你有没有关注到这么一个现象“区块链技术正逐渐渗透越来越多的行业”。

近两年随着区块链技术的普及以及国家对区块链技术的关注与重视，越来越多的企业开始了解并尝试将区块链技术运用到自己的相关业务当中。

但依然有很多人（企业）对区块链技术不甚了解，今天我们就来简单聊聊四大神奇的区块链创新技术：分布式存储技术、非对称加密技术、哈希算法、共识机制。

在正式开始之前，我们在来简单科普一下什么是区块链？区块链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。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。

01

分布式存储技术

了解了区块链的大概形式之后，你可能会想：“不过只是一种简单记录东西的方式而已，有什么新奇的呢”？

其实区块链的迷人之处在于它的分布式存储机制，即点对点分布式技术（peer-to-peer，简称P2P）亦可理解为分布式账本，它依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。网络上的每则信息/交易都由所有参与者（或“节点”）共享和存储。

这样做的好处是可消除单点故障担忧，降低网络遭到黑客攻击/信息丢失的几率。此外，没有一个实体拥有存储在网络上的数据，这意味着没有人可以滥用数据为自己谋私利。用户控制他们自己的数据，决定这些数据的用途。

网络参与者未来可根据需要出售他们的数据，如果你将搜索记录存储在区块链版本的浏览器上（如：百度、Google等）上，那么你可以将该搜索记录出售给广告商，广告商会直接向你支付相应费用。

或许你会想：把个人信息存储在一堆陌生人的电脑上，岂不是对隐私的侵犯？幸运的是，区块链协议有一个解决方案：加密，通过加密技术可以隐藏网络参与者的身份和交易内容。

广义来说，哈希是一种数学函数。它可以把任意长度的输入（一个单词、一个句子

或整本书），通过公式来创建一个看似随机的、由字母和数字组成的固定长度的输出。哈希函数的有趣之处在于它除了可以把无限量的内容缩减为一小段字符外，它还是唯一性的单向函数即输入中的任何微小变化都会导致完全不同的哈希输出。

因此，要验证两个文件是否完全相同就很容易。你没必要字对字的检查，而是创建该文档的哈希值并将其与原始文档的哈希值进行对比，检查该哈希值的对应字符是否匹配。如果对原文档进行了细小的改动，则哈希值将完全不同，而不用再去检查整份文件的所有细节才可确保没有遗漏任何内容。

讨论完哈希算法，我们来继续讨论区块链加密的第二个关键组成部分：非对称加密，也称为公钥/私钥加密。

非对称加密指在加密和解密两个过程中使用不同密钥。在这种加密技术中，每位用户都拥有一对钥匙：公钥和私钥。在加密过程中使用公钥，在解密过程中使用私钥。公钥是可以向全网公开的，而私钥需要用户自己保存。这样就解决了对称加密中密钥需要分享所带来的安全隐患。

非对称加密与对称加密相比，其安全性更好：对称加密的通信双方使用相同的秘钥，如果一方的秘钥遭泄露，那么整个通信就会被破解。而非对称加密使用一对秘钥，一个用来加密，一个用来解密，而且公钥是公开的，秘钥是自己保存的，不需要像对称加密那样在通信之前要先同步秘钥。

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。

共识机制是网络参与者就“单一版本的事实”达成一致的方式。网络参与者使用一致性算法来确认发起的交易是有效的，发送资产的人实际上拥有这么多资产。用一个日常的例子来说明就是，一个中国微博大V、一个美国虚拟币玩家、一个非洲留学生和一个欧洲旅行者等他们互不相识，但他们都一致认为你是个好人，那么基本上就可以断定你这人还不坏。

我们历来需要可信赖的第三方来确认我们正在交易的资产（货币，财产等）尚未在其他地方花费过，但共识机制允许分布式网络无需信任第三方就可以验证交易是否合法，同时解决了交易的双花问题。

区块链有许多不同的共识机制，其中比较常见的共识机制：工作量证明（Proof-of-Work，PoW）、权益证明（Proof-of-Stack，PoS，又译持有量证明）、容量证明（Proof-of-space，PoSpace，又称Proof-of-Capacity，PoC）等。

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。