区块链

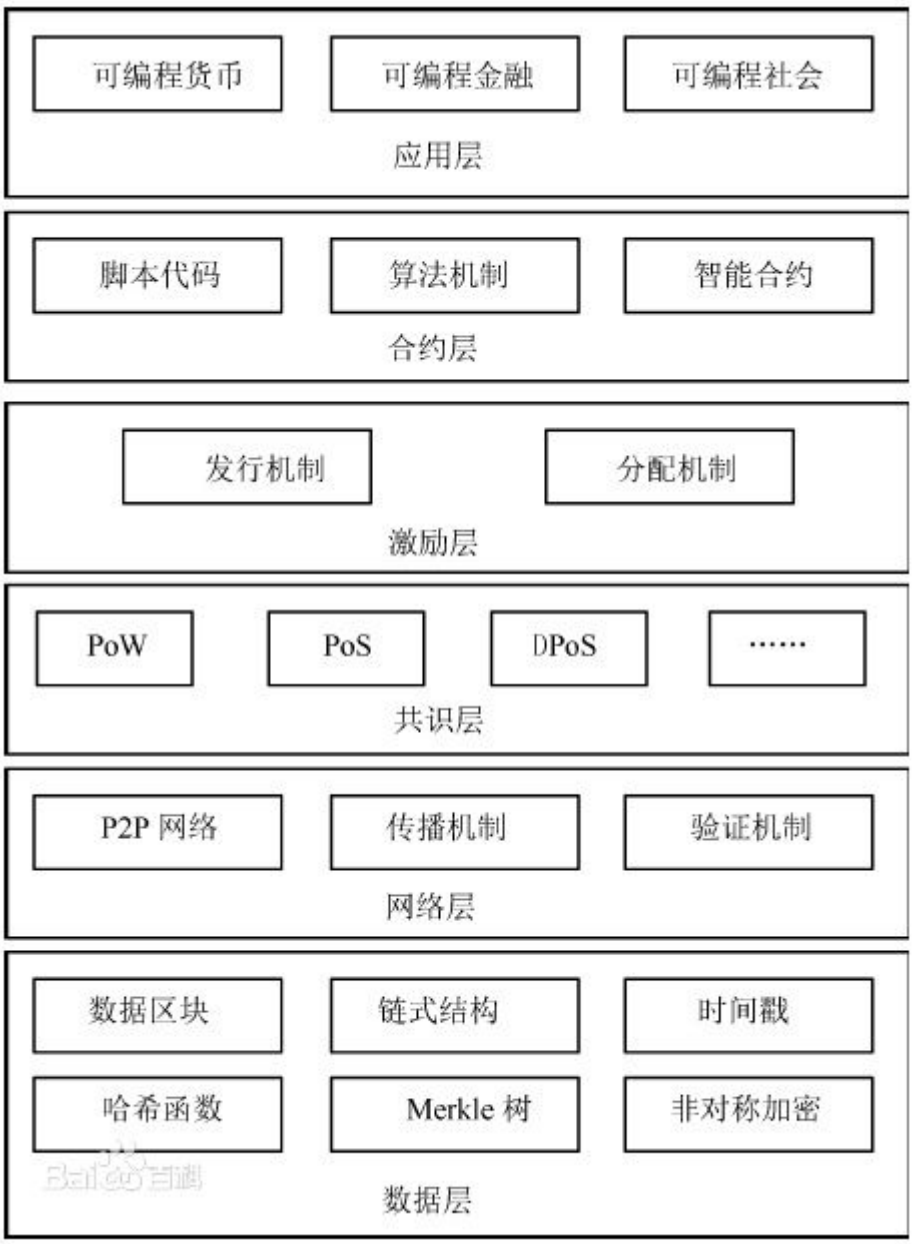
- 概念：区块链是数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

  此外，区块链（Blockchain）是比特币的一个重要概念，火币网联合清华大学五道口金融学院互联网金融实验室、新浪科技发布的《2014—2016全球比特币发展研究报告》提到区块链是比特币的底层技术和基础架构。**本质上是一个去中心化的数据库，同时作为比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。**

- 含义：狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。

  广义来讲，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方式。

- 基础架构模型：一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。 其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；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；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；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力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。



- 分类：
    1. 公有区块链（PublicBlockChains)：公有区块链是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是目前应用最广泛的区块链，各大bitcoins系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。
    2. 联合（行业）区块链（ConsortiumBlockChains)：由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程(本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的API进行限定查询。
    3. 私有区块链：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。目前(Dec2015)保守的巨头（传统金融）都是想实验尝试私有区块链，而公链的应用例如bitcoin已经工业化，私链的应用产品还在摸索当中。
- 特征
    1. 去中心化：由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

得益于区块链的去中心化特征，比特币也拥有去中心化的特征，在火币联合清华大学五道口金融学院互联网金融实验室、新浪科技发布的《2014—2016全球比特币发展研究报告》中就有详细报告。

2. 开放性：系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。
3. 自治性：区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对"人"的信任改成了对机器的信任，任何人为的干预不起作用。
4. 信息不可篡改：一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。
5. 匿名性：由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

- 应用

1. 艺术行业：Ascribe让艺术家们可以在使用区块链技术来声明所有权，发行可编号，限量版的作品，可以针对任何类型艺术品的数字形式。它甚至还包括了一个交易市场，艺术家们可以通过他们的网站进行买卖，而无需任何中介服务。
2. 法律行业：BitProof是目前近些年来涌现的众多文档时间戳应用中最为先进的，将会让传统的公证方式成为过去。相对于包括Blocksgin和OriginStaemp这样的免费版本，BitProof提供更多的服务，包括有一个是针对知识产权的。有趣的是，BitProof最近和一家旧金山的IT学校进行合作，把他们学生的学历证书都放在区块链上，完全重新定义了如何让文凭和学生证书的处理和使用方式。
3. 开发行业：Colu是首个允许其它企业发行数字资产的企业，他们可以将各种资产来"代币化"让许多人印象深刻。尽管免费的比特币钱包Counerparty也允许发行简单的代币，并且在其他钱包持有者之间进行交易，Colu的代币可以设置有各种状态和类型，能够脱离或者重新回到这个系统，并且当在区块链上存储数据过大的时候能够将数据存储在BitTorrent的网络上。
4. 房地产行业：他们计划能够让整个产业链流程变得更加现代化，解决每个人在参与房地产面临的各种问题，包括命名过程，土地登记，代理中介等。

   金融角度看待区块链

   货币的本质：货币只是一种广泛价值共识，本身不具有价值沉淀。

   资产与货币的关系：货币描述资产。

   什么是数字资产：资产数字化，可细分，可交易，价格由供需市场决定，而不是价值中介——货币决定。