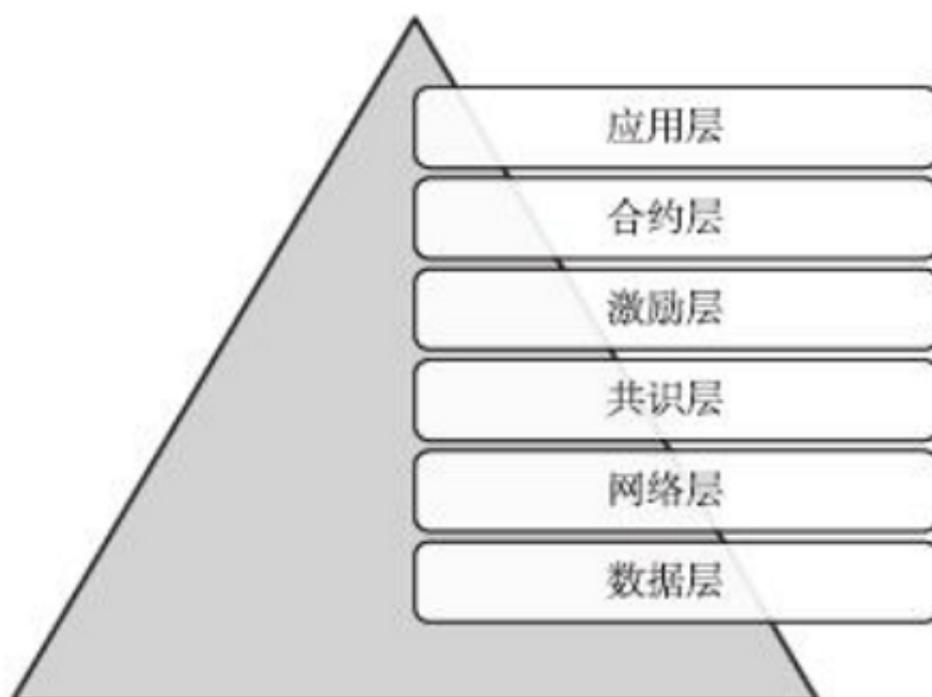


来到币圈这么长时间了，对于什么是区块链想必大家已经很清楚。但是说到区块链的模型架构怕是很多人还不太了解。其实区块链系统由自下而上是由六层组成的，分别是数据层、网络层、共识层、激励层、合约层和应用层组成。如下图所示：



(一) 数据层 数据层封装了底层数据区块的链式结构，以及相关的非对称公私钥数据加密技术和时间戳等技术，这是整个区块链技术中最底层的调制解调器构，其中大多数技术都已被发明数十年，并在计算机领域使用了很久，无须担心其中的安全性，因为如果这些技术出现安全性上的巨大漏洞，则意味着全球金融技术都会出现严重的问题。中本聪在设计比特币时，为每个区块设置了1MB（兆）大小的容量限制，但由于目前比特币的交易量迅速提升，1MB的区块空间能容纳的交易数量有限，所以要考虑扩容区块链来突破这个限制。

(二) 网络层 网络层包括分布式组网机制、数据传播机制和数据验证机制等，由于采用了完全P2P的组网技术，也就意味着区块链是具有自动组网功能的。这种P2P组网技术，在早先应用于BT（比特流）和eMule（电驴）之类的P2P下载软件中，也是一种相对来说非常成熟的技术。

(三) 共识层 共识层主要封装网络节点的各类共识机制算法。共识机制算法是区块链技术的核心技术，因为这决定了到底由谁来进行记账，记账者选择方式将会影响到整个系统的安全性和可靠性。目前已经出现了十余种共识机制算法，其中最为知名的有工作量证明机制（Proof of Work, PoW）、权益证明机制（Proof of Stake, PoS）、股份授权证明机制（Delegated Proof of Stake, DPoS）等。在下一节中将会详细介绍这些共识机制。

(四) 激励层 激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的

发行机制和分配机制等，该层主要出现在公有链（Public Blockchain）中，因为在公有链中必须激励遵守规则参与记账的节点，并且惩罚不遵守规则的节点，才能让整个系统朝着良性循环的方向发展。所以激励机制往往也是一种博弈机制，让更多遵守规则的节点愿意进行记账。而在私有链（Private Blockchain）中，则不一定需要进行激励，因为参与记账的节点往往是在链外完成了博弈，也就是可能有强制力或者有其他需求来要求参与记账。

（五）合约层 合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础。以以太坊为首的新一代区块链系统试图完善比特币的合约层。比特币尽管也包含了脚本代码，但是并不是图灵完备的，即不支持循环语句；以太坊在比特币结构的基础上，内置了编程语言协议，从而在理论上可以实现任何应用功能。如果把比特币看成是全球账本的话，那么就可以把以太坊看作是一台“全球计算机”——任何人都可以上传和执行任意的应用程序，并且程序的有效执行能够得到保证。

（六）应用层 应用层则封装了区块链的各种应用场景和案例。比如搭建在以太坊上的各类区块链应用就是部署在应用层，所谓可编程货币和可编程金融也将会搭建在应用层。

在区块链的这个模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识机制的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。其中数据层、网络层和共识层是构建区块链应用的必要因素，否则将不能称为真正意义上的区块链。而激励层、合约层和应用层则不是每个区块链应用的必要因素，有部分的区块链应用并不完整地包含着这三层结构。