




人工智能通识教程

（农林院校版）


<https://ai4ag.github.io>





第六章

区块链：云中锦书



引子

“云中谁寄锦书来？雁字回时，月满西楼。”

——李清照《一剪梅》



- 海量农业数据如鸿雁往返，连接着农业生产、管理和流通的每个环节，其数据流通中的安全性、真实性和信任问题则亟待可靠的技术保障。
- 区块链技术以其去中心化、防篡改、可追溯的特性，为农业数据的安全流通、可信共享提供了新的解决之道，推动了农业产业链各主体之间的信任构建与高效协作。

视频引入

插入一段区块链应用视频，如农产品溯源

区块链的起源——传统交易模式



集中化风险

增加成本
效率低

不总可靠

区块链的起源——传统交易模式



当心黄焖鸡米饭的鸡肉来自黑作坊

除了环境脏乱差,无证加工点最大风险是食品原料来源不明

昨天

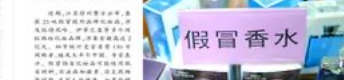


食药安全

食药安全

23吨冒牌化妆品被130万人买走了

化妆品网兜水深,假化妆品不可放心用



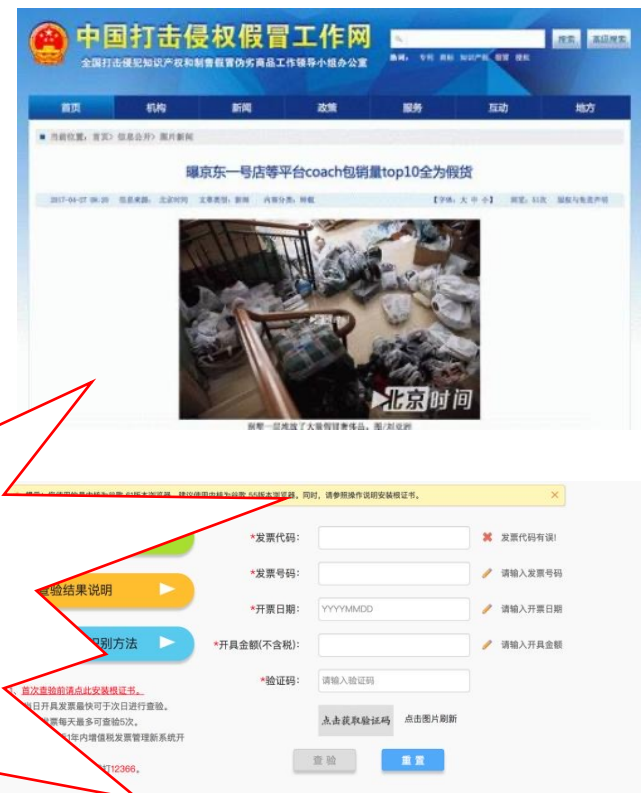
假冒香水



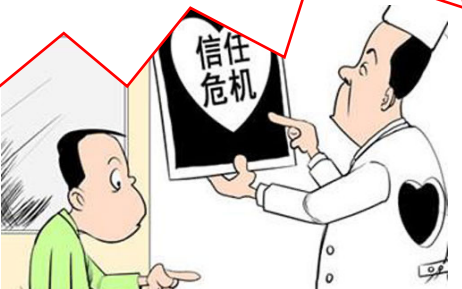
总局公布10起食品保健食品欺诈和虚假宣传典型案例



顾客京东上网购白酒被鉴定为假货 商家拒绝提供进货



信任问题成为当前各领域发展主要障碍之一



如何解决信任问题?

区块链的起源——比特币



Bitcoin: A Peer-to-Peer Electronic Cash System

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

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.

Commerce on the Internet has come to rely almost exclusively on **financial institutions** serving as **trusted third parties** to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the **trust based model**.

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitco.in/pdf/bitcoin.pdf>

区块链的起源——比特币

- 在创世区块中，“中本聪”植入了一段文字：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” (2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘)。这是英国泰晤士报当天的头条新闻标题，既证明区块的创建时间为18:15:05 GMT，也代表了对中心化金融系统的暗讽。



区块链的起源——比特币

01

匿名

“中本聪”发布
比特币白皮书，上
世

2008年11月



比特币系统正式上线并挖
出了第一个区块即创
世区块

2010年5月

第一个比特币Slush出现，
集合多节点合作挖矿，
并挖出了首个区块

2012年11月

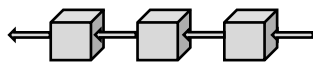
4

激励

2140年后

比特币发行完毕，之后的
挖矿不再包含比特币
奖励

区块链的定义



狭义：按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。



广义：利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

——2016年《中国区块链技术和应用发展白皮书》

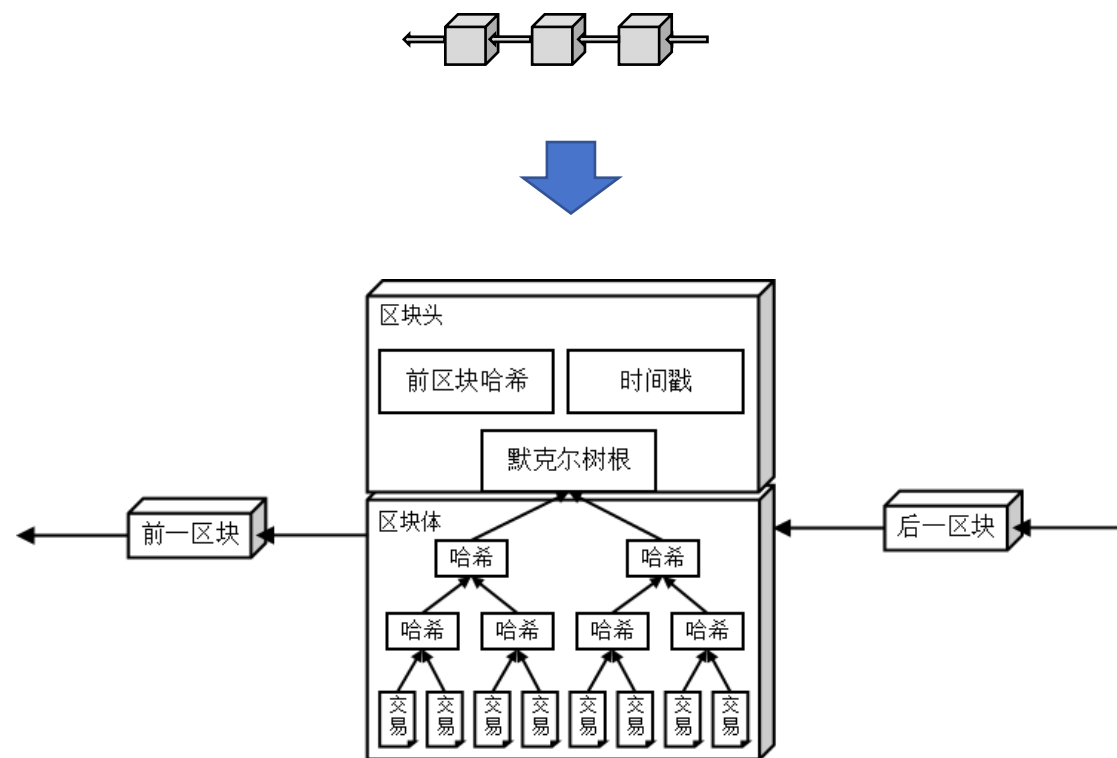
区块链的定义

狭义：按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

链式数据结构：

待美化

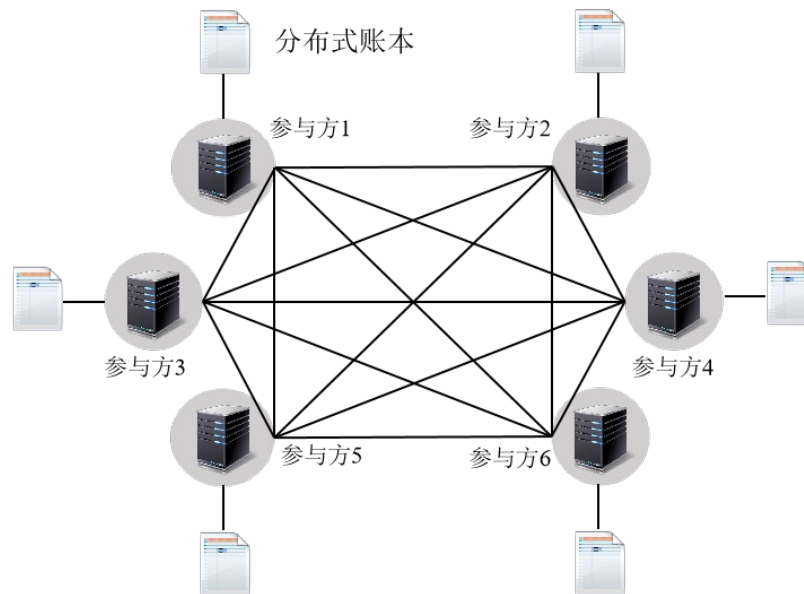
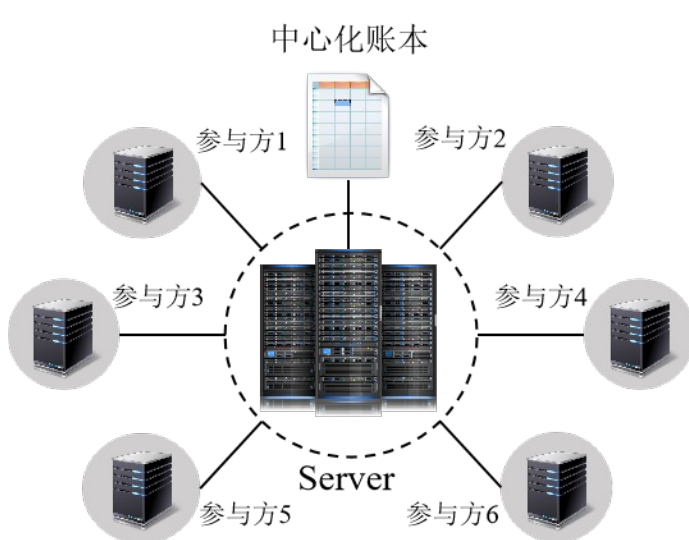
- 区块头：关键信息集合
- 类似协议报文头部，一般是固定长度，不同的区块链结构可以设计不同头部。一般包含区块相关重要字段，如前区块哈希（Previous Hash）、时间戳（Time Stamp）和默克尔树（Merkle Tree）的根。
- 区块体：交易数据存储
- 区块体是验证过的交易，以密码学中的一种著名工具——默克尔树（Merkle Tree）的形式打包起来，其



区块链的定义

狭义：按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

分布式账本——分布式记账方式由所有参与方共同记录和更新账本，每个参与方都存储完整账本数据的副本。



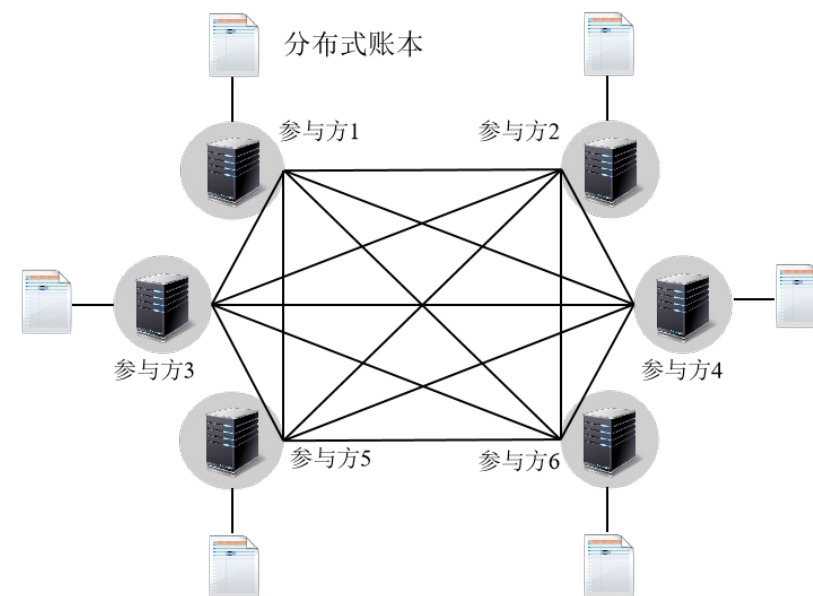
区块链的定义

狭义：按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

分布式账本工作机制：

待美化

- 多副本存储：分布式记账方式由所有参与方共同记录和更新账本，每个参与方都存储完整账本数据的副本。
- 共识机制：通过共识算法确保所有节点对账本状态达成一致，避免数据不一致。
- 数据可信度保障：任一参与方持有的账本数据副本与其他参与方的不一致，不会导致账本的变动，除非大部分参与方同意变动内容才有可能实现对账本的修改，因此能够保



区块链的定义

广义：利用**块链式数据结构**来验证与存储数据、利用**分布式节点共识算法**来生成和更新数据、利用**密码学**的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的**智能合约**来编程和操作数据的一种全新的分布式基础架构与计算范式。



自由讨论

待美化

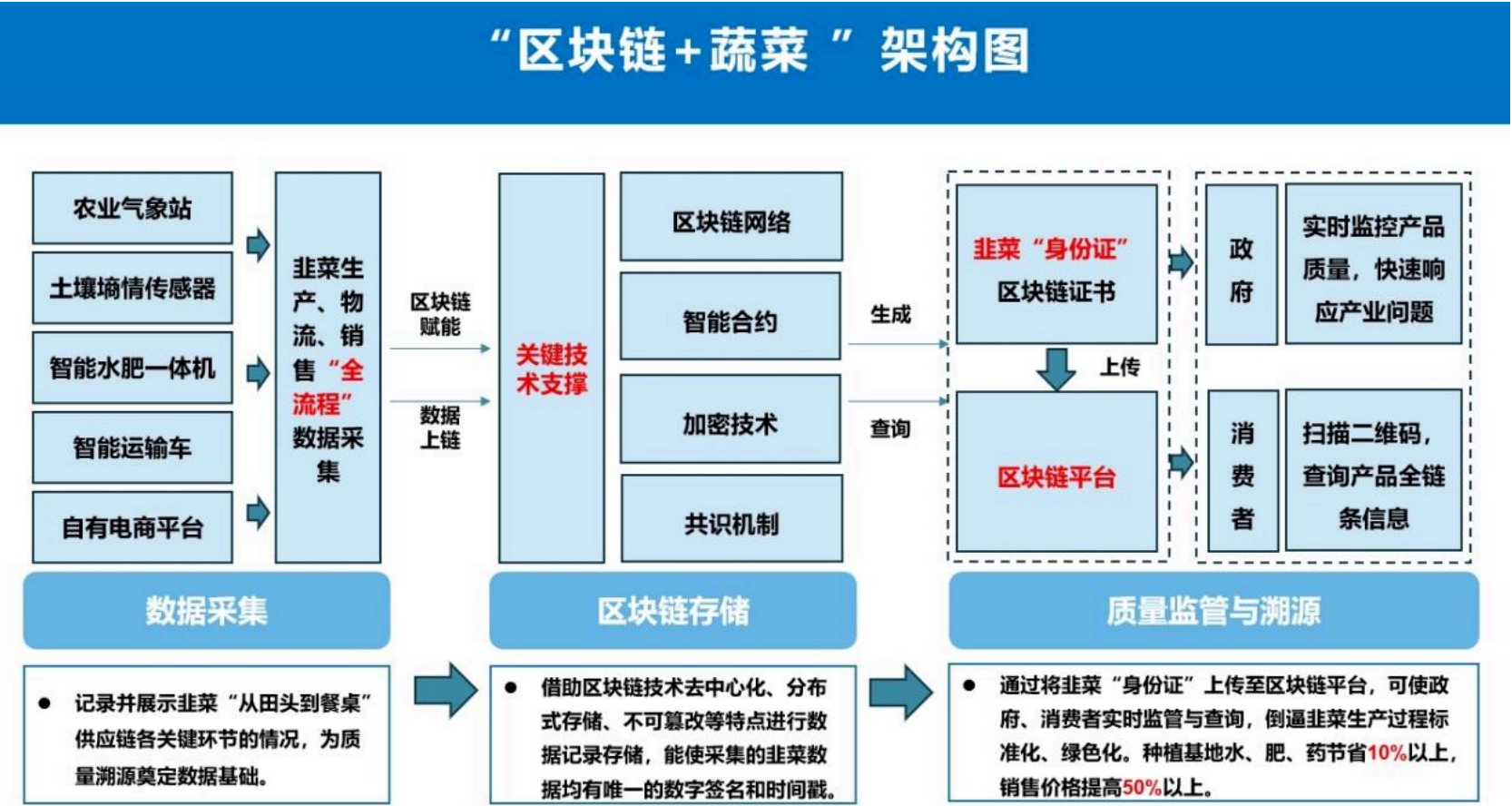
- 区块链农产品溯源应用中，农产品相关数据到底放在了哪里？

链上数据：关键溯源信息（如产地、质检结果、交易记录）存储在区块链上，确保不可篡改

链下存储：大量媒体文件（图片、视频）存储在分布式存储系统，链上仅存储哈希值

混合式架构：合链上+链下的混合存储方式，平衡数据安全性与存储成本

讨论要点：如何平衡数据透明度与隐私保护？哪些信息适合放在链上，哪些适合放在链下？



课间思政时间

- 播放思政视频

区块链的技术特性

待美化，分五页

去中心化

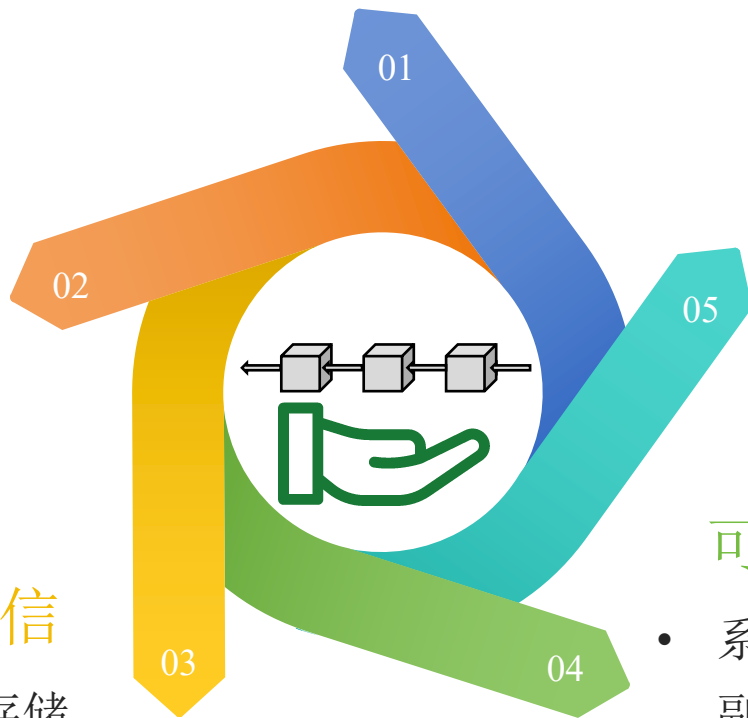
- 区块链网络采用无中心或弱中心的分布式架构,任何一个节点都拥有一份完整的区块链账本,并共同承担维护网络和账本数据的责任。

可追溯性

- 通过区块链网络的块链式结构可以有效追溯任意一笔交易从当前状态到起源处的流转情况。

数据可信

- 区块链分布式账本由全网节点共同存储和维护,使用多种技术保证了区块链中数据的难以篡改、可追溯和不可否认。



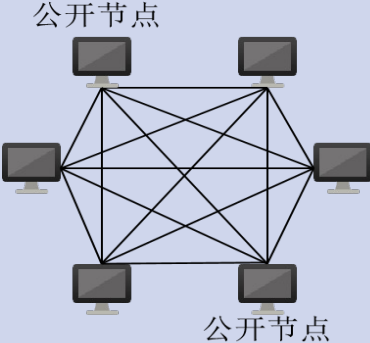
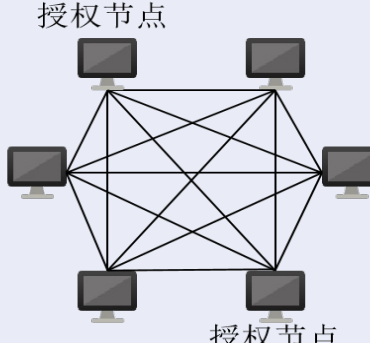
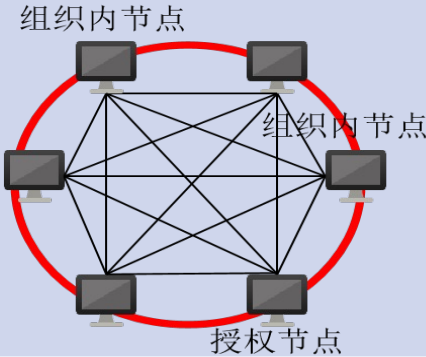
透明性

- 区块链网络中的交易规则由所有节点认可、公开透明并共同维护,按照既定规则对交易合法性进行验证并打包上链。

可靠性

- 系统中每个节点都拥有账本副本,以所有副本的一致性可保证数据的可信。
- 分布式网络本身的鲁棒性保证了网络仍然能够保持正常运行和数据的可信可用。

区块链的部署分类

开放程度 ↑ 开放	比较	结构示意图	参与者	中心化程度	代表
	公有链		任何人	完全去中心化	比特币 以太坊
	联盟链		多机构	弱中心化	HyperLedger FISCO BCOS
	私有链		机构内	(弱) 中心化	企业内部私链

区块链的部署分类

待美化

比较	结构示意图	参与者	中心化程度	代表
公有链		任何人	完全去中心化	比特币 以太坊

- **随进随出：**任何人都可以随时加入公有链中进行读取交易、发起交易和参与共识等，也可以随时退出区块链网络。
- **完全去中心化：**公有链中的所有节点具有完全对等的地位和权利，不存在特殊权限的节点，形成完全对等的分布式网络。
- **交易匿名：**节点加入网络时使用密码学算法生成账户地址，无需与现实世界中的真实身份相关联，因此节点可以任意进入网络，不需要进行任何约束和证明，与其他类型区块链相比，用户具有较强的匿名性。
- **使用激励机制：**为了实现更高的去中心化程度，公有链鼓励所有节点参与维护账本，而对负责打包区块的节点进行奖励有利于更多的节点参与共识。

公有链的去中心化程度最高，主要用于密码货币领域，典型代表是比特币和以太坊等，其他密码货币也基本上以比特币为基础进行设计和运行。

区块链的部署分类

比较	结构示意图	参与者	中心化程度	代表
联盟链		多机构	弱中心化	HyperLedger FISCO BCOS

- **身份认证：**联盟链一般需要对加入的成员进行身份认证，经过认证的节点才能加入，发起交易、参与记账等功能都需要经过授权才能进行；由于联盟链一般使用于机构间，因此节点通常属于某个机构，而参与维护的机构可以拥有多个节点。
- **多中心化：**由于设置了身份认证机制，参与共识的节点规模与公有链相比来说较小，因此联盟链的去中心化程度与公有链相比较弱
- **数据保护：**链上数据的访问开放程度也是可选的，即可以完全开放访问也可以限定在联盟机构内部开放访问；不同的联盟链还会提供一定的数据保护机制，如超级账本 Hyperledger Fabric 中的通道机制等。
- **激励机制可选：**与公有链相比，联盟链的重点在于打通并记录机构间的业务流，因此参与共识并维护账本的节点一般是指定的，激励机制是可选的，并不影响共识。
- **交易吞吐量较高：**公有链相比省去了确认记账权的时间，且联盟链相对于公有链来说规模较小，因此交易吞吐量较高。

联盟链拥有更高通量、更灵活和更可控的特点，成为企业应用的主流选择，尤其是在企业间需要解决信任问题的场景中，如农产品溯源链、政务联盟链等。

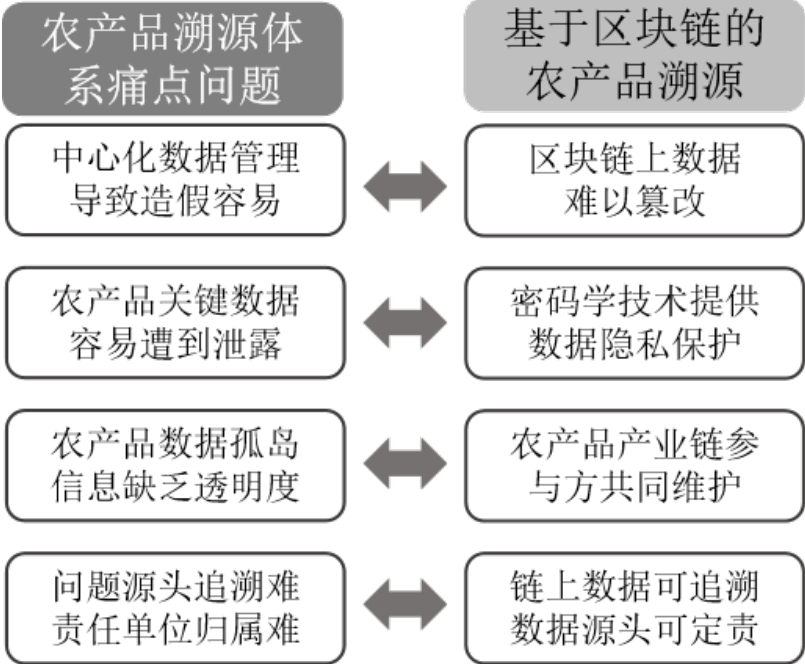
区块链的部署分类

待美化

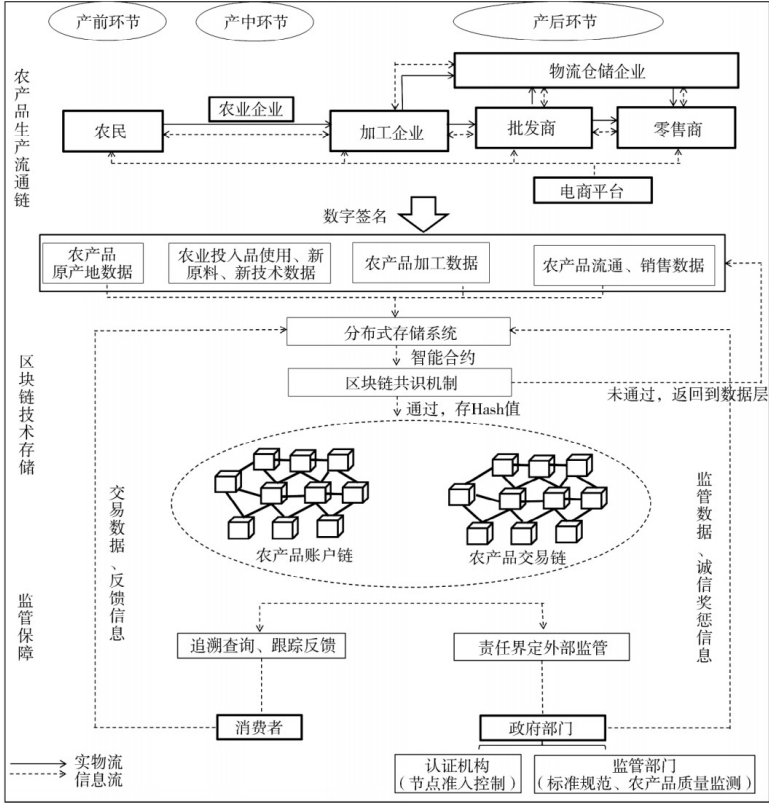
比较	结构示意图	参与者	中心化程度	代表
私有链		机构内	(弱) 中心化	企业内部私链

- 不对外开放：私有链是一种不对外开放的区块链，仅限机构内部成员访问和使用
 - 内部审核机制：节点的进出、交易和共识等权限都在某个机构内部进行审核，属于某个机构内部的区块链。非机构成员不允许加入私有链（除非经过特殊授权），
 - 部门角色参与：机构成员以不同的部门角色加入私有链中对其进行共同维护。
- 私有链解决的是机构内各部门间的信任问题，其目的和运行机制与联盟链类似，主要用于机构内部的数据管理和数据审计等场景。

案例分析——农产品溯源



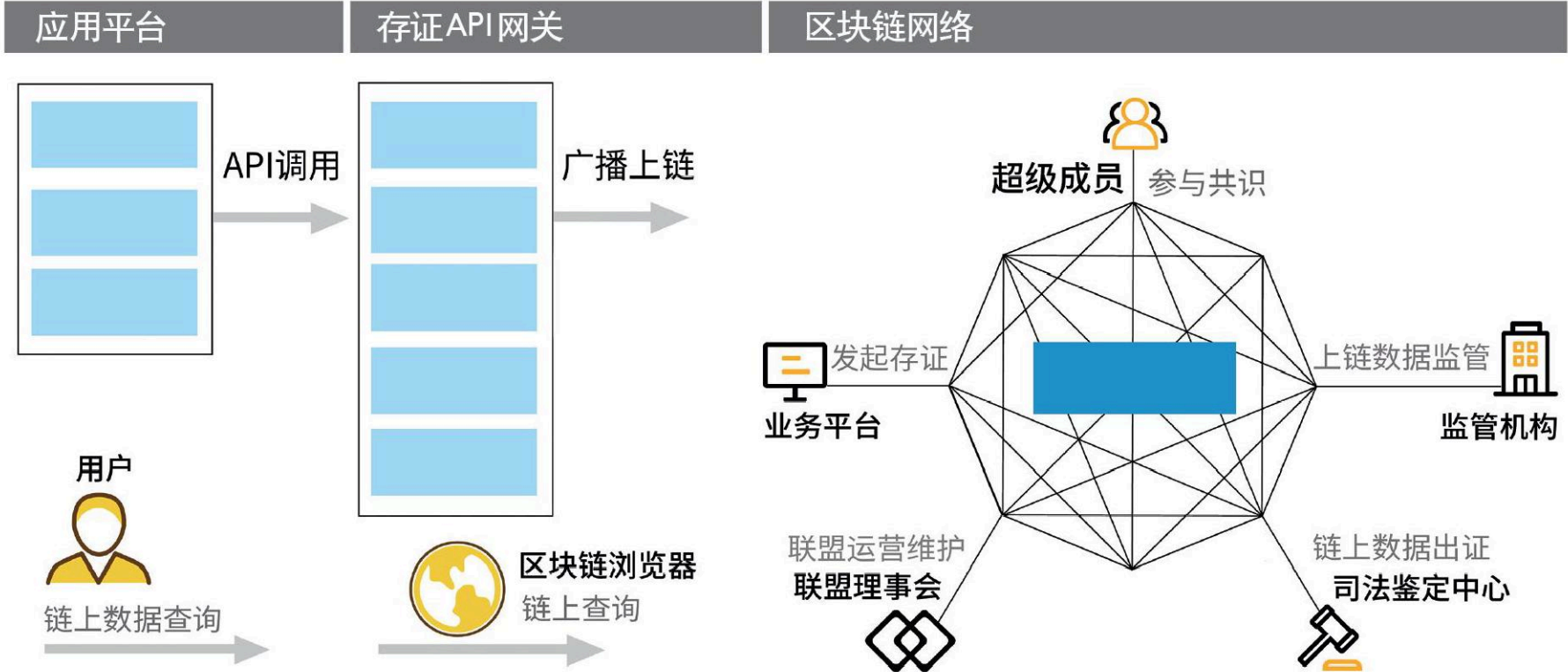
待美化



案例分析——司法存证

找一段司法存证的视频

基于区块链的电子证据司法存证示意图



来源：法大大

开放讨论

待美化

1、文学与艺术领域

NFT 让数字文学作品、艺术创作成为可交易的“唯一资产”，这是否会重塑文学艺术的创作动机？例如，创作者是否会更倾向于生产“适合上链交易”的内容，而非纯粹表达思想情感？

区块链的“时间戳”功能可记录文学作品的创作时间与版本迭代，能否有效解决“抄袭争议”？

2、法学领域

区块链存证（如电子合同、版权证明）已被部分法院认可，这是否会推动法律证据体系从“纸质优先”向“数字优先”转型？

课堂总结

核心概念

链式数据结构：区块按时间顺序相连，形成不可篡改的记录

分布式账本：所有节点共同维护账本，无需中心机构

共识机制：确保全网节点对数据状态达成一致

智能合约：自动执行的程序，实现业务逻辑

待美化

技术特性

去中心化：无中心或弱中心架构，节点地位平等

数据可信：密码学保障，难以篡改和伪造

可靠性：多副本存储，系统鲁棒性强

可追溯性：块链式结构，完整记录流转过程

应用场景

农产品溯源：全生命周期可追溯

司法存证：电子证据不可篡改

金融支付：去中心化价值传递

供应链管理：提高透明度和效率