什么是去中心化区块链（去中心化是区块链最根本的特征解析）

从区块链诞生以来，去中心化一直被业界作为区块链的核心属性之一。但最近一段时间以来，国内一些业界大佬纷纷开始否认这一点，甚至有人声称去中心化这个词是区块链行业翻译产生的重大误导，呼吁翻译成“点对点”，任何区块链应用的规则制定者就是根本的中心。这是一种极其错误的倾向，可能会误导很多区块链创业者，使其在探索区块链应用落地的过程中走弯路。

什么是“去中心化”？

“去中心化”翻译自英语单词Decentralization，是由前缀de-、词干central、后缀-ization组成。其中，词干central意为“中心”，后缀-ization意为“……化”，而前缀de-
则有离开、除去、取消、相反等含义。因此，将其翻译为去中心化是非常准确的。

那么，去中心化具体而言是什么含义呢？

以太坊创始人Vitalik Buterin于2017年2月发表的《The meaning of decentralization》一文中，详细阐述了去中心化的含义。他认为应该从三个角度来区分计算机软件的中心化和去中心化：架构、治理和逻辑。

架构中心化是指系统能容忍多少节点的崩溃而可以继续运行；治理中心化是指需要多少的个人和组织能最终控制这个系统；逻辑中心化是指系统呈现的接口和数据是否像是一个单一的整体。

区块链是全网统一的账本，因此从逻辑上看是中心化的，这一点无可置疑。从架构上看，区块链是基于对等网络的，因此是架构去中心化的。从治理上看，区块链通过共识算法使得少数人很难控制整个系统，因此是治理去中心化的。架构和治理上的去中心化为区块链带来三个好处：容错性、抗攻击力和防合谋。

区块链与传统分布式系统的5点区别

作为一种全新种类的分布式系统，区块链往往被错误地当作是一个分布式的数据库或日志系统，实际上区块链与传统的分布式系统之间有着本质的区别——去中心化。现在我们来审视一下区块链与传统分布式系统的主要区别：

（1）一致性算法：区块链需要解决的是拜占庭将军问题，即网络中存在一个或多

个欺诈节点，可能会故意违反协议或传输错误的数据，因此区块链往往采用拜占庭容错的一致性算法（通常称为共识算法），如BFT、PoW、PoS等；而传统分布式系统只需考虑节点失效和通讯错误的情况，往往采用paxos、raft之类的一致性算法，这类算法不能对抗欺诈节点。

（2）中央控制方：在区块链网络中是不存在中央控制方的，没有一个节点可以控制或协调账本数据的生成，各节点通过共识算法进行协调，生成一致的账本。而传统发布式系统则往往是由一个机构进行控制，统一调度各节点参与运算。

（3）规则制定：区块链的规则就是共识协议，又称共识机制，共识算法是其中的一部分。共识机制一般是由一个人或一个团队设计制定，并开发出相应的程序，提供给社区使用。这一点似乎与传统的分布式系统一样，但区块链的共识机制的改变、升级是需要社区对此有一致的共识，如果不能达成共识，则任何人都可以实施硬分叉，另建一个社区、一条链。这就是共识机制的去中心化过程。

（4）计算模式：由于区块链节点之间不具有相互信任，因此区块链的业务计算是通过智能合约完成的，智能合约代码在网络上的所有（或部分）节点上同时运行，其执行结果通过共识算法在全网进行验证，通过这种计算上的冗余来保证计算结果的一致性。而传统分布式系统则无需考虑这些问题，同样的运算只需在一个或少数几个节点上进行，结果也无需其他节点验证，可以获得很高的效率。

（5）性能：区块链是以相对的低效率来换取公正，目前主流的公有链每秒只能处理几笔到几十笔交易，更高效的区块链软件正在研发之中；而分布式系统的性能理论上可以无限提升，目前已达到每秒数十万笔交易。

由此可见，区块链是一种特殊的分布式系统，通过解决拜占庭将军问题实现了非信任网络环境下的最终一致性，代价是相对较低的效率。如果剔除区块链的去中心化因素，由一个或几个中心节点来控制整个系统，则这种效率的牺牲变得毫无必要，区块链就退化为传统的分布式系统。

关于“多中心化”和“弱中心化”

这两个概念似乎是国人发明的，也许是孤陋寡闻，笔者尚未找到国外有类似的概念，也没有找到对二者含义的明确描述。这里只能根据字面意思来进行分析。

所谓“多中心化”，意思是在链上存在多个中心节点，还有其他非中心的普通节点，所有的交易必须通过中心节点进行处理。其实，这种模型与区块链的“全节点/轻节点”模型是一样的，关键之处有二：

一是在所有的业务场景下，轻节点是否有权任意选择一个或多个全节点来参与交易。也就是说，全节点之间是否可以自由竞争，如果存在一个业务场景，全节点是垄断的、排他的，这样的模型就不是“多中心”而是“单一中心”；

二是全节点的数量是否足够的多。如果全节点很少，则很容易实现共谋，形成寡头垄断，这样的模型仍然是中心化的。

至于“弱中心化”，就更像是个文字游戏，弱中心在某些场景下就是强中心、单一中心，否则就不能称其为“中心”了。

“去中心化”不等于去监管

人们之所以试图否认区块链的“去中心化”特征，或许是因为错误地认为去中心就是要去监管。

其实并非如此。监管与“去中心化”并不冲突，“去中心化”去的是中央控制方和中介方，而不是监管方。

区块链技术从来就不排斥监管，监管节点可以方便地接入任何一个区块链网络。由于区块链的公开透明特性，监管机构反而可以更加方便地监控整个系统的交易数据，而且由于区块链的防篡改特性，交易一旦发生后即不可更改、不可删除，那种数据造假蒙蔽监管的情况就不可能发生了，更有利于监管机构对市场行为进行监督。由此可见，区块链将成为监管科技（RegTech）的重要工具。

对于监管机构需要干涉交易的情况，如法院冻结资产等，区块链也提供了可用的手段，例如著名的以太猫游戏（CryptoKitties）中就有类似的设计。

CryptoKitties中设计了一个CEO角色，该角色由掌握指定私钥的用户所有，通过智能合约，CEO有权随时停止以太猫的创生、繁殖和交易，如果将该角色的私钥交由监管机构管理，监管机构就可以在必要的时候介入，对系统进行所需的控制。

这种监管机制仍然是去中心化的，因为所有的监管规则都事先写在智能合约里，即使是监管方也无法任意更改。这种去中心化的监管模式使得监管机构在获得必要的监管能力的同时，也必须依法监管，不能任意妄为。

去中心化是区块链最根本的特征

综上所述，笔者认为：去中心化是区块链最根本的特征，只有从去中心化的角度来考虑，才能找到真正适用区块链的应用场景，如中国银联跨行信用卡积分交换平台、苏宁金融区块链黑名单共享平台等。如果否认区块链的去中心化本质去寻找应用场景，则将会是缘木求鱼，最终用低效率的区块链技术实现了一个传统的中心化系统。

当然，区块链是去中心化的，并不意味着这个世界上只能有区块链。未来，去中心化的区块链网络与中心化的传统互联网是可以和谐共处、合作共赢的，中心化机构可以作为普通的参与方接入区块链，为区块链网络上的用户提供专业化的服务。