1、 请分别阐述以下区块链相关概念和机制：账本、交易、挖矿、共识、智能合约。

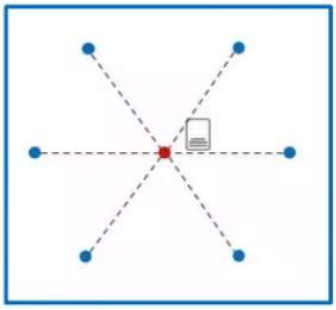
2、 请举例说明区块链在“数据追溯”方面的应用案例。

3、 请举例说明区块链在“共享经济”方面的应用案例。

注：手写拍照提交，如果提交失败或者提交超时，请将答卷命名为“专家系列讲座课程作业0326_学号_姓名”发送到邮箱425375041@qq.com。

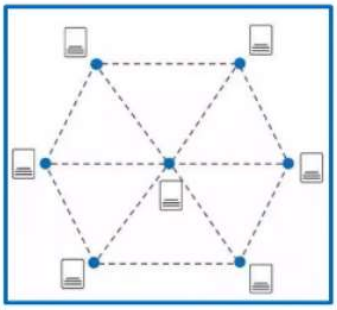
什么是“账本”

中心决定节点，节点依赖中心，节点离开了中心就无法生存



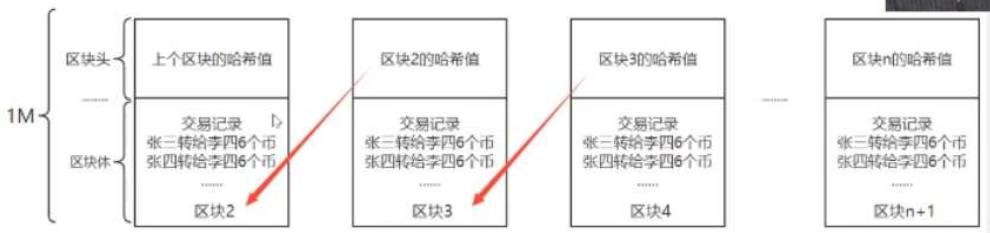
中心化账本

任何人都是一个节点，任何人也都可以成为一个中心



去中心化账本

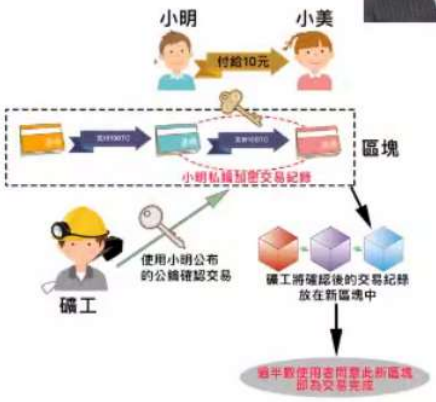
什么是“账本”



- 按区块存储交易记录，下一个区块存储上一个区块的哈希值，形成链接的关系
- 区块的大小是可变的，最大不超过1M，区块头存储挖矿需要的信息，区块体存储具体的交易数据，通过这些交易数据，能够计算出当前账本情况
- 目前已经有40万区块，需要占用至少20G磁盘空间

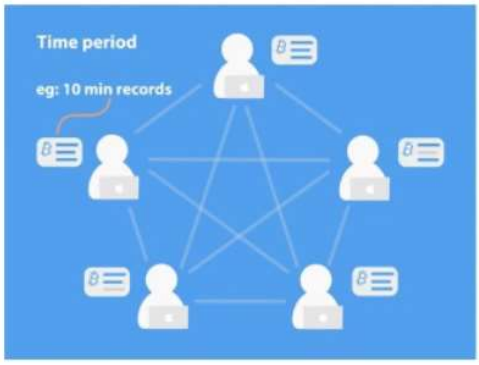
什么是“交易”

- 在现实中，今天小明要给小美10元
- 而在虚拟货币的世界，则转变成：小明的帐号（为一串英数混合的代码）支付10比特币给小美的帐号，而这条交易纪录经过小明的私钥加密后，会发送给区块链的所有人，而愿意提供计算能力的矿工会使用小明公开的公钥来解开小明私钥加密的讯息，如果解得开就代表这交易纪录是小明所发送的，确认是小明发的交易要求后，此笔交易纪录会放进预备产生的新区块中，等待过半数使用者确认小明的帐号有足够的比特币能支付，此笔交易就算完成，新的区块也会生成并接在区块链的尾端。

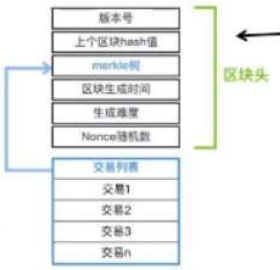


什么是“挖矿”

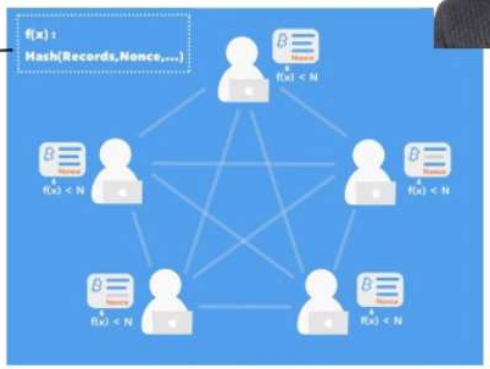
- 首先，按固定时间段划分，所有节点记录这段时间内的账本。以比特币网络为例，交易信息会通过P2P网络广播到所有在线节点，在线节点会记录十分钟左右的交易记录。
- 在线节点每十分钟打包交易信息，并需要争取记账权，争取到记账权的节点就是这次的leader，其他所有节点要以它的账为准。那么如何争取记账权？



什么是“挖矿”



区块头构成



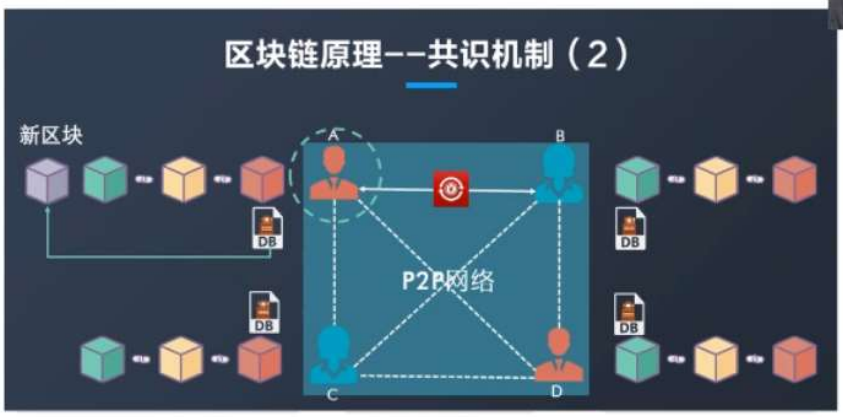
竞争记账权

在比特币里就是工作量证明（PoW算法）。工作量证明如何实施？节点都对自己的账本做哈希（Hash）计算，如果账本内容不变，每次计算出来的哈希值不变，所以需要在账本里面插入一个随机数，每次修改随机数再计算哈希值，直到计算出的哈希值小于预设的阈值。即f(x)假设为哈希计算，参数是账本和随机变量，要反复尝试出f(x)<N的随机数为止。

什么是“共识”

产生新的交易数据—>对数据进行加密和签名—>广播数据—>每个成员都拥有一份数据

什么是“共识”

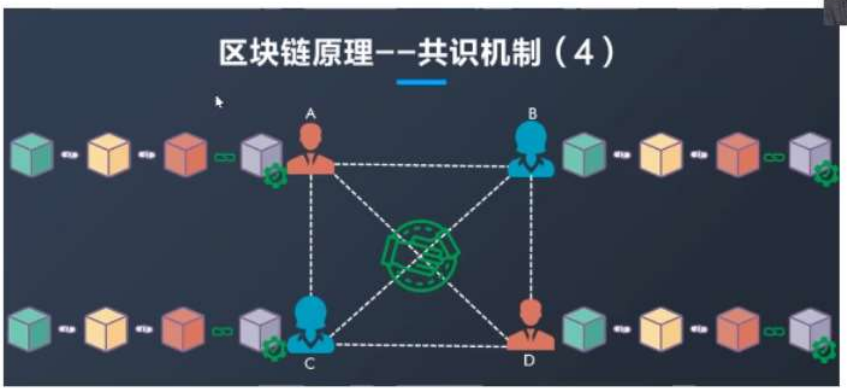


具有优先记账权的成员负责将当前系统中所有未上链的交易数据打包成数据区块

什么是“共识”

记账者将新的区块在网络中广播，每个成员对新区块的有效性进行验证，包括数据的正确性、链条的完整性

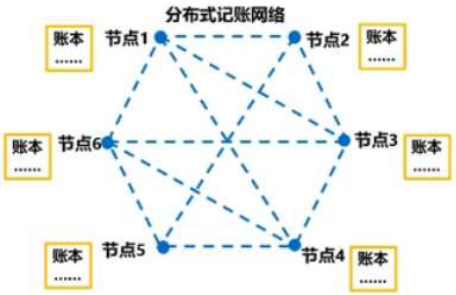
什么是“共识”



新区块验证通过结束，所有成员将同步最新的区块链来更新自己存储的账本数据

区块链简介

区块链是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术



区块链简介

A 公有区块链
网络中的节点可任意接入，网络中的数据读取权限不受限制，任何人都能参与共识过程，比特币属于典型的公有链

B 私有区块链
共识机制、验证、读取等行为被限制在一定范围内，由一个实体控制，仅对实体内部开放

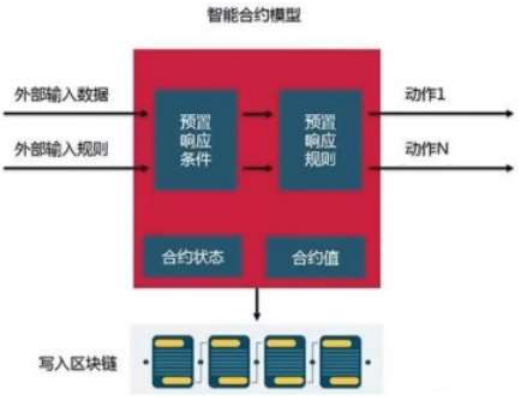
C 联盟区块链
介于公有链和私有链之间，更符合大部分行业场景，适度对外开放

什么是智能合约

定义：智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议

一般解释：智能合约实际上就是运行在以太坊网络中的一段开放源代码的程序

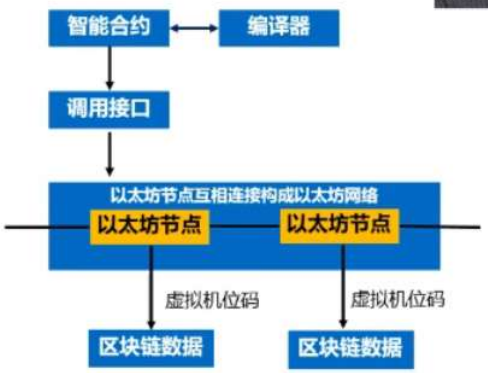
特点：满足触发条件自动执行



什么是“智能合约”

智能合约是一份可以自动执行的法律合约

智能合约的开发部署



智能合约举例

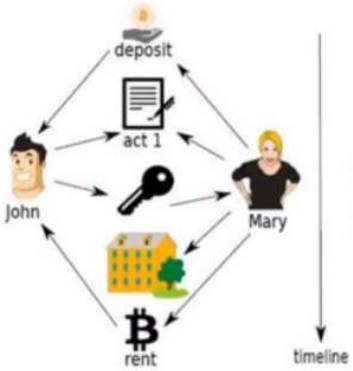
为了帮助房东甲，我们需要把合同转换成代码（智能合约）

房东甲和租客乙之间的智能合约代码：

--如果今天是30号；

--租金还未支付；

--那么从乙的账户上转账2000元到房东甲的账户上。



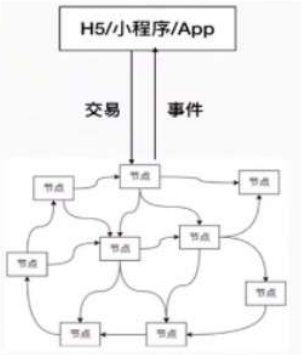
什么是DAPP

DAPP是Decentralized Application的缩写，译为**分散式**应用程序，或**去中心化**应用程序

中心化

中心化应用

去中心化



去中心化应用

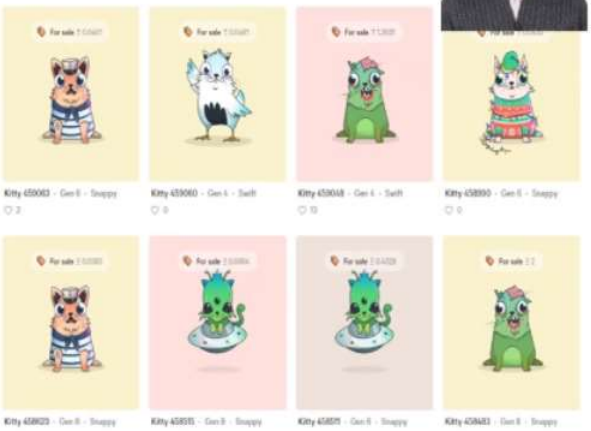
DAPP实例-TRONbet

玩法：

- 选定一个值
- 选择“博大”或“博小”
- 然后摇一个数
- 如果选择博大，摇出的数要比选定的数更大才能获胜
- 如果选择博小，摇出的数要比选定的数更小才能获胜
- 不同胜率奖励的倍率不同

DAPP实例- CryptoKitties

- CryptoKitties是基于区块链的一款电子猫咪养成游戏。
- 玩法：
  - 游戏团队早期每15分钟会在游戏里释放一款新的电子猫
  - 玩家可以从游戏团队或者其他玩家手里购买电子猫，然后进行养成，经过养成可以升值
  - 一定阶段的猫咪可以进行交配，繁殖出下一代的猫



DAPP实例- WeiFund

WeiFund 使用基于 Web 3.0 以太坊技术，采用智能合约，为用户提供众筹解决方案，通过提供每个人都可以访问的众筹实用程序来带动这些众筹平台。所有关键方面都是完全去中心化的

区块链的其他应用

区块链，可以应用到各种行业和领域

食品溯源

金融领域

数字版权

政务审计

物流行业

食品溯源

- 食品追溯链的记录主体众多
- 记录可能被篡改和伪造

食品溯源

- 将牛肉生产的所有信息写入文件，将文件的哈希值保存在区块中
- 在食用每块牛肉前，可以清楚知道这块牛肉的来源
- 区块链的信息无法篡改，保证每一条信息都是真实可靠的

物流场景

京东的物流车送完货要从乙地回甲地，此时顺丰正好有一批货要从乙地运往甲地。如果京东能够帮顺丰运回去就好了。作为回报，顺丰可以给予京东一定的运费，但是肯定比自己运的代价要小。而本来空车回去的京东也可以得到一点收益

物流场景

- 顺丰害怕京东把货物送丢了
- 京东把货物送丢了，却否认自己替顺丰送货
- 京东害怕送完货顺丰不给钱
- 京东送完货，顺丰否认让京东送货，拒绝给钱

各自不信任，结果只能是顺丰自己送货，与此同时，京东空车回去

物流场景

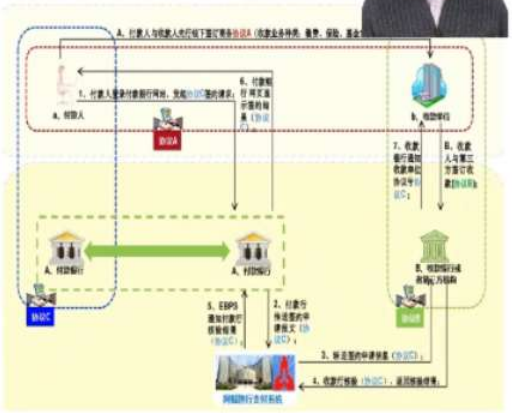
京东和顺丰制定一份智能合约：

- 如果京东安全把货送达，顺丰付给京东100元
- 如果京东2天内没有安全把货送达，京东需要赔偿顺丰200元

这样双方就都安心了

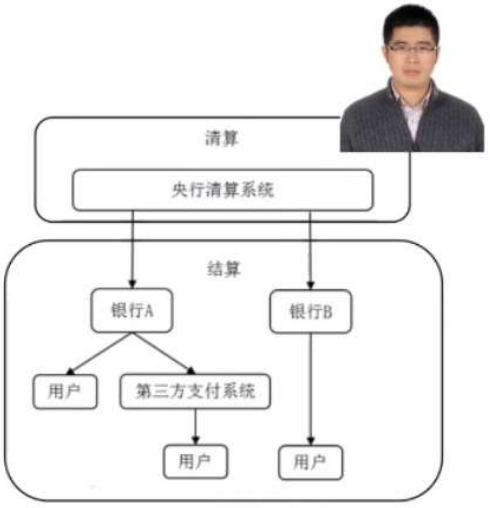
金融场景

甲做生意赚了100亿，要从工商银行转到建设银行，银行的支付清算系统处理流程繁多，处理周期长



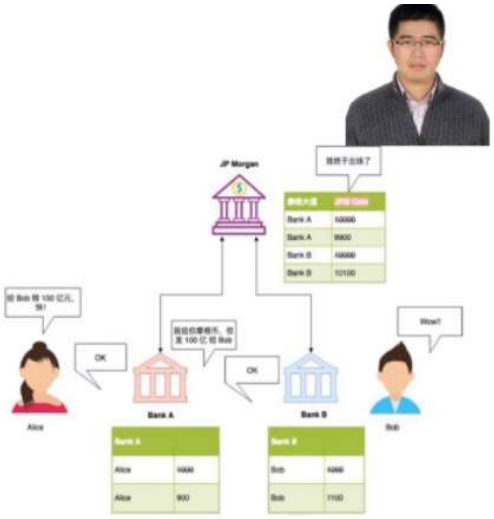
金融场景

在银行间资金转移过程中，需要依赖一个中央清算所或者关联银行。从实行到结算，支付的工作流程要花费数天，而且中间方还要收取一定费用



金融场景

- 使用区块链，交易的执行、清算和结算可以同时进行，交易完成后，自动写入分布式账本里，同时更新其他节点的账本，大幅缩短结算周期
- 结合智能合约，当交易发生时，可以准确、迅速的自动进行处理



数字版权

大年初一，春节档电影上映当天，某二手交易平台上便出现了大量“枪版”电影。三天后，清晰度更高的盗版资源开始陆续出现。春节假期尚未结束，春节档电影便集体被高清盗版资源沦陷

数字版权

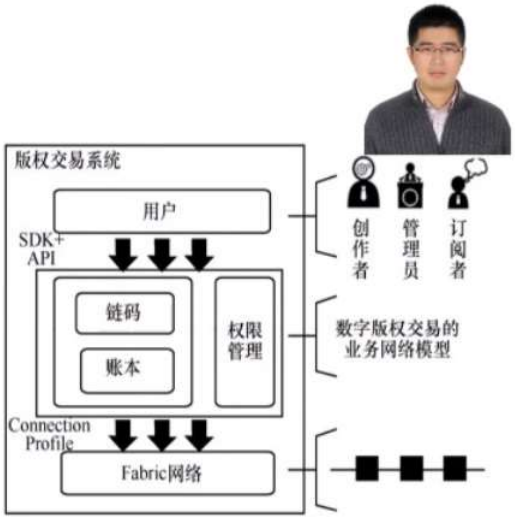
数字作品在传播过程中，容易被人复制，从而导致版权泄露，同时，很难查出泄露源头

数字版权

通过hash算法等区块链加密技术，将作品的权属信息变成唯一的、真实的且不可篡改的区块，保存在区块链中

由作品的产生开始，版权的每一次授权、转让，都能够被恒久的记录和追踪。

通过秘钥检验使用者是否被授权，没有权限则拒绝任何访问



政务审计

甲领导来到环保局要求查看A河的水质量，查看结果是水质优良。结果当天，该河流被曝光水污染严重，领导大怒

环保局：该河是由水务部门负责治理，上报结果就是质量良好

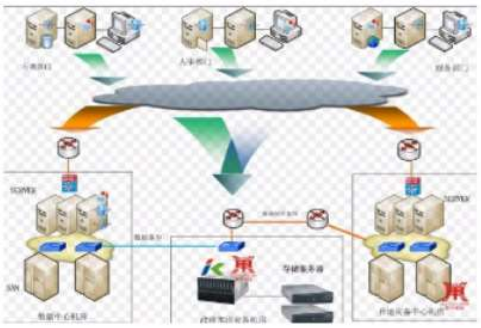
水务部门：明明上报的就是存在污染，水务局的记录就是存在污染

经过长时间的数据收集和查证，发现环保局有人偷偷改了记录

政务审计

不同部门之间的数据库不共享，在数据传递过程中可能被篡改

一旦出现问题，查证需要耗费较多时间



政务审计

- 区块链以时间戳的形式在特定时间点固化凭证，在确保信息真实、完整方面能节省大量的工作资源
- 智能合约能自动化执行部分审计流程，提高审计工作效率

大数据简介

数据是数字经济的核心要素

习近平总书记：实施国家大数据战略加快建设数字中国

- 保障一：要推动大数据技术产业创新发展
- 步骤三：构建以数据为关键要素的数字经济
- 步骤一：运用大数据提升国家治理现代化水平
- 步骤二：运用大数据促进保障和改善民生
- 保障二：要切实保障国家数据安全
- 保障三：善于获取数据、分析数据、运用数据，是领导干部做好工作的基本功

李克强总理：

- “力争让群众企业办事像‘网购’一样方便”
- “要通过政务信息系统整合共享，打通‘放管服’改革的‘经脉’，让‘放管服’改革插上新的翅膀”
- “各地区各部门一定要明确，政务数据服务是政府应该提供的公共服务”
- “只要不涉及国家安全等数据，该向社会提供的就要提供”

“区块链 + 大数据”的典型案例

数瑞产品体系

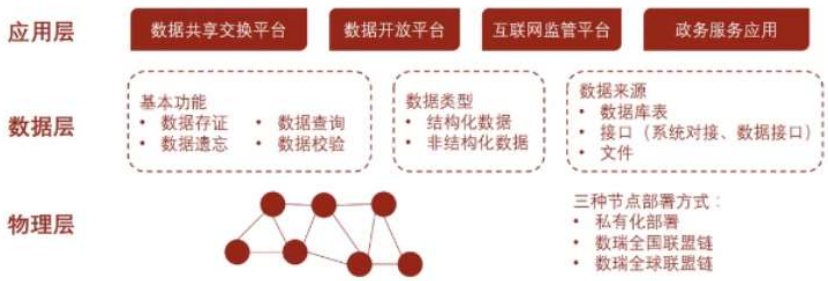
可信图式账本　　可信合约引擎　　可信数据管道

支持多种编程语言，所有产品均可独立与已有数据平台灵活集成，优化已有的应用和平台

“区块链 + 大数据”的典型案例

案例：数据可信存证平台

- 数据留存：蓝光存储低成本留存数据快照
- 过程留痕：线上合约过程留痕不可篡改防抵赖
- 数据溯源：数据、系统、业务审计监管
- 数据校验：数据唯一性查询，助力地方数字经济发展



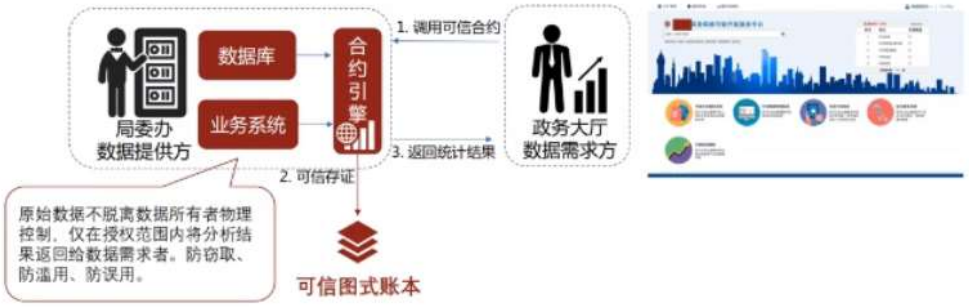
“区块链 + 大数据”的典型案例

案例：政务数据可信开放服务平台试点

应用场景：数瑞+数据开放=可信数据开放

数据失控痛点

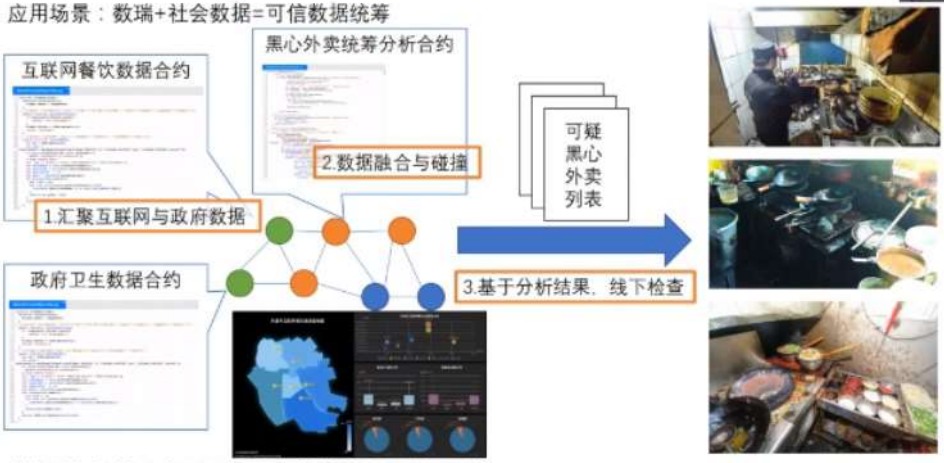
- 数据使用方式与申请理由不一致
- 数据与其他数据碰撞
- 数据留存、修改后对外发布不正确的数据
- 数据转手给其他第三方
- ……



“区块链 + 大数据”的典型案例

案例：社会数据统筹可信开放应用示范

应用场景：数瑞+社会数据=可信数据统筹

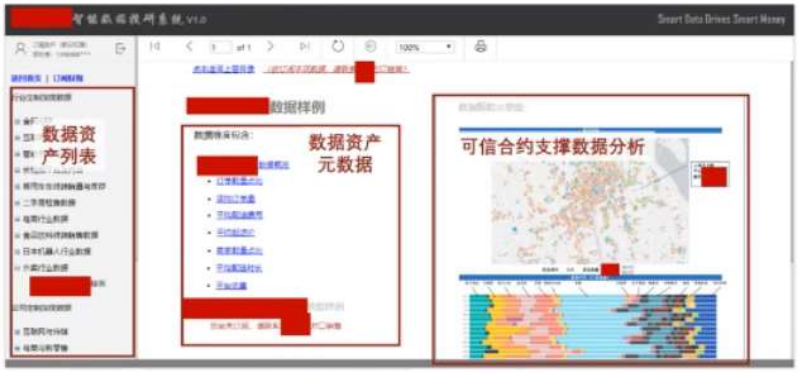


某市网信办试点→基于互联网与政府数据实现互联网+监管

“区块链 + 大数据”的典型案例

案例：上海某金融公司智能数据投研系统

应用场景：数瑞+数据交易=可信资产交易平台



数瑞支撑某公司数据资产可信流通平台

“区块链 + 大数据”的典型案例

案例：阳光面试（音视频实时防篡改系统）

应用场景：数瑞+海量非结构化数据存证

物联网简介

物联网智能服务与生态：大量、复杂、异构的物联网基础设施相互协同，构成海量、智能、集成的物联网应用

设备开放共享的问题

问题一：设备互操作问题

技术互操作
支持常见机器间通信的硬件/软件组件、系统和平台

语义互操作
两个或多个系统或组成部分之间交换信息以及对已经交换的信息加以使用的能力

语法互操作
通过通信协议传输的信息需要有明确定义的语法和数据格式

问题二：设备可信问题

调用的信息正确性
保证被调用的信息与原先要求的是一样的

自身信息安全性
保证自己的信息不会被他人任意调用、窃取

问题三：责权效问题

定责
提供方、流转方、使用方共同定责

定权
明晰数据所有权归属、共同管理权、有限使用权

定效
确定在流程中哪些设备发挥了效用

区块链+物联网

随着区块链在物联网应用的发展，更多是使用在"共享经济"方面上，使得更多闲置的物品和设备能够被有效的利用起来

P2P电力交易微网

电动车点对点充电项目

电子钱包

P2P充电网络

余电上网交易系统

"区块链 + 物联网" 的典型案例

区块链在电能交易方面

纽约布鲁克林的LO3 Energy公司搭建居民P2P电力交易微网

澳大利亚的Power Ledger公司构建太阳能发电余电上网交易系统

"区块链 + 物联网" 的典型案例

区块链在便利电动汽车充电与共享方面

德国能源巨头Innogy和物联网平台企业Slock.it合作推出基于区块链的电动车点对点充电项目

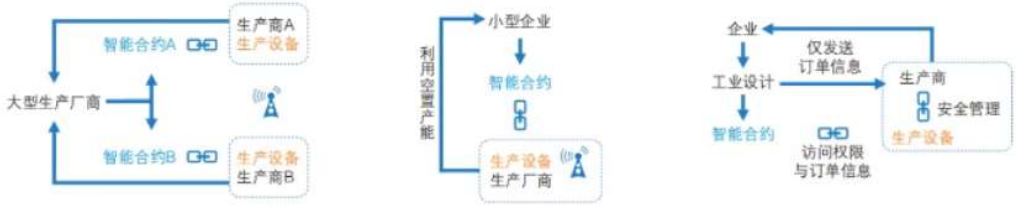
意大利能源集团Enel X旗下eMotorWerks发布了基于区块链技术的P2P充电网络

瑞士银行、德国电力公司莱茵集团与汽车技术公司采埃孚合作，为电动汽车创造区块链电子钱包

“区块链 + 物联网”的典型案例

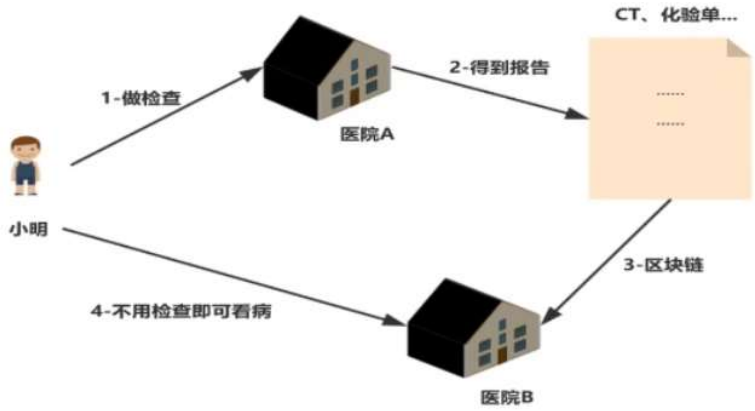
区块链在智能制造方面

供应链多方协作　　产能共享　　设备安全管理



“区块链 + 物联网”的典型案例

区块链在医疗方面



“区块链 + 物联网”的典型案例

区块链在租房方面

传统租房

虚假信息

纸质合同

通过查询历史记录，更好的了解房屋的信息，从而避免虚假房源，网络信息与实物不符的情况

纸质合同转为智能合约，能够自动执行条款，避免出现赖账，扣押金等问题

引入区块链的租房

历史记录

租房合同

信息上链