**区块链的安全可信表现在哪里**

1. 区块链的信息无法篡改，保证每一条信息都是真实可靠的。任何人都不可能更改区块链中的信息，所以所有信息都是可信任的
2. 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。区块链对区块形式的数据进行哈希加密并加上时间戳，然后将哈希广播出去，使其公开透明而且不可篡改，这解决了电子现金的安全问题。

**软件危机**

软件危机是指在[计算机软件](https://wiki.mbalib.com/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA%E8%BD%AF%E4%BB%B6)的开发和维护过程中所遇到的一系列严重问题。

软件危机是落后的软件生产方式无法满足迅速增长的计算机软件需求, 从而导致软件开发与维护过程中出现一系列严重问题的现象。 这些严重的问题阻碍着软件生产的规模化、[商品化](https://wiki.mbalib.com/wiki/%E5%95%86%E5%93%81%E5%8C%96" \o "商品化)以及[生产效率](https://wiki.mbalib.com/wiki/%E7%94%9F%E4%BA%A7%E6%95%88%E7%8E%87)，让软件的开发和[生产](https://wiki.mbalib.com/wiki/%E7%94%9F%E4%BA%A7)成为制约[软件产业](https://wiki.mbalib.com/wiki/%E8%BD%AF%E4%BB%B6%E4%BA%A7%E4%B8%9A)发展的“瓶径”。

**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。**

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。

交易：节点之间发生的支付。

挖矿：在最新区块链的数据上，生成一个符合条件的区块，链入区块链的过程，就是挖矿。最简单的一种说法就是，在区块链上通过其特定计算公式，最快得到正确答案的人就会获得相应虚拟货币奖励，这一过程就是挖矿，即通过PoW工作量证明（Proof of Work）算法，解决数学问题，来争取记账权。

共识：就是所有分布式节之间怎么达成共识，通过算法来生成和更新数据，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。以比特币为例，采用的是“工作量证明”（Proof Of Work，简称POW）。工作量是需要算力的，通过工作量证明，有效的防止了篡改和伪造，因为如果要达到伪造和篡改的工作量，大概需要上亿元成本跟的算力。

智能合约（英语：Smart contract ）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。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。智能合约概念于1995年由Nick Szabo首次提出。智能合约的目的是提供优于传统合约的安全方法，并减少与合约相关的其他交易成本。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，满足触发条件自动执行。

**请举例说明区块链在“数据追溯”方面的应用案例。**

甲在一家牛肉店吃了一顿牛肉后肚子疼。

1. 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
2. 在食用每块牛肉前，可以清楚知道这块牛肉的来源，包括大到牛肉是来自哪一头牛身上的哪一部位，牛的健康状况，小到每一片牛肉是由谁切的，所有信息都可以追溯。
3. 区块链的信息无法篡改，保证每一条信息都是真实可靠的。任何人都不可能更改区块链中的信息，所以所有信息都是可信任的

**请举例说明区块链在“共享经济”方面的应用案例。**

案例1：德国Innogy共享充电桩

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汽车点对点充电项目。用户无需与电力公司签订任何供电合同，只需在智能手机上安装Share&Charge APP，并完成用户验证，即可在Innogy广布欧洲的充电桩上进行充电，电价由后台程序自动根据当时与当地的电网负荷情况实时确定。由于采用了区块链技术，整个充电和电价优化过程是完全可追溯和可查询的，因此极大地降低了信任成本。需要充电时，从APP中找到附近可用的充电站，按照智能合约中的价格付款给充电站主人。