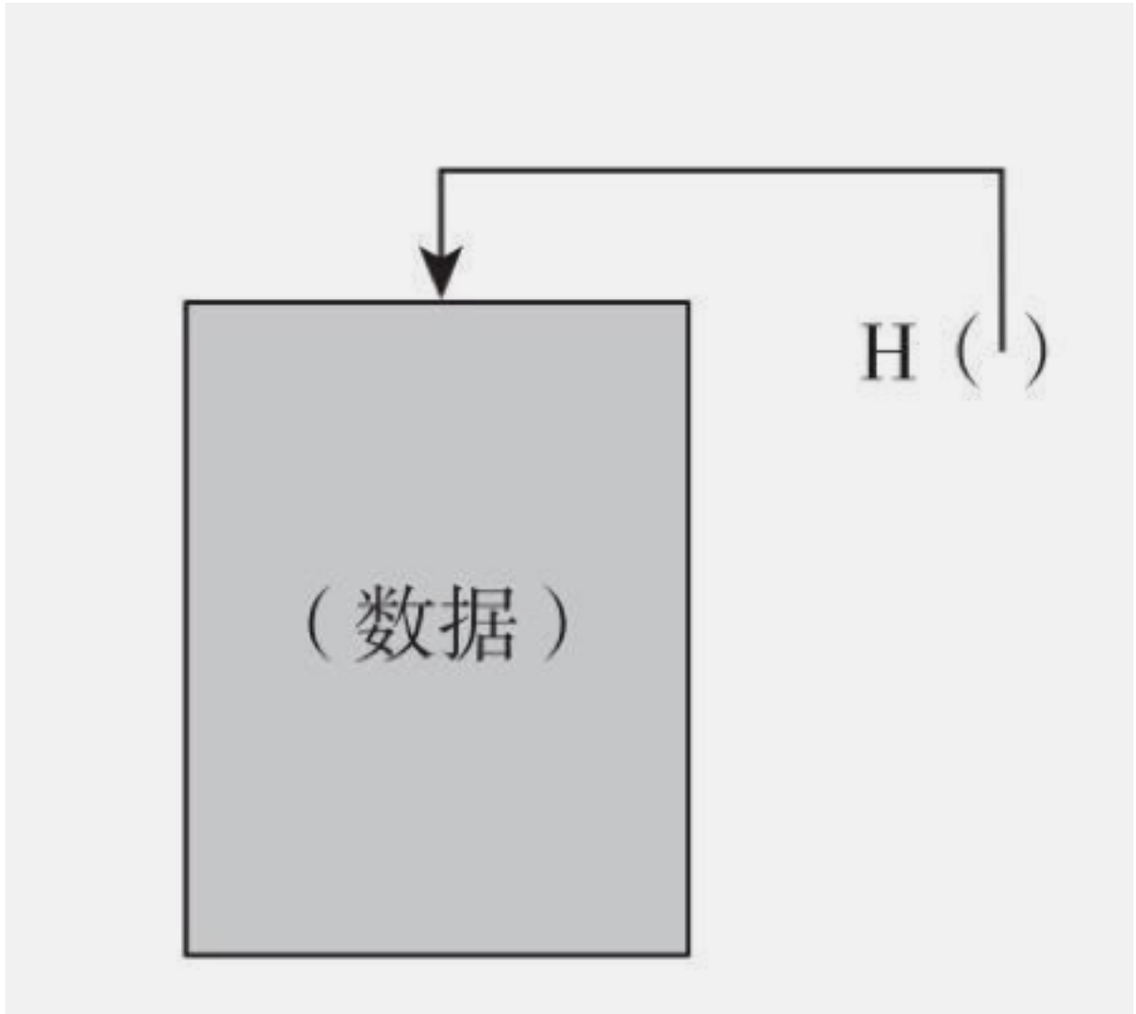
花费

Hash指针

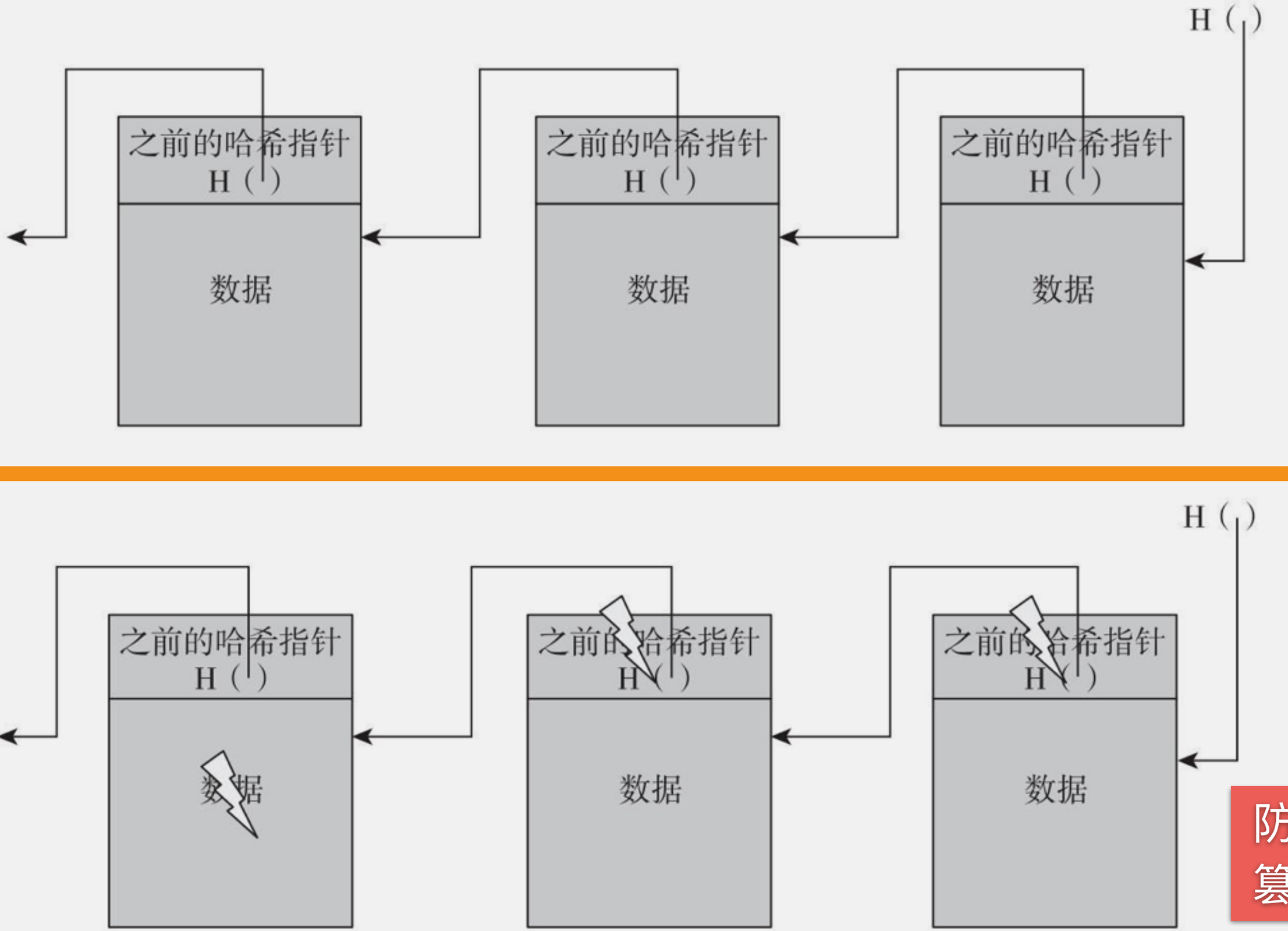
Hash指针：
是一个指向存储数据
及其数据Hash的指针

取回数据
验证数据是否改变

区块链的关键思想

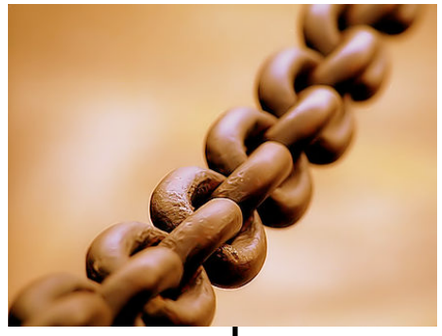


区块链

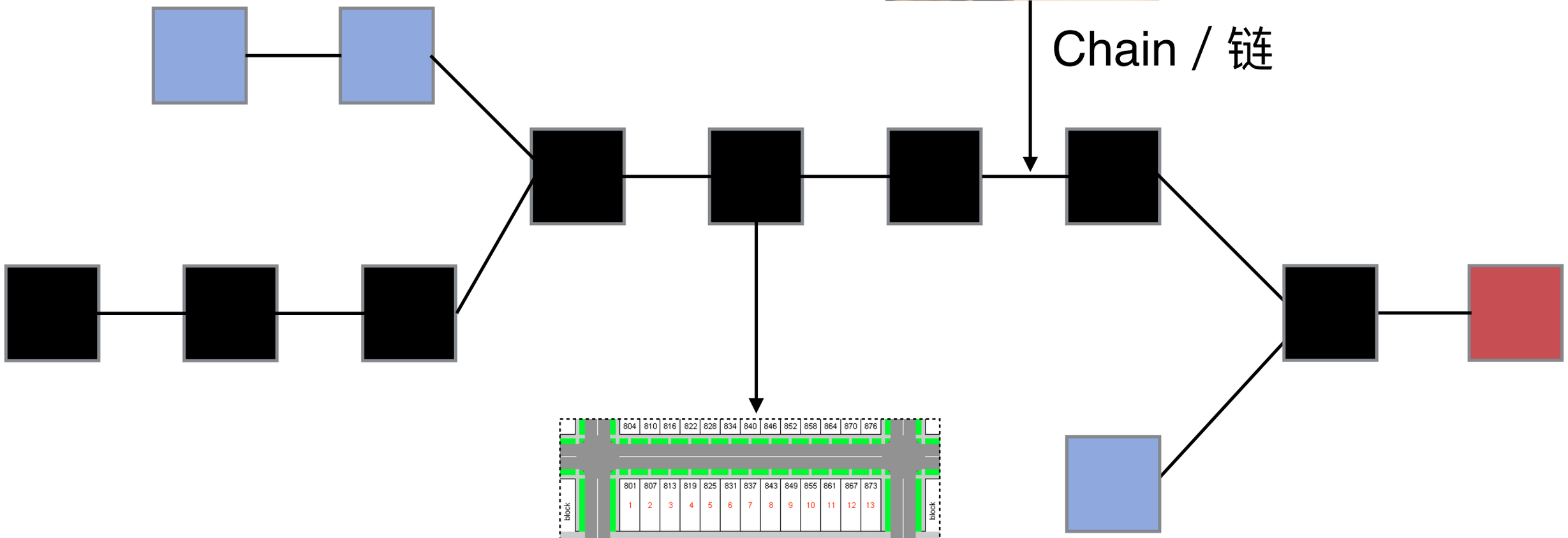

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
防止
篡改

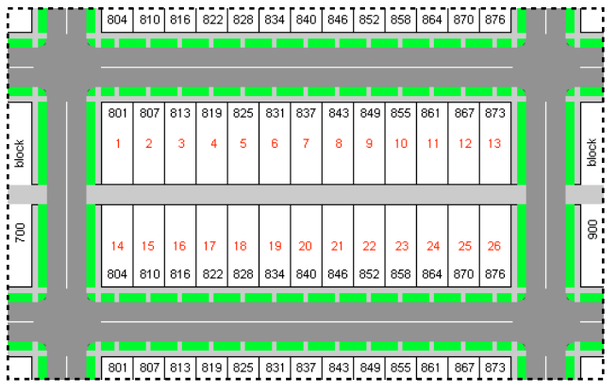
区块链结构

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



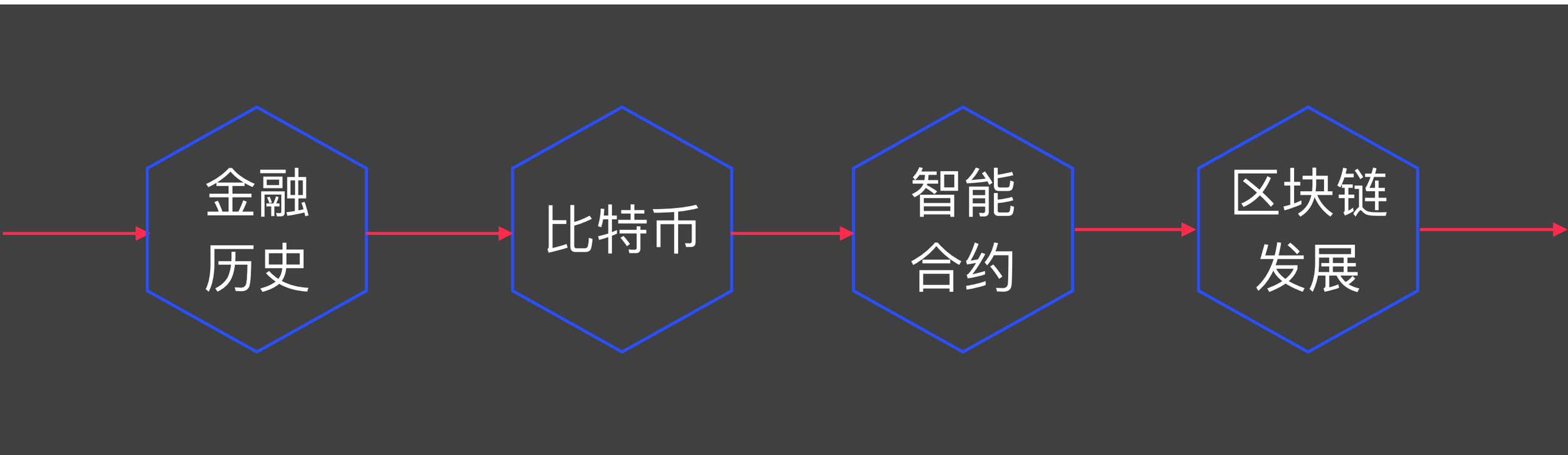
Chain / 链





Block / 区块

金融视角

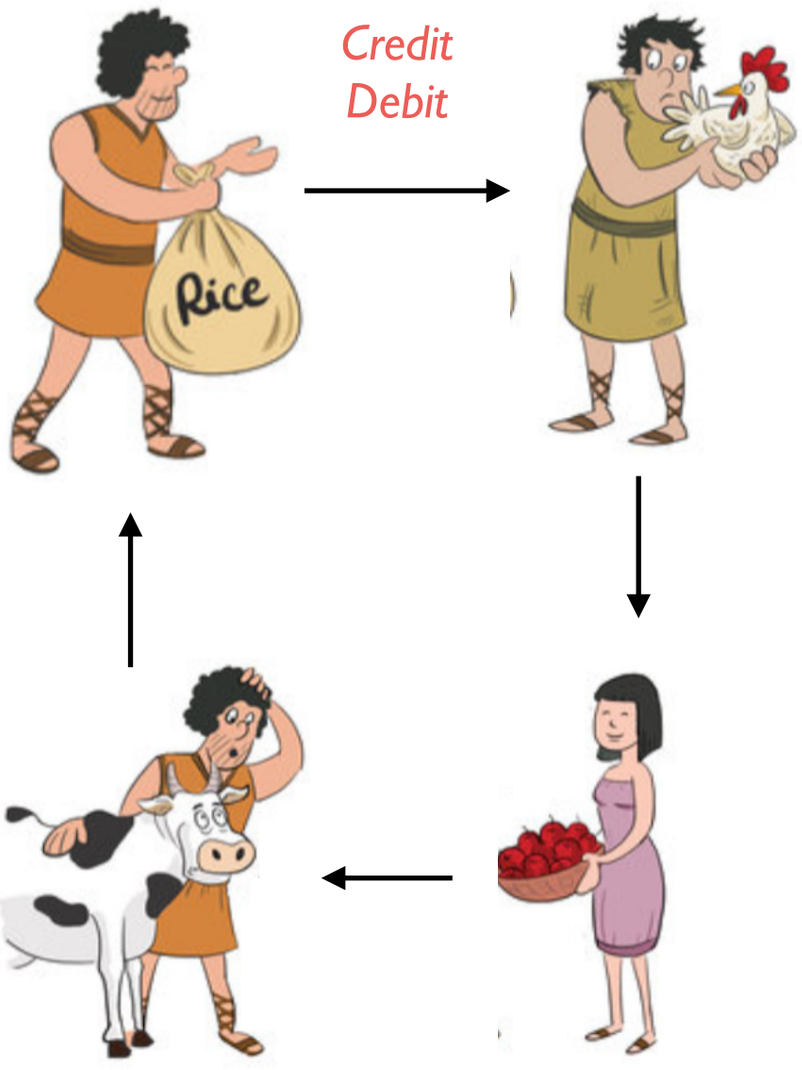


金融历史

Barter

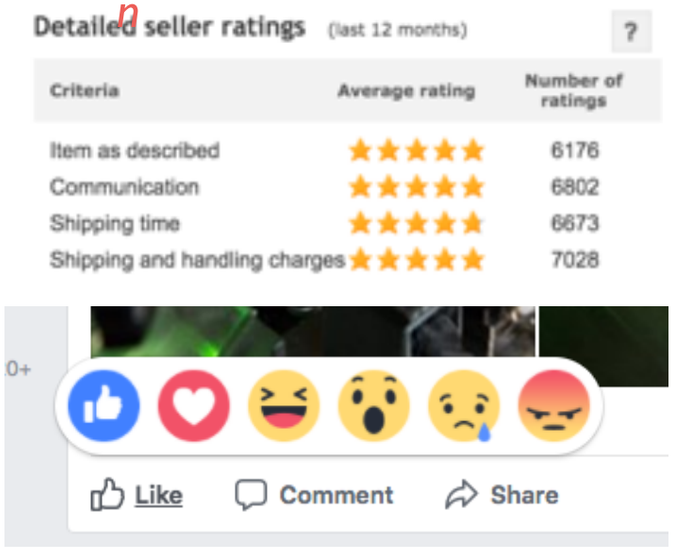
https://en.wikipedia.org/wiki/Barter

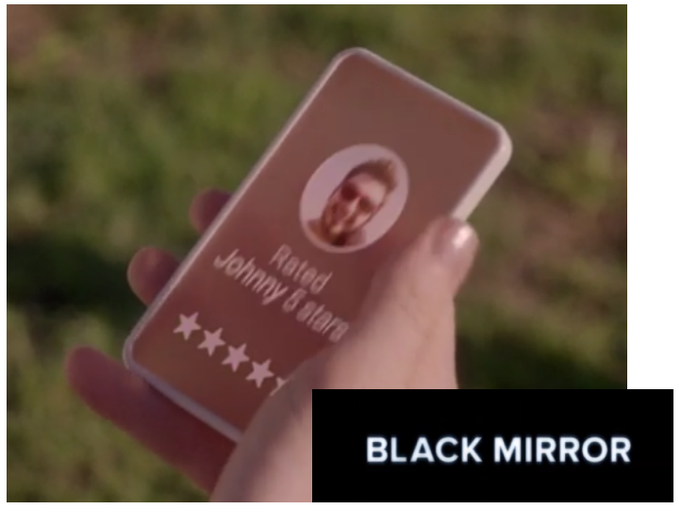
Credit Debit



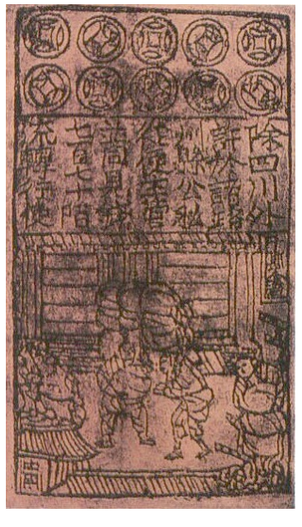
https://en.wikipedia.org/wiki/Money

Reputation





Money



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

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 →

法币

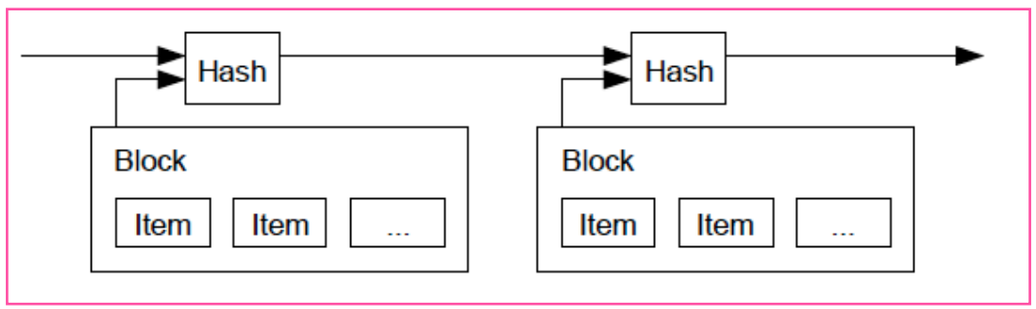

新版
2015年版 第5套
人民币
那些事...
中国人民银行
100
壹佰圆
样币
样币禁止流通
钞票正面
钞票背面
ZHONGGUO RENMIN YINHANG
100
YUAN
2015年
样币禁止流通
多一份金融了解
多一份财富保障
2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。
① 光变镂空开窗安全线
位于票面正面右侧。垂直票面观察，安全线呈品红色；与票面成一定角度观察，安全线呈绿色；透光观察，课件安全线中正反交替排列的镂空文字“¥100”。
② 雕刻凹印
票面正面毛泽东头像、国徽、“中国人民银行”行名、右上角面额数字、盲文及背面人民大会堂等均采用雕刻凹印印刷，用手指触摸有明显的凹凸感。
③ 胶印对印图案
票面正面左下方和背面右下方均有面额数字“100”的局部图案。透光观察，正背面图案组成一个完整的面额数字“100”。
④ 光彩光变数字
位于票面正面中部。垂直票面观察，数字以金色为主；平视观察，数字以绿色为主。随着观察角度的改变，数字颜色在金色与绿色之间交替变化，并可见到一条亮光带上下滚动。
⑤ 白水印
位于票面正面横号码下方。透光观察，可以看到透光很强的水印面额数字“100”。
⑥ 人像水印
位于票面正面左侧空白处。透光观察，可见毛泽东头像。
⑦ 横竖双号码
票面正面左下方采用横号码，其冠字和前两位数字为暗红色，后六位数字为黑色；右侧竖号码为蓝色。
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

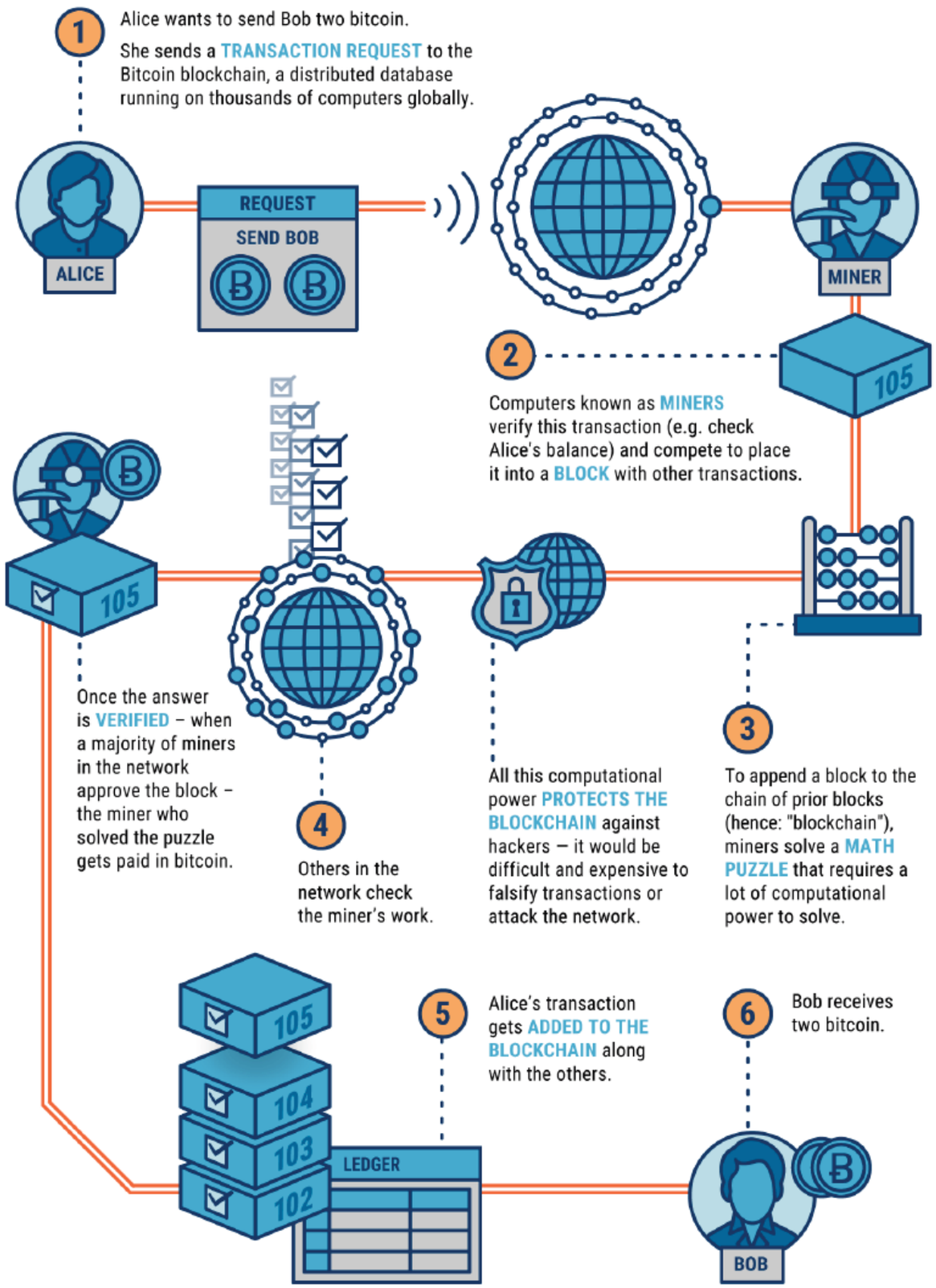
比特币隐含在汇款方到收款方的转账交易中，用户用自己私钥来证明

传统银行依靠发行和结算，比特币依靠挖矿

Blockchain Overview

比特币和区块链

What is Blockchain Technology @ CBSInsights



比特币 … 超级账本

区块链

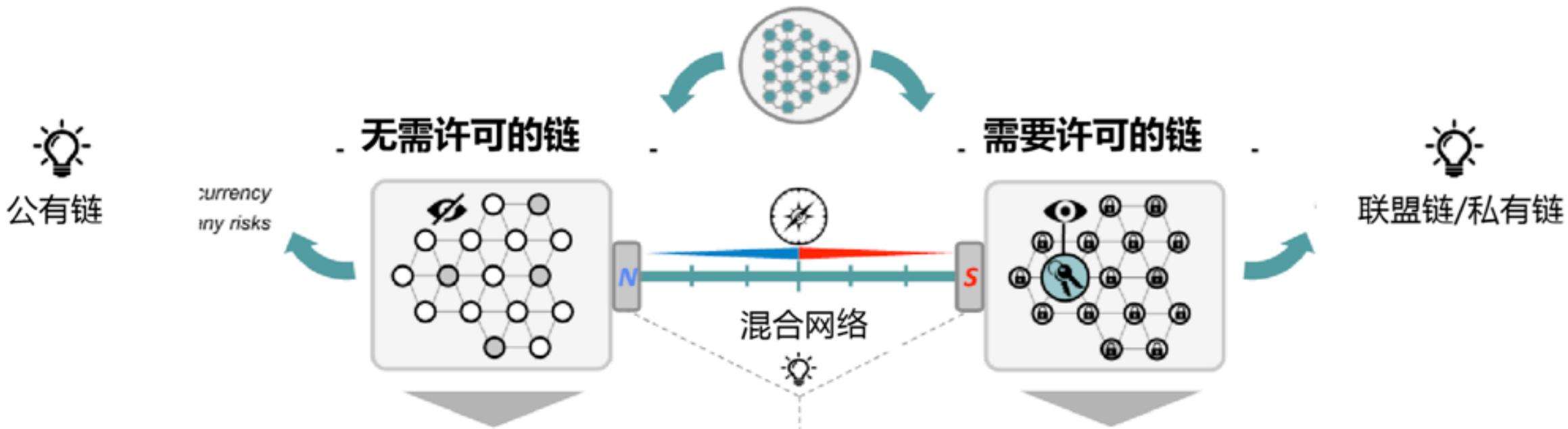
比特币 超级账本

以太坊 R3 Corda

EOS … …

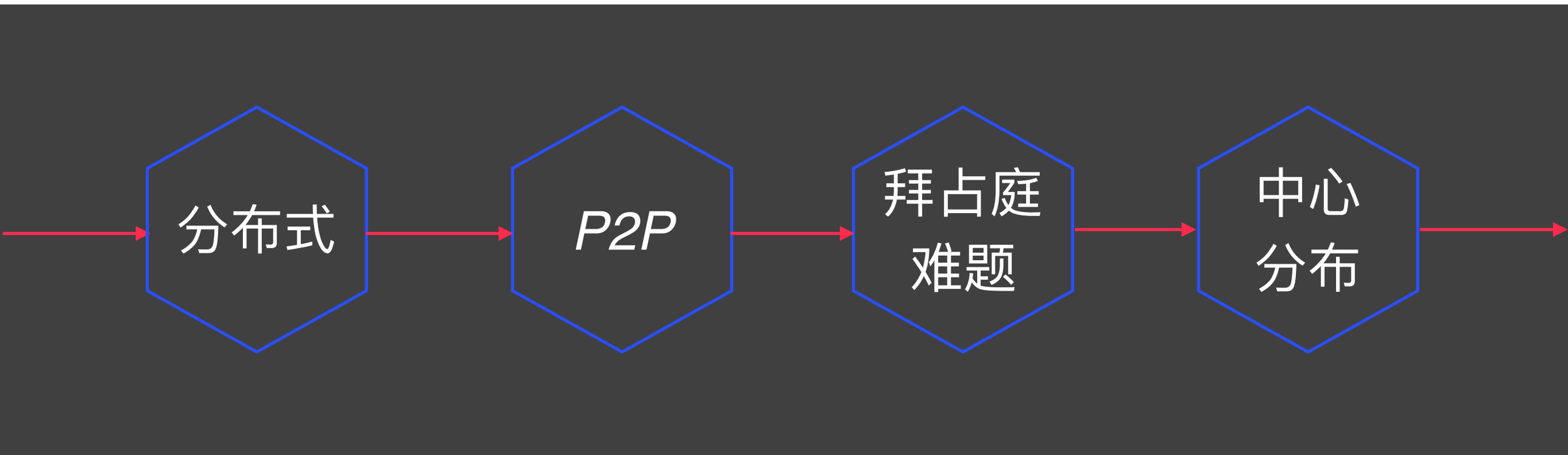
区块链

区块链分类



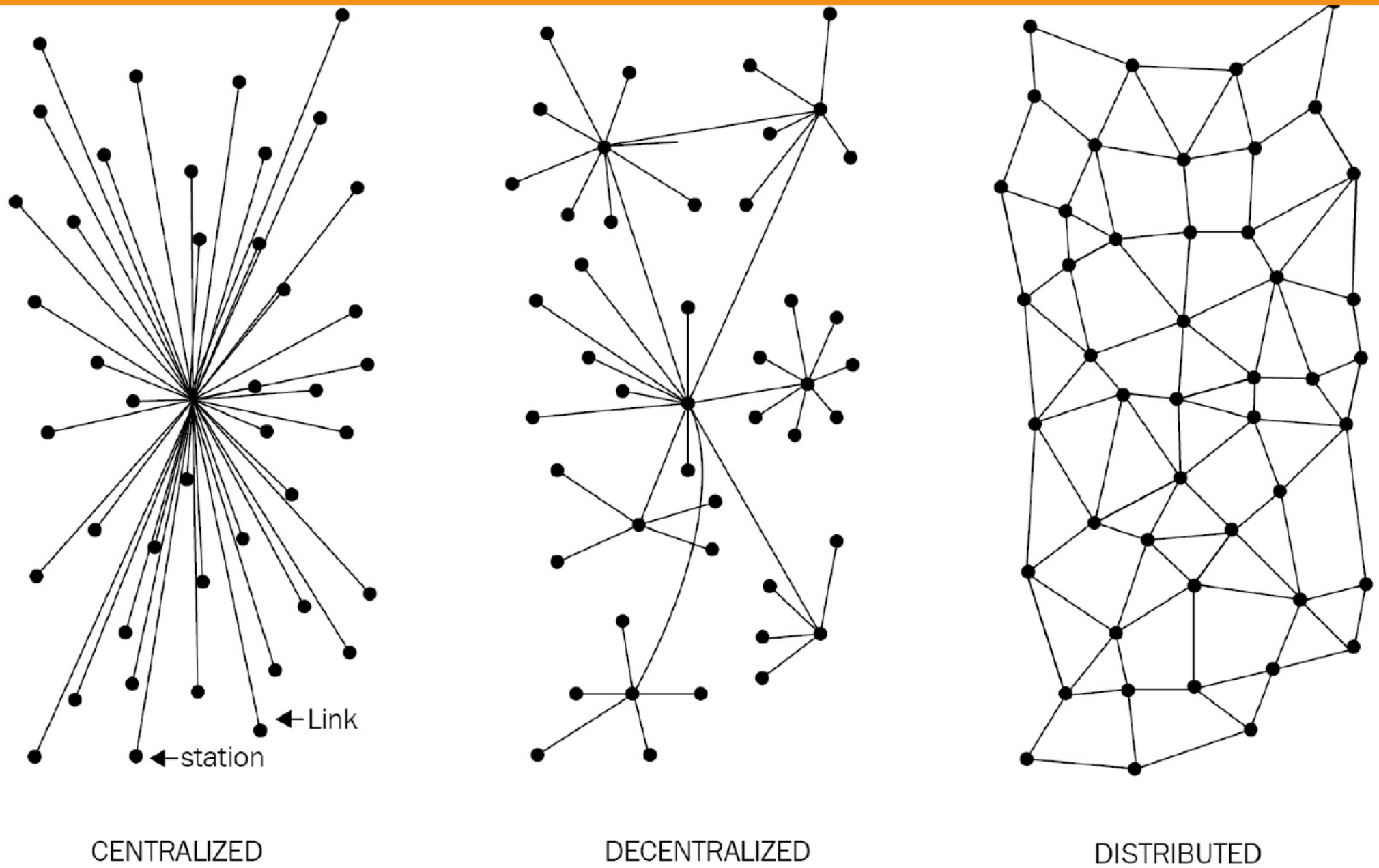
• 用户匿名	• 用户验证
• 网络接入不受限	• 网络接入需要管控
• 账本写入的见证者列表是不确定的	• 账本写入的见证者列表是确定的
• 没有系统管理员	• 有系统管理员，可配置和管控系统

网络视角



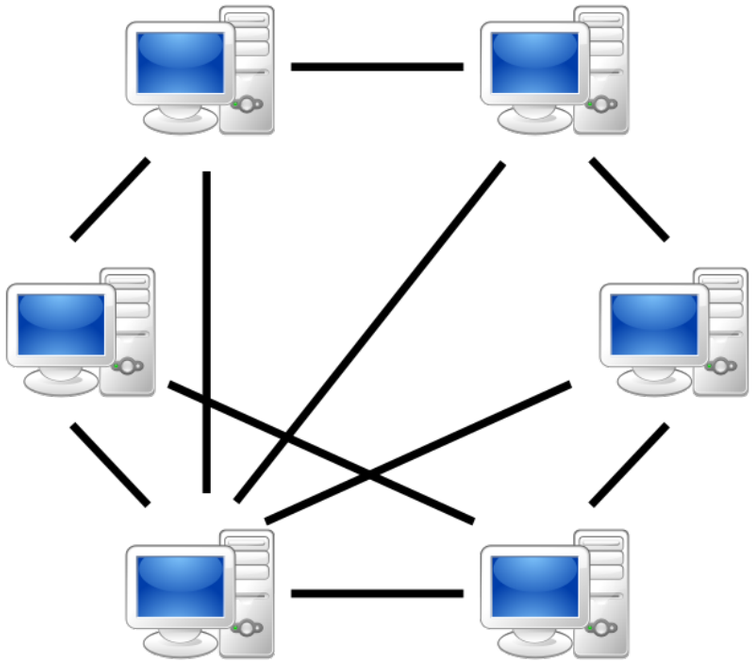
网络和系统的不同类型

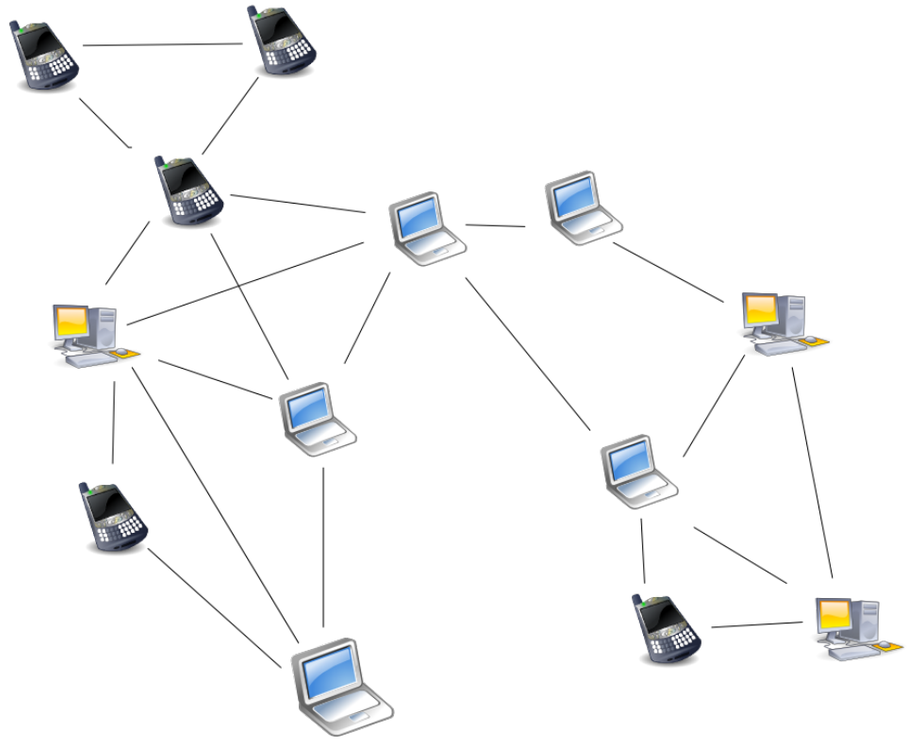
有效性 | 迅速决策 | 更好动机 | 减少管理负担

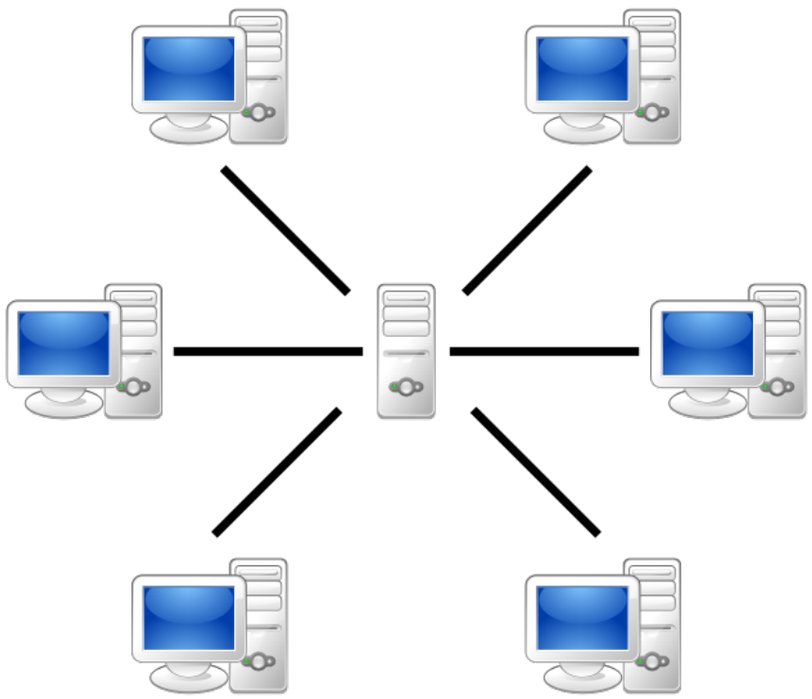


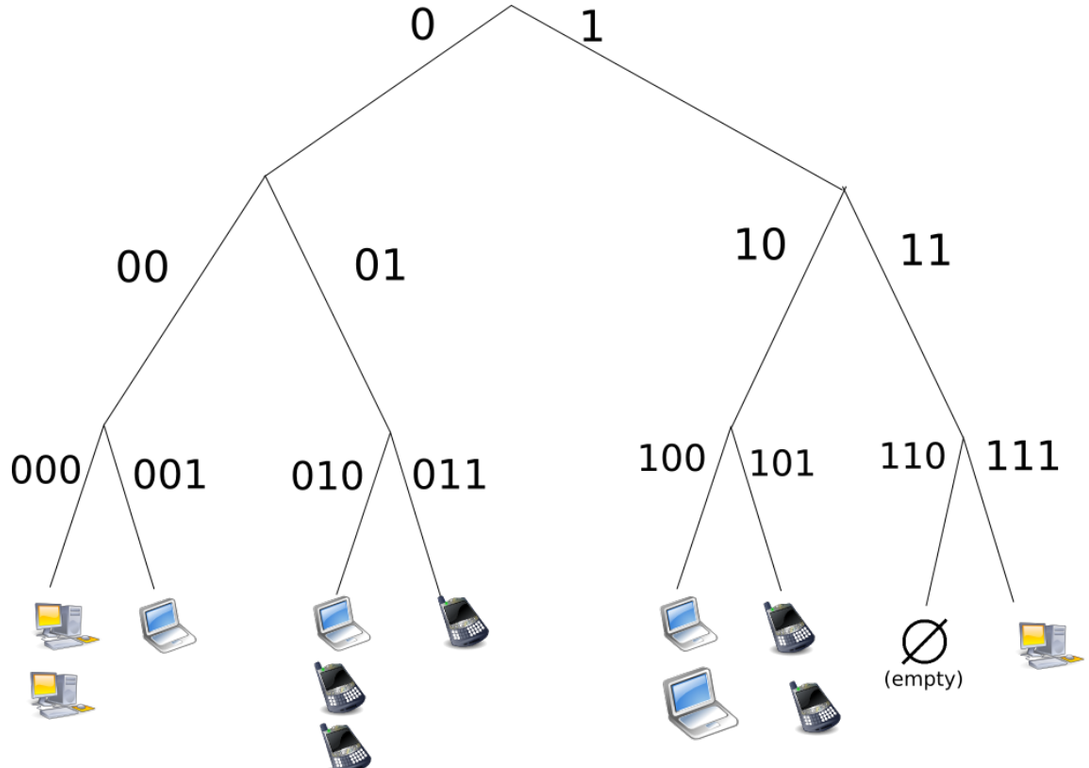
Different types of networks/systems

对等网络(Peer-to-Peer)









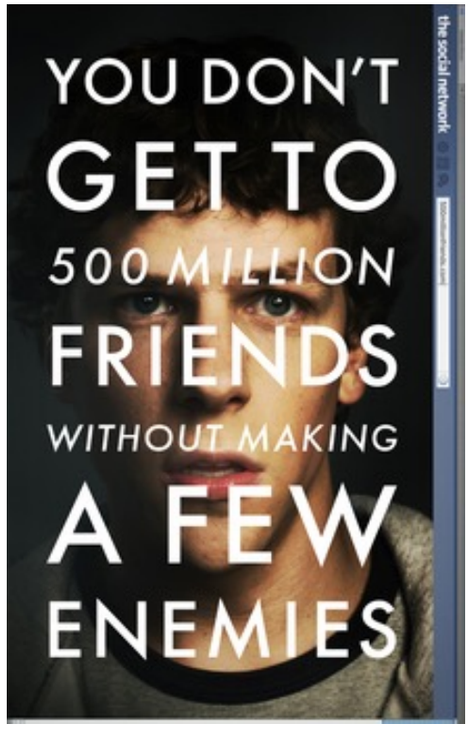
P2P的力量

napster™

1999

Sean Parker

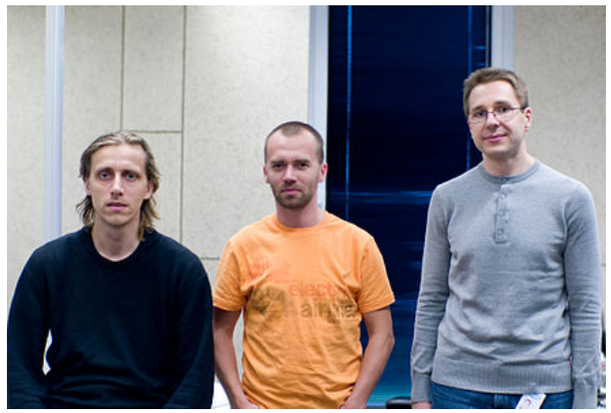
facebook



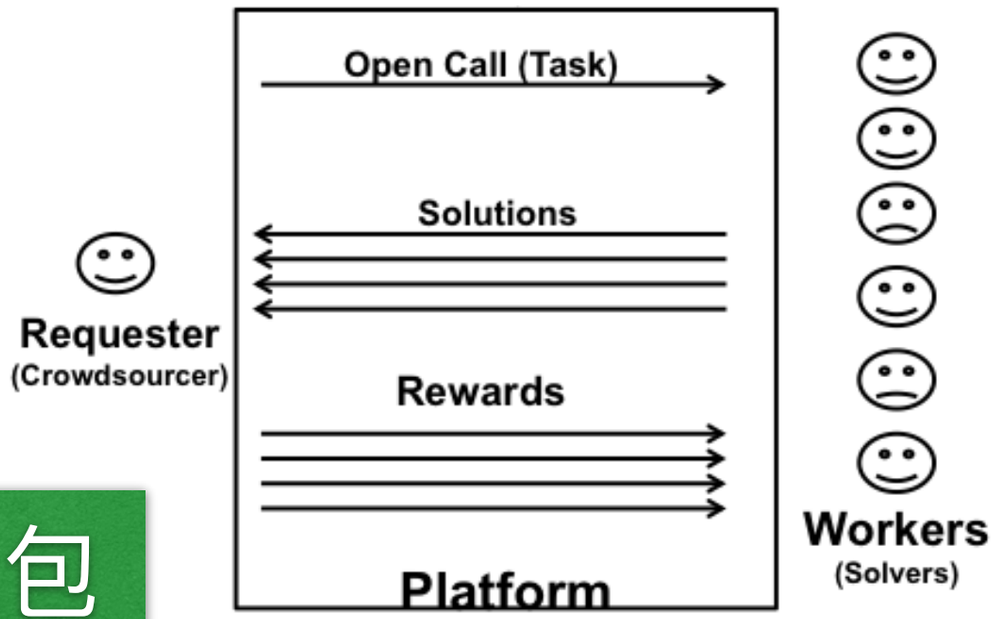
The Social Network

skype™

2003



KaZaA



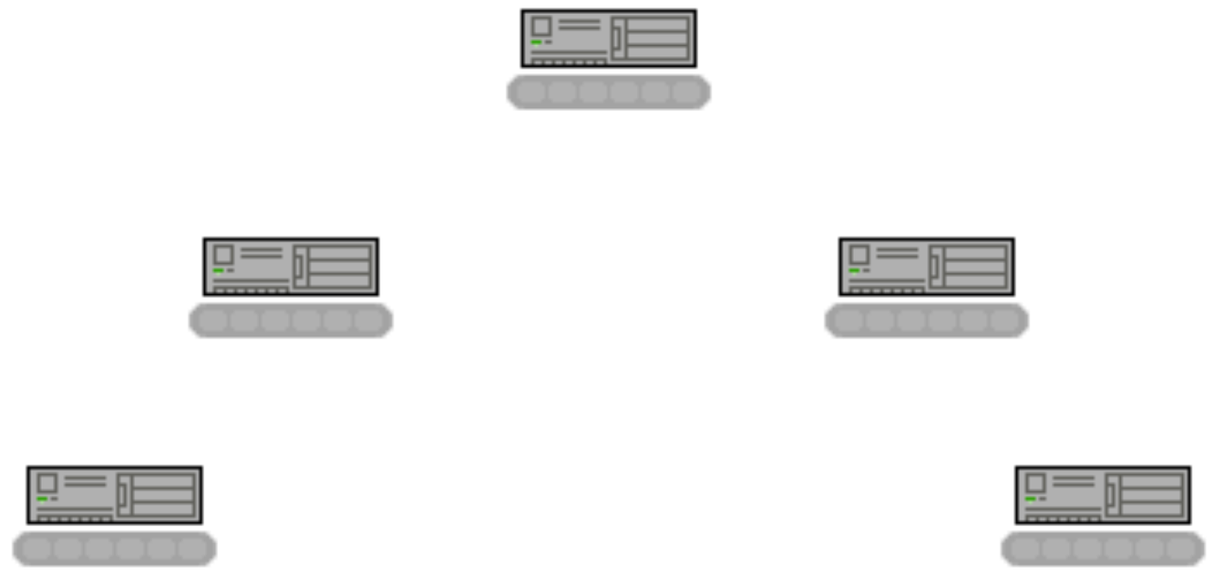
众包

BitTorrent

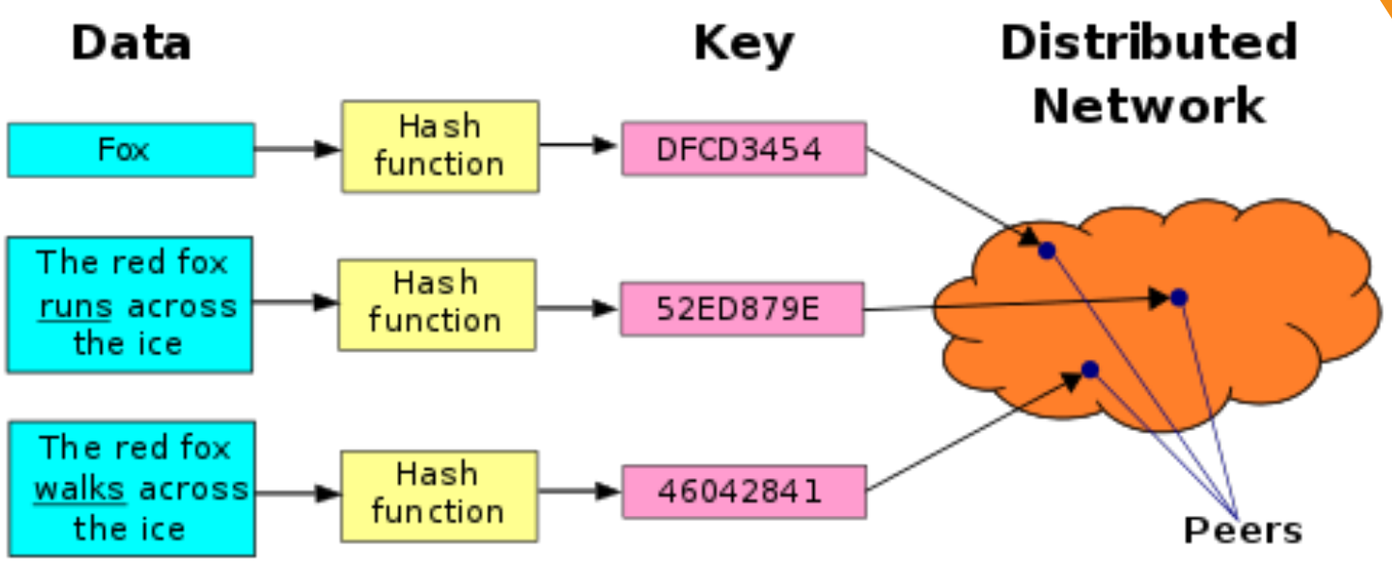
2001

Bram Cohen

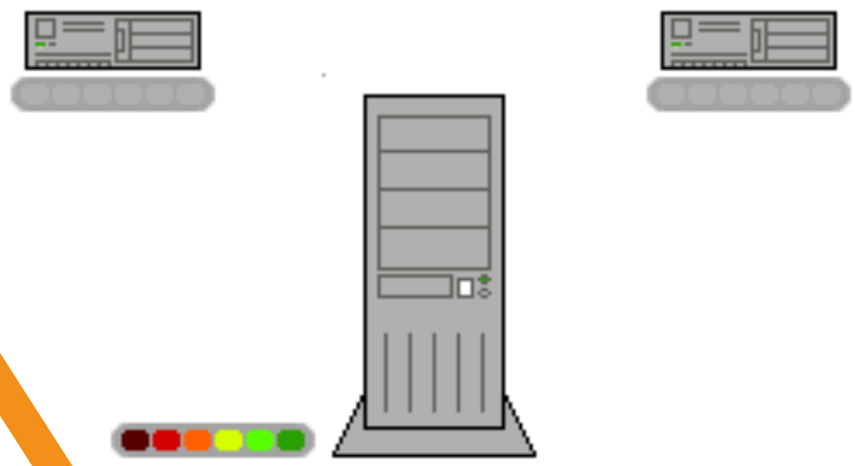
BitTorrent



Distributed Hash Table



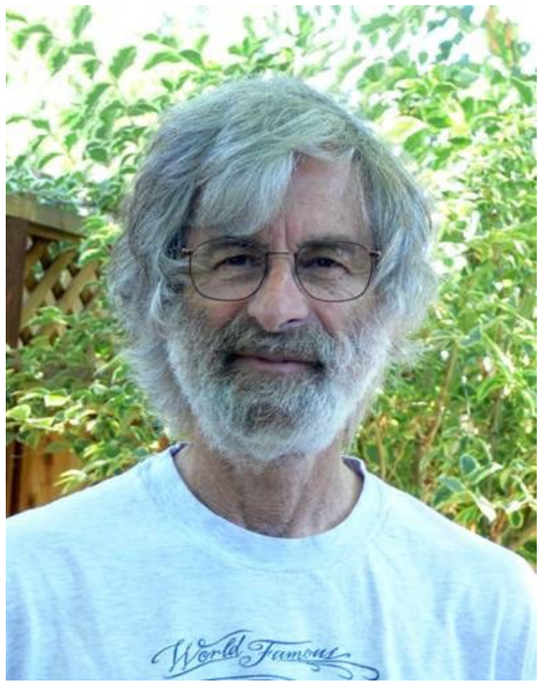
https://en.wikipedia.org/wiki/Distributed_hash_table



激励

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

拜占庭将军问题



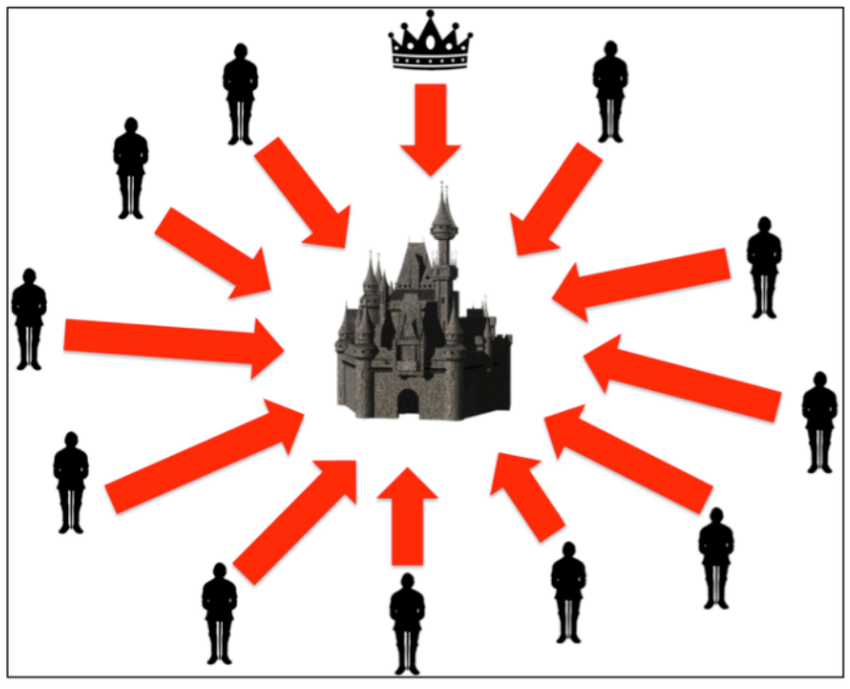
LESLIE LAMPORT

2013图灵奖

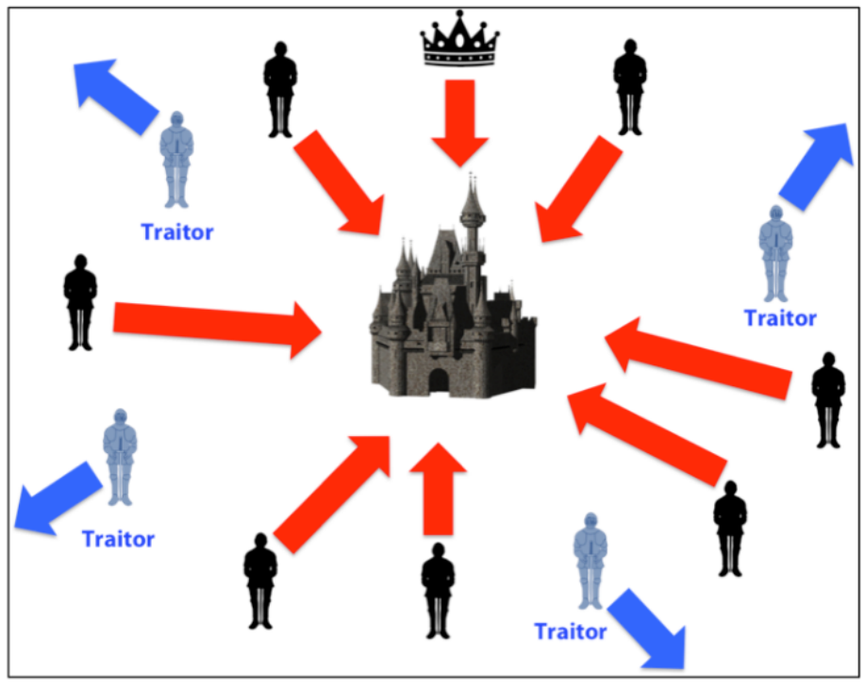
The Byzantine Generals Problem

1982

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International



Coordinated Attack Leading to Victory



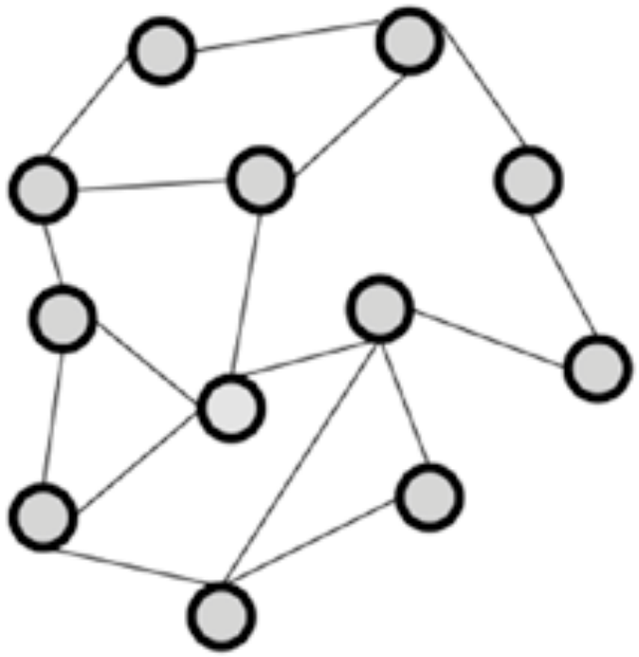
Uncoordinated Attack Leading to Defeat

Paxos Made Simple

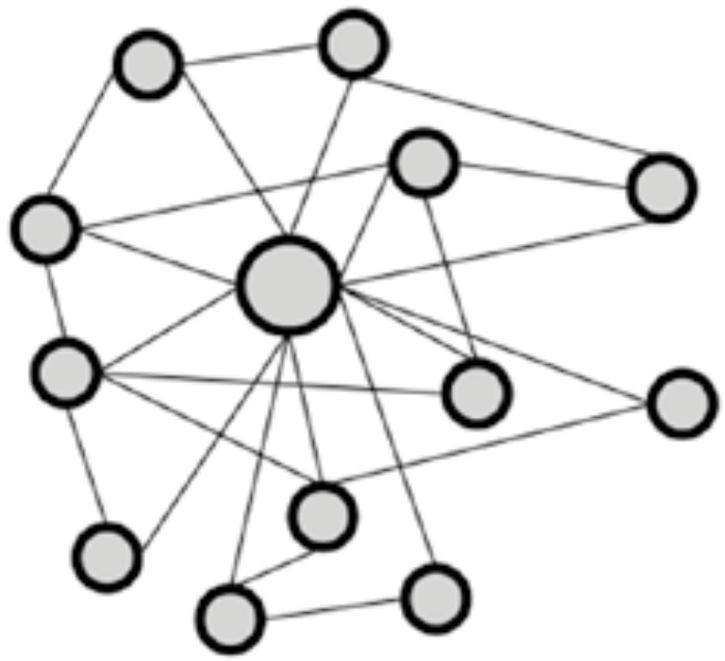
2001

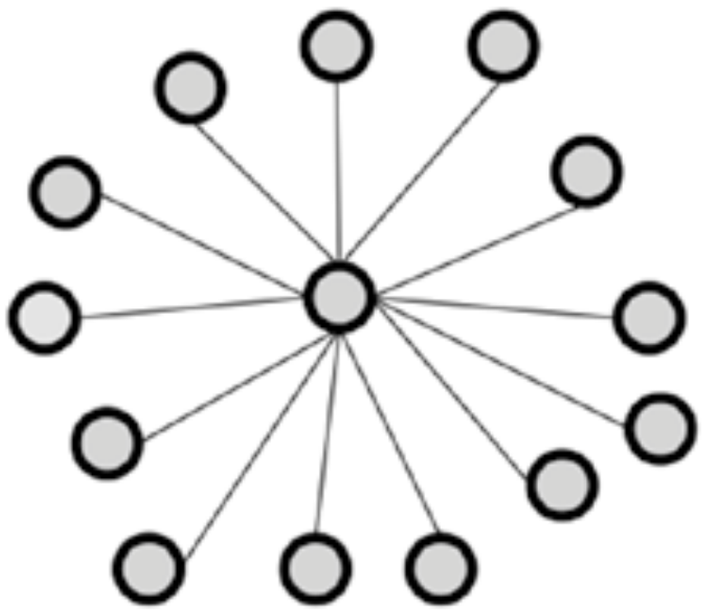
The Paxos algorithm, when presented in plain English, is very simple.

分布还是集中

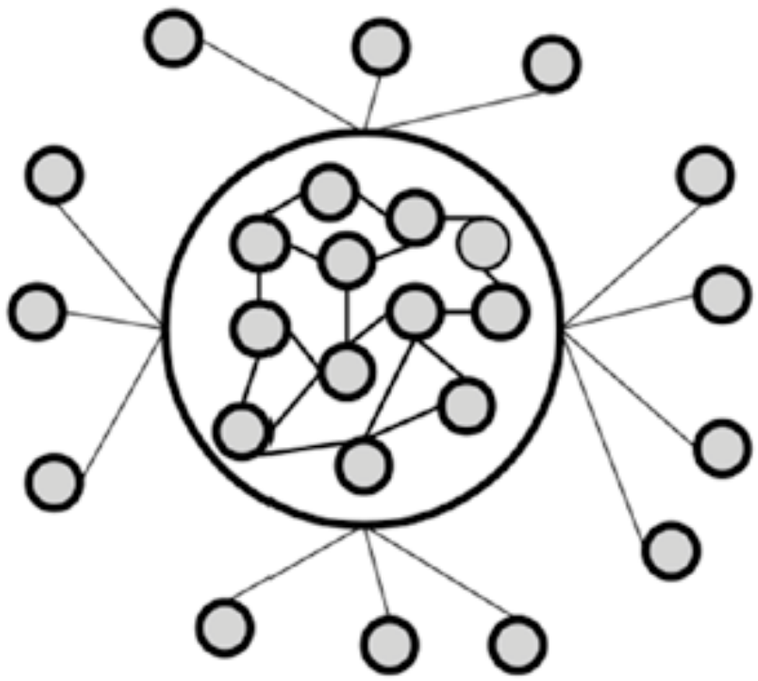


没有纯粹的
中心化系统
或者
分布式系统

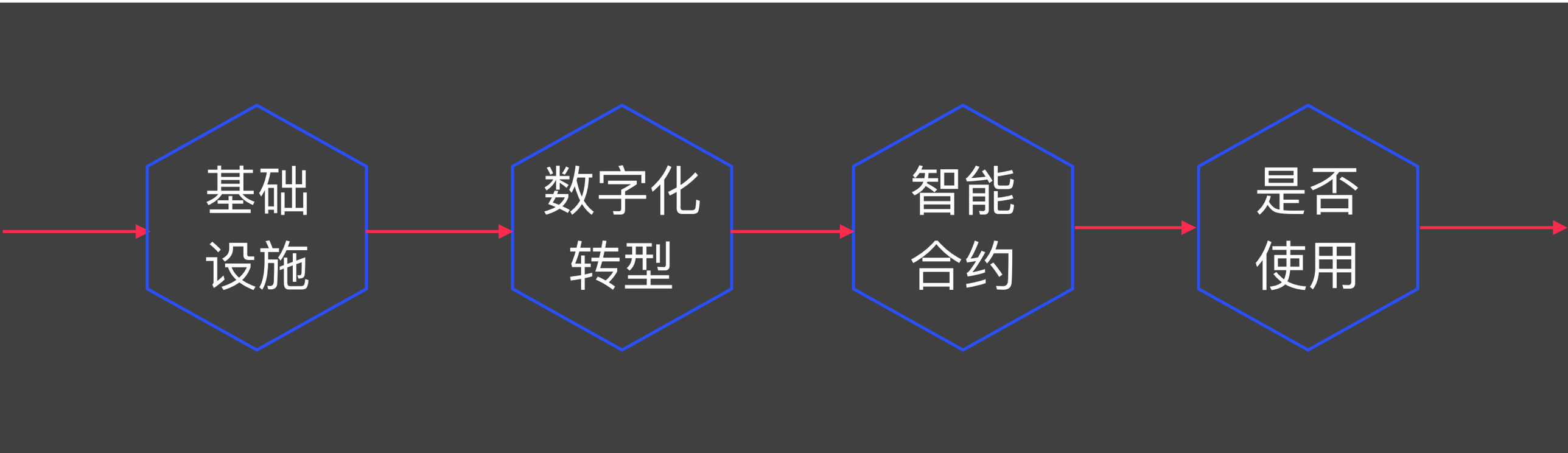




Internet
Email
IM
SNS



计算视角



区块链是一种计算机基础设施

?

P2P

区块链

Client-Server

助力数字化转型

数字化转型：采用数字技术改进服务流程和商业模式

- 个人
- 企业
- 行业
- 政府
- 社会

- 数字化转换
  - 非数字
- 数字化升级
  - 新技术

- 信息
- 数据
- 网络
- 智能
- 价值

- 数字技术
- 数字竞争
- 数字客户

IDC预测

2020-2023全球数字化转型投资7.4万亿美元

2023年ICT中投资50%以上是数字化转型

- 数字资源
- 组织结构
- 策略目标

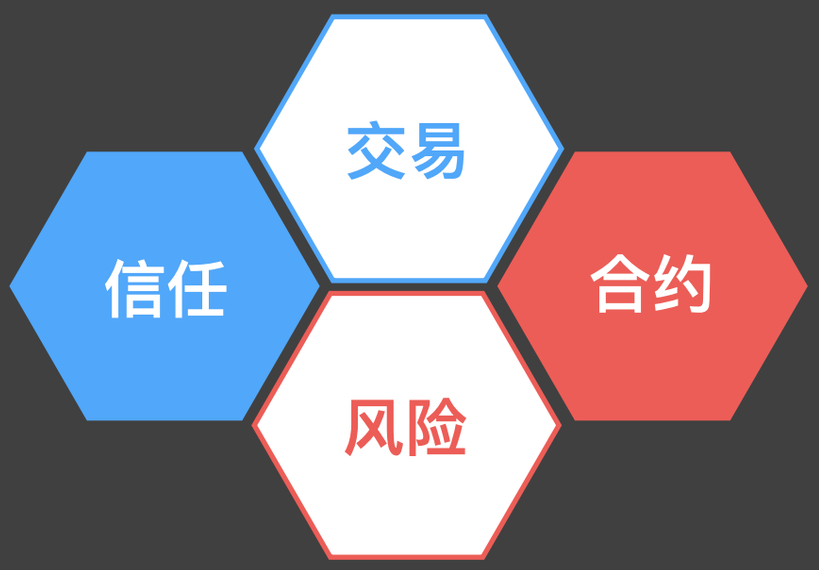
数字经济

基于数字货物和服务的商业模式，经济收益主要由数字化技术带来的经济形式。

智能合约

一组数字形式描述的承诺

包括合约参与方可以执行这些承诺的协议



Nick Szabo 1990

以太坊 2013

实际合约 | 部分合约 | 非合约

规则逻辑 | 软件代码 | 自动执行

身份标识 | 系统状态 | 发生事件

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

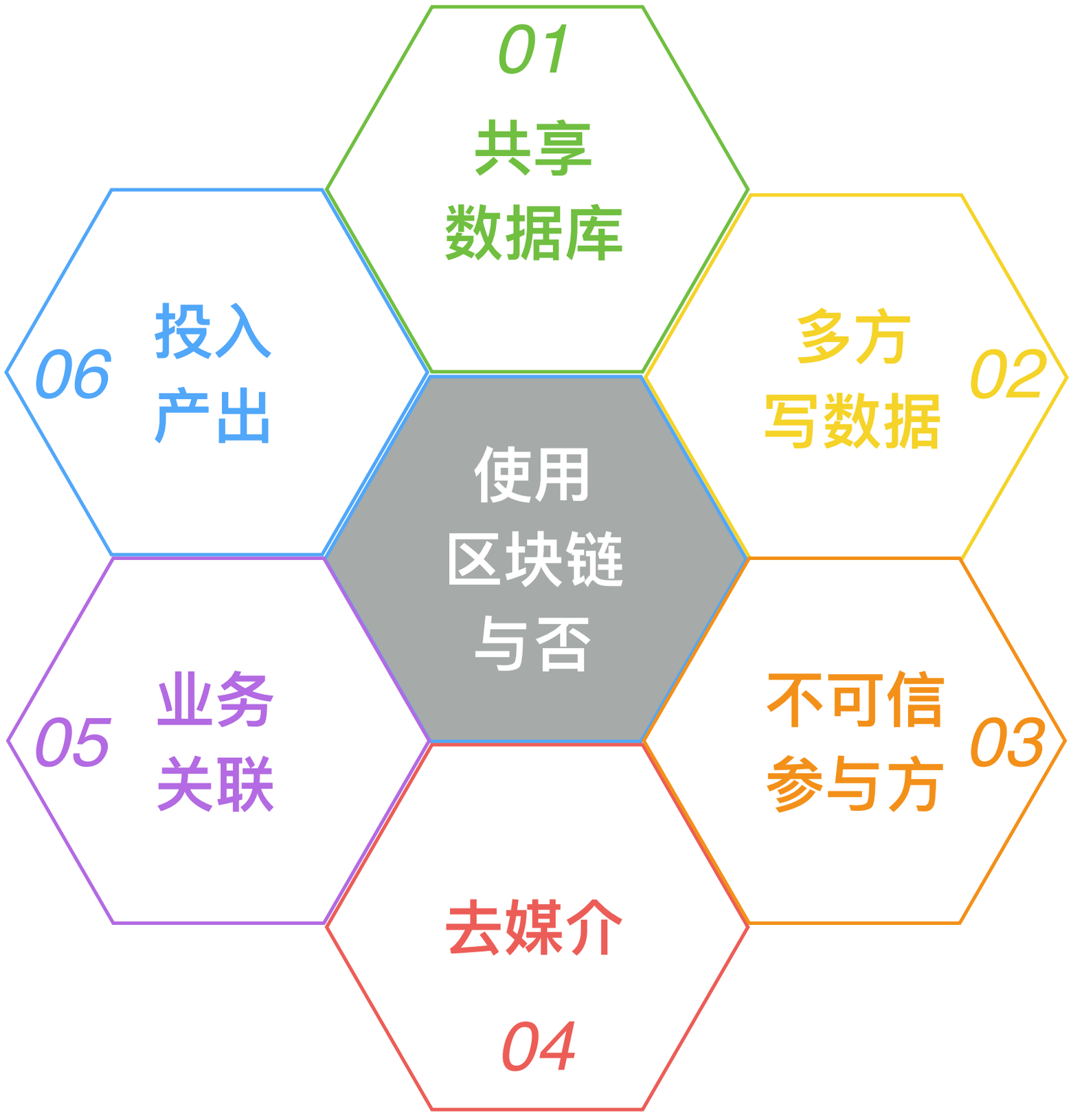
传统合约

- 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

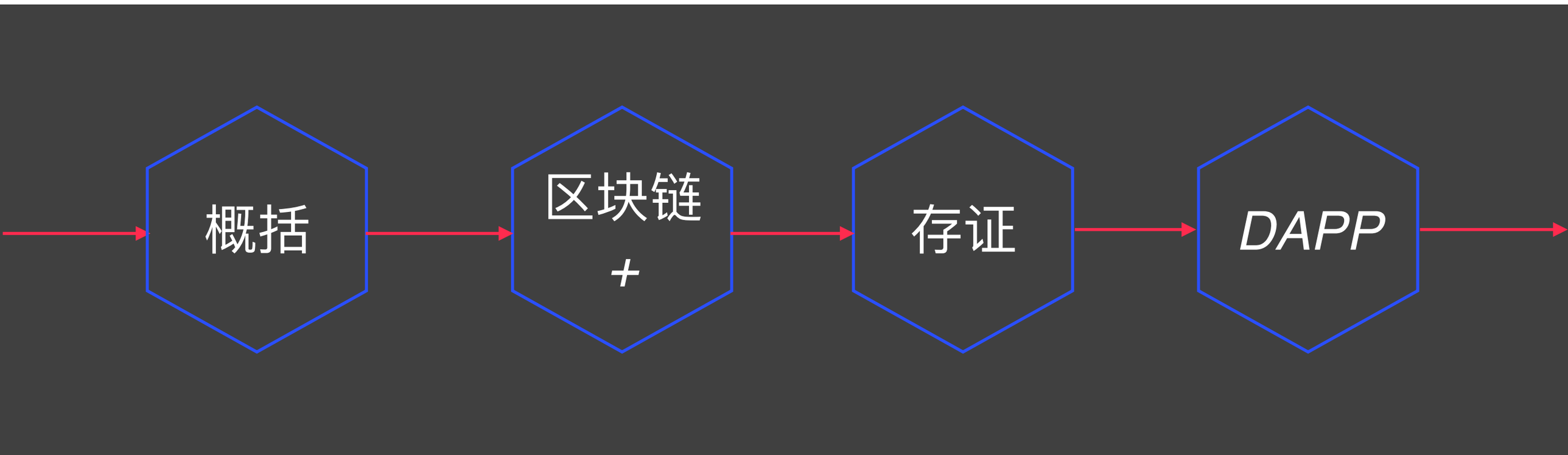
智能合约

- 完全数字化
- 自动执行
- 代码定义规则

是否需要使用区块链



区块链发展

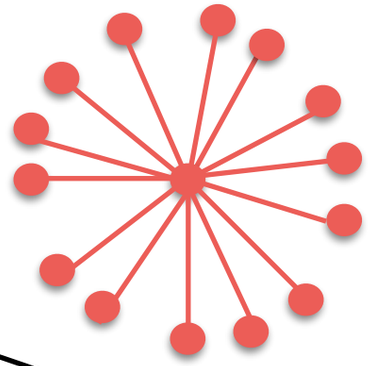


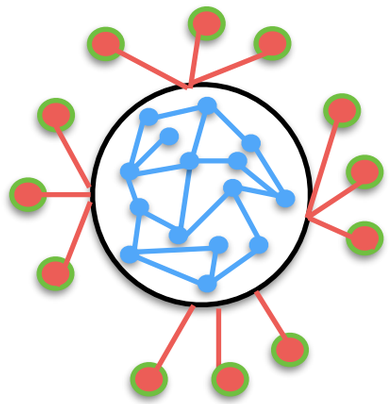
Blockchain Overview

区块链发展现状

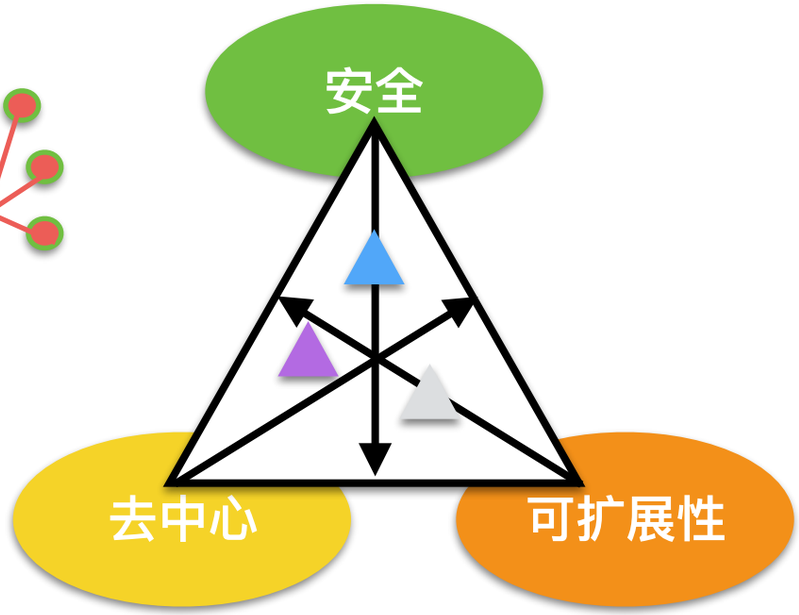
安全 信任 隐私

增加信任

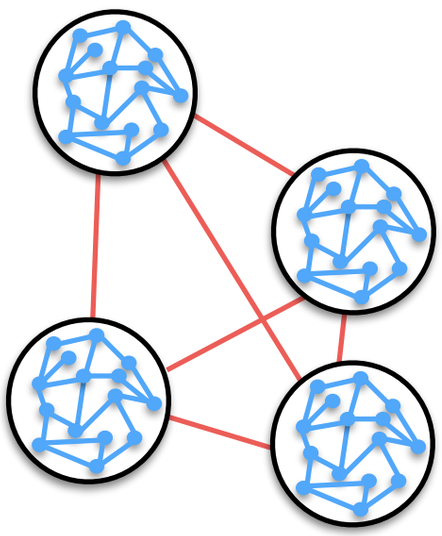


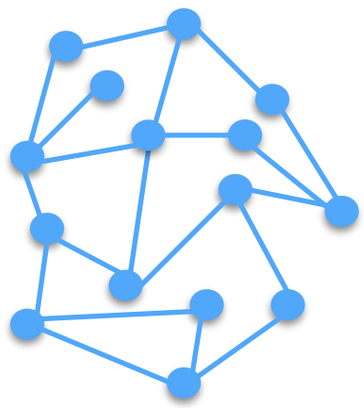


数据上链



适度去中心





2009

公链

智能合约

货币

ICO

企业区块链

1.0

2.0

3.0

Block chain

区块链＋

实体经济

Blockchain Overview

区块链+是互联网+一部分

数字化

网络化

智能化

有形资产：汽车、住宅、食品

无形资产：选票、创意、信誉、健康信息

记录、追踪、监测、转移所有资产

政治

文化

智能手机

智能家居

智能汽车

智能城市

可穿戴设备

物联网传感器

自我跟踪设备

区块链存证和资产上链

一般	托管交易、保税合同、仲裁、多方签名、...
金融交易	股票、私募、集资、基金、债券、年金、...
公共记录	产权证、车辆登记、营业执照、结婚证、...
证件	驾驶证、身份证、护照、选民登记、...
私人记录	借据、贷款合同、投注、签名、遗嘱、...
证明	保险证明、证权属明、公证文件、...
实物资产	家宅、酒店客房、汽车租赁、汽车使用、...
无形资产	专利、商标、版权、订位、域名、...

DAPP

自治、自足
去中心化

数字资产

DAC

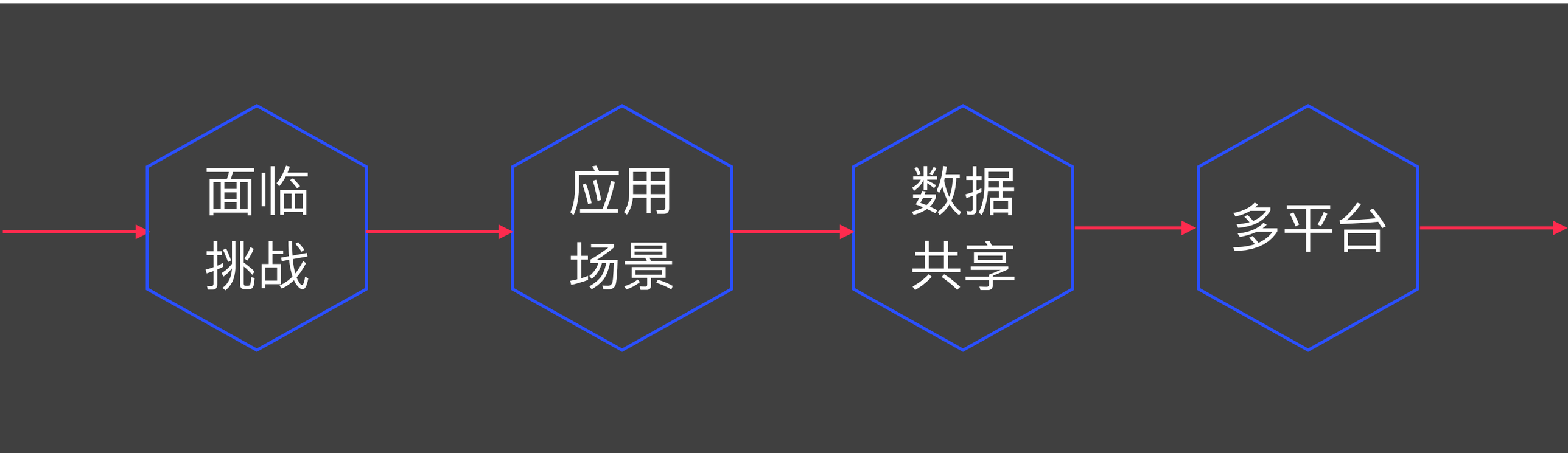
智能合约 → DAPP → DAO → DAS

OpenBazaar　LaZooz　Twister　Storj　Bitmessage

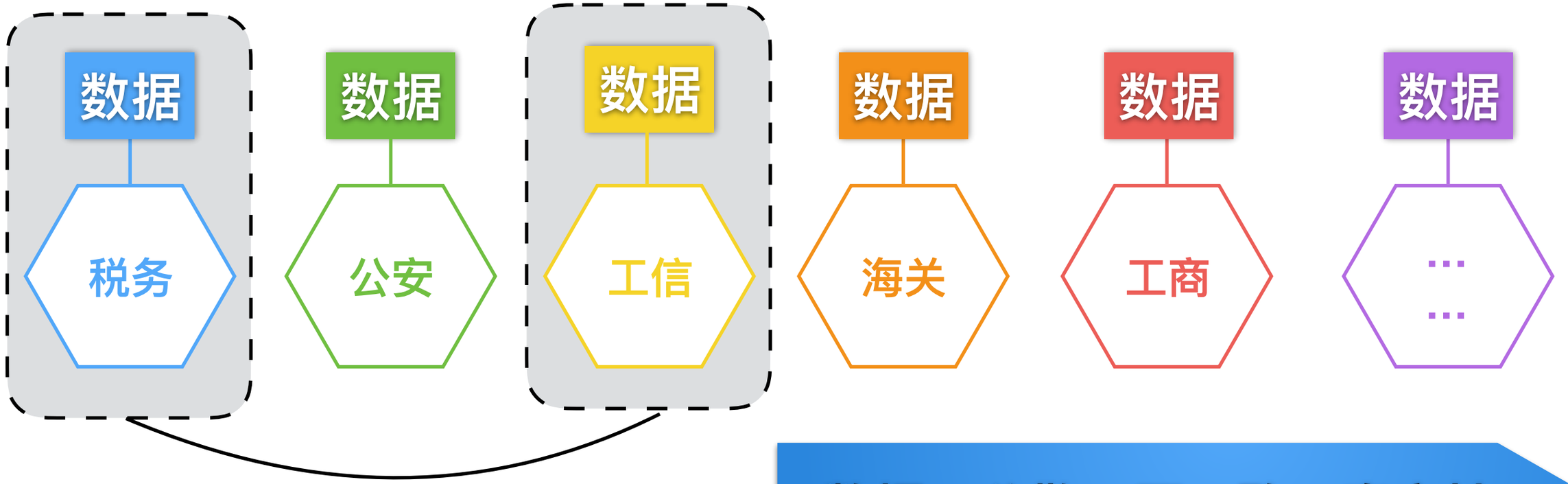
Craigslist　Uber　Twitter　Dropbox　短信

区块链逻辑

>>> 以机动车业务为例 <<<

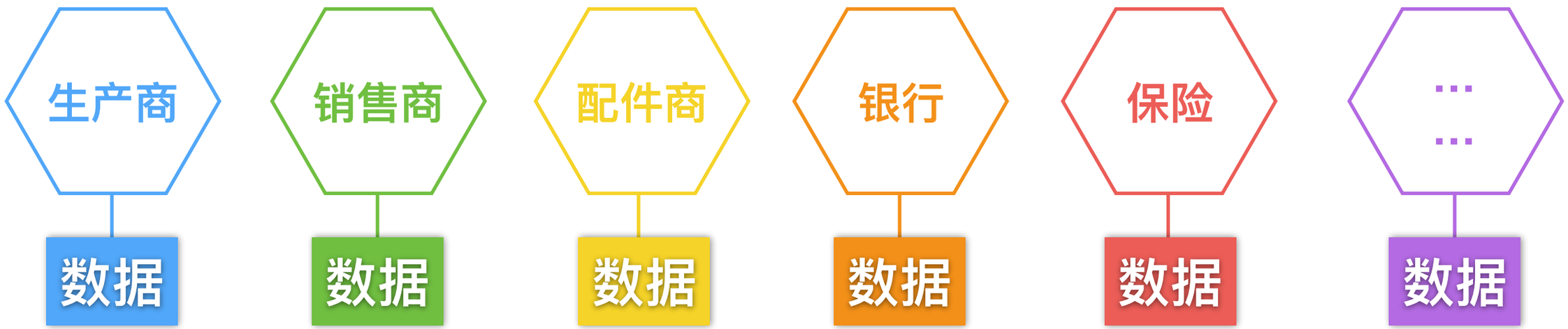


机动车业务面临挑战



数据：分散、不一致、真实性

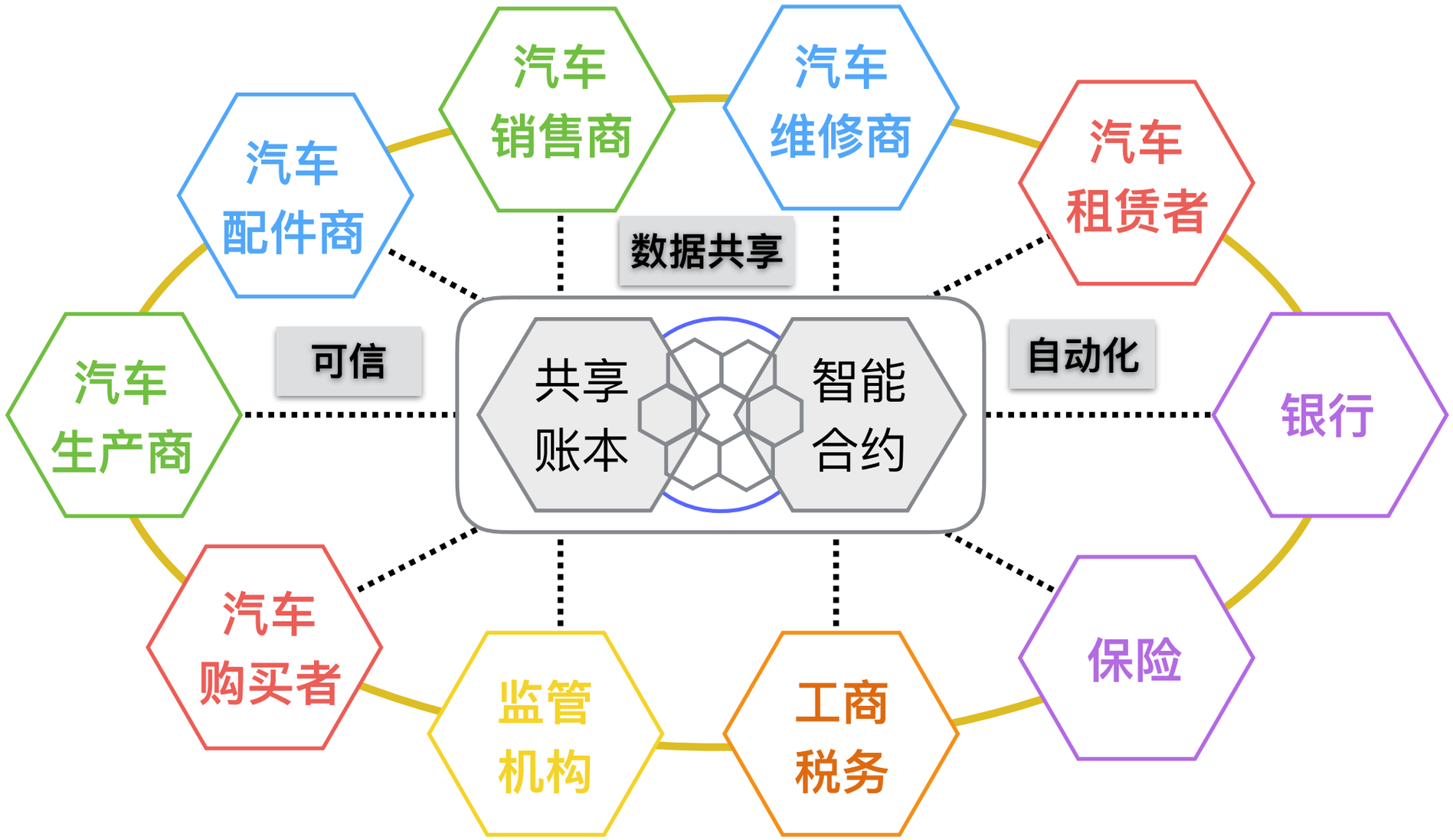
流程：复杂、跨部门、人工处理



区块链应用场景

数据一致性

全生命周期管理

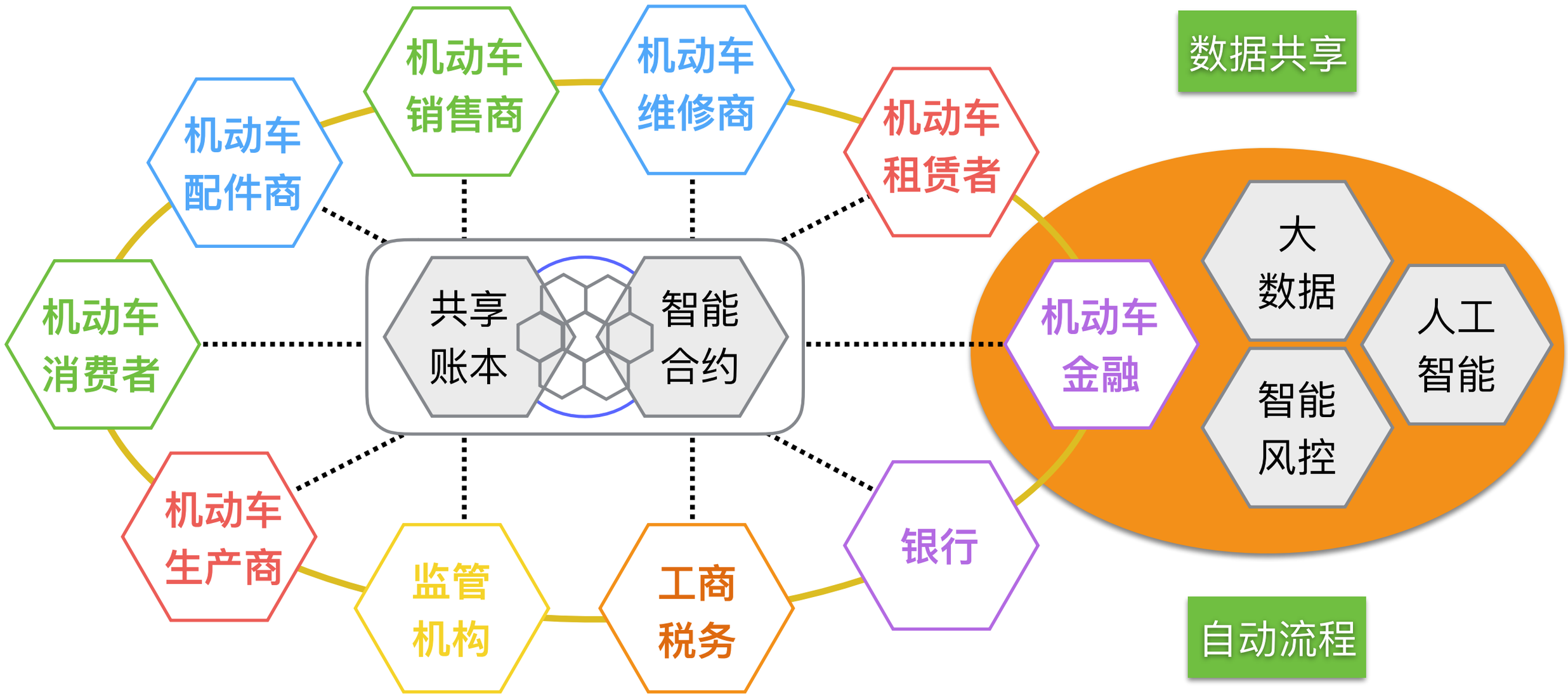


多中心

区块链增信

Blockchain Overview

区块链->>防欺诈



基于多来源数据比对防欺诈

基于自动化和智能合约防欺诈

Blockchain Overview

区块链->>数据分享平台

机构和人员注册认证

注册 | 认证 | 权限

机动车数据采集

Web | App | 共享

GPS | OBD | 车联网 | IoT | 手机 | 专用

机动车配件商

机动车销售商

机动车维修商

机动车租赁者

机动车消费者

共享账本

智能合约

保险公司

机动车生产商

监管机构

工商税务

银行

金融增值

数据增值

按需计费

名单共享

人员 | 物流

车辆 | 资金

联盟链

机动车数据分析

欺诈分析 | 价格分析 | 车辆分析 | 人员分析

机动车数据上链

Blockchain Overview

区块链->>其余系统

机构和人员注册认证

注册

认证

权限

机动车数据采集

Web

App

共享

GPS

OBD

车联网

IoT

手机

专用

业务平台

物流

数据采集平台

金融增值

数据增值

按需计费

名单共享

数据集市

智能风控

支付平台

O2O

IOT

大数据平台

区块链平台

人员

车辆

物流

资金

机动车数据分析

联盟链

机动车数据上链

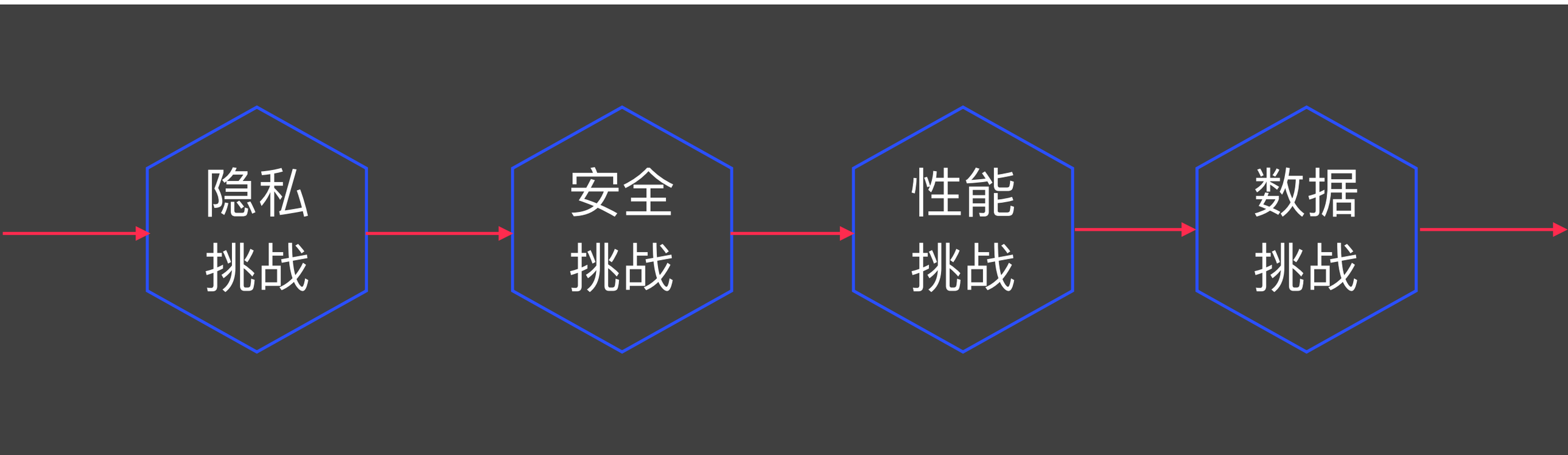
欺诈分析

价格分析

车辆分析

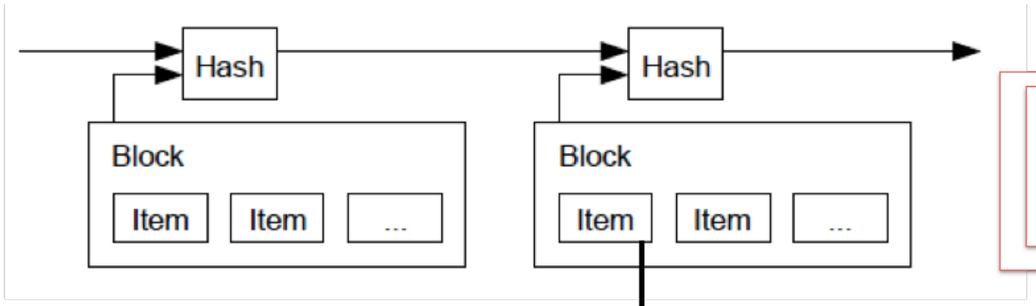
人员分析

区块链挑战

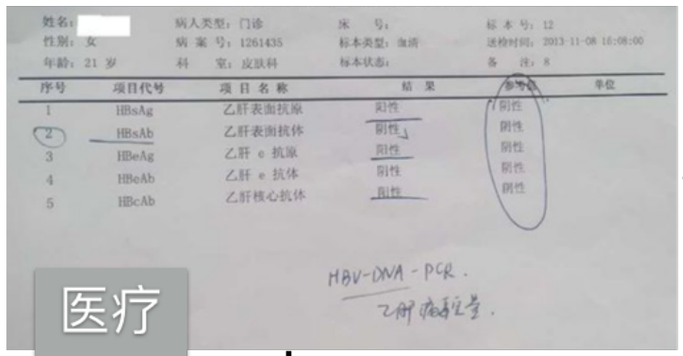


隐私挑战

公开



隐私



医疗病历

交易地址

交易内容

匿名

真实身份

理论安全

Monero

ZCash

实际安全

旁路攻击

聚类分析

辨识身份

关联身份

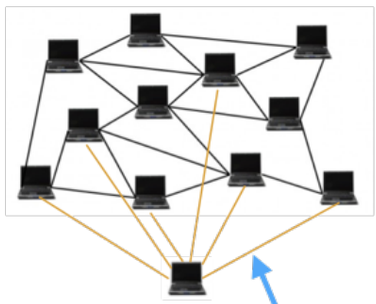
交易标记

内容加密

密钥管理

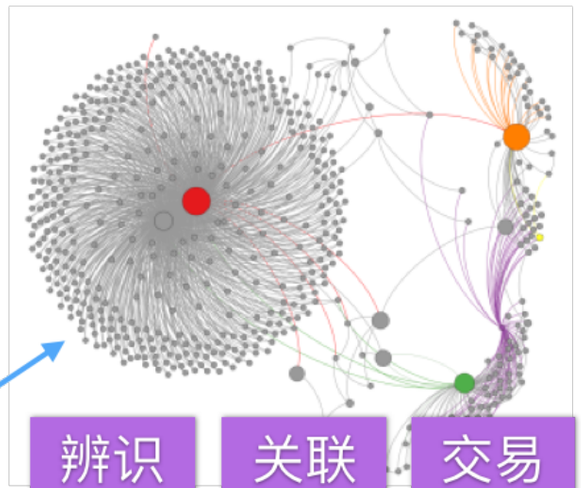
身份管理

分片



Tor

协议分析



安全挑战

可验证

是否所有节点都参与共识

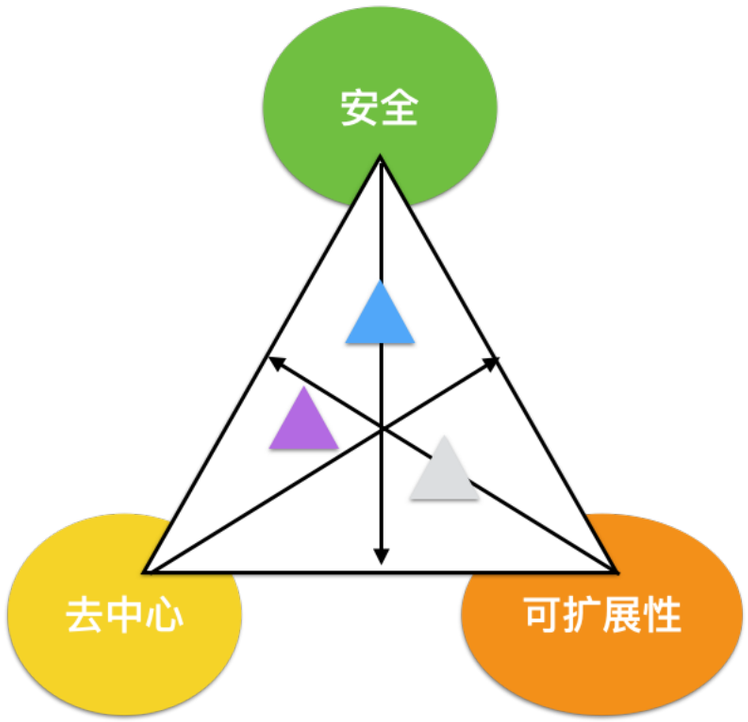
是否所有节点都存储交易数据

如何选择节点参与共识存储交易

共识

51%攻击

33.3%比例



PoW

PoS

DPoS

PBFT

资源

选举

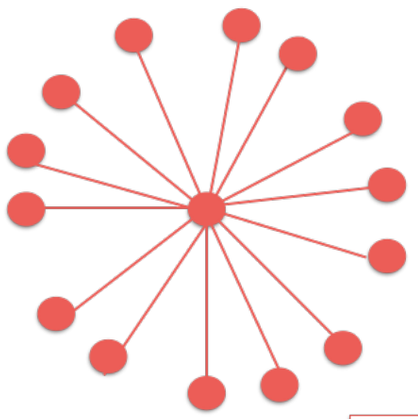
双花攻击

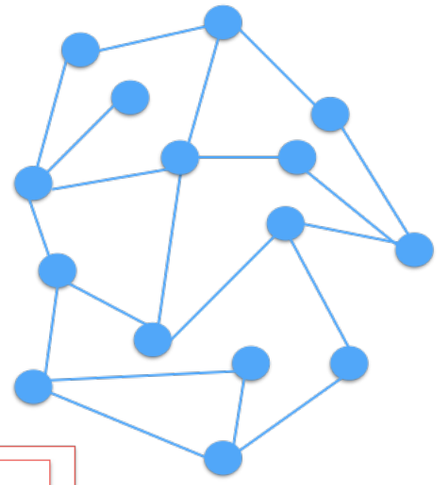
女巫攻击

贿赂攻击

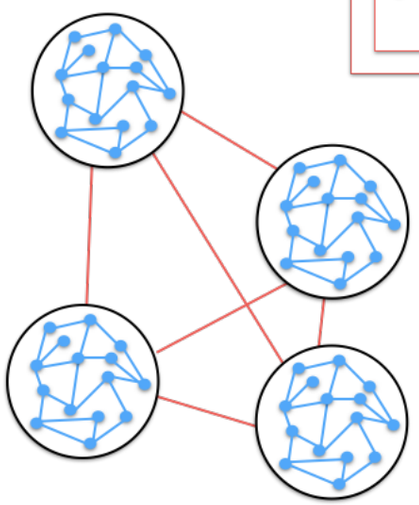
xxxx攻击

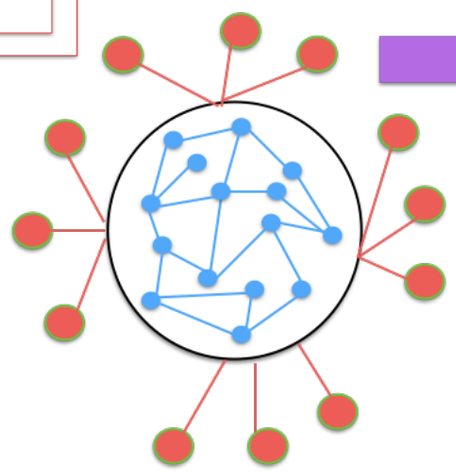
性能挑战

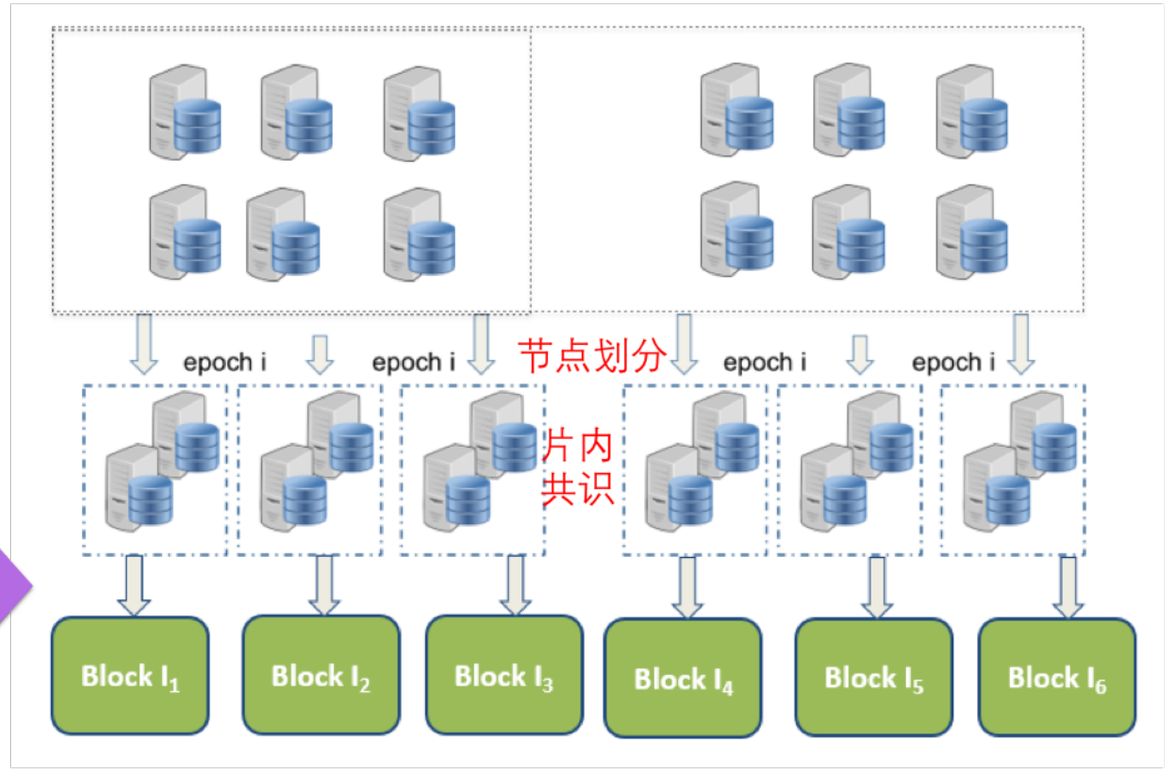




可扩展







地址分片	服务分片
随机数分片	* *分片

算力分散	片间通信
随机性	权衡

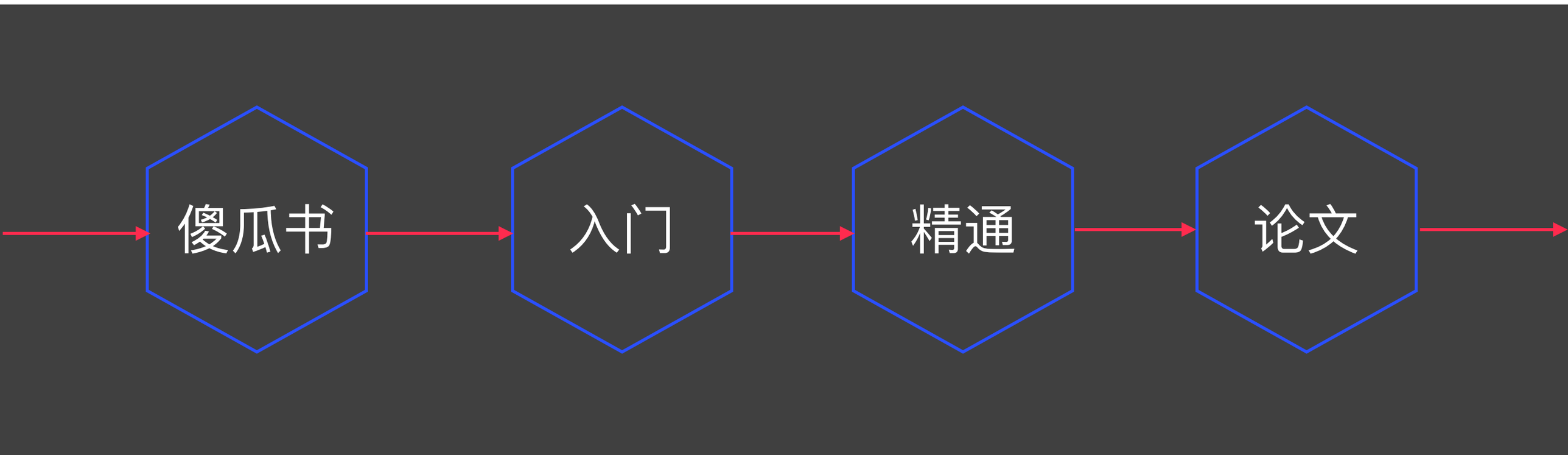
数据挑战

上链是有成本

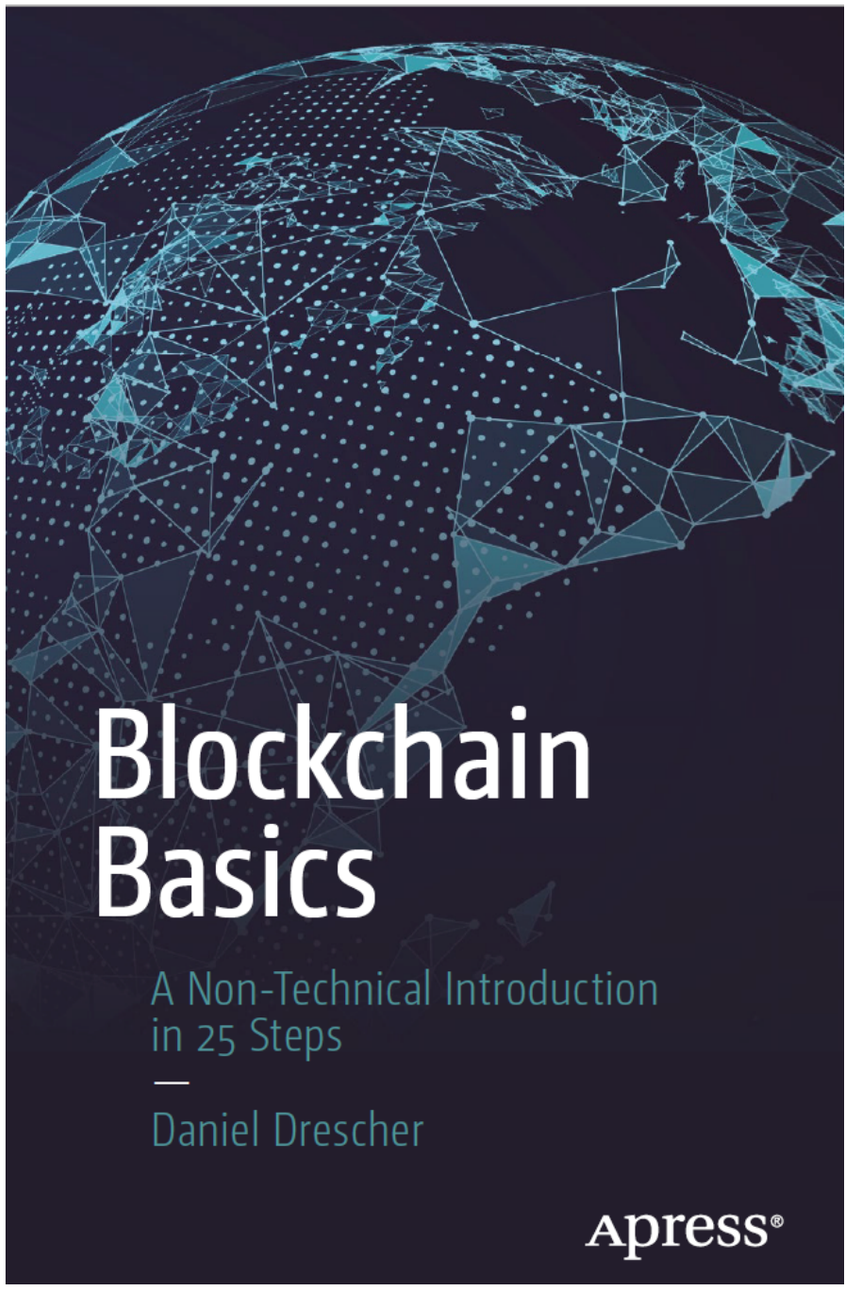
上链数据

链下数据如何保证真实性

书籍推荐

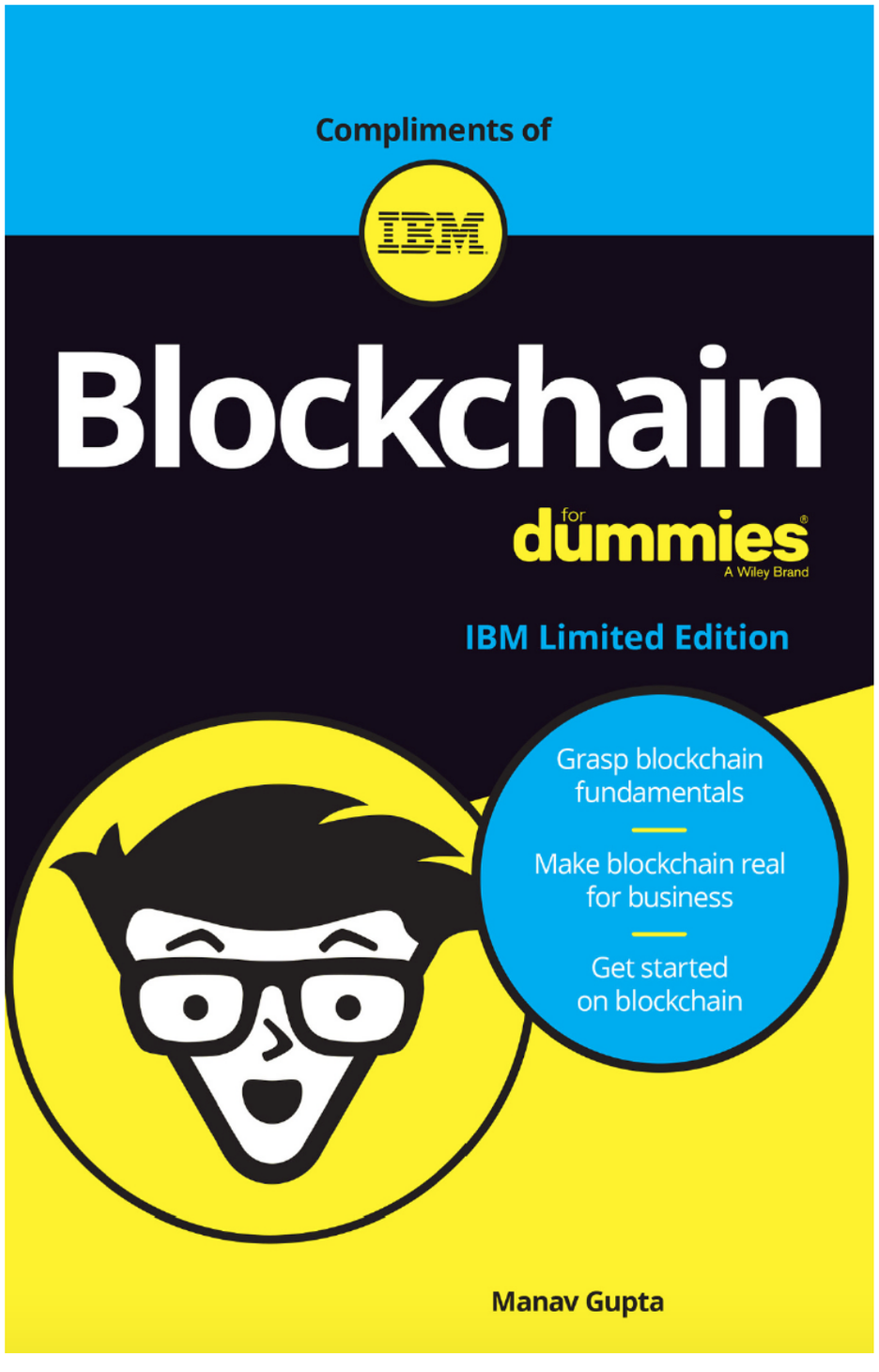


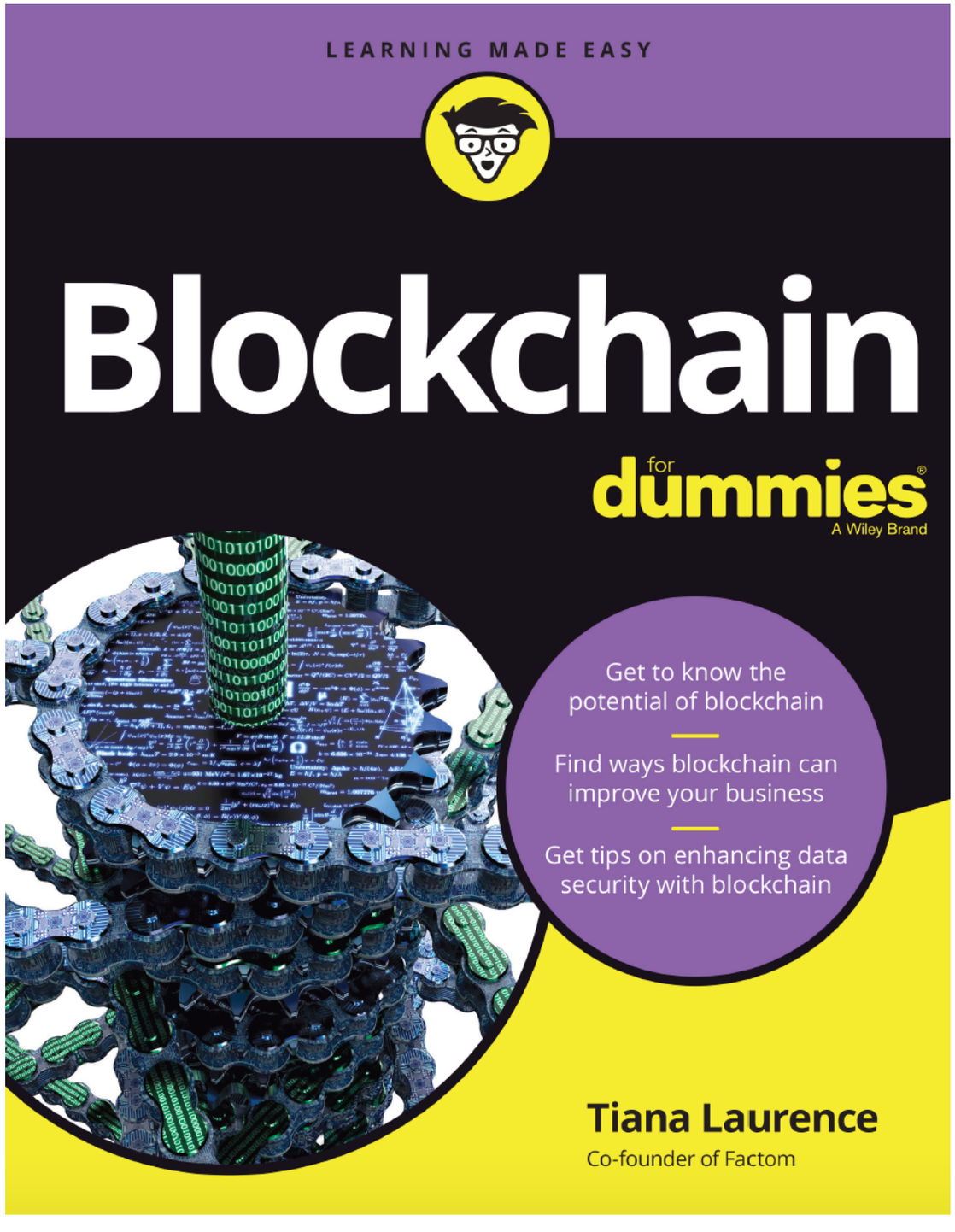
傻瓜书


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

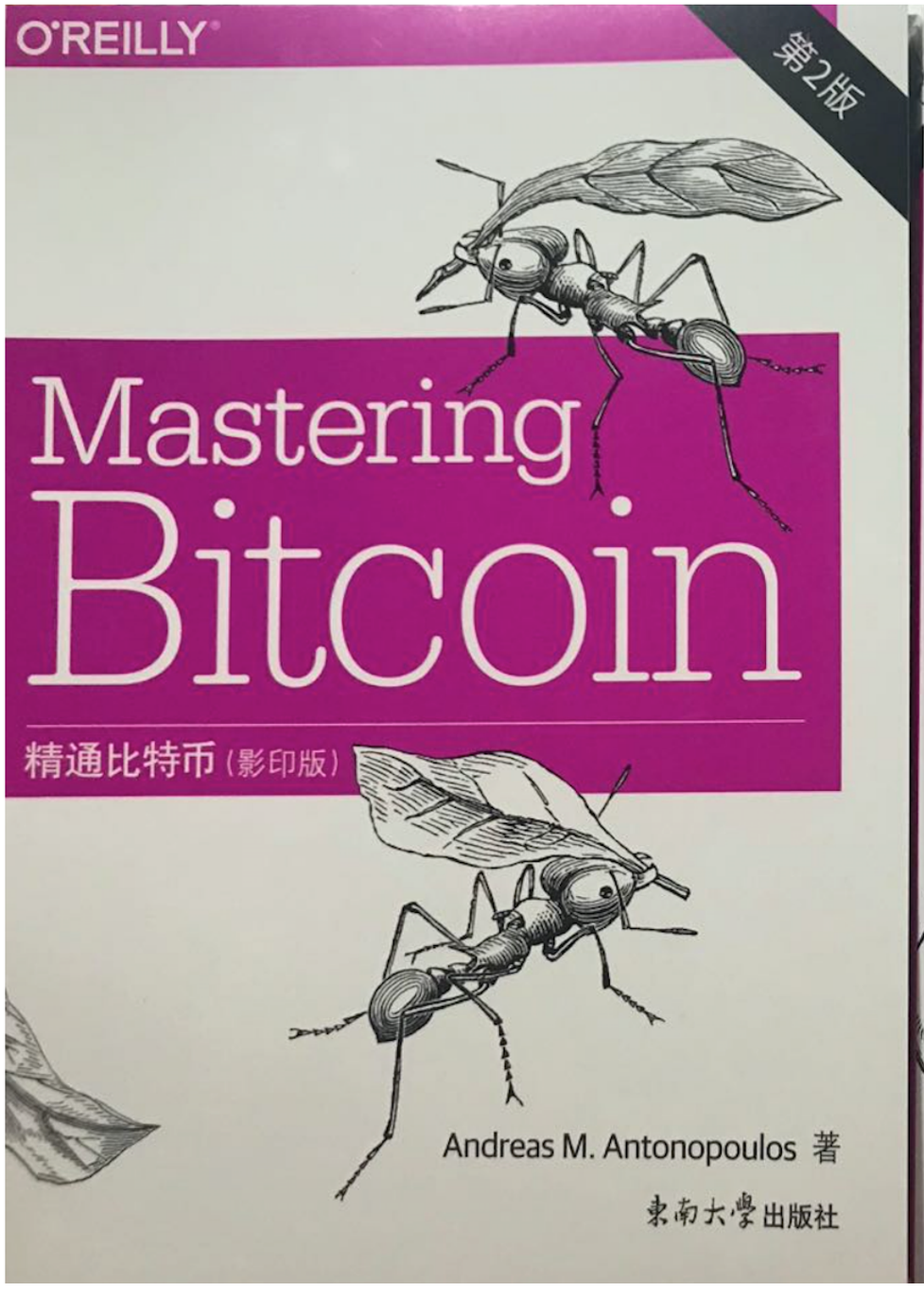

Apress®
区块链
基础知识 25 讲
Blockchain
Basics
A Non-Technical Introduction
in 25 Steps
—
[英] 丹尼尔·德雷舍（Daniel Drescher） 著
马丹 王跃桑 张绍阳 译
中国工信出版集团
人民邮电出版社

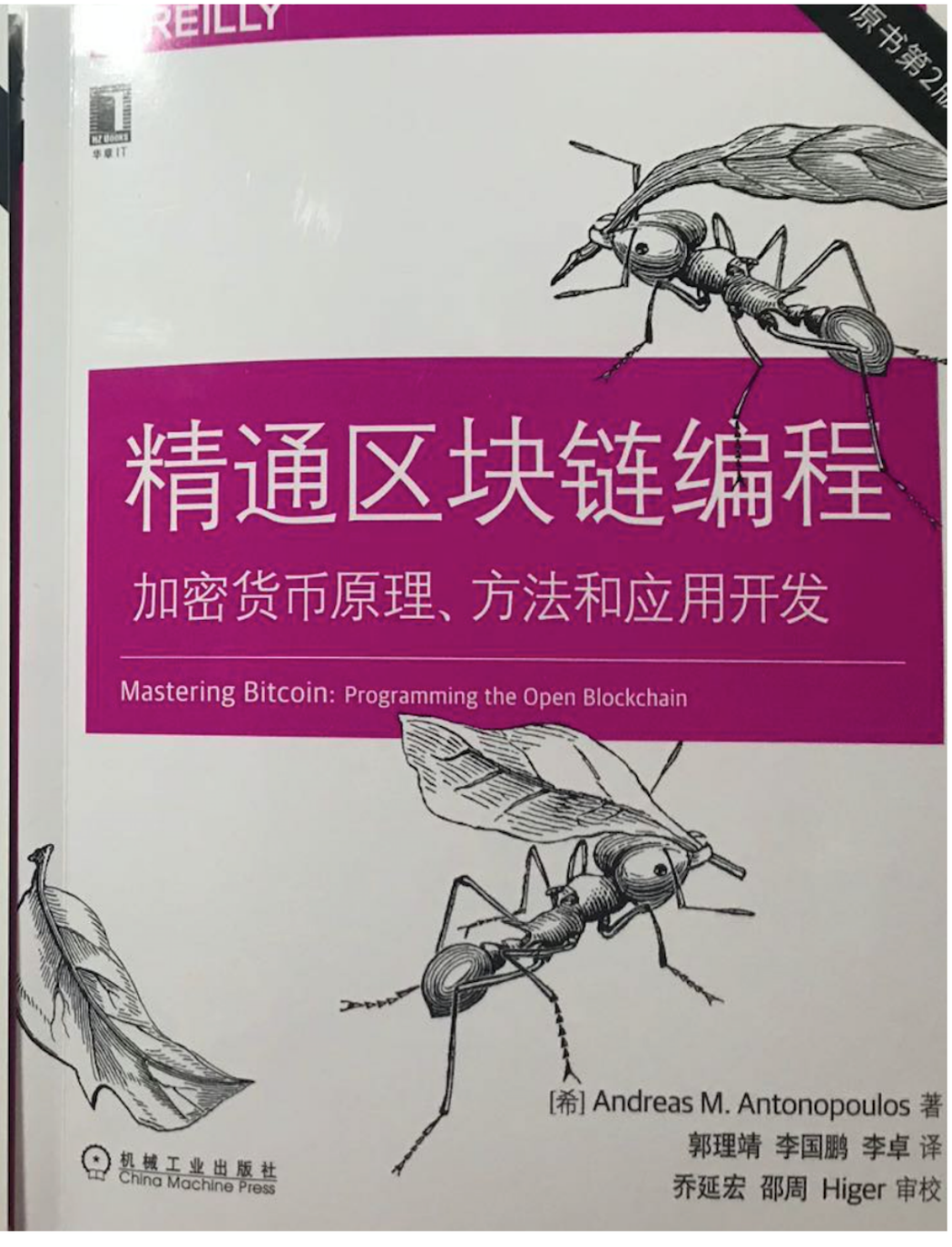
傻瓜书


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

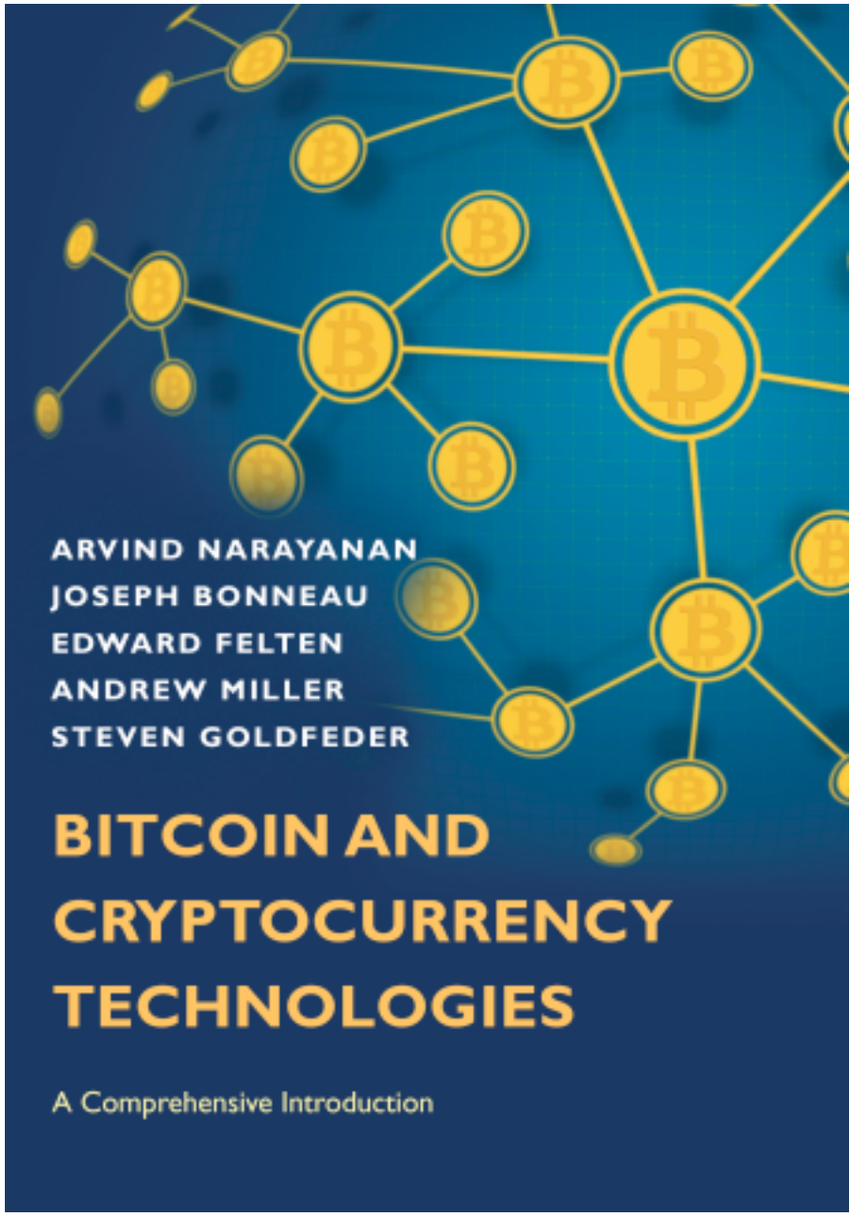

LEARNING MADE EASY
Blockchain
for dummies
A Wiley Brand
Get to know the potential of blockchain
Find ways blockchain can improve your business
Get tips on enhancing data security with blockchain
Tiana Laurence
Co-founder of Factom

比特币


O'REILLY
第2版
Mastering
Bitcoin
精通比特币（影印版）
Andreas M. Antonopoulos 著
東南大學出版社


REILLY
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

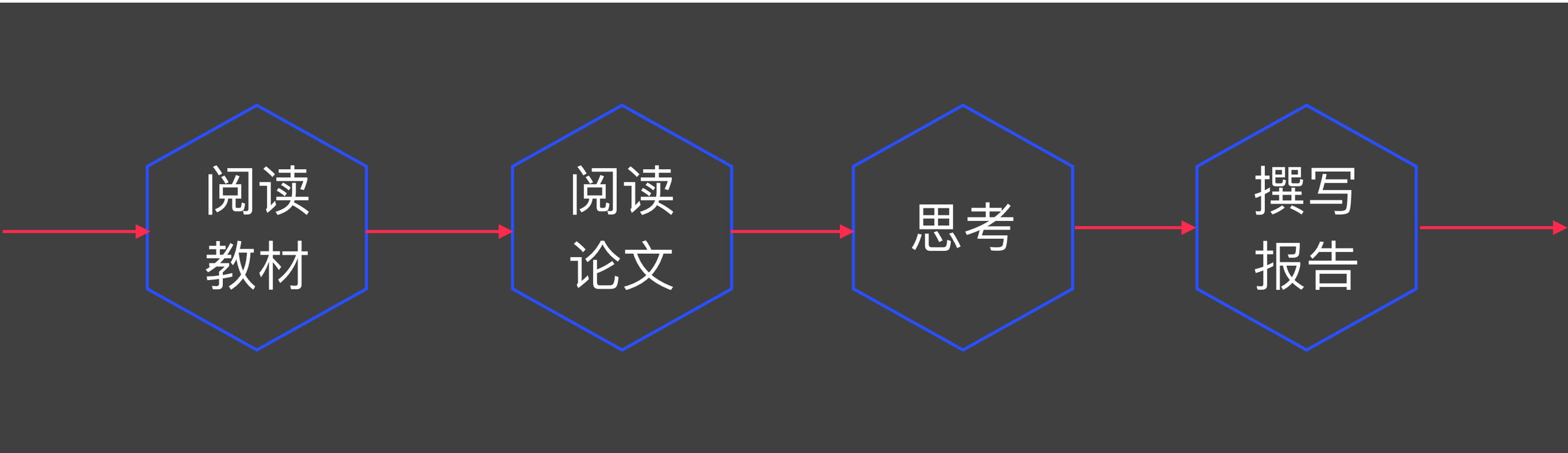
精通


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


BITCOIN
AND
CRYPTOCURRENCY
TECHNOLOGIES
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

提问时间

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30日晚上
12点前提交

谢谢！

孙惠平
sunhp@ss.pku.edu.cn