区块链四大核心技术解析（哪一项是基石）

区块链这个概念的火爆程度在今年可谓是达到了历年来的巅峰，大家纷纷开始了解区块链。一步步了解后，知道区块链是比特币的底层技术，是制造信任的机器，是个分布式账本，是继互联网之后的又一大革命，是智能经济的未来不可缺少的技术……各种各样的解释充斥在各大信息头条。

但提起区块链背后的核心技术时，总是令人费解。今天就让我们来简单聊聊，区块链的四大核心技术。

01区块链独特的数据结构

区块链这个名字自身就比较独特，由区块和链构成。在形式上，类似于我们的微信朋友圈，每一条朋友圈都是一个区块，串起来的整个朋友圈，就像一条链，而左边的时间标志就像区块链里的时间戳，什么时候发的朋友圈会有记录，不过时间戳会精确到几分几秒。需要注意的是，朋友圈按时间顺序记录和存储信息的结构仅仅是与区块链的结构相似，并不是说朋友圈就等同于区块链了。

不同的是，朋友圈发的内容比较纷杂，而区块链里的每一个区块内容相对比较固定。一般都是一些数据记录：区块头里面上一区块的哈希值、该区块的最终随机数、区块的体积大小、交易的具体信息，如交易双方及其数字签名、交易额等等。每个区块头包含的哈希值就像是上一个区块所有数据的“数字指纹”，因此每个区块之间就有了一种环环相扣的“关系”，这层关系形成了一个链条，让旧的区块链数据一旦任何一个字符被改动，后面所有的哈希值都会发生变动。这样的一个结构和内容构成了整个区块链。

02分布式存储

在了解了区块链的大概内容和形式之后，我们会想，既然只是这样一种简单的方式记录东西而已，有什么新奇的呢？其实区块链最吸引人的是其分布式存储的机制，即去中心化的思想。区块链中每一个区块上的信息记录，都是由参与记账的每一个电脑，即节点竞争记录的，并背后并没有任何企业、公司来管理。

为了防止某些恶意节点来搞破坏，对于采用 PoW 共识机制的区块链中的新数据，需要得到大部分节点的一致确认和同意，至少也需要有
51%的节点同意，因此某个节点想篡改数据是很难的。

03密码学

作为一个可以传输价值的区块链，如果安全仅靠节点数取胜，当然令人难以置信，因此区块链运用了一个杀手锏——密码学。密码学中的非对称加密技术是保障安全的重要部分。对称加密就相当于开门和锁门用了同一把钥匙，非对称加密则相当于开门锁门用了两把不同的钥匙，一个叫公钥，一个叫私钥，公钥锁门，只有私钥可以开，而用私钥锁门，也只有公钥可以开门。

这两种密钥一般都存储在钱包里，私钥一旦丢失，资产也荡然无存。在区块链中，公钥和私钥的形成都经过哈希算法和椭圆曲线算法等多重转化而成的，字符都比较长和复杂，因此比较安全。

04共识机制

为了保证节点愿意主动去记账，区块链形成了一个重要的共识机制，这种共识机制也被称为区块链的灵魂。PoW （算法机制）是最初的一种共识机制，所有参与的节点通过比拼计算能力来竞争记账权，这是相对比较公平和去中心化的一种方式，但是所有人都参与，却只能选一个节点，会浪费大量资源和时间成本。

因此，后面又出现了PoS（权益证明机制）共识机制，持有数字货币时间越长，持有的资产越多，就越有可能获得记账权和奖励，节省了时间，但有人说这违背了去中心化的初衷，容易出现马太效应；再后来出现了 DPoS（委托权益证明机制）,节点选出代表节点来代理验证和记账，更加简单高效，但也有人说这也在一定程度上牺牲了一些去中心化。

05小结

以上就是区块链的核心技术，当然区块链还运用到了别的很多学科和技术，如数学、经济学、计算机学科等等，它们共同构建了区块链这项神奇的技术。

那么，你认为区块链最厉害的技术是什么呢？欢迎在留言区分享你的观点。