Blockchain Technology

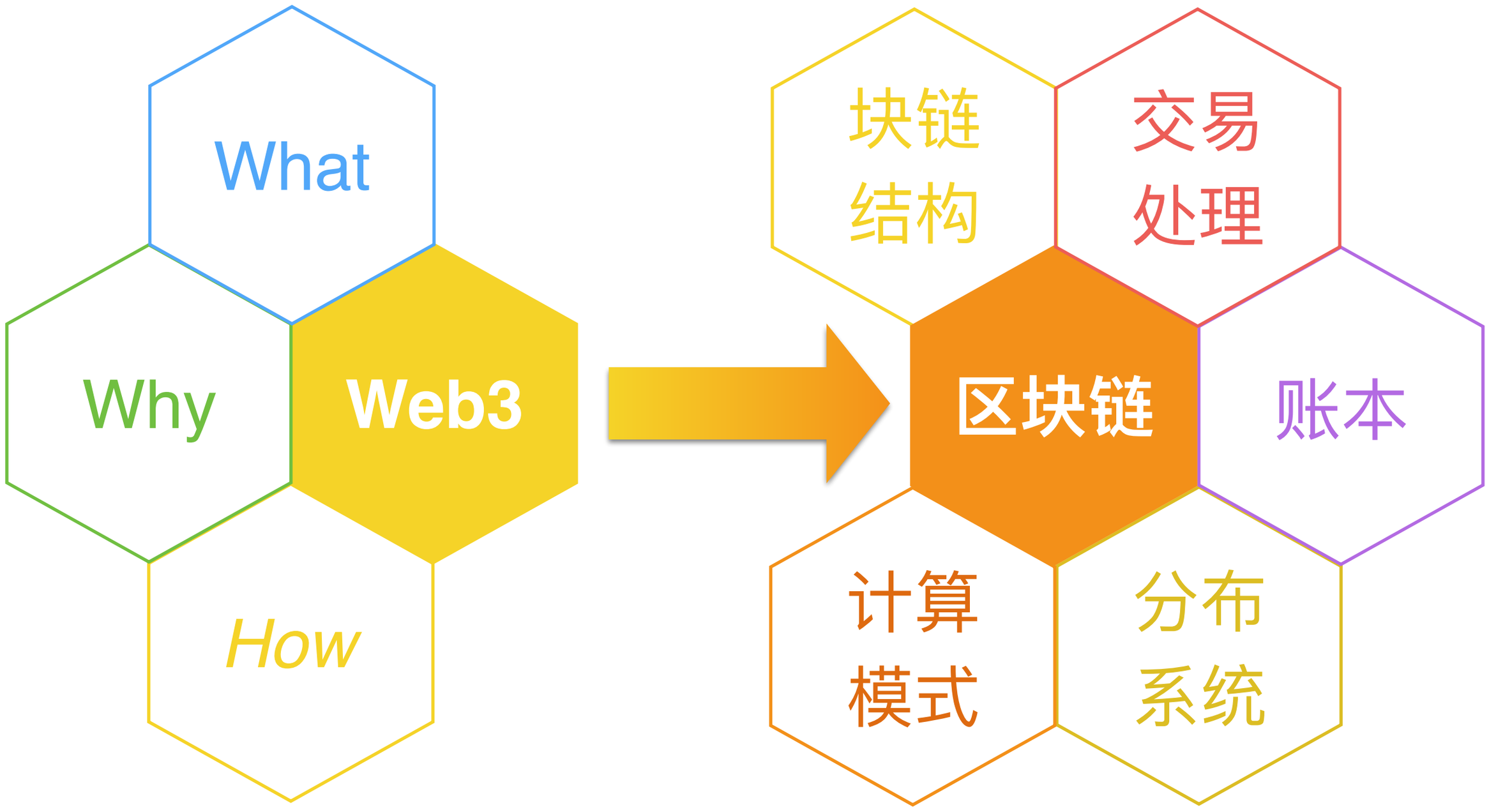
2023.02.21

区块链简介

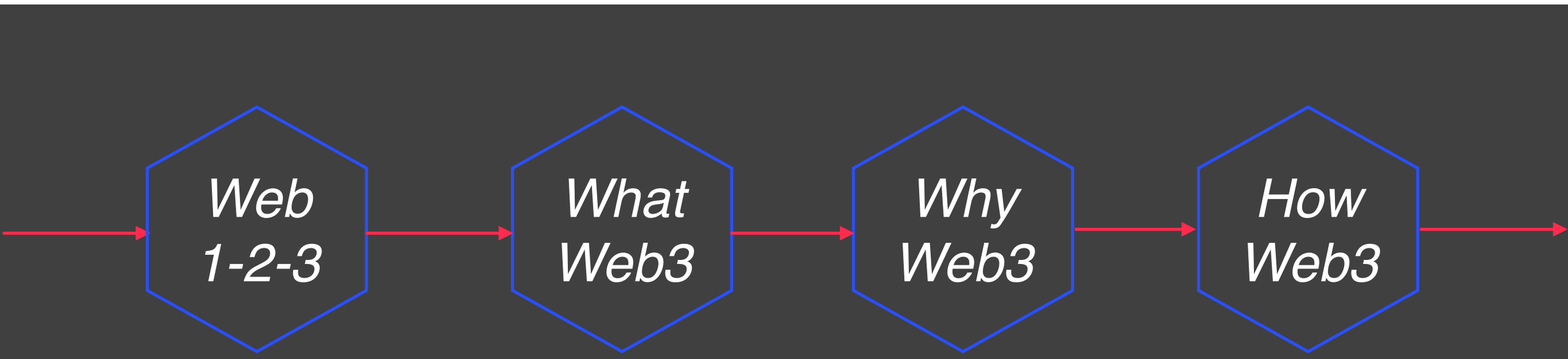
北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

主要内容



Web3



Web1–2–3

The Evolution of the Web

FABRIC VENTURES

Web 1.0

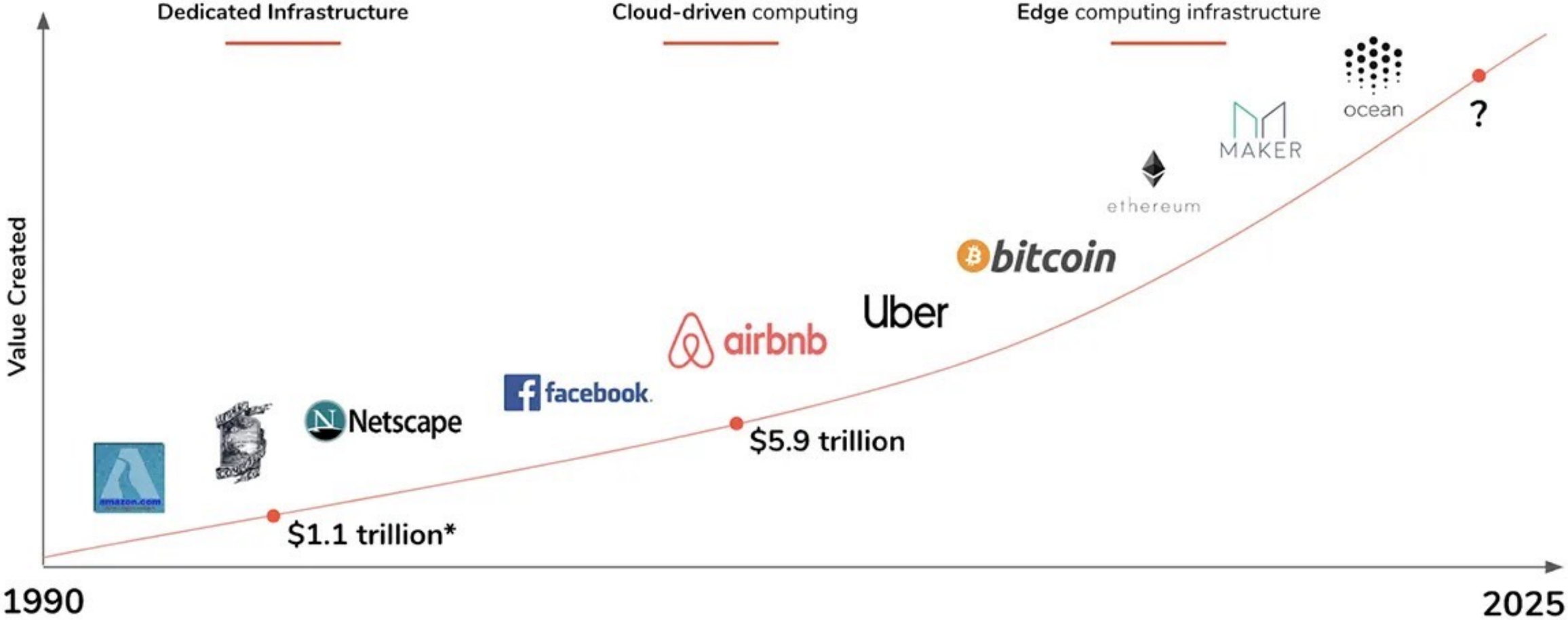
Green shoots of **E-commerce**
Desktop browser Access
Dedicated Infrastructure

Web 2.0

'Social' networks
'Mobile-first' always on
Cloud-driven computing

Web 3.0

AI-driven services
Decentralised data architecture
Edge computing infrastructure



* Internet companies market cap as of 2000

What Is Web 3.0 & Why It Matters @ Fabric Ventures

https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

Why Web3?

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

Big Tech

信息➡网络➡外部性➡平台➡流量➡垄断➡创新

How Does Web3 Work

DAO
Decentralized autonomous organization

A DAO is a headless corporation that raises and spends money. All decisions are voted on by members and executed by encoded rules on a blockchain.

They are often formed by congregations of strangers who are geographically dispersed but share a common goal.

Web3

A new version of the web, built on blockchains, that would (in theory) be decentralized, democratic, and peer-to-peer.

Cryptocurrencies, NFTs, and DAOs are all part of Web3 and enable a read/write/own internet.

Cryptocurrency

A form of currency that doesn't rely on a central bank, government, or other intermediaries. Technically, it's a software that runs on blockchains.

There are currently thousands of cryptocurrencies, but the most common include Bitcoin and Ether.

Blockchain

A "distributed ledger" — i.e., a database hosted by a network of computers instead of a single server — that offers users an immutable and transparent way to store information.

It's the backbone for Web3 technologies like cryptocurrencies and NFTs.

NFT
Non-fungible token

An NFT is a digital deed representing ownership over a unique digital object. These objects commonly include artwork or digital versions of collectibles, such as the illustrated avatars of the Bored Ape Yacht Club or Time magazine covers. They are authenticated on a blockchain.

What Is Web 3.0 @ Havard Business Review

https://hbr.org/2022/05/what-is-web3

DAPP

自治、自足
去中心化

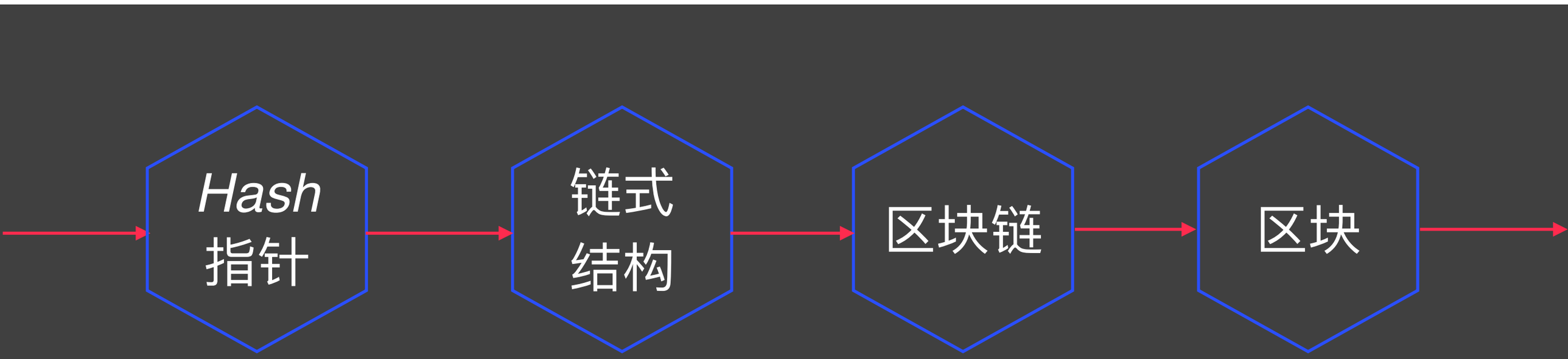
数字资产

DAC

智能合约 → DAPP → DAO → DAS

OpenBazaar	LaZooz	Twister	Storj	Bitmessage
Craigslist	Uber	Twitter	Dropbox	短信

块链结构

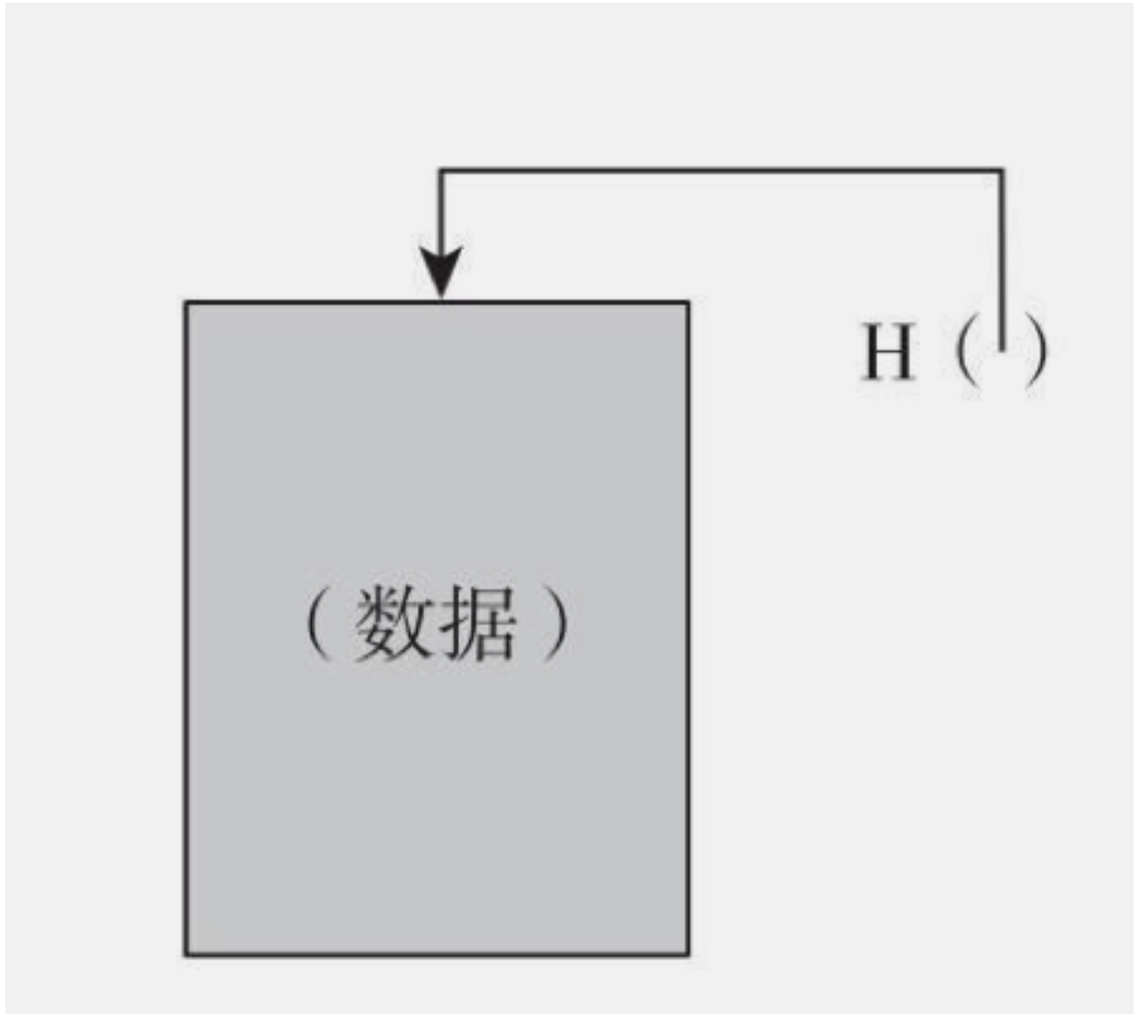


Hash指针

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

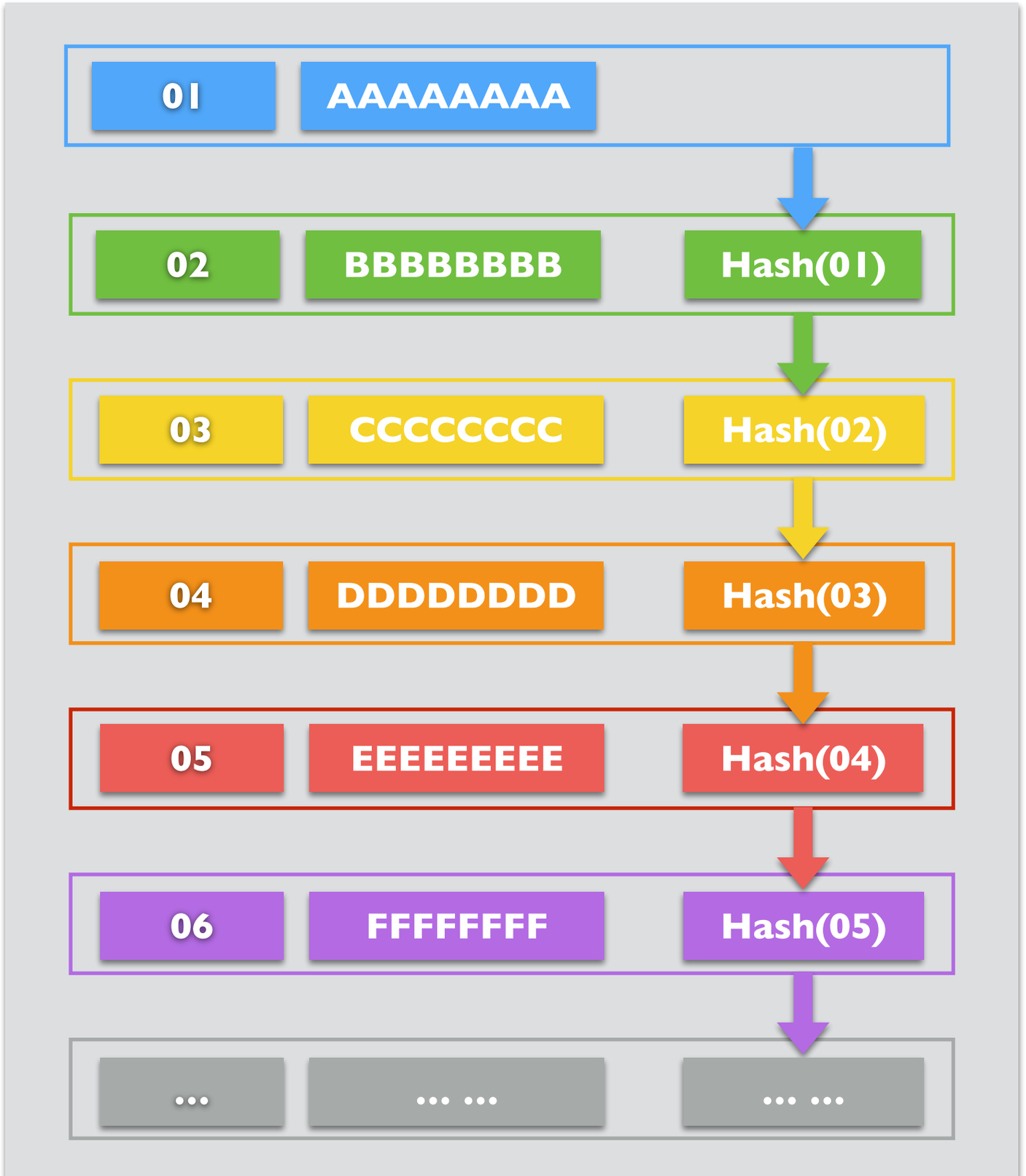


Hash指针作用

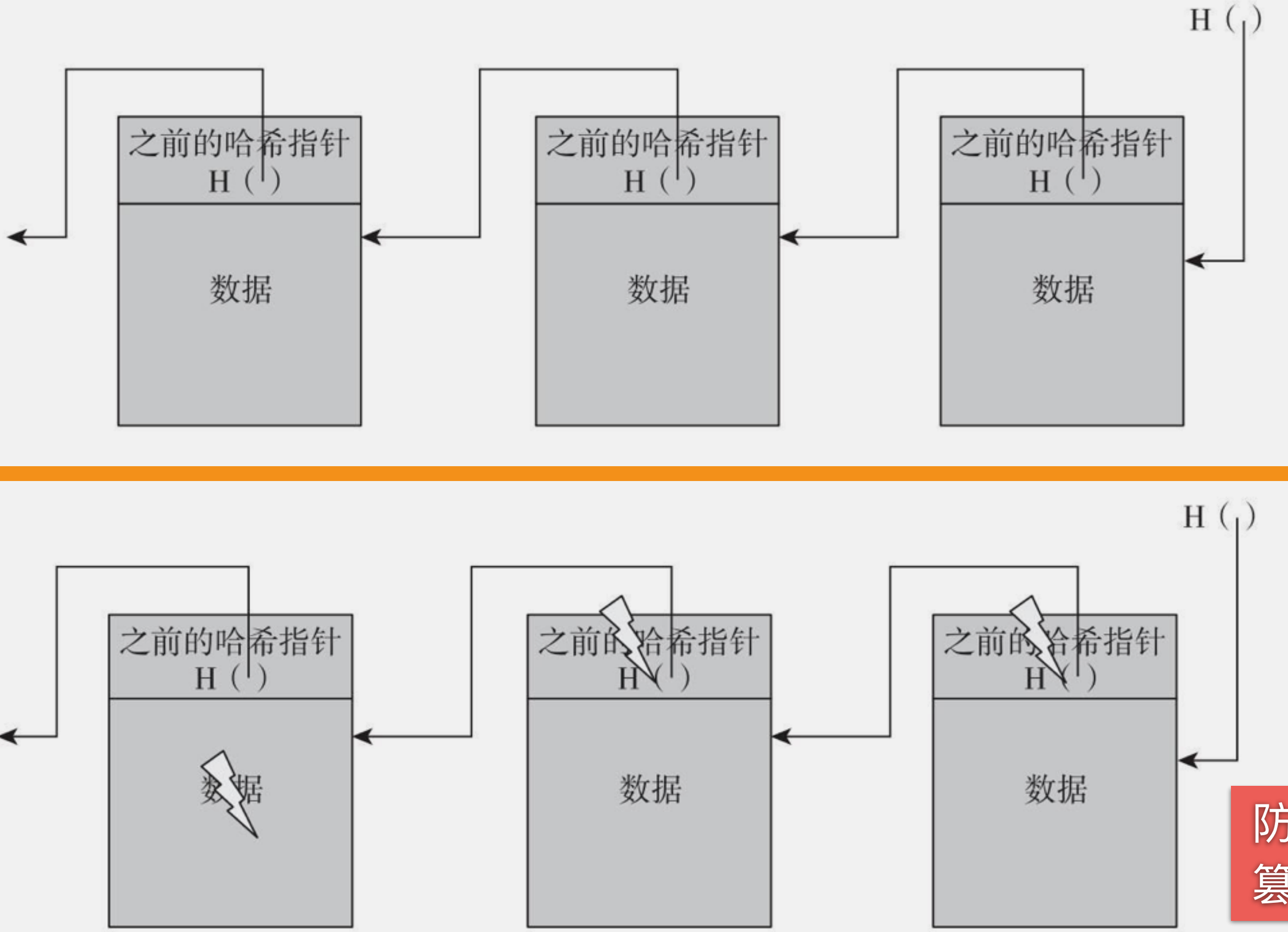
数据库表

01	AAAAAAAA
02	BBBBBBBB
03	CCCCCCCC
04	DDDDDDDD
05	EEEEEEEEE
06	FFFFFFFF

修改记录的难度

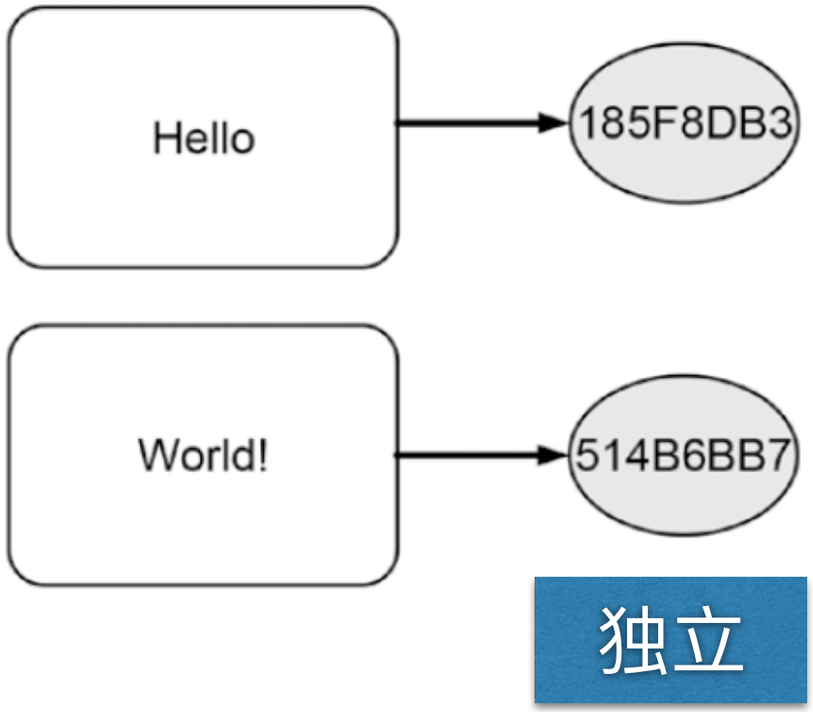


区块链

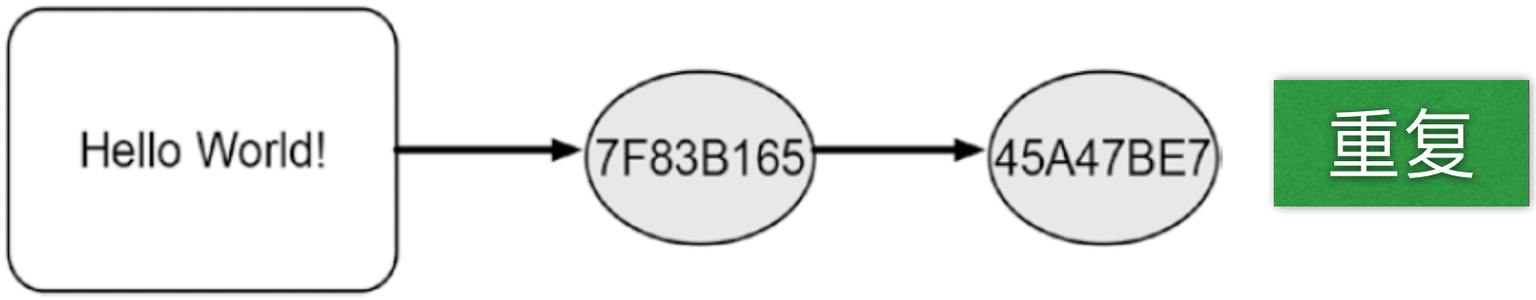

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
防止
篡改

Hash数据模式

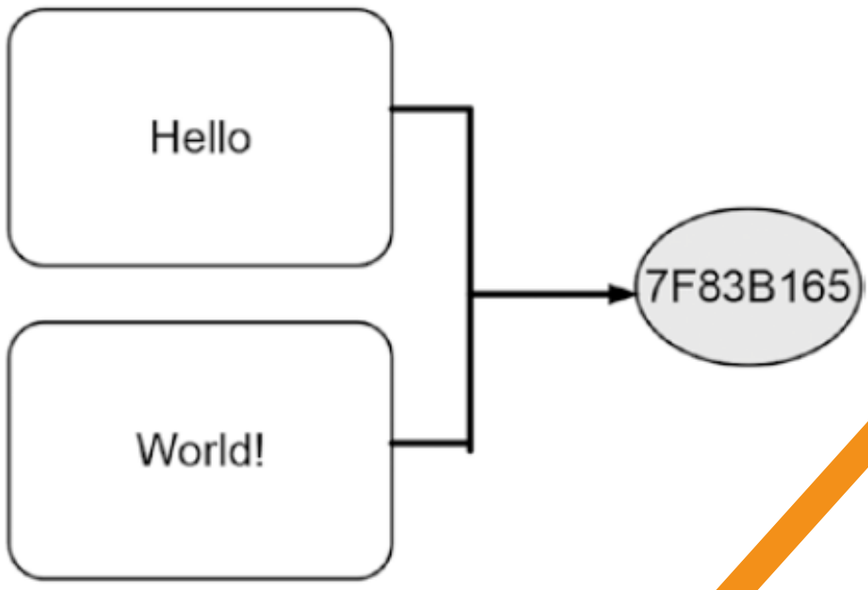
Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS



独立

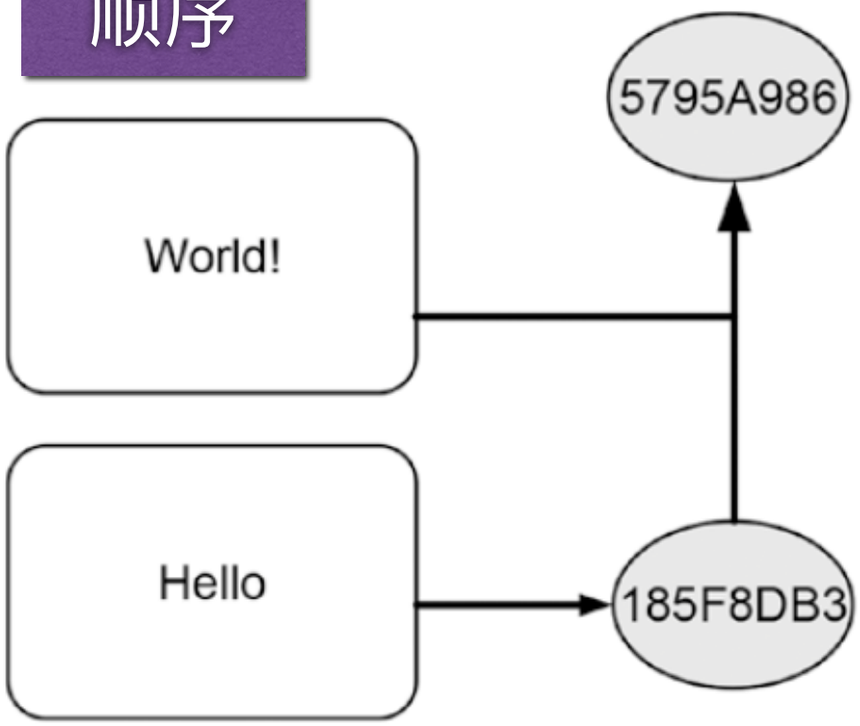


重复

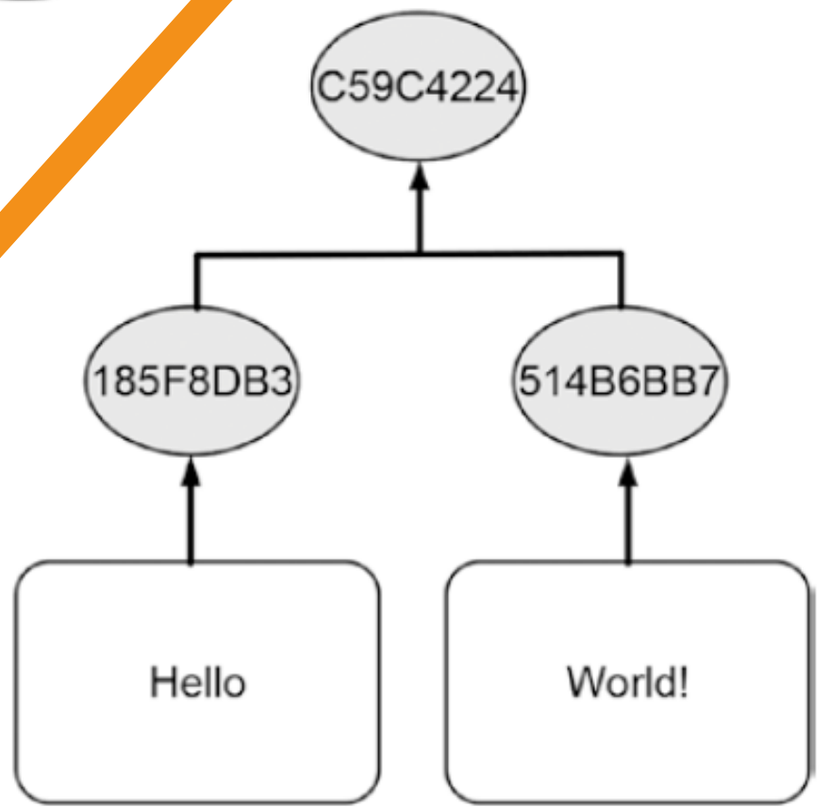


联合

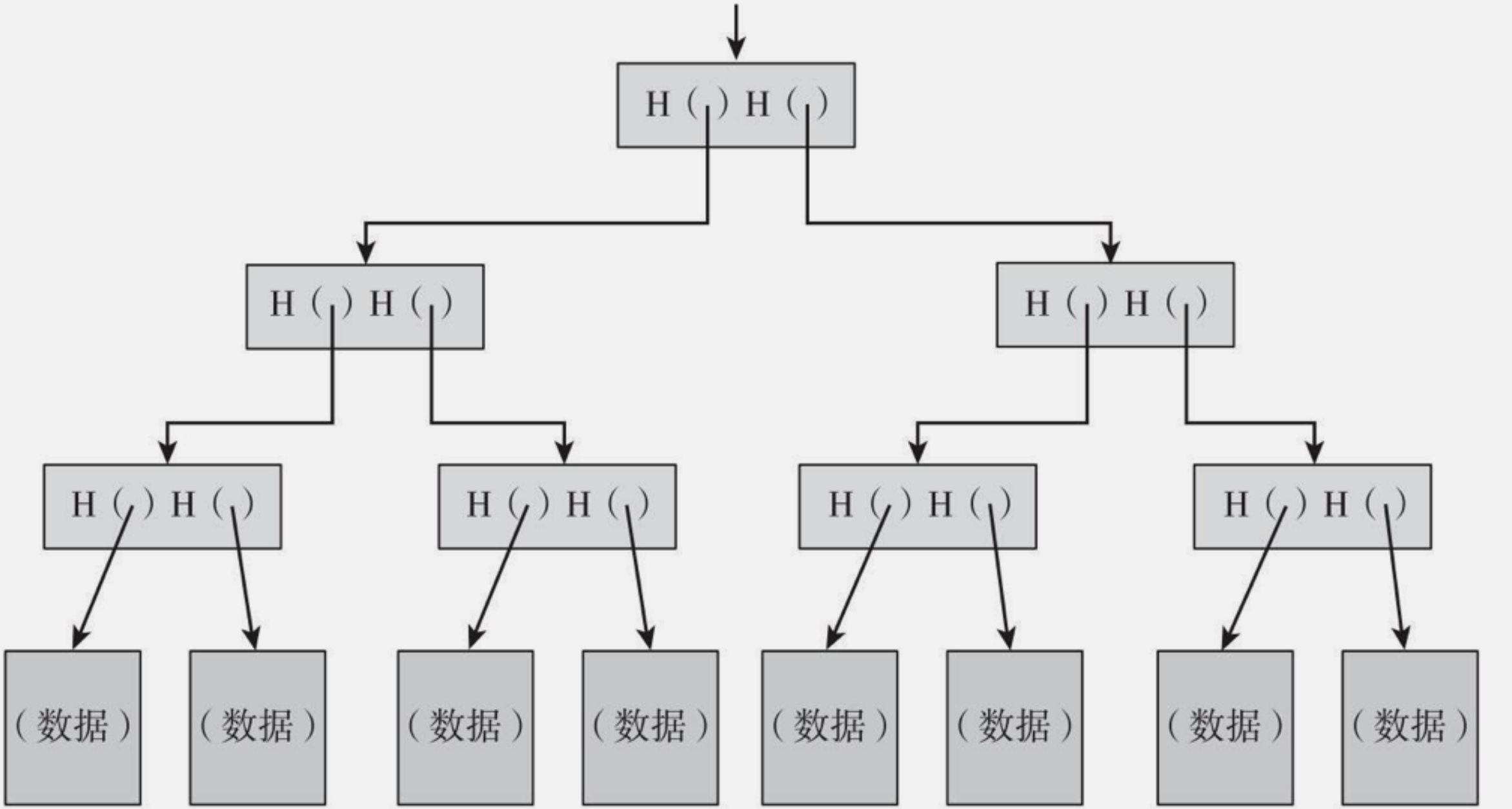
顺序



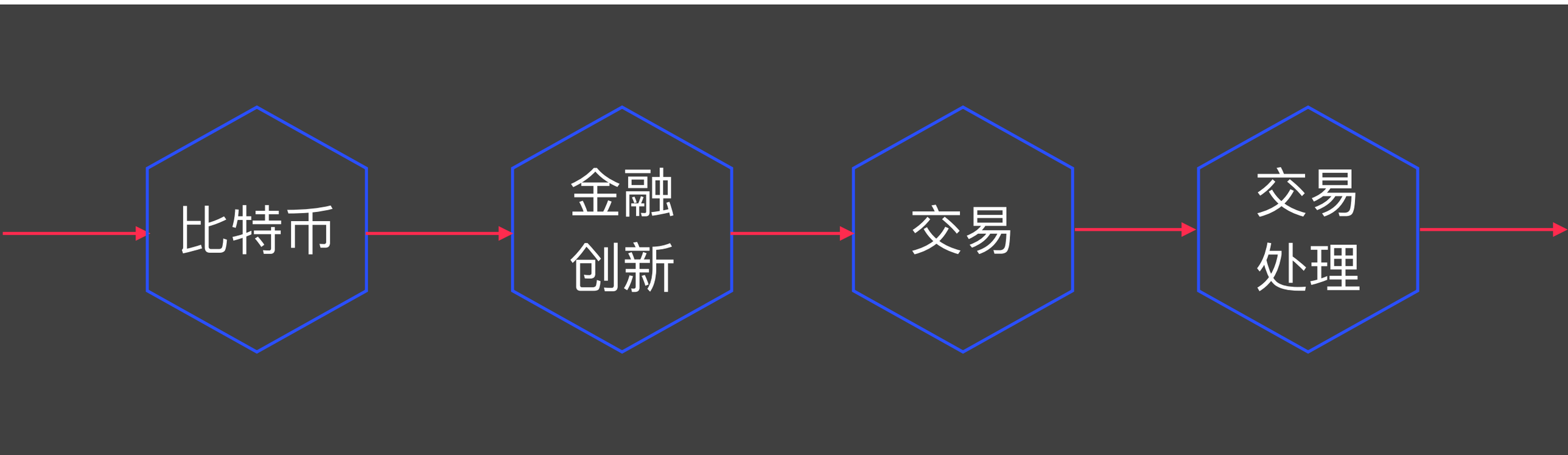
层次



梅克尔树



交易处理

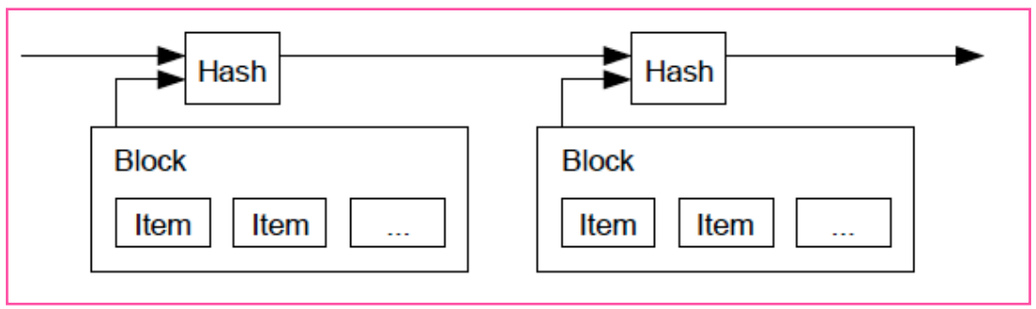


比特币产生

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.

法币

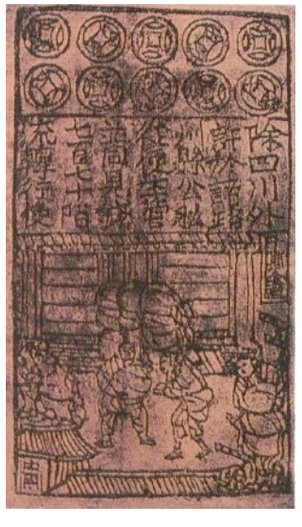

新版
2015年版 第5套
人民币
那些事...
中国人民银行
100
壹佰圆
样币
样币禁止流通
钞票正面
钞票背面
ZHONGGUO RENMIN YINHANG
100
YUAN
2015年
样币禁止流通
多一份金融了解
多一份财富保障
2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。
① 光变镂空开窗安全线
位于票面正面右侧。垂直票面观察，安全线呈品红色；与票面成一定角度观察，安全线呈绿色；透光观察，课件安全线中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

金融交易

Barter

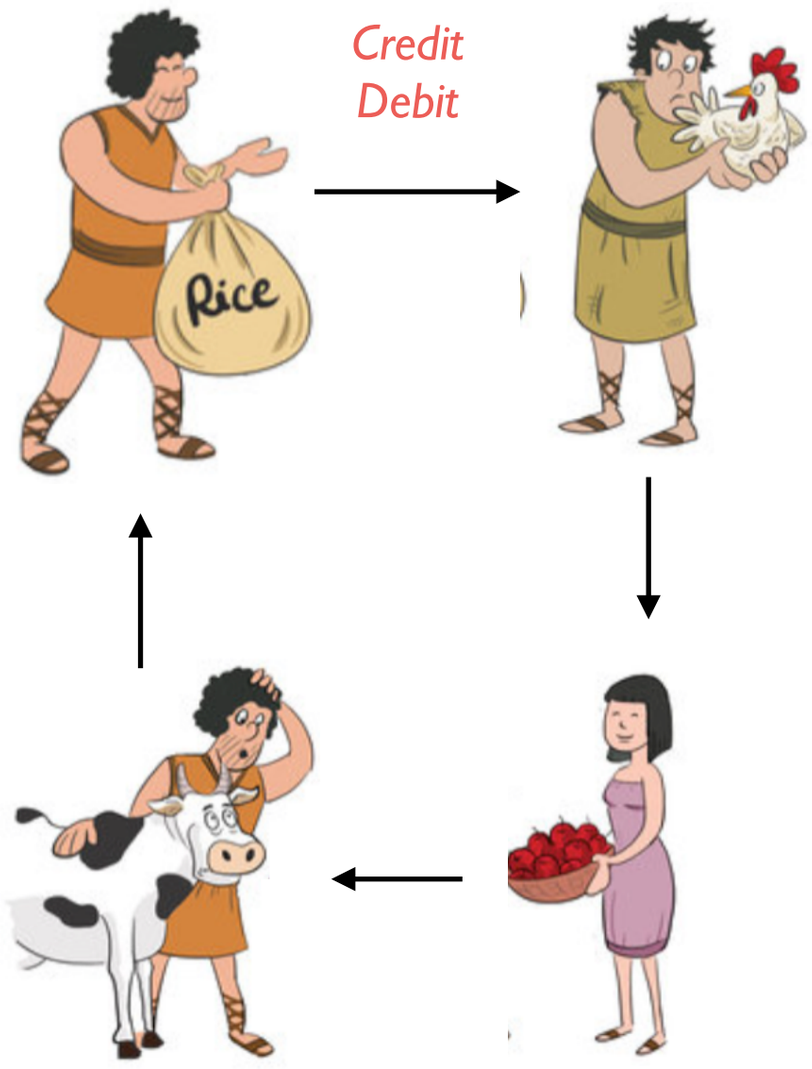
https://en.wikipedia.org/wiki/Barter

Money



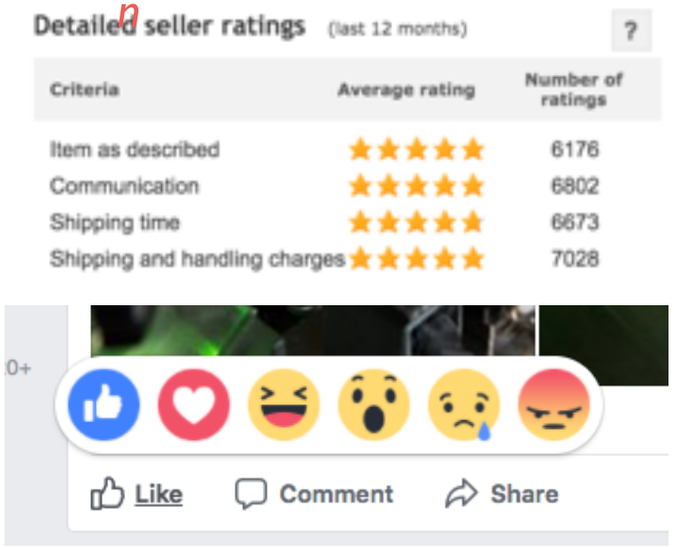
https://en.wikipedia.org/wiki/Credit

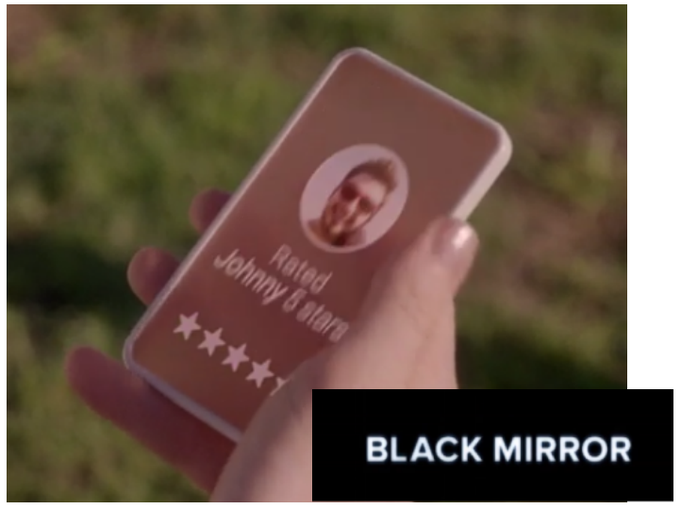
Credit Debit

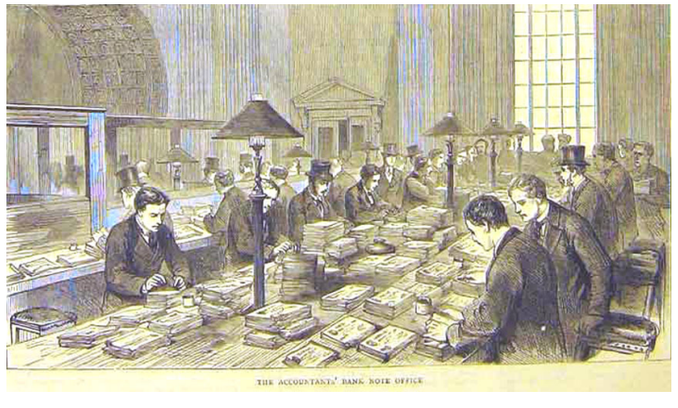


https://en.wikipedia.org/wiki/Money

Reputation





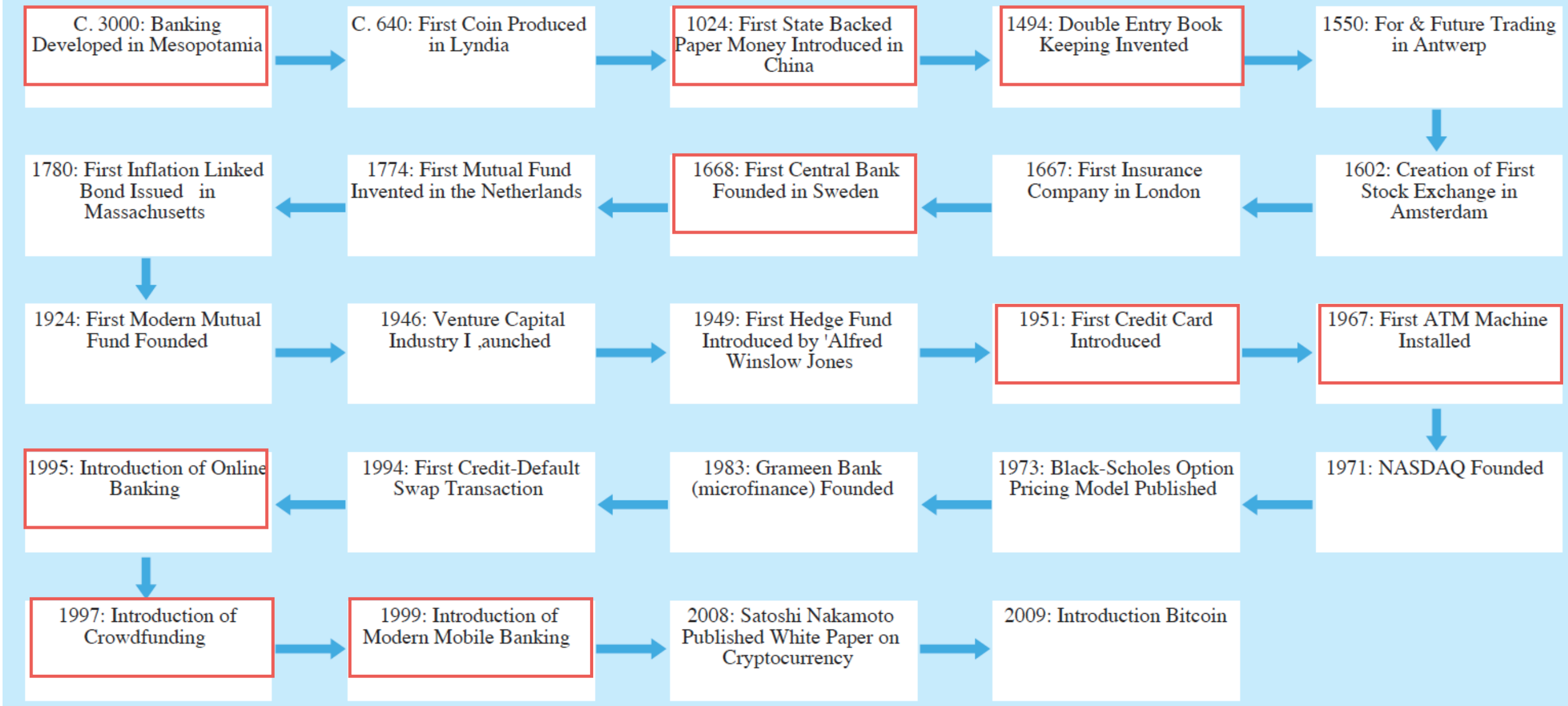


Bank

Credit Card

金融创新

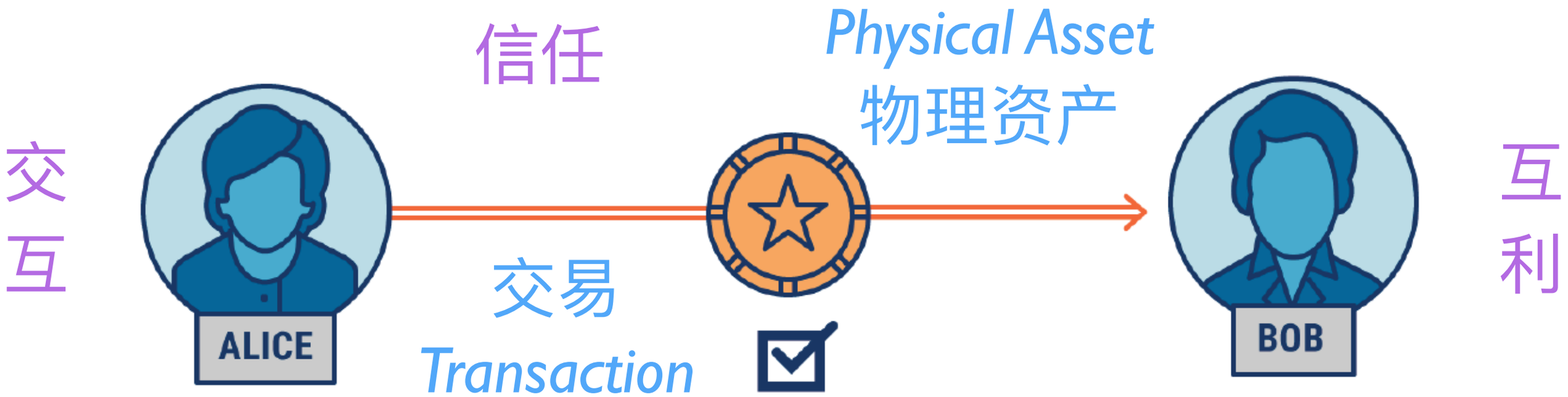
→ 金钱 → 纸币 → 复式记账 → 银行 → 信用卡 → ATM →

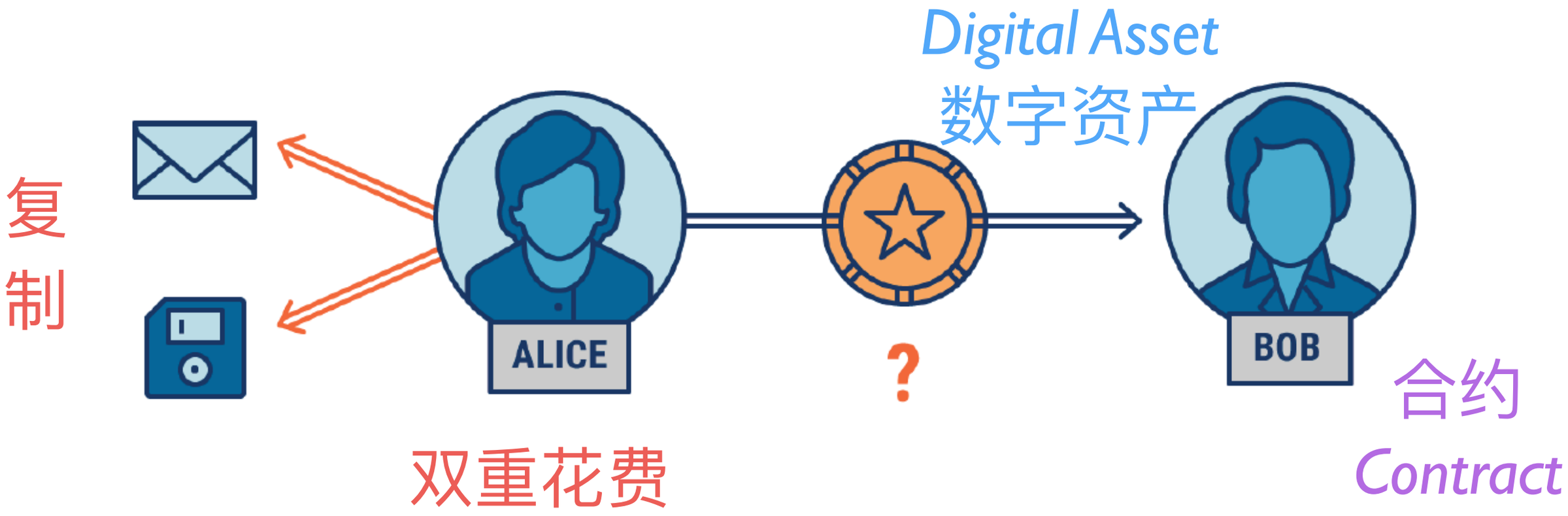


→ 在线银行 → 众筹 → 移动支付 → Bitcoin → 区块链 →

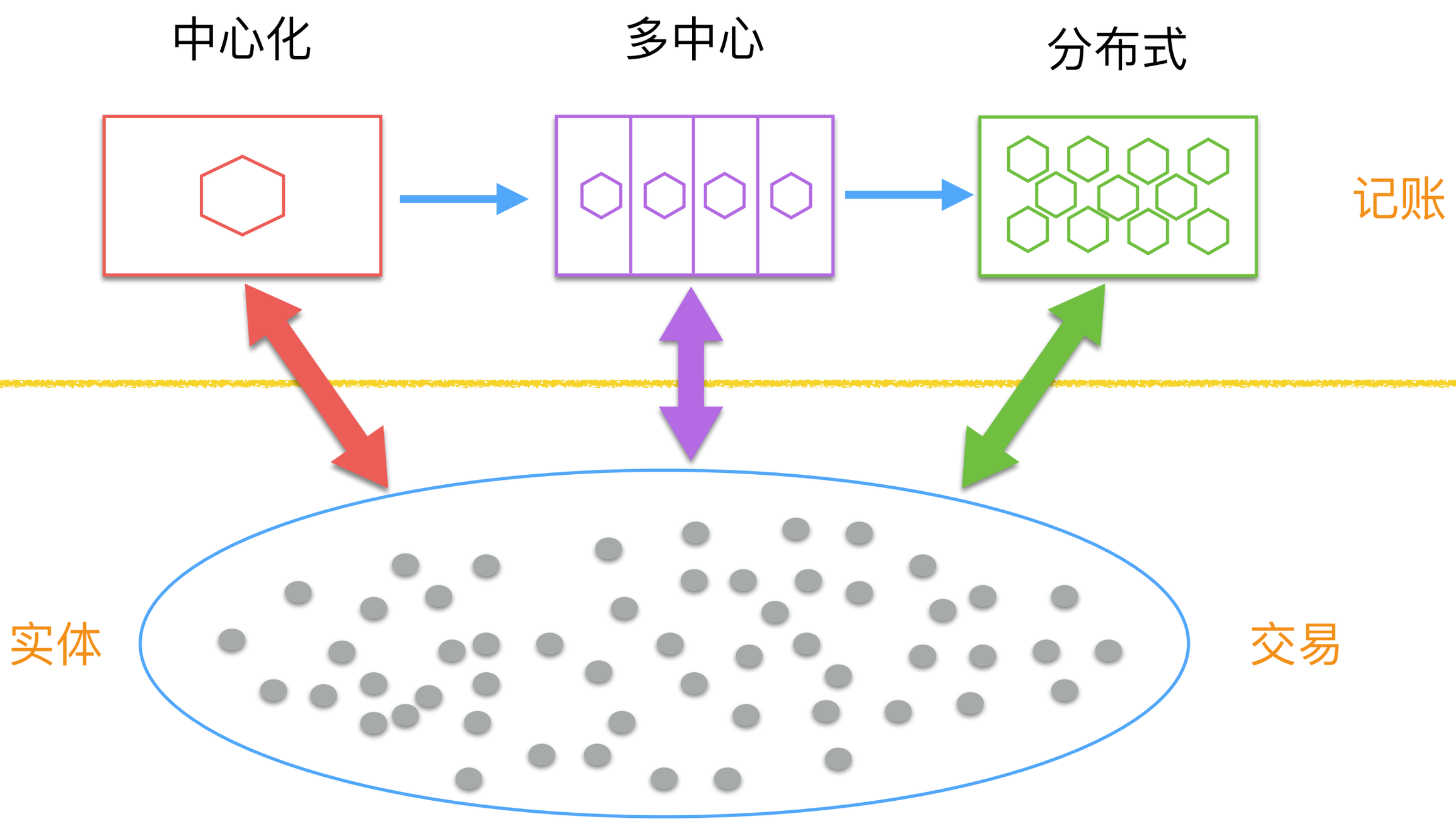
交易：物理 vs. 数字

What is Blockchain Technology @ CBSInsights

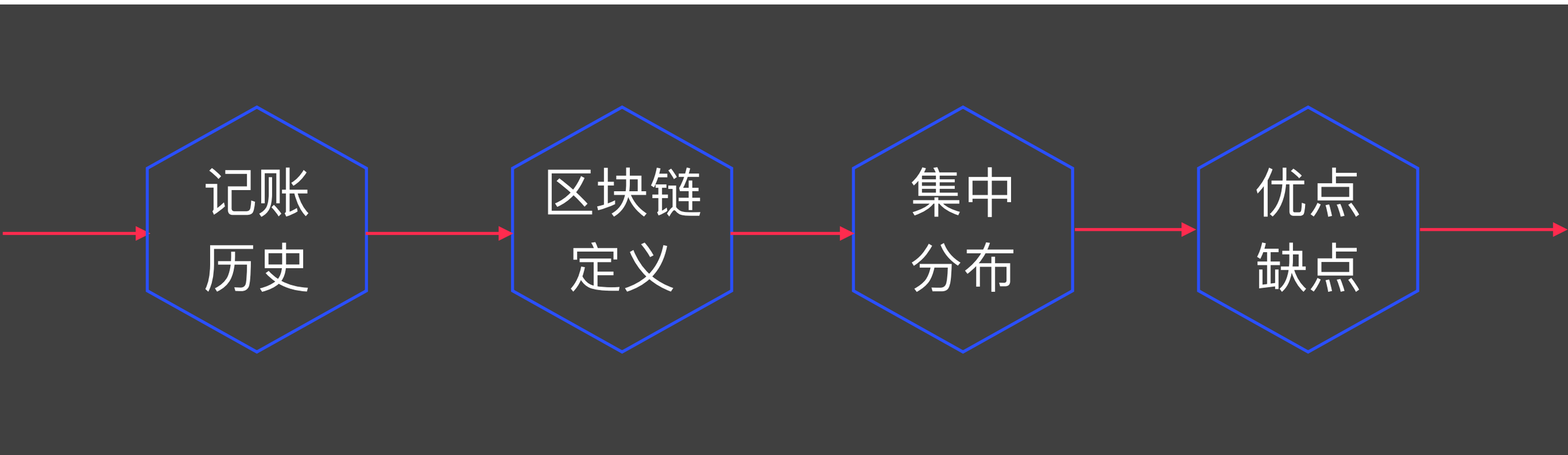




交易处理

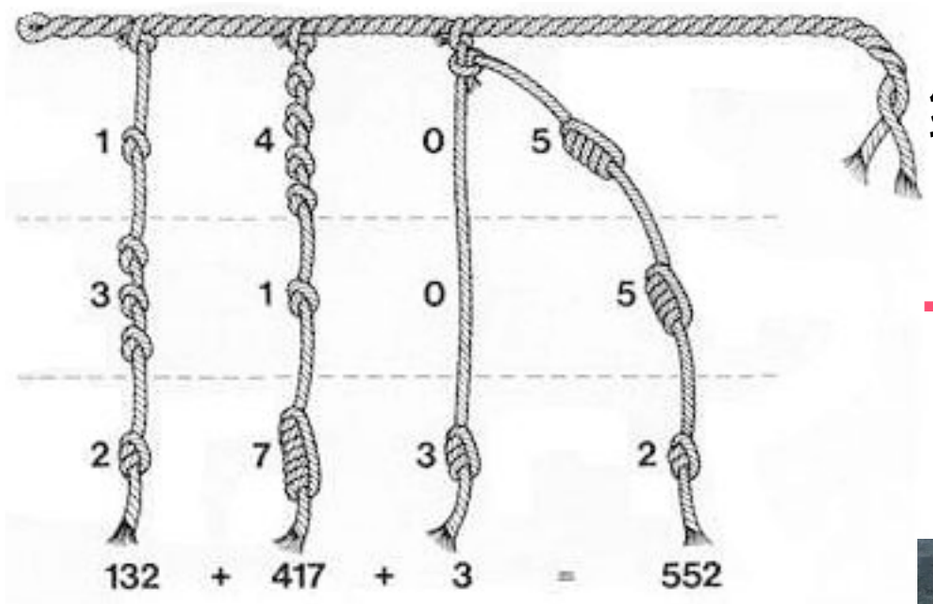


账本

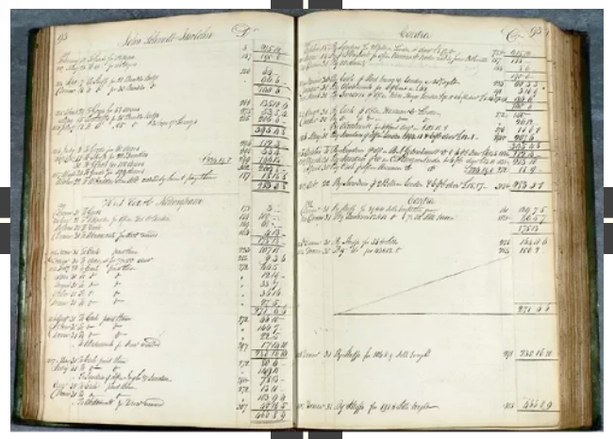


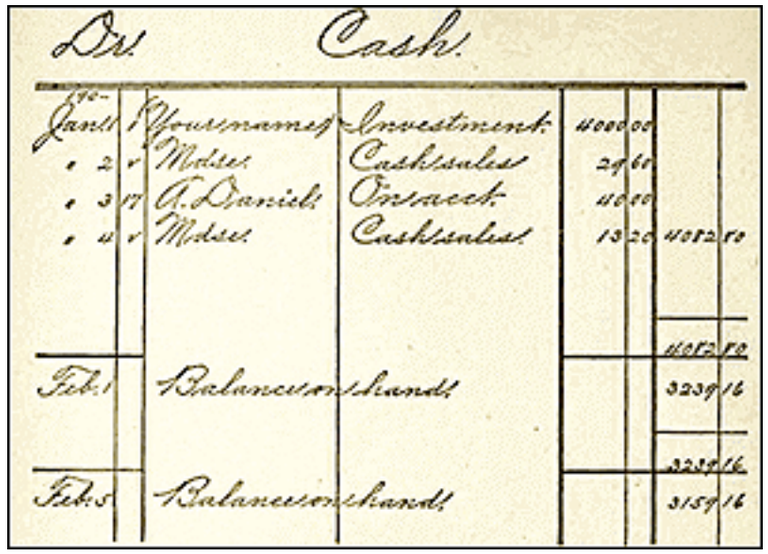
记账历史

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



结绳





单式

复式

电子

物理

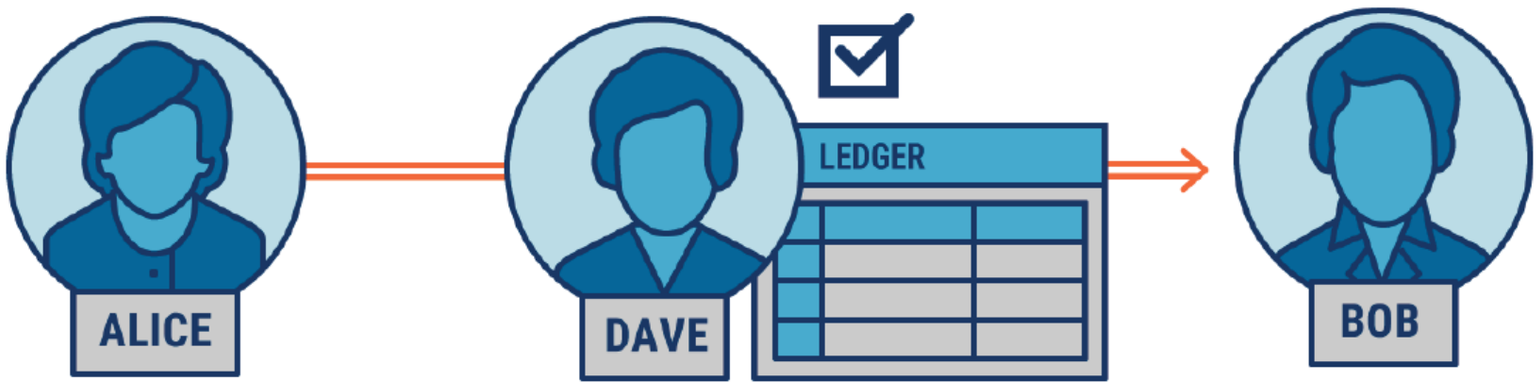
区块链定义

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



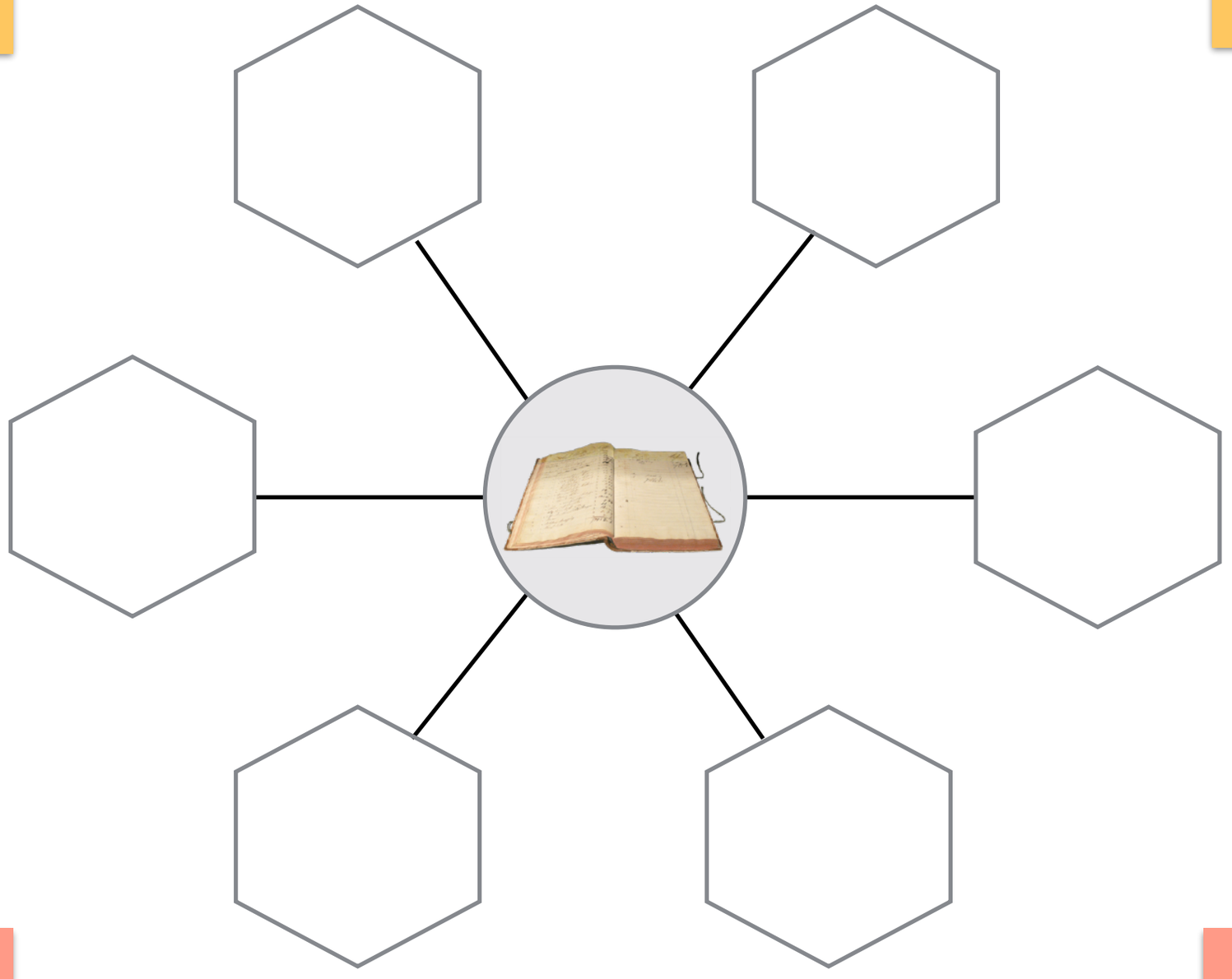
集中

分布

集中式账本的优缺点

中心化

第三方



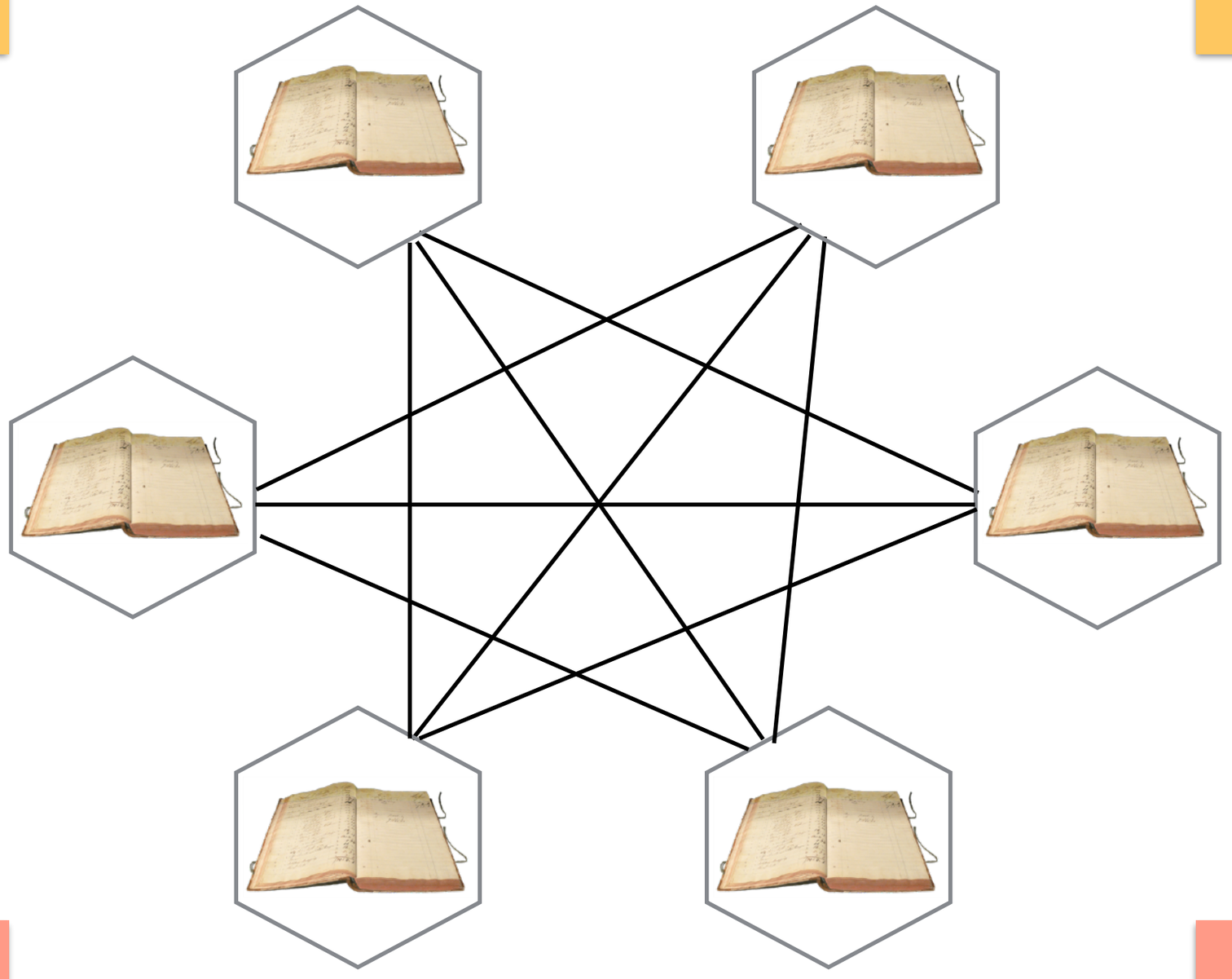
脆弱

信任

分布式账本的优缺点

一致性

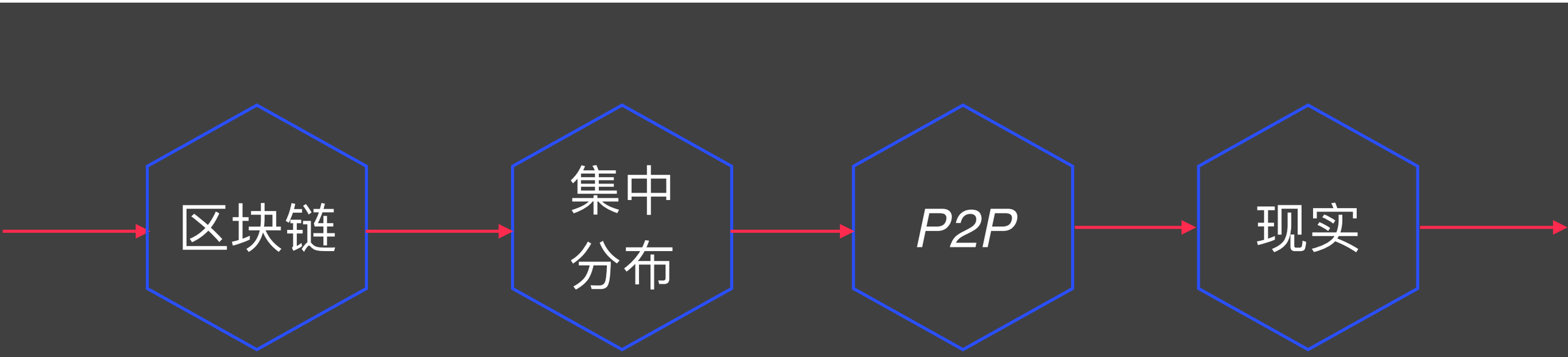
完整性



效率

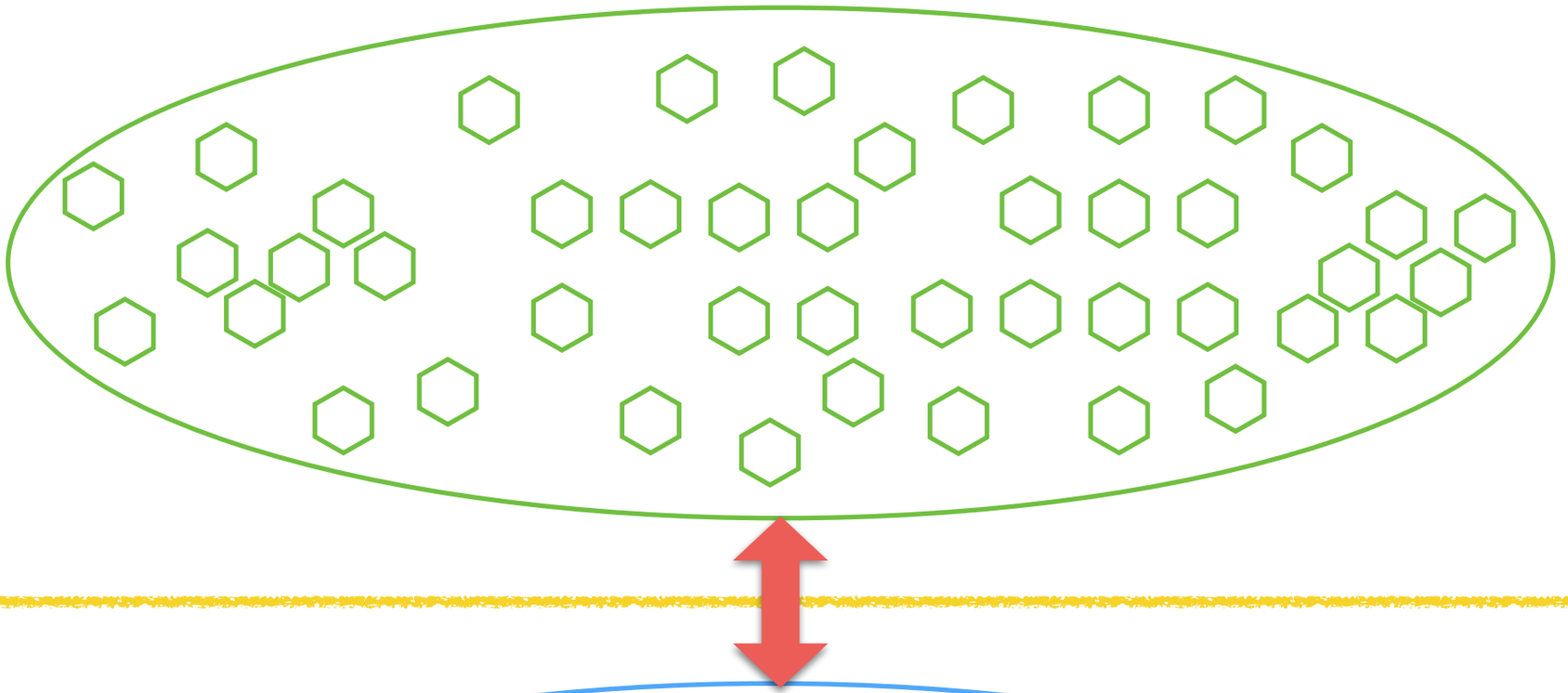
花费

分布系统



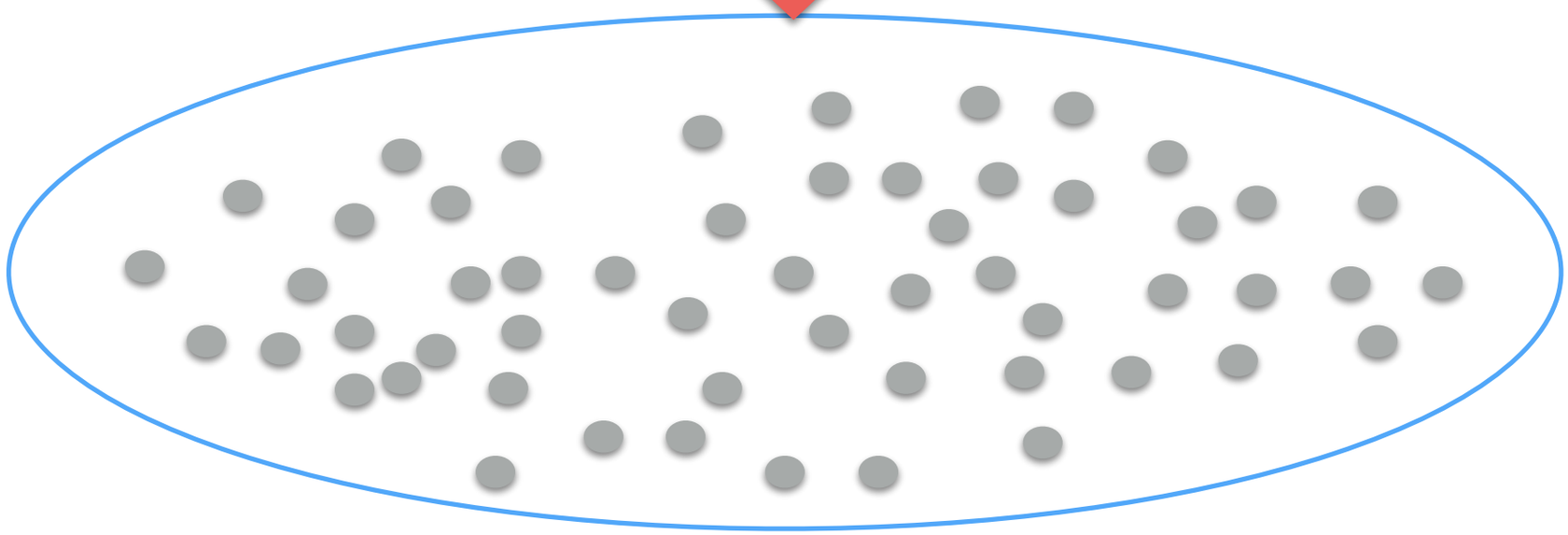
区块链系统

记账
网络



区块
传播

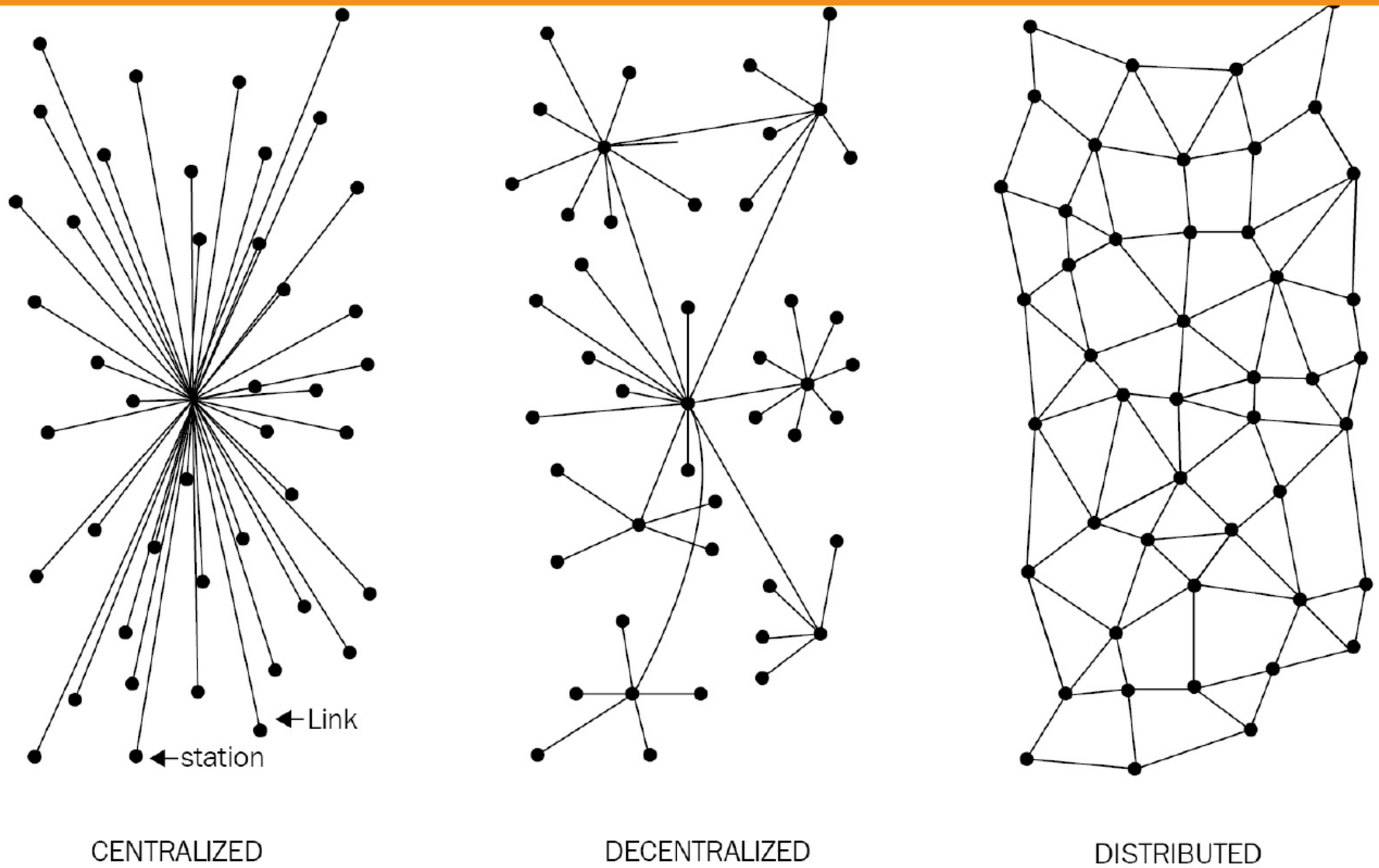
交易
网络



交易
传播

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

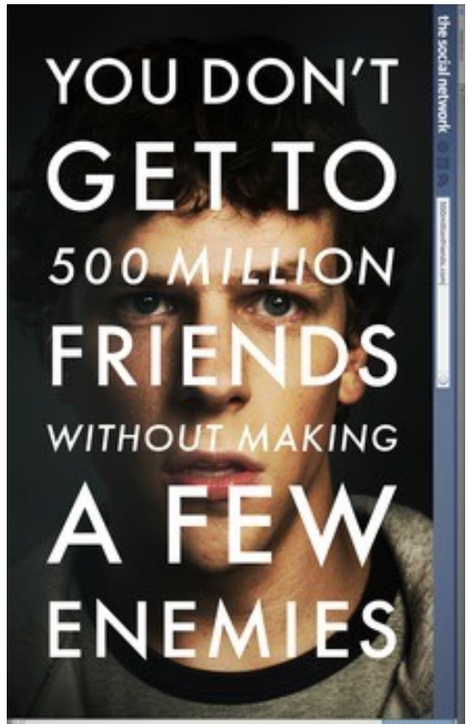
P2P的力量

napster™

1999

Sean Parker

facebook

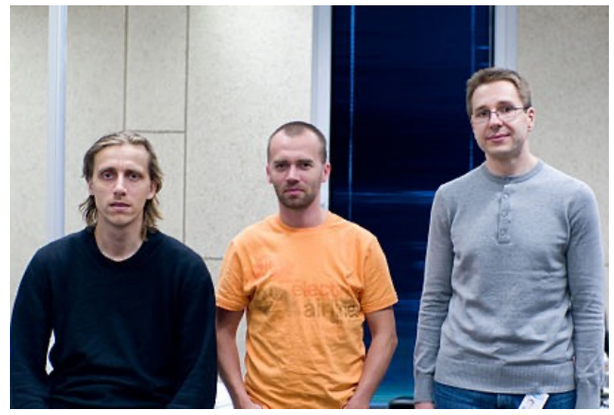


The Social Network

skype™

2003

KaZaA

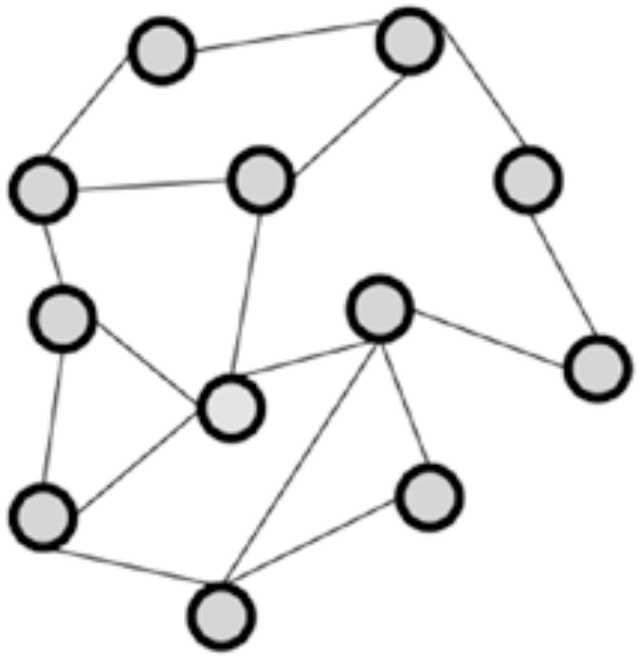


2001

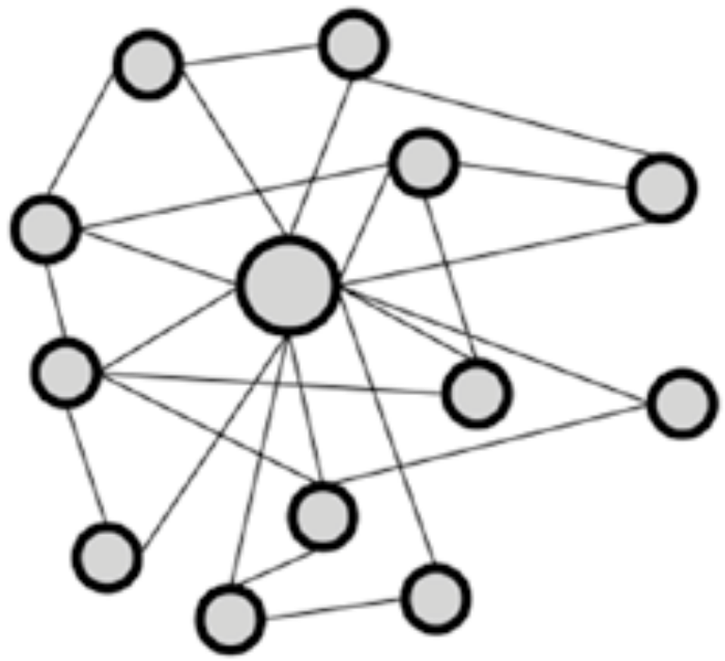
Bram Cohen

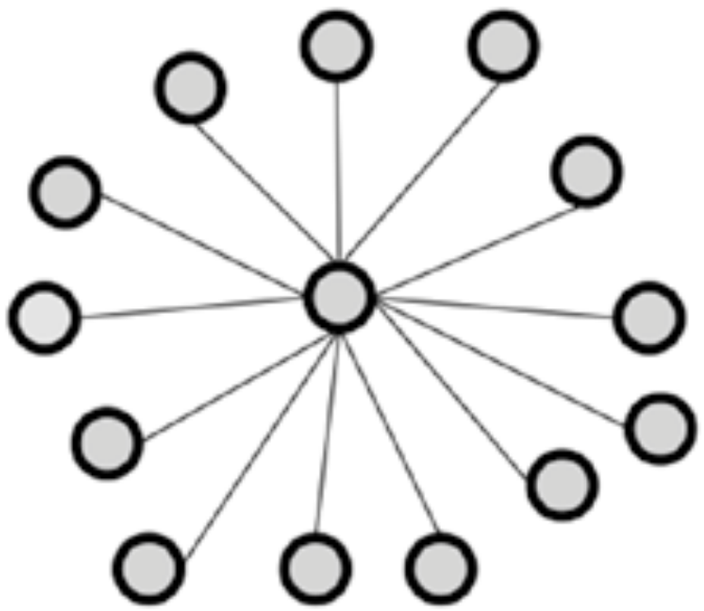
BitTorrent

分布还是集中

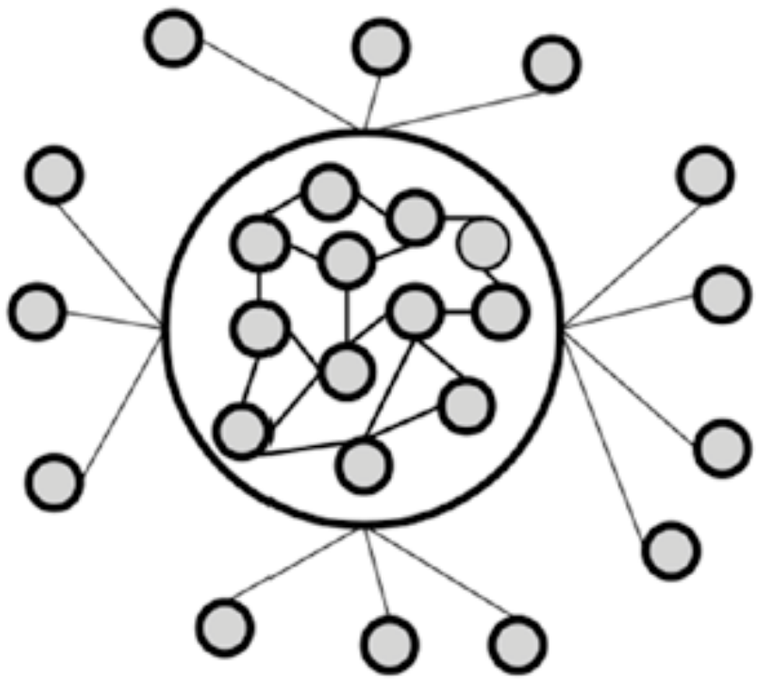


没有纯粹的
中心化系统
或者
分布式系统

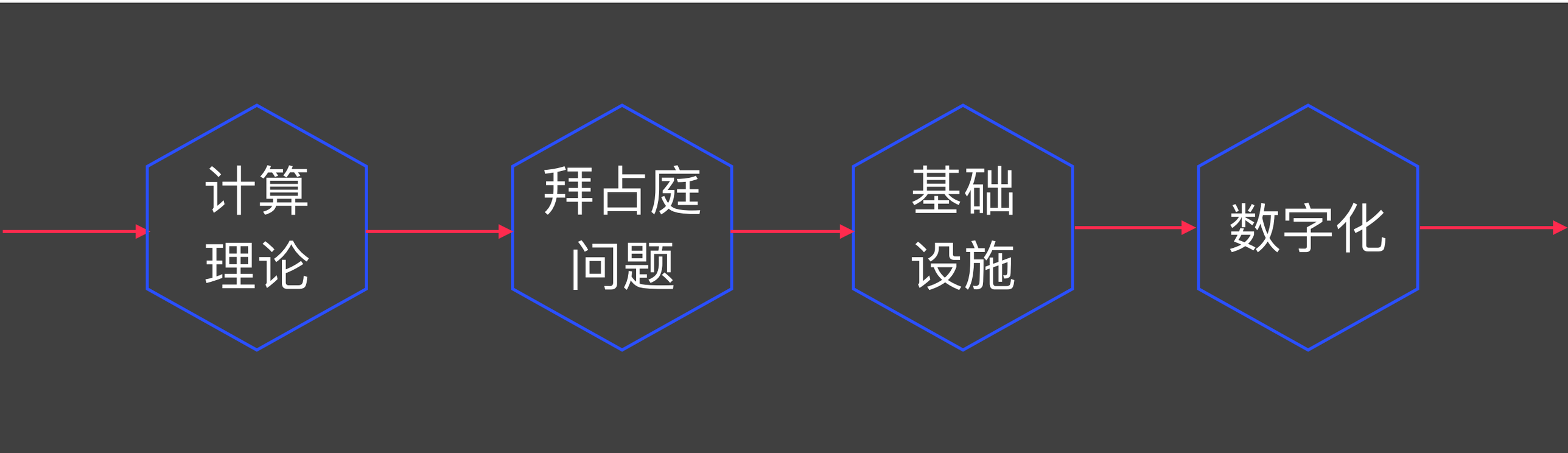




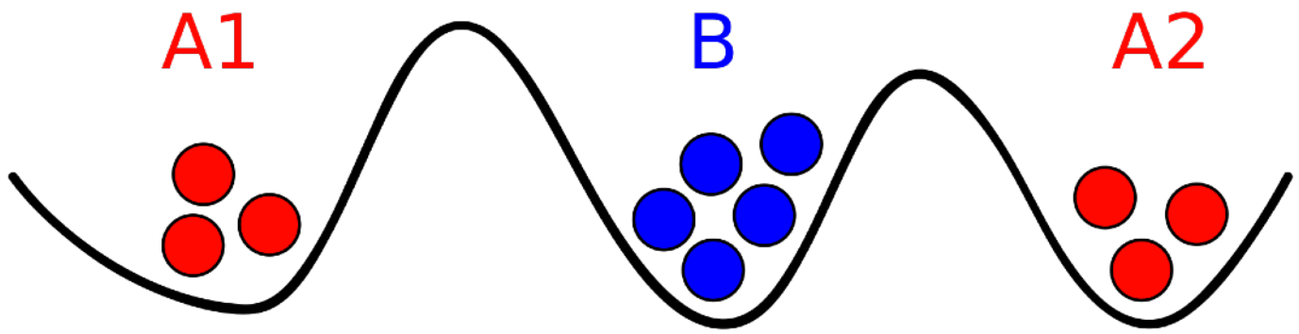
Internet
Email
IM
SNS



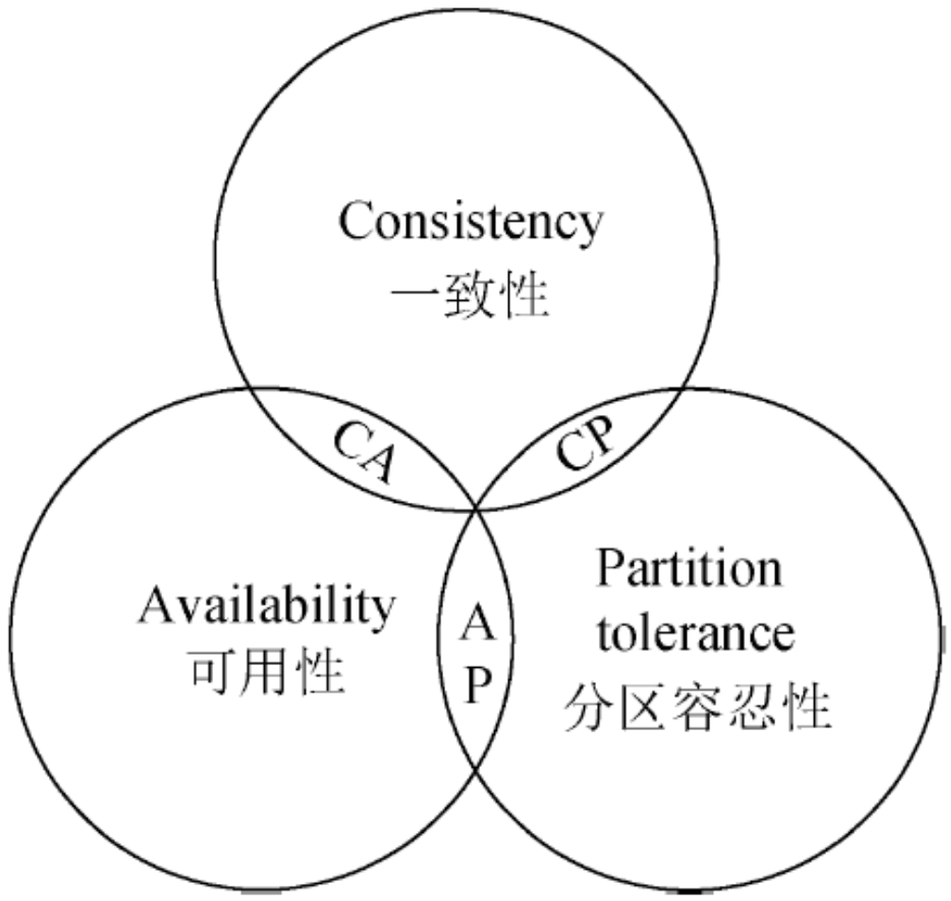
计算模式



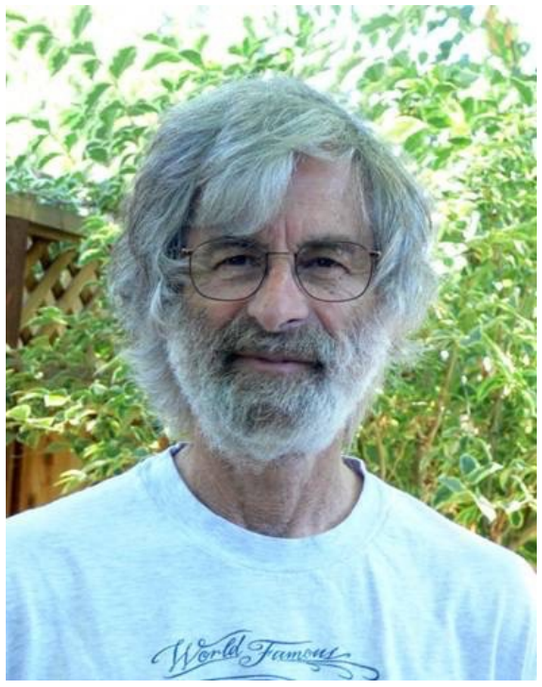
两军问题、FLP、CAP



FLP
不可能定理



拜占庭将军问题



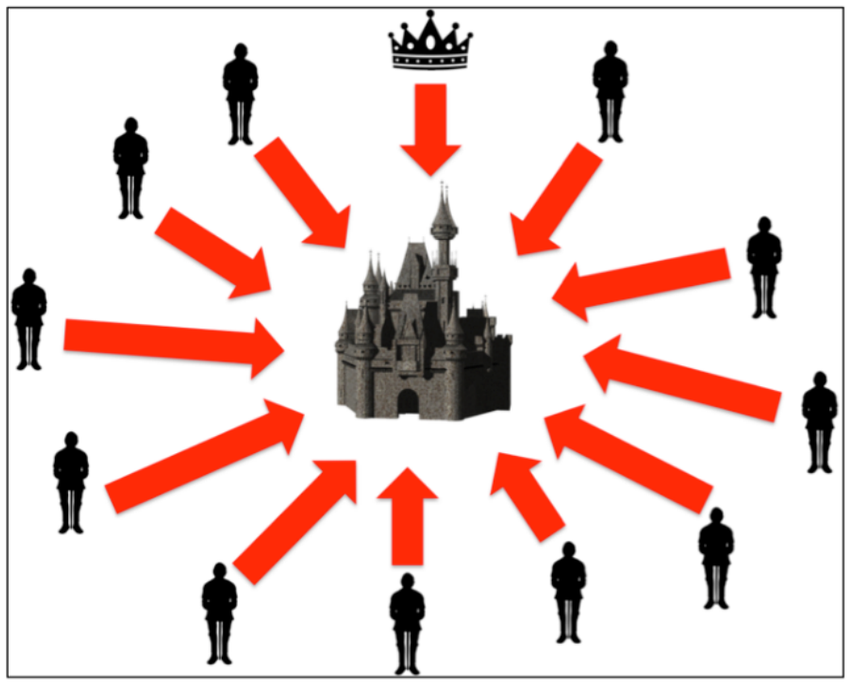
LESLIE LAMPORT

2013图灵奖

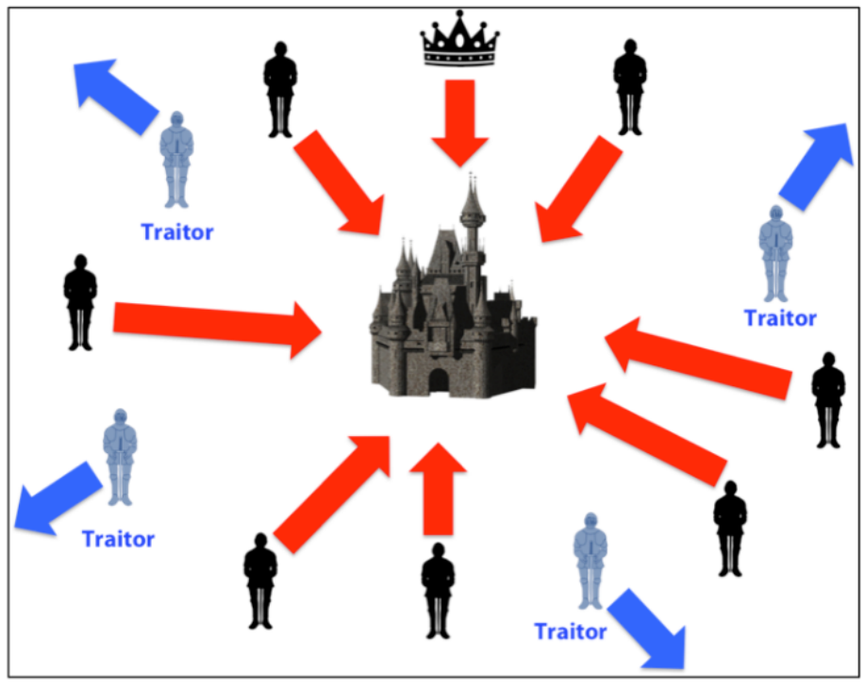
The Byzantine Generals Problem

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.

Blockchain Overview

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

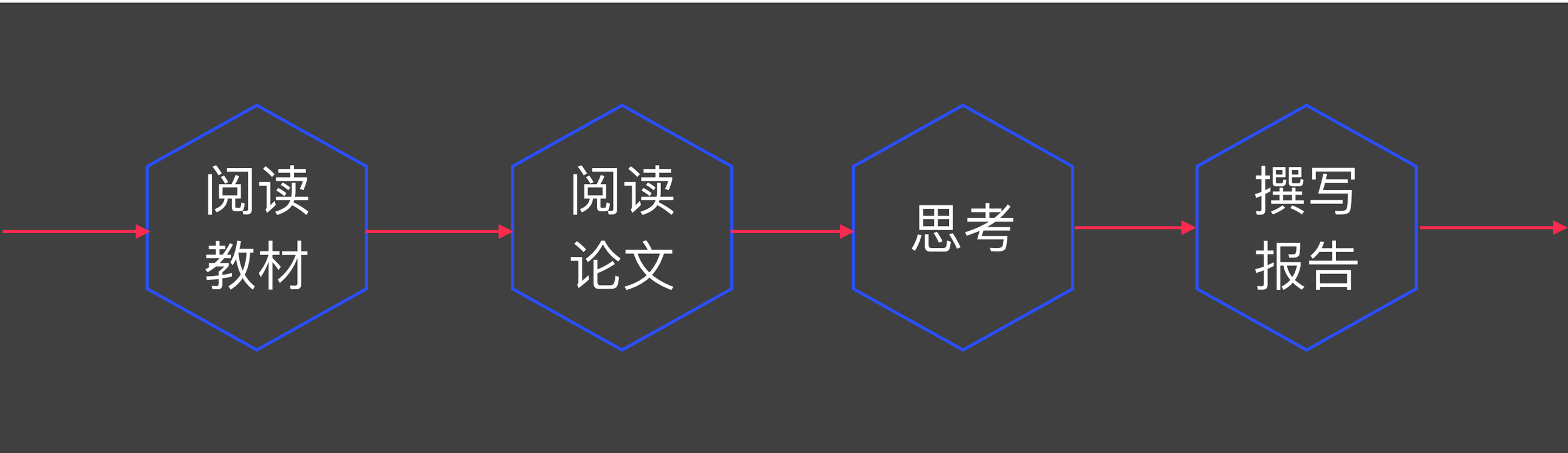
2023年ICT中投资50%以上是数字化转型

- 数字资源
- 组织结构
- 策略目标

数字经济

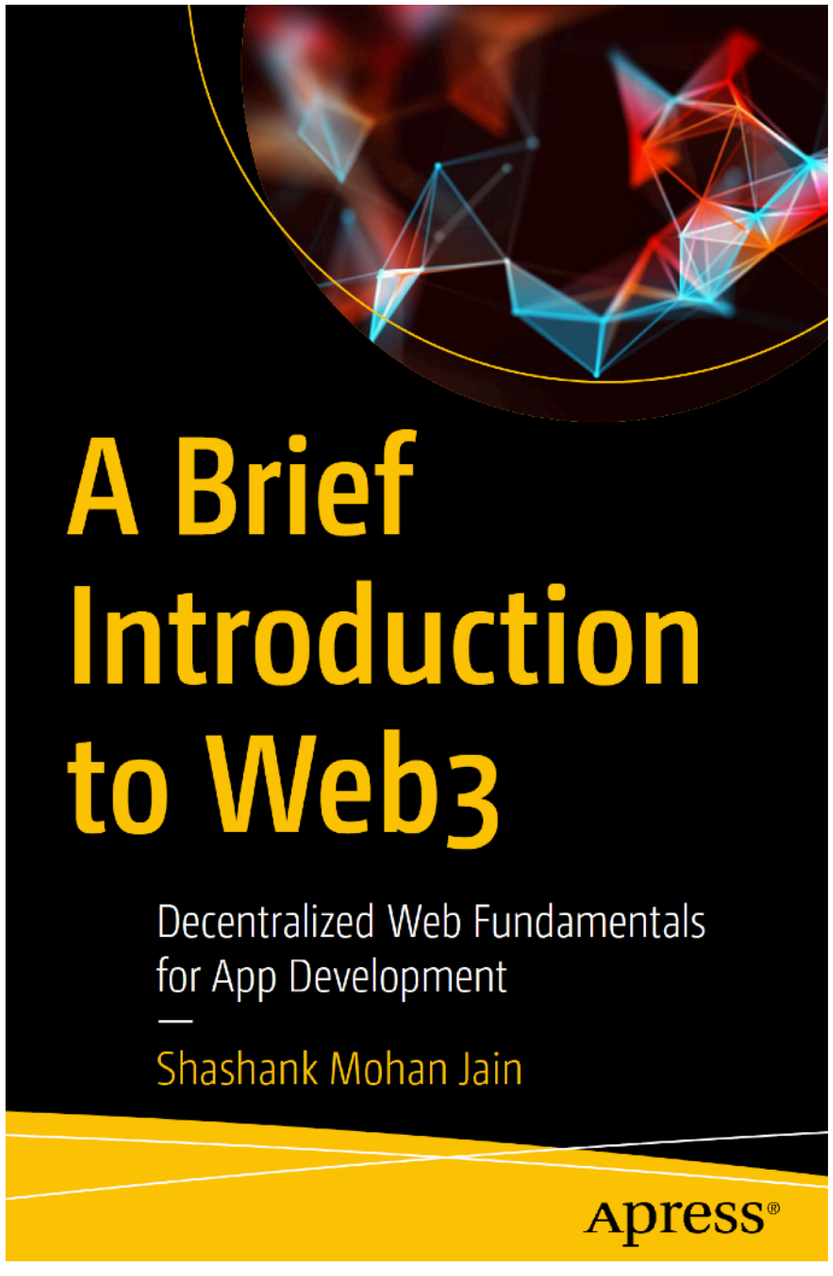
基于数字货物和服务的商业模式，经济收益主要由数字化技术带来的经济形式。

课后作业



Homework

阅读参考书



看：第1-2章

有余力的同学可以检索如下关键词：

What is Web3?

选择你认为重要资料扩展阅读

谢谢！

孙惠平
sunhp@ss.pku.edu.cn