什么是去中心化？

在说“货币”时，我们讨论的是数字世界中的价值表示。在互联网上的数字世界中，人们曾设计出各种各样的电子现金或数字现金方案，在为《区块链：技术驱动金融》一书撰写前言时，杰里米·克拉克收集了约 100 种支付系统。他写道：“在通往比特币的道路上，布满了无数失败的尝试。”在所列的各种系统中，他认为大众所知道的只有
PayPal。当然，在移动支付超前发展的中国，我们都很熟悉支付宝与微信支付。
一直以来，数字世界中的“货币”有三种形式（见下图）：

- 中心化的在线支付；
- 中心化的计算机点数或互联网积分；
- 去中心化的电子现金。


交易的去中心化
自动化
交易的去中心化
完全自治
发行的去中心化
自动化
发行的去中心化
完全自治
网络的部分去中心化
分布式网络
网络的去中心化
完全开放，非基于信任的
有协调的社区
由人协调与管理
完全去中心化的社区
由机制实现的自治

不过，之后在发展区块链技术和将之应用的过程中，我们又不得不从最极致的理想状态往实用方向调整，比如：

- 现在多数区块链项目都是由基金会管理的。以太坊是由创始人维塔利克·布特林（人称“V神”）和以太坊基金会居中协调的，而不像比特币社区那样是完全自治的。
- 常在金融系统中使用的联盟链，以及部分节点数量不多的基础公链，如小蚁（NEO）、EOS，更应被视为分布式网络，没有实现完全的去中心网络。
- 通过以太坊发行基于 ERC20 标准的通证，通证的发行规则是由项目方确定的，在运行过程中会酌情更改规则。它们的发行不是自动的或自治的。
- 常被视为区块链 3.0 代表的 EOS 在智能合约部分引入了李嘉图合约和社区仲裁机制，也即交易部分不再是完全交给机器自动执行，在需要时人可以参与和干涉。

我们反复讨论比特币系统的设计，是因为它早已经把最极致的情况展现在所有人面前。而在将区块链技术落地应用的过程中，从最极致的去中心化往实用主义方向调整并不是倒退，而是事物发展的必然过程。

比特币是如何实现去中心化的？

那么，比特币系统具体是如何实现极致的去中心化的呢？
在比特币白皮书《比特币：一个点对点电子现金系统》中，中本聪详细地解释了他是如何设计这个系统的。在其中，他确立了此后所有区块链系统的主要设计原则。

- 一个真正的点对点电子现金应该允许从发起方直接在线支付给对方，而不需要通过第三方的金融机构。
- 现有的数字签名技术虽然提供了部分解决方案，但如果还需要经过一个可信的第三方机构来防止（电子现金的）“双重支付”，那就丧失了（电子现金带来的）主要好处。
- 针对电子现金会出现的“双重支付”问题，我们用点对点的网络技术提供了一个解决方案。
- 该网络给交易记录打上时间戳（timestamp），对交易记录进行哈希散列处理后，将之并入一个不断增长的链条中，这个链条由哈希散列过的工作量证明（hash-based proof-of-work）组成，如果不重做工作量证明，以此形成的记录无法被改变。
- 最长的链条不仅仅是作为被观察到的事件序列的证明，并且证明它是由最

大的CPU处理能力池产生的。只要掌控多数CPU处理能力的计算机节点不（与攻击者）联合起来攻击网络本身，它们将生成最长的链条，把攻击者甩在后面。

- 这个网络本身仅需要最简单的结构。信息尽最大努力在全网广播即可。节点可以随时离开和重新加入网络，只需（在重新加入时）将最长的工作量证明链条作为在该节点离线期间发生的交易的证明即可。

威廉·穆贾雅在《商业区块链》一书中对比特币白皮书摘要进行了分析，他总结了四个要点：

1. 点对点电子交易；
2. 不需要金融机构；
3. 加密证据而不是中心化的信用；
4. 信用存在于网络，而不是某个中心机构。

而从这个摘要中，我们提炼出了比特币系统设计的五个要点（见图 4）：比特币的区块链系统是由分布式账本（即狭义的区块链）和去中心网络（点对点网络）组成的，形成链条的方式是工作量证明共识机制。最长链是由网络中的算力共同决定的，因而它是可信的，节点离开和加入依据的是最长链是可信的这一原则。这些组合起来形成了比特币系统。