区块链的基础知识

区块链为何能成为 Web3 与 元宇宙的基础设施

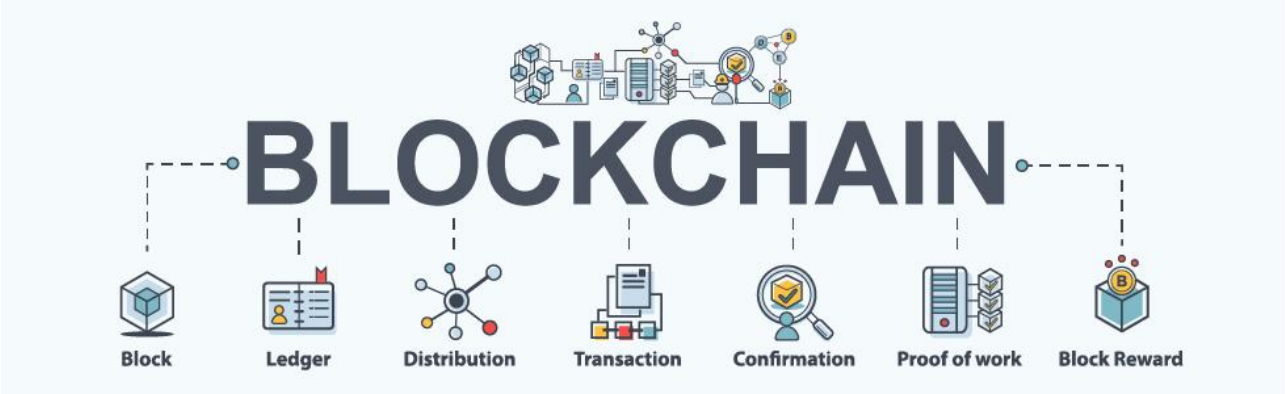
吴嘉婧

中山大学，软件工程学院

提纲

区块链的社会意义

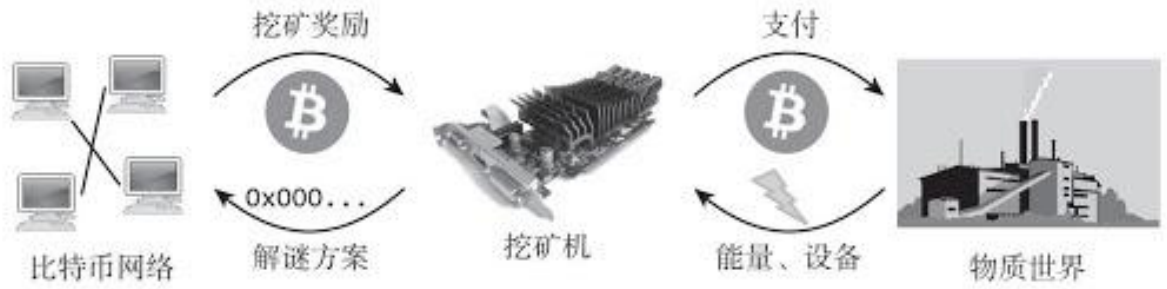
- 区块链的挖矿生态
- 区块链技术会给世界带来什么意义?



导言：PoW 挖矿的一些事实

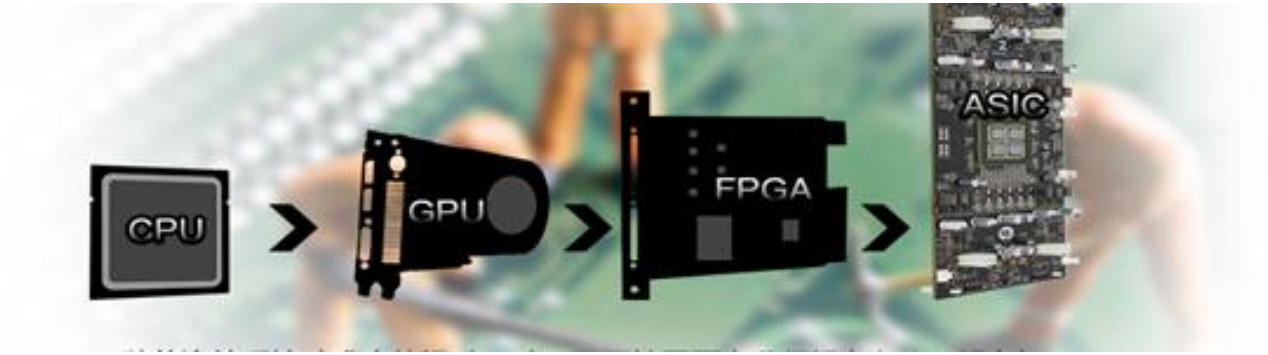
Proof-of-Work

证明 **资源消耗**



导言： PoW 挖矿算力的进化

- 普通的 CPU（2009 年）、到后来的 GPU（2010 年） 和 FPGA（2011 年末）、到后来的ASIC 矿机（2013 年年初，目前单片算力已达每秒数百亿次 Hash 计算）、再到现在众多矿机联合组成矿池（知名矿池包括 F2Pool、BitFury、BTCC 等)



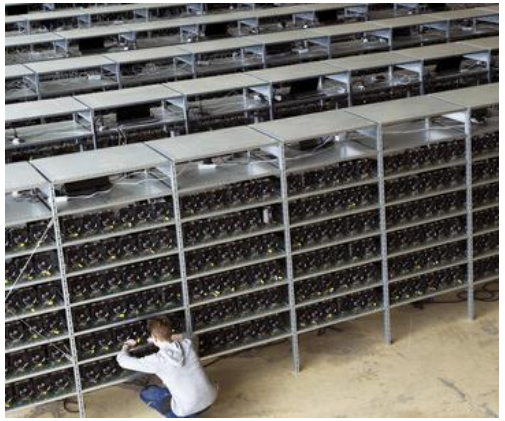
- 截止1/5/2018, 全网的算力已超过**每秒2.6*10^18 次** Hash 计算，超过**世界500强超级计算机算力总和**的**100倍!**

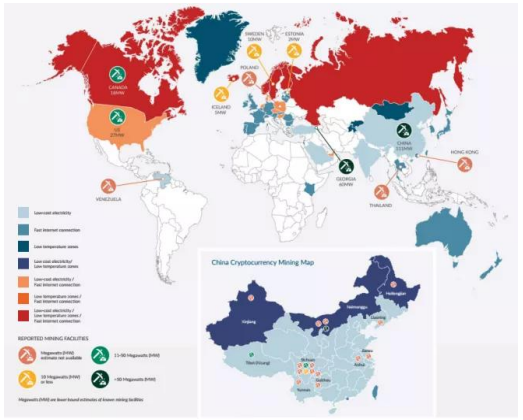
导言： PoW 挖矿的一些事实

- **“仅增”账本**
  - 每 10 分钟左右生成一个不超过 1 MB 大小的区块，记录了这 10 分钟内发生的验证过的交易内容，串联到区块链尾部
- **难度调整**
  - 根据上一周期的挖矿时间来调整挖矿难度（通过调整限制数“0”数目），来调节生成区块的时间稳定在 10 分钟左右。
- **不会通胀的货币**
  - 每个区块的成功提交者可以得到系统 6.25 个比特币 的“出块奖励” + 交易手续费
  - 每个区块的奖励最初是 50 个比特币，每隔 21 万个区块自动减半，即 4 年时间，最终在2140年比特币总量稳定在 2100 万个

导言： PoW 挖矿的一些事实 —— 矿场

- 中国的挖矿算力 曾经 占了全世界大概 70% 的份额
  - 一是由于矿机的生产主要在中国，
  - 二是中国电费有一定优势，
  - 三是与国内大的经济和政策形势有关系。
- 国内禁止挖矿





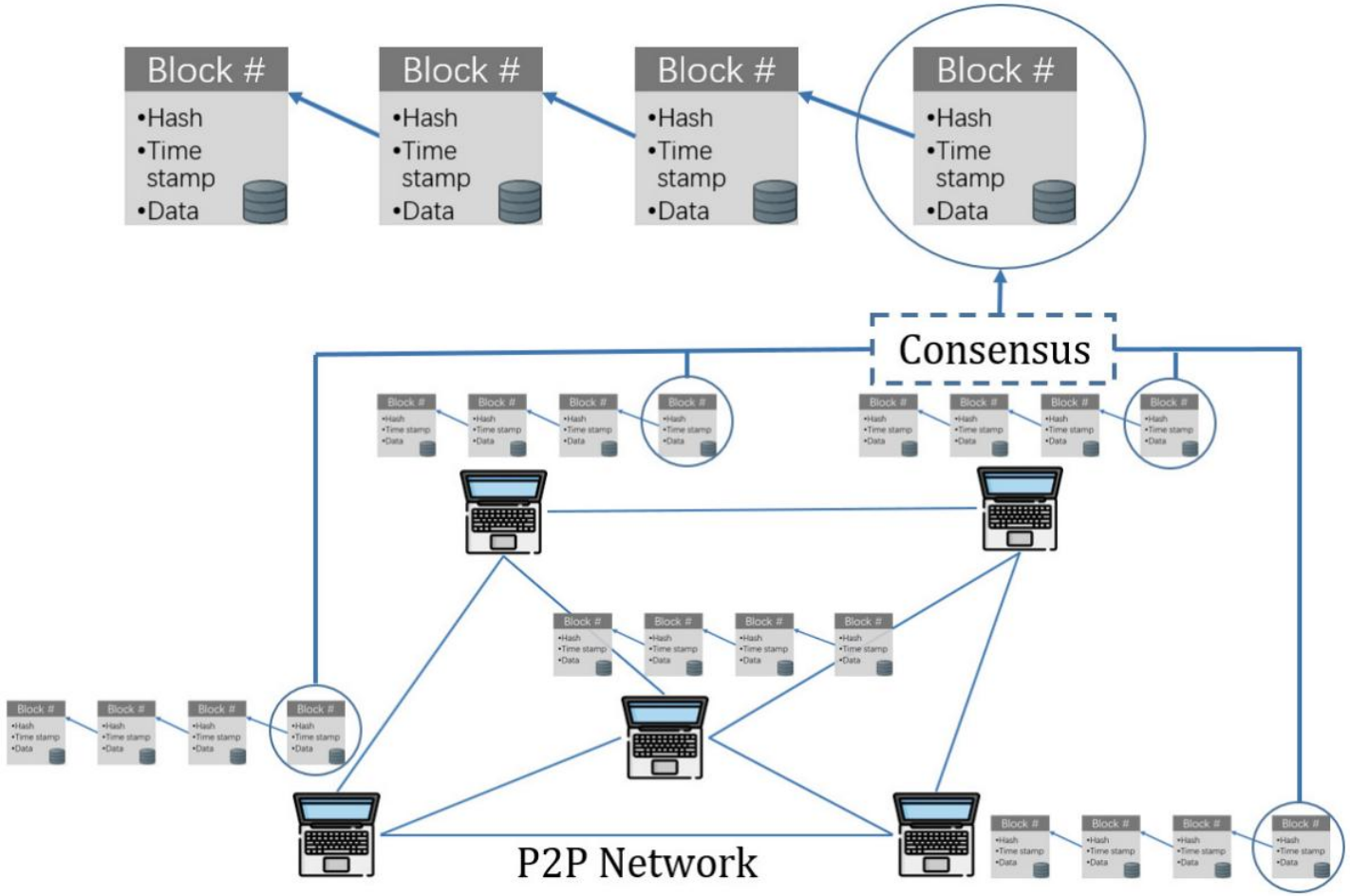
本课内容

- 2个灵魂之问
  - Q1: 区块链是什么？ （第3课）
  - Q2: 区块链技术会给世界带来什么的影响或改变？ （第4课）

灵魂之问2：区块链会给世界带来什么影响 或 改变?

Overview of Blockchain

- A decentralized database built on a P2P Network



导言：区块链的起源

更高效交流的手段

文字

（精神）

信息传递：语言 → 文字 → 印刷术 → 电报 → 互联网

信息

（信息传递网络）

TCP/IP

楔形文字
记录生意

货币

（物质）

价值传输：大麦 → 黄金 → 纸币 → 移动支付 → 比特币

信用

PayPal

（价值传输网络）

区块链

时间：公元前3000年左右

地点：美索不达米亚平原（伊拉克境内，古巴比伦）

导言：区块链的起源

货币的国家化：国家/机构发放铸币/纸币

- 铸币（固定价值）：

币价 = 币真实价值

↓

币价 = 币真实价值 – 铸币成本

↓

币价 = 一半的真实价值– 铸币成本

↓

币价 = 越来越少的真实价值

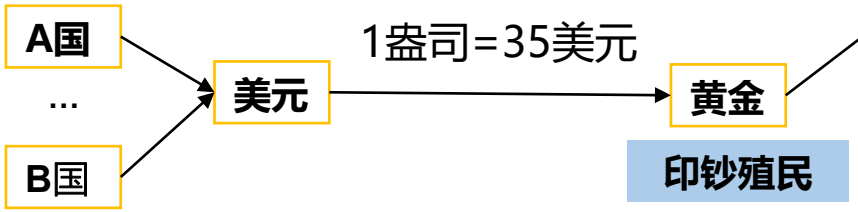
- 纸币

币价=纸币上的面值　　基于信用

导言：区块链的起源

货币的国际化

- 布雷顿森林体系



美元与黄金挂钩

和平后，全球生产力大幅提升

↓

美元增发，黄金开采速度跟不上

脱钩

- 汇率安排多样化、储备货币多元化

美元硬通货，美元仍然处于国际货币体系中的中心位置

导言：区块链的起源

- 2008年9月，以雷曼兄弟的倒闭为开端，金融危机在美国爆发并向全世界蔓延。

人们普遍担忧法定货币和美联储等机构的信誉

- 2008年10月31日纽约时间下午2点10分，中本聪发布*Bitcoin: A Peer-to-Peer Electronic Cash System*
- 2009年1月比特币网络上线，推出了第一个开源的比特币客户端软件

当前的货币体系为什么会引起人们的担忧?

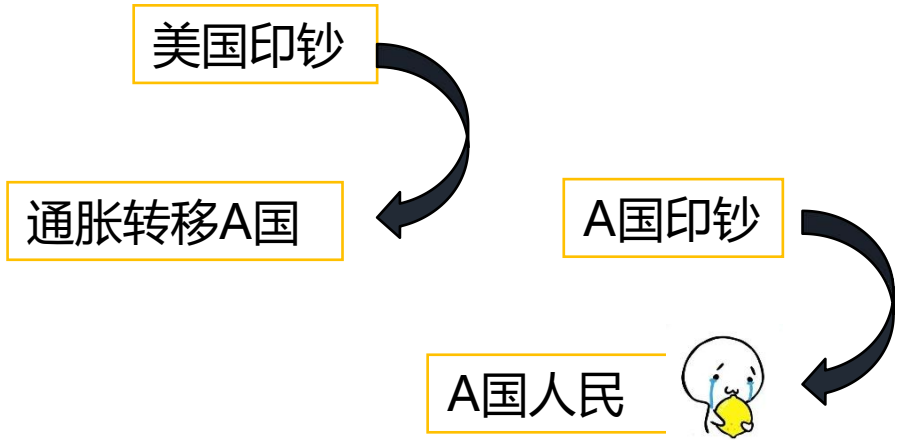
导言：区块链的起源

当前的货币体系为什么会引起人们的担忧?

因为手中的钱是**信用**，不是具有真实价值的钱

经济学：印钞能救经济，印钞能拉动需求，印钞能促进投资

量化宽松政策



市场里一共有20个苹果，5个消费者，每人有20元，市场上一共有100元，苹果5元一个。

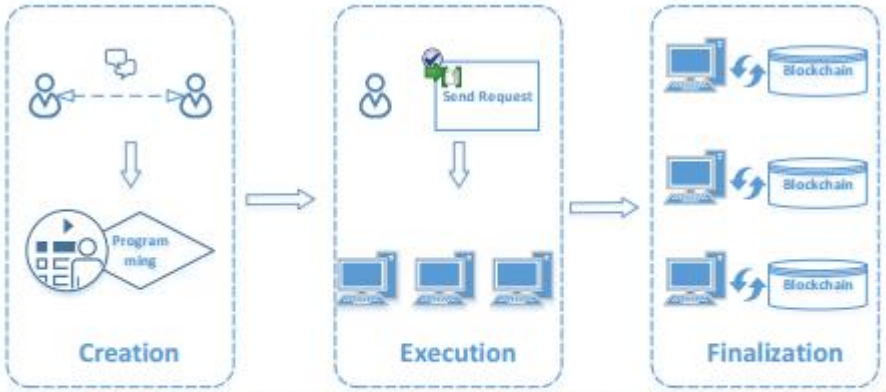
另一个人带来了100元，市场上有200元，因为苹果是唯一能买的东西，所以苹果变成了10元一个，原本手里有20元的人购买力从4个苹果变成了2个苹果。

导言：区块链的世代

Blockchain 3.0

可编程世界

Blockchain 2.0



智能合约

Blockchain 1.0

记账

导言：区块链脚本 的 演化

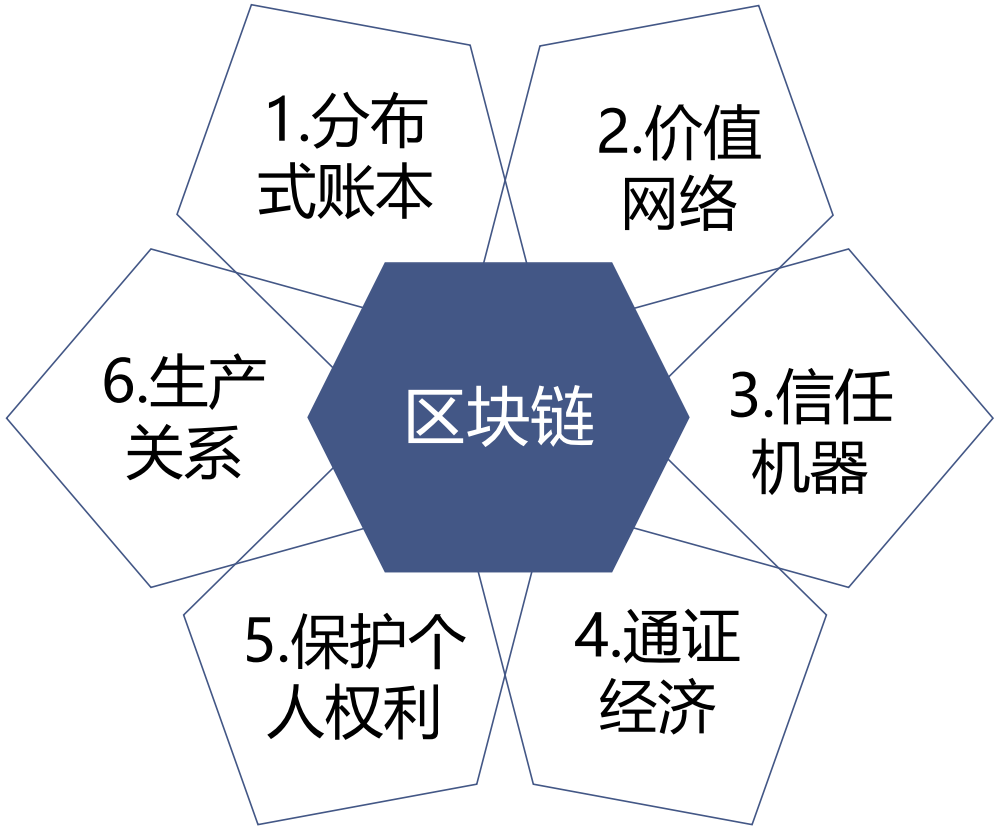
❑ 比特币 与 比特币脚本

- 缺陷：非图灵完备；
- 停机问题不可解（存在有Bug的代码逻辑，如死循环，分布式系统无法解决此问题；强制不允许循环）；
- 缺少状态（基于UTXO模型，去中心化的代价大: 全局搜索一个账户信息来确定余额）

❑ 智能合约

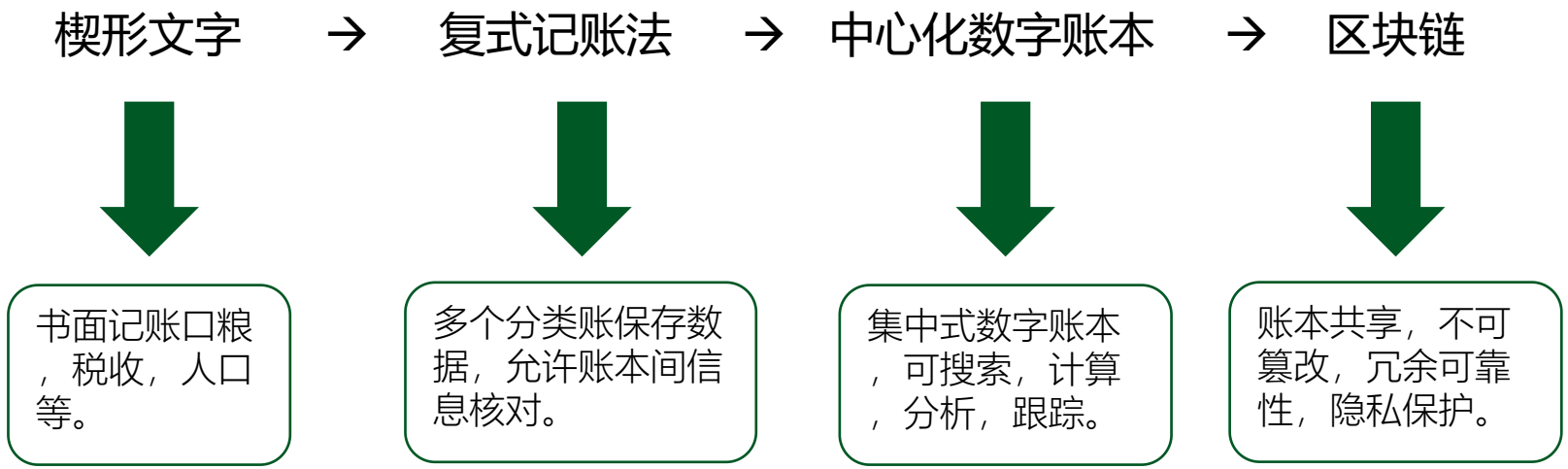
- 2015年“以太坊”提出 Smart Contract；
- 就像高级语言编写执行逻辑 —— 区块链的 Windows；
- 支持“图灵完备”的高级语言；
- 代币系统（ERC20）——支持代币生态
- 多重签名合约
- …

区块链本质 —— 6 个方面



区块链的本质 —— 2.1 分布式账本

- **账本：通过确认所有权，身份，状态，权威，映射经济和社会关系**
- **账本的演变**



- **区块链提高了记账的可靠性、准确性以及隐私性**

区块链的本质—— 2.2 价值网络

信息网络

信息可以无成本地复制

TCP/IP

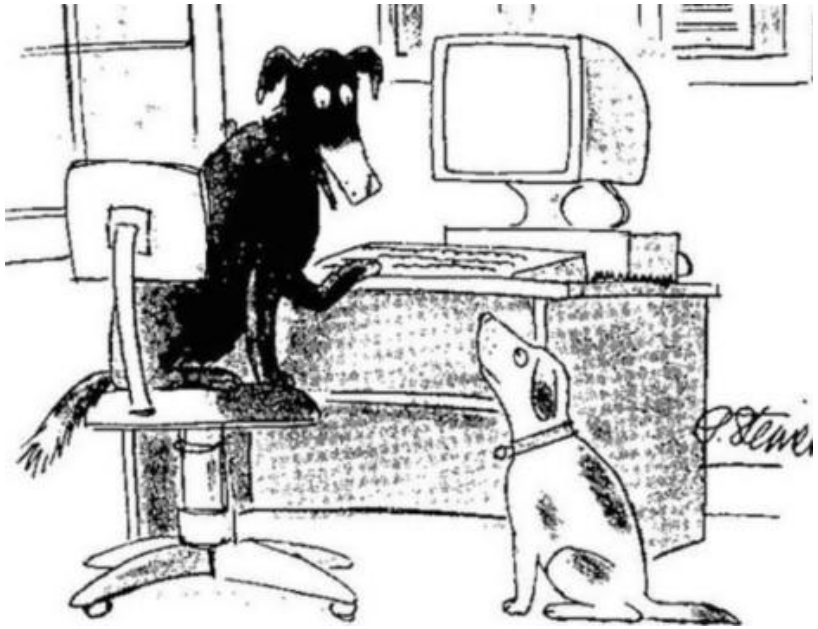
价值网络

价值只能转移，不能复制

区块链

2.3 信任机器

- 信任 是 人类协作 及 经济社会 的核心
- 在一个匿名的环境里，相信陌生人是困难的事情



"On the Internet, nobody knows you're a dog."

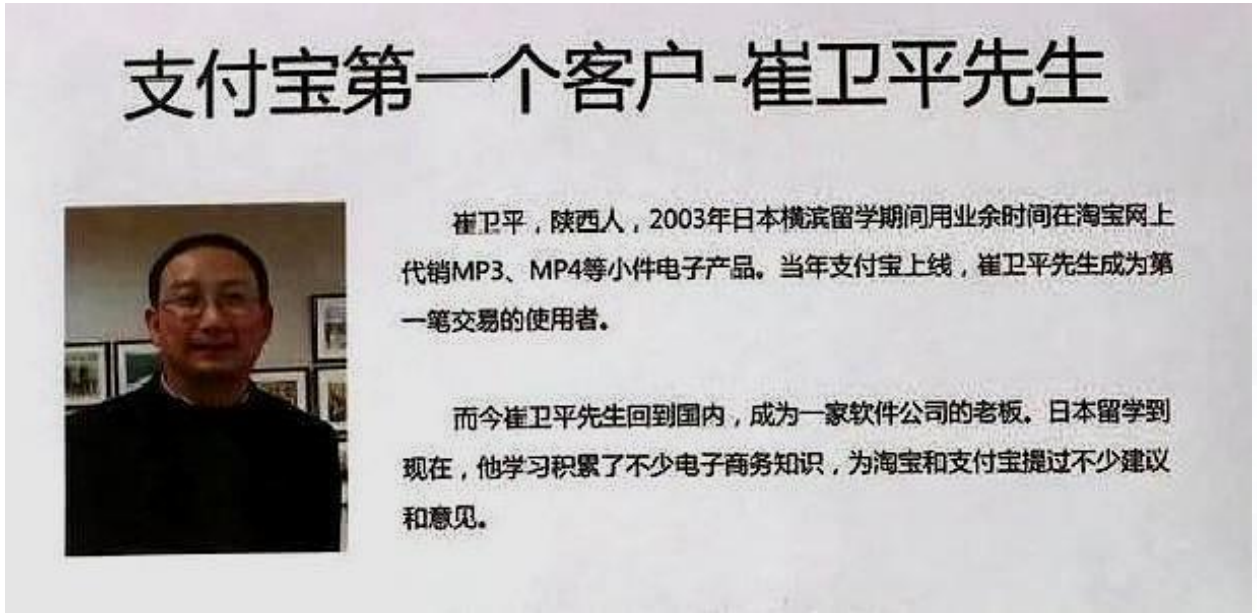
Peter Steiner 1993年发表于《纽约客》

2.3 信任机器 —— 信任与社会

- 目前，中国社会的总体信任进一步下降，已经跌破60分的信任底线。
- 人际不信任程度进一步扩大，只有不到一半的调查者认为社会上大多数人可信，
- 只有两到三成信任陌生人。

2.3 信任机器 —— “信任”的价值

- 支付宝第一个客户：日本留学生，想在淘宝上卖掉一台数码相机
- 交易号“20031012655033 6”被挂在支付宝的大楼里，马云给了1000万的花呗额度

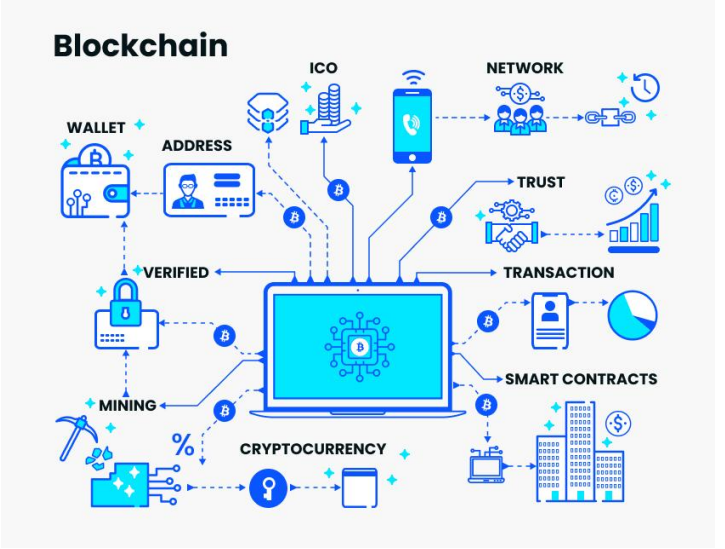


区块链的本质 —— 2.3 信任机器

- 两个陌生人要达成协作，要依靠第三方
- 传统转账，需要银行等第三方

- 信息中介/信用中介：信息不对称、交易双方无法建立信任
- 金融机构很多是提供中介服务（银行、证券交易所）

- 区块链
  - ❑一种能取代中介机构的技术协议
  - ❑一个能解决信任问题的安全可靠的网络



区块链的本质 —— 2.3 信任机器

❑ 4月19日特斯拉用户维权事件

上海车展维权女子被行拘 特斯拉称对不合理诉求不妥协

汽车　2021/4/20 08:26 发布　2021/4/20 10:28 更新

上海市公安局青浦分局通报称，消费者应以合法合理途径表达诉求维护权益

4月20日，上海警方通报特斯拉车展事件。张某因扰乱公共秩序被处以行政拘留五日，李某因扰乱公共秩序被处以行政警告。图/截自上海市公安局官方微博

【财新网】（记者 刘雨锟）上海车展特斯拉维权车主因扰乱公共秩序被处以行政拘留

11:00

当事人是2021年2月河南安阳特斯拉违章事故车主张女士。4月19日，张女士登上特斯拉展台展示车车顶，高喊“刹车失灵”对特斯拉表达不满。张女士称，当时其父驾驶特斯拉Model 3试图减速，但发现“刹车踏板僵硬，很难踩动”，而后制动失效，Model 3连撞两辆汽车，撞到水泥护栏后方才停下。

特斯拉随后给出调查结果，称当时制动系统未见异常，ABS等安全功能均处于开启状态，发生事故是因为车辆超速。双方在车辆是否超速、是否接受第三方鉴定等诸多方面各执一词。张女士从3月至今一直在维权。（详见财新网报道《女车主爬上车顶大喊刹车失灵 特斯拉称将继续沟通》）

上海市公安局青浦分局在通报中称，在上海车展现场，张某与另一名李某肆意吵闹，一度引发现场秩序混乱，张某爬上车顶还造成车辆一定程度受损。目前，张某因扰乱公共秩序被处以行政拘留五日，李某被处以行政警告。

警方还称，消费者应通过合法合理途径，表达诉求维护权益，切勿采取过激行为，否则将承担法律责任。

11:02

此次车主维权事件以消费者成功退车而告终。此事引发了汽车行业全行业讨论。多家汽车公司主动调降了退换车门槛。（详见财新网报道《西安奔驰女车主维权后续：厂家降低换车门槛》）

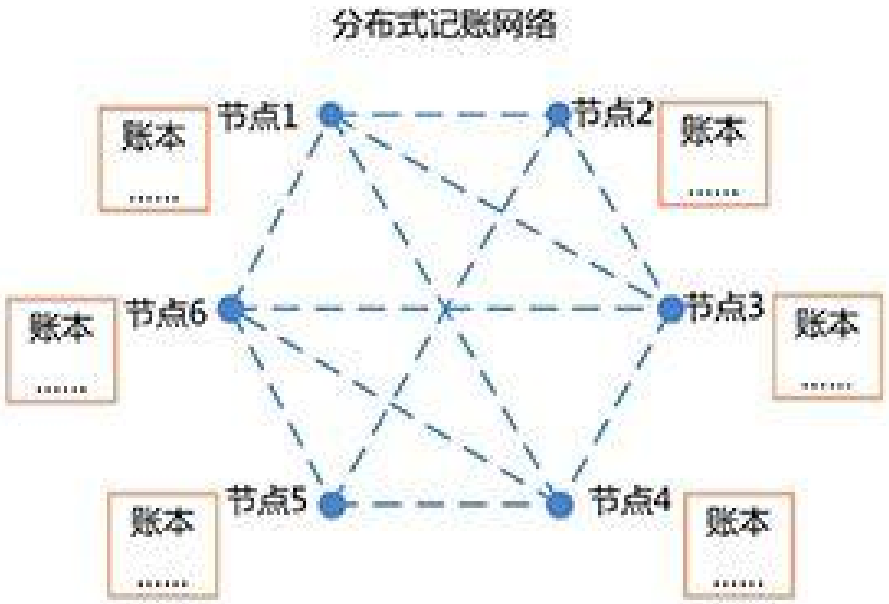
一名行业专家曾告诉财新记者，车主维权事件的根本原因是中国缺乏第三方争议处理机构，消费者遇到问题只能在汽车厂家、经销商和政府部门之间辗转，问题处理流程漫长也并不透明，容易让消费者产生愤怒情绪，进而采取极端方式维权。这名专家建议借鉴国外经验，成立第三方机构。

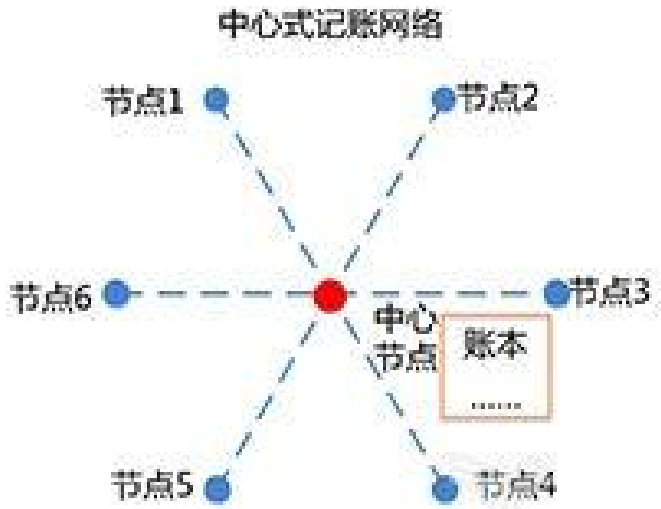
作为全球最著名的新能源车企，特斯拉频频在刹车系统或自动驾驶方面陷入争议。在事故后续调查中，特斯拉以技术精英面目给出的结论很容易造成压迫感，刺激部分车主坚持不达目的誓不罢休的强硬态度。汽车行业专业人士指出，相比技术层面的争议，在和中国车主沟通方面，特斯拉还有很多细节需要完善。■

写评论...

区块链的本质 —— 2.4 通证经济

- 基于分布式记账网络实现通证经济





区块链的本质 —— 2.4 通证经济

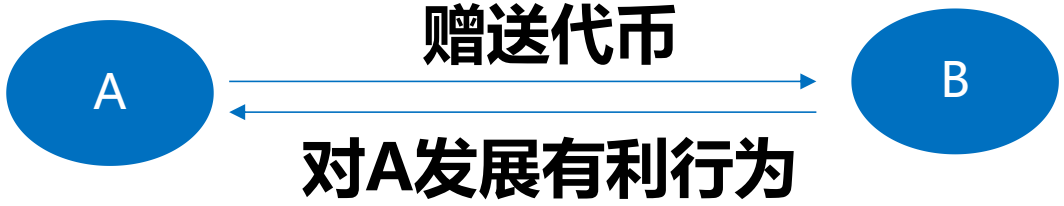
- Token (通证、代币)
  - 通过加密技术，保证 数字资产 的真实性、可流通
  - 数字权益证明 —— NFT （非同质化代币）

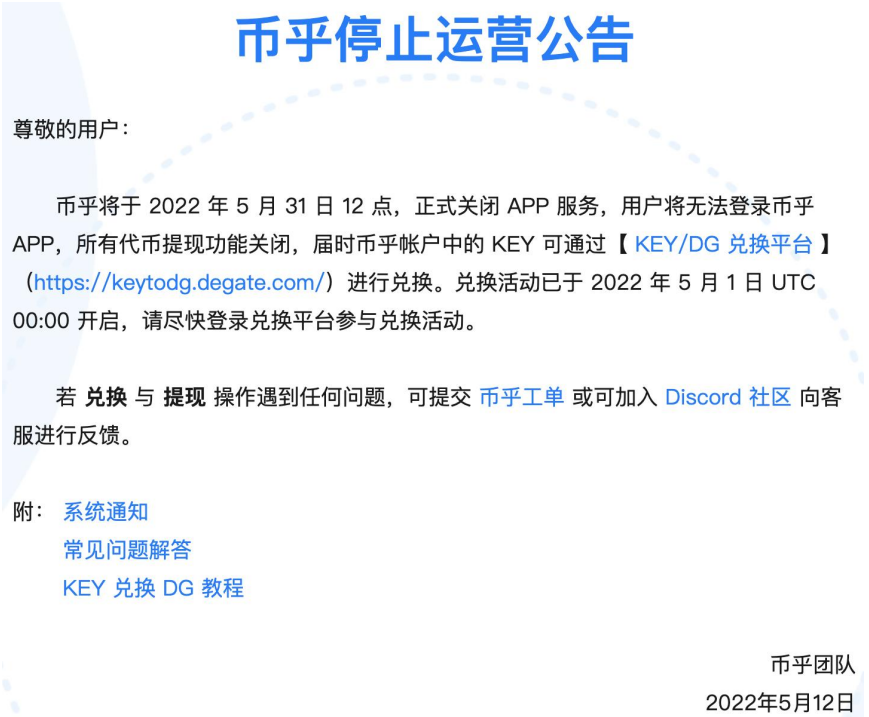
- **货币属性**：为了支付而产生的一代区块链产品，如 比特币
- **代币属性**：为了区块链生态而产生的二代区块链产品，如 NFT

区块链的本质 —— 2.4 通证经济

❑ 创新场景

- B 购买初创公司 A 的产品，获得一定代币赠送，等公司壮大，可以通过一定的利润回购这些代币
- A 发行一个产品，B 开发
- 币乎 —— “好文有好报”
  - 用户贡献文章，得到代币
  - 社区壮大，币升值，双赢





区块链的本质 —— 2.5 保护个人权利

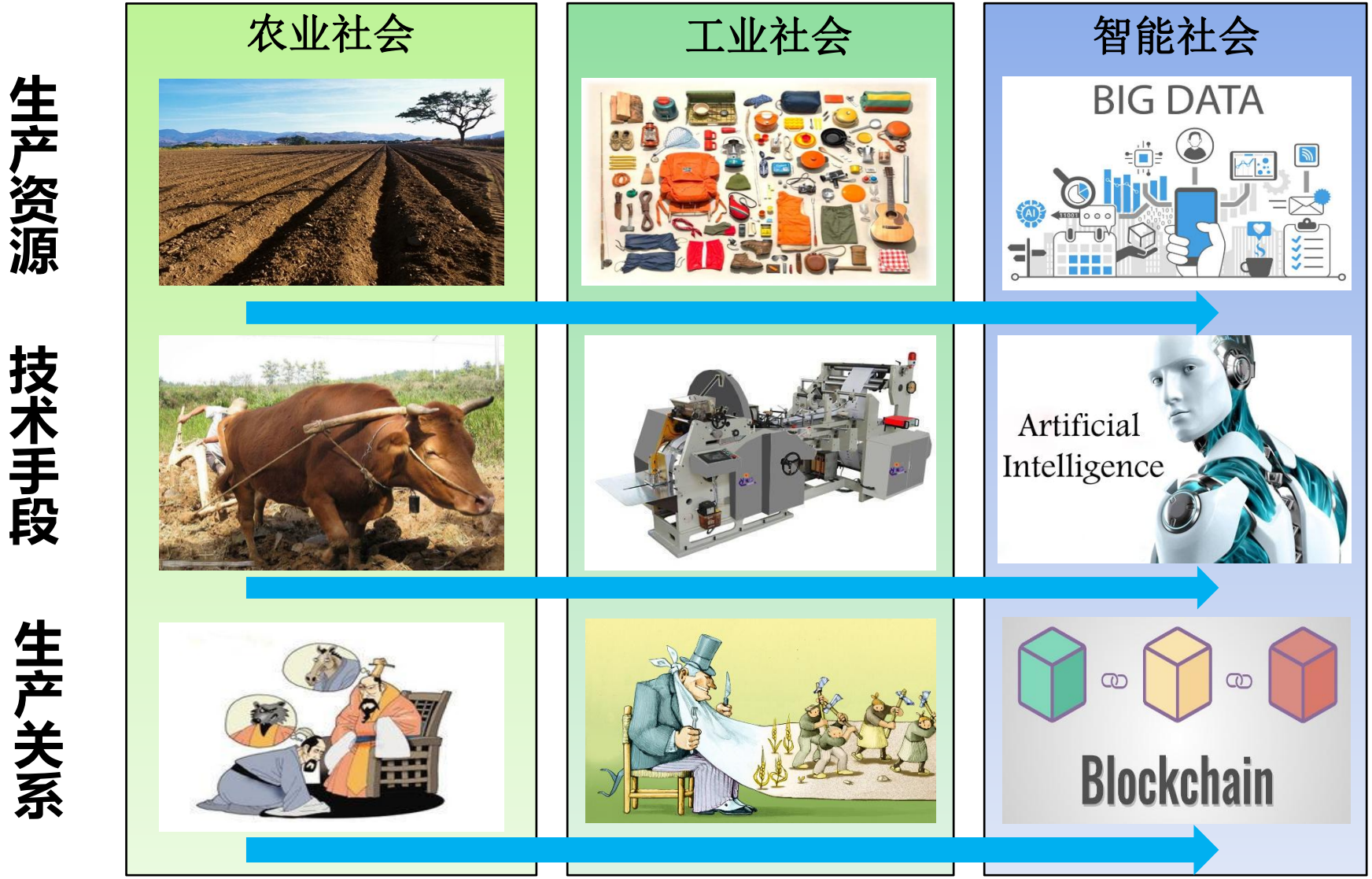
- 社会发展早期，个人力量单薄
  - 为推动社会发展，个人让渡部分权利给一个中心化体系，保证系统资源高效运转。
- 社会的进步导致个人创造的价值极大的增加
  - 而中心化体系（垄断企业）践踏个人权利，个人无法享受其创造的信息价值。
- 将来的社会
  - 通过“去中心化体系”保护个人权利
  - 使得个人享受其创造的信息价值

区块链的本质 —— 2.5 保护个人权利

- 如何保护个人权利?
  - 避免：免费用户被当作产品的一部分
  - 遏制：马太效应导致的互联网霸权
  - 防止：隐私被侵犯
  - 惩治：大公司作恶

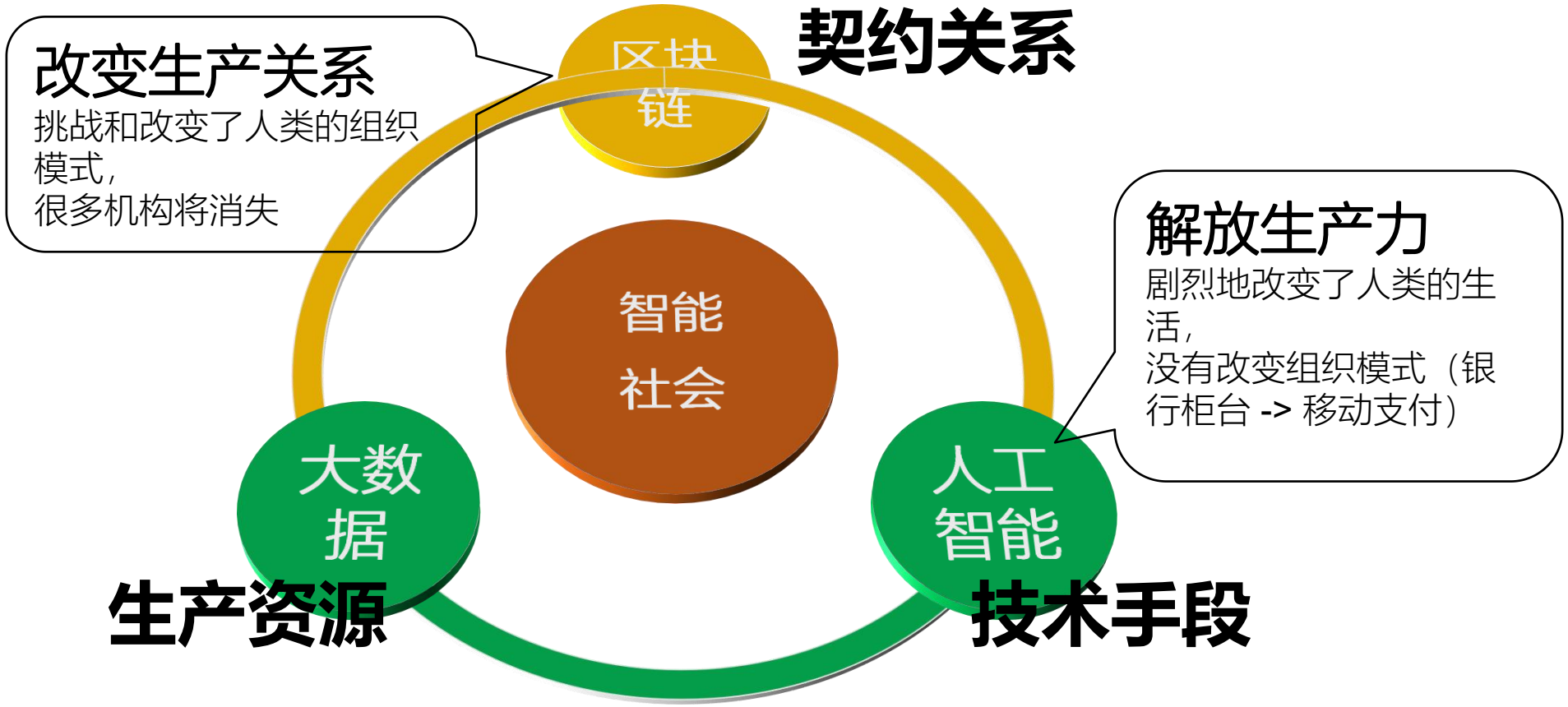
区块链提供了一个**更自由，更透明，更公平**的环境
打破**数据垄断**，实现**信息流通**与**价值共享**

区块链的本质 —— 2.6 生产关系



区块链的本质 —— 2.6 生产关系

- **“契约关系”**：对生产资料、技术手段的分配



第二部分内容的 **总结**

回答了灵魂之问2: 区块链技术会给世界带来什么的影响或改变?