那么，比特币和区块链到底有什么分别？二者为何纠缠不清？区块链到底有何魔力？今天，第二期《链上公开课》就来揭开区块链的神秘面纱。

知识点1：概念和本质

按照严谨定义的表述，区块链技术是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。

我们看到通俗的表述是：区块链作为比特币的底层技术，是一种去中心化的分布式记账系统，具备去中心化、不可篡改、公开透明、可溯源、匿名性等特征。目前业内还有一种说法，区块链本质是上是一个防伪系统，即通过公开透明、不可篡改、可溯源实现防伪。

如果说做一个不恰当的比喻来描述区块链，网上的一个例子就很形象，故事是一群牛从美国西部赶往美国东部：牛仔0出发到达小镇酒馆1，向所有人公布这群牛的数

量、价格等信息，然后把这群牛交给牛仔1；接着牛仔1继续出发到达小镇酒馆2，向所有人公布这群牛的数量、价格等信息，然后把这群牛交给牛仔2；以此类推，直到这群牛被运到美国东部。

这群牛就是一个一个的区块，牛仔（0、1、2...）就是分布式记账的矿工，公布就是全网广播，而串起来牛群的路线就是区块链。

知识点2：四大组成部分

区块链作为记账系统，是由分布式数据库、点对点通信技术、加密算法、共识机制4个部分构成。

以比特币为例，分布式数据就是区块中的交易数据，存放在每一个比特币用户的客户端节点中，所有节点就构成了分布式数据库，因为全网记账，所以任何一个节点被恶意破坏都不会影响数据库的真实性。

点对点通信技术，相对好理解，就是P2P网络，大家用过的电驴、迅雷等下载软件就是用了点对点通信技术，即各个计算机节点直接相连，节点可以自由进入和退出，整个网络不依赖中心服务器。

加密算法，就是上文提到的椭圆曲线加密算法，也就是区块链必备知识点“非对称加密”，非对称的意思是一个钥匙不能同时上锁、解锁，在比特币区块链网络中是公钥加密，私钥解密。这就好比一个保险柜，公开钥匙可以锁上，但不能解锁；私钥可以解锁，但不能锁上。

共识机制，是对区块链的记账权进行集体验证的机制，说大白话就是，“你获取了记账权，大家都认可且没有异议”的机制。目前有三种，第一个是工作量证明（POW），比如比特币、以太坊。第二个是股权证明（POS），比如点点币，第三个是股权代表证明机制（DPOS），比如比特股。

知识点3：几大特性

其实，区块链的特性就是由四大组成部分决定的，包括去中心化、公开透明、不可篡改、可溯源、匿名性。

区块链系统是基于P2P网络的，每个节点都可以查询，同时记账信息要全网广播，这就是公开透明的由来。

不可篡改，是源于区块链链状的记账模式，区块链网络中任何一个区块尾都是下一个区块头，这达成了可以溯源的效果；同时，再加上分布记账、加密算法和全网广播，让不可篡改成为可能，因为破坏者不能修改所有矿工的账本。

基于P2P网络，通过分布式数据库、加密算法，保证了区块链数据库完整、连续，无法篡改，最终实现了没有中心化权威机构，也让大家相信区块链记账的真实性，达成算法信任或者机器信任，这就是去中心化。

匿名性更准确的说法是“非实名性”，也就是说，每个节点在区块链网络中是用了一个虚拟身份，任何转账行为都只能看到两个虚拟身份，而非真实身份的信息而已。