区块链不是一个颠覆性的新技术，它是一个技术组合。其关键技术包括P2P动态组网、基于密码学的共享账本、共识机制（拜占庭将军问题）、智能合约等技术。中本聪将这些技术创新性的巧妙组合在一起，并在此基础上引入完善的激励机制，用经济学原理来解决传统技术无法解决的问题。

区块链以参与方式分类可以分为：

公有链

公有链对外公开，用户不用注册就能匿名参与，无需授权即可访问网络和区块链。节点可选择自由出入网络，公有链上的区块可以被任何人查看，任何人也可以在公有链上发送交易，还可以参与网络上形成共识的过程，即决定哪个区块可以加入区块链并记录当前网络状态。公有链是真正意义上的完全去中心化的区块链。公共连中的共识机制一般是工作量证明（PoW）或者权益证明（PoS），用户对公共识形成的影响力直接取决于他们在网络中拥有的资源占比。公共链同城也称为非许可链。

联盟链

联盟链仅限于联盟成员参与，区块链上的读写权限、参与记账权限按照联盟的规则来制定。也称为许可链。联盟链的共识过程由预先选好的节点控制，当网络上有超过2/3的节点确认一个区块，该区块记录的交易将得到全网确认。联盟链可以根据应用场景向公众开放，由于参与公式的节点比较少，联盟链一般不采用工作量证明的挖矿机制，而是使用权益证明或者PBFT、RAFT等共识算法。联盟链对交易的确认时间、每秒交易数都与公有链有较大区别。

私有链

私有链仅在私有组织使用，区块链上的读写权限、参与记账按照私有组织规则来制定。私有链的应用场景一般是企业内部的应用或者政府应用。私有链的价值主要是提供安全、可追溯、不可篡改、自动执行的运算平台，可以同时防范来自内部和外部对数据的安全攻击。

区块链的颠覆性价值主要包括以下5方面：

1、简化流程，提升效率；

2、降低交易对手的信用风险

3、减少结算或者清算时间

4、增加资金流动性，提升资产利用效率

5、提升透明度和监管效率，避免欺诈行为。

区块链的本质是一个对等网络（peer-to-peer）的分布式账本数据库。区块链本身是遗传连接的数据区块，其链接指针是采用密码学哈希算法对区块投进行处理所产生的区块头哈希值，下一个区块中记录了其上一个区块的哈希值。

区块链解决的问题

1、拜占庭将军问题

拜占庭罗马帝国在军事行动中，采取将军投票的策略来决定是进攻还是撤退，也就是说如果多数人决定进攻，就进攻。但是军队中如果有奸细（比如将军已经反水故意乱投票，或者传令官叛变擅自修改军令），那怎么保证最后投票的结果真正反映了忠诚的将军的意愿呢？

区块链技术采用共识算法对新增的区块或者交易达成共识，一份新增的信息，得到大部分影响力较高的节点认可的时候，便成为真实有效的信息。这类解决拜占庭将军为题的共识算法称为BFT共识，区块链主要采取的就是BFT共识。

2、双重支付（“双花问题”）

双重支付问题即用同一笔钱完成两次或者多次支付，例如，某个节点宣布同时给与A节点和B节点一次支付信息，如何记录这条支付信息是给与A的还是给与B的，是区块链用于解决双花问题的关键。区块链技术通过区块链接形成的时间戳技术加上验证数据是否满足UTXO（未花费交易）和数字签名，有效避免双重支付问题。拿比特币技术距离，如果有人用同一笔UTXO构造了两笔支付给不同交易方的交易，则比特币客户端只会转发最先被侦听到的那个。节点会选择将那笔交易包入之后的区块，当其中一笔交易所在的区块后面有5个链接的区块，这笔交易得到了6次确认，则认同该笔交易。比特币区块链上，6次去人后基本可以保证比特币交易不被双花。

区块链技术中的一些基本概念：  
1、数据区块

数据区块一般包含区块头和区块体两部分。如图1所示，区块头封装了当前的版本号、前一区块的地址、时间戳、随机数、当前区块的目标哈希值等信息，区块体则主要包含了交易计数和交易详情。

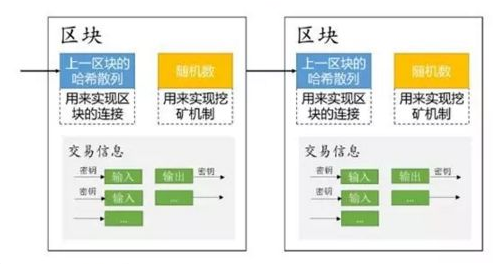


图1 数据区块结构示意图

2、时间戳和不可篡改性

时间戳是一个字符序列，用来唯一标识某一刻的时间。在区块链系统中，获得记账权限的节点在链接区块时需要在区块头中加盖时间戳，时间戳为未来基于区块链的互联网和大数据增加了一个时间唯独，使得数据更容易追溯，并可以重现历史数据。同时，时间戳可以作为存在性证明的重要参数，它能够证实特定数据必然在某个特定时刻是存在的，保证了区块链数据库的不可篡改和不可伪造，这也为区块链技术应用于公正、知识产权注册等领域提供了可能。

3、分布式数据库

拿比特币系统来说，比特币系统的区块记录了所有比特币的交易信息，每一个比特币用户的比特币收支情况都被永久的嵌入了数据区块中供别人查询。这些数据区块的交易数据存放在每一个比特币用户的客户端节点中，所有的这些节点组成了比特币及其鲁棒的分布式数据库系统。任何一个节点的数据被破坏都不会影响整个数据库的正常运转，其他的健康节点都保存了完整的数据库。

4、哈希函数

区块链中的数据除了原始数据和交易记录还保存着它们的哈希函数值，即将原始的数据编码为特定长度的、由数据和字母组成的字符串后，记入区块链。哈希函数之所以适合存储区块链数据，因为它有以下几个优点：  
 1、哈希函数处理过的数据是单向性的，通过哈希值几乎不可能计算出原始的输入值；

2、哈希函数处理不同长度的数据所耗费的时间是一致的，输出的哈希值也是定长的；

3、哈希函数的输入值即使只相差一个字节，输出值的结果也会截然不同。比特币系统最长采用的哈希函数是双SHA256函数，即进行两次SHA256哈希处理。