区块链的四大核心技术

一般来说，区块链的核心技术主要有四个部分，分别是共识机制、分布式存储、智能合约以及密码学。每个技术，在整个区块链系统里都有它们各自的作用。

共识机制

共识机制，其实就是我们之前所说的挖矿原理，因为区块链的分布式网络中，没有中央权威。因此，网络需要一个决策机制来促成参与者达成一致。而共识机制就是一种协调大家处理数据的机制。

因为每个人都可以参与的话，记录下来的数据这么多，到底该用谁的呢？所以，共识机制就决定了这些数据中，谁获得数据的记账权。共识机制主要起到了数据的维护作用。

目前比较常见的共识机制有：工作量证明 PoW（Proof of Work）、权益证明（Proof of Stake）以及委托权益证明（Delegated Proof of Stake）。

分布式存储

分布式储存，简单来说，就是一种将数据分散存储到多个地方的数据储存技术，而且存储的数据可在多个参与者之间共享，人人可以参与，并具有相同的权力，一起记录数据，主要起到了数据储存的功能。

分布式存储是一种数据存储技术，通过网络使用每台机器上的磁盘空间，并将这些分散的存储资源构成一个虚拟的存储设备，数据分散的存储在网络中的各个角落。

所以，分布式存储技术并不是每台电脑都存放完整的数据，而是把数据切割后存放在不同的电脑里。就像存放 100 个鸡蛋，不是放在同一个篮子里，而是分开放在不同的地方，加起来的总和是 100 个。

对于比特币来说，它的交易记录必须要有地方存放，不然没人知道今天有哪些人做了交易，同时根据去中心化的思想，这些交易记录不能够只存在一台电脑里面，那么就只能存放在世界上所有的电脑里面（前提是电脑里面安装了比特币软件）。

这样做的好处是：虽然每个人的电脑硬盘容量有限，但是所有人的电脑硬盘加起来容量几乎是无限的，而且就算你通过黑客手段修改了自己计算机里面的交易记录，但是你没法修改全世界每台电脑的交易记录。

从表面上理解，上面说的这种存储方式很粗暴——每台电脑都存放世界上所有人的交易数据。但其实对于比特币来说，只有一些节点才会存放世界上所有人的交易记录，这些节点往往是那些挖矿的矿工，只有他们的电脑才能完整的记录下世界上所有的交易记录，大家不用担心矿工修改记录，因为世界上的矿工有很多，而且几乎相互都不认识。同时他们修改记录需要付出的代价非常大，几乎没有人能承担这个成本。

智能合约

智能合约，是一种旨在以信息化方式传播、验证或执行合同的计算机协议。有点像一种大家把规则都制定好，由机器自动去执行的技术。

因为网络中存储和维护好的数据，总需要有人去执行的，而智能合约正好可以在没有第三方的情况下，也能进行可信的交易，而且这些交易可追踪且不可逆转。所以，智能合约在系统中，主要起到了数据的执行作用。

智能合约（Smart contract）是一种以计算机语言编写、由计算机自动验证和执行的代码化的合同，是纸质合同的数字化形式。

智能合约概念于 1994 年由计算机科学家、法学家及密码学家尼克 • 萨博（Nick Szabo）首次提出。他对智能合约的定义是“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。”

智能合约概念面世后，自然面临如何落地的问题：

第一，谁来执行合约？显然，签署合约的双方不应成为执行人。

这带来一系列问题：如何激励他为你执行合约而不是免费？他如何保持公正和中立？他缺位、消失或者拒不执行怎么办？

第二，如何通过计算机程序支付现金和资产？

当时技术条件尚未成熟，无法解决上述问题，因此智能合约迟迟无法变为现实。

数字货币和区块链诞生以后，上述问题得以顺利解决：

1. 执行智能合约的机制：去中心化网络+共识机制+受激励的矿工

2. 价值转移功能：内生可编程的数字货币

3. 去中心化的永不停机的计算网络，保持中立、公平、永远工作

区块链不仅内嵌数字货币系统，而且可编程可扩展，具有去中心化、不可篡改、过程透明、可追踪等优点，天然适合于智能合约。

从此，智能合约才从理论构想变为落地的现实，从而插上了飞速发展的翅膀。区块链给智能合约提供了最佳的技术土壤，而智能合约功能也大大扩展了区块链的应用前景。目前一般认为，智能合约是基于区块链技术的自动执行的数字合约形式。

密码学

密码学，是一种特殊的加密和解密技术，区块链系统中，应用了多种多样的密码学技术，包括哈希算法、公钥私钥、数字签名等等，以此来保证整个系统的数据安全，并且证明了数据的归属。

有了它我们才能在网络中证明“我是我”，才能证明这是我的比特币而不是你的比特币。

所以，当一笔数据产生后，会由共识机制进行数据维护，通过分布式储存记录在链上，然后交由智能合约去执行，最后由密码学保障整个体系的安全，大家各司其职，共同构建出了整个区块链系统。