**区块链：**

1. 智能合约：

类似函数，调用后得到最新的比特币余额存入数据库

1. 共识机制：

节点的数据账本写入公共账本需要经过共同投票，这个过程就是共识机制

1. 数据加密：

每个节点有公钥私钥，一个节点发出数据，别的节点可以用这个节点的公钥验证是不是它写的数据，这个节点可以用私钥在数据上签名，这个签名别的节点模仿不了

**区块链概念**：

区块链是[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/19276232)数据存储、[点对点传输](https://baike.baidu.com/item/%E7%82%B9%E5%AF%B9%E7%82%B9%E4%BC%A0%E8%BE%93/8491956)、共识机制、[加密算法](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95/2816213)等计算机技术的新型应用模式。区块链（Blockchain），是[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690)的一个重要概念，它本质上是一个[去中心化](https://baike.baidu.com/item/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96/8719532)的数据库，同时作为[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690)的底层技术，是一串使用[密码学](https://baike.baidu.com/item/%E5%AF%86%E7%A0%81%E5%AD%A6/480001)方法相关联产生的[数据块](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%9D%97/107672)，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（[防伪](https://baike.baidu.com/item/%E9%98%B2%E4%BC%AA/9638550)）和生成下一个区块

**区块链技术特点：**

1. 去中心化：

在区块链结构中，信息交互、核对身份等过程都不存在中心节点，而是分布在多个节点构成的去中心化的结构网络中。网络中的各节点，彼此的功能和作用都是一样的。在不同节点间进行数据传输时，负责接收的节点会对发送节点进行一次身份验证，在验证成功后，会将其接收到的数据在全网进行广播。

可以防止因中心节点遭受攻击而使整个网络瘫痪（传统物联网体系的中心化结构）。

1. 数据可追溯：

时间戳，生成块时有写入时间，所以交易可追溯

1. 安全可信：

区块链技术采用非对称密码学原理，结合哈希函数对交易进行签名，使得信息不能被伪造，即便是黑客窃取了信息由于不知道私钥，也无法知道信息内容。同时借助分布式系统的各节点的工作量证明等共识算法形成的强大算力抵御外部攻击，保证区块链数据不可篡改和不可伪造，因而具有较高的安全性。

1. 共识机制：

在区块链技术体系中，使用非对称加密算法中与公钥相关联的地址来当作节点用户的标识，因此就不再需要传统的基于PKI的认证机构，避免了认证机构出现问题时导致的认证安全问题。区块链利用共识的算法，在全网节点构建一种信任机制，在这种机制中，各个节点没有必要将身份信息共享，只需要将地址进行交互即可，并且节点还可以变化自己的地址。

1. 分布式数据库：

区块的作用就像一个记账溥，可以记录整个区块链上的交易，而且这些记录都可以一直被其他节点查验（分布式数据库体系）。当一些节点受到攻击或是数据遭受破坏时，由于其他的节点依然保存有完好无损的信息，因此并不会对系统产生影响。