



链滴

# 什么是区块链

作者: [jchain](#)

原文链接: <https://ld246.com/article/1595420288321>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

从比特币系统发现区块链

## 去中介化

电子现金的货币发行不需要一个中心化机构（比如央行），而是由代码和社区共识完成个人与个人之间的电子现金交易无需第三方中介的担保（支付宝，微信等）介入

## 需要解决的问题

在数字世界中，要创造一种“去中介化”，“去中心化”的电子现金，需要着重解决下面的问题

1. "电子现金" 如何公平公正的发放出来，而不被任何中心化的机构和个人控制？
2. 如何将一笔交易从一个人到另一个人，而无需中介的协助？
3. 电子现金如何防伪造？比如 如何保证 一份电子现金 不会发生多次交易？

## 比特币系统设计分为3层

1.应用层 (application layer)

2.应用协议层 (application protocol layer)，也叫比特币协议

发行货币 和 处理用户间的比特币转移

这一层相当于 中央银行(发行货币) 和 银行(处理转账) 等金融机构

3.通用协议层 (general protocol layer) 也称为 比特币区块链(bitcoin blockchain)

分布式账本 和 去中心化网络

## 比特币系统架构

通常被分为5层,对应的是比特币协议和比特币区块链两部分

1. 应用层：实现转账和记账功能
2. 激励层：发行机制和分配机制
3. 共识层：POW工作量证明
4. 网络层：P2P网络，广播机制，验证机制
5. 数据层：区块数据,链式结构,数字签名,散列函数(Hash),梅克尔树,非对称加密/公钥私钥

比特币设计时，把计算机算力竞争和经济激励相结合，形成了工作量证明(POW)共识机制。

矿机在竞争中（算力题）完成货币发行和记账，这样也完成了区块链账本和去中心化网络的运维

形成了一个完整的循环：矿机挖矿（算力竞争），完成去中心化记账（运转系统），获得比特币形式经济奖励

其中工作量证明共识机制承上启下，连接上层应用和下层技术：

上层为电子现金的发行，转账，访伪

下层为去中心网络的节点达成一致，更新账本

# 区块链的定义

1.区块链是一种源自"比特币"的底层技术。也就是说,比特币是区块链技术的第一个获得成功的应用

2.区块链是数字世界中进行"价值表示"和"价值转移"的技术。区块链硬币一面表示价值的加密数字货币或者通证,另一面是进行价值转移的分布式账本和去中心化网络

分布式账本和去中心化网络也常被称为"链",它可被视为一个软件平台;而表示价值的通证通常被称为"币"