去中心化是区块链的精髓所在

人物简介

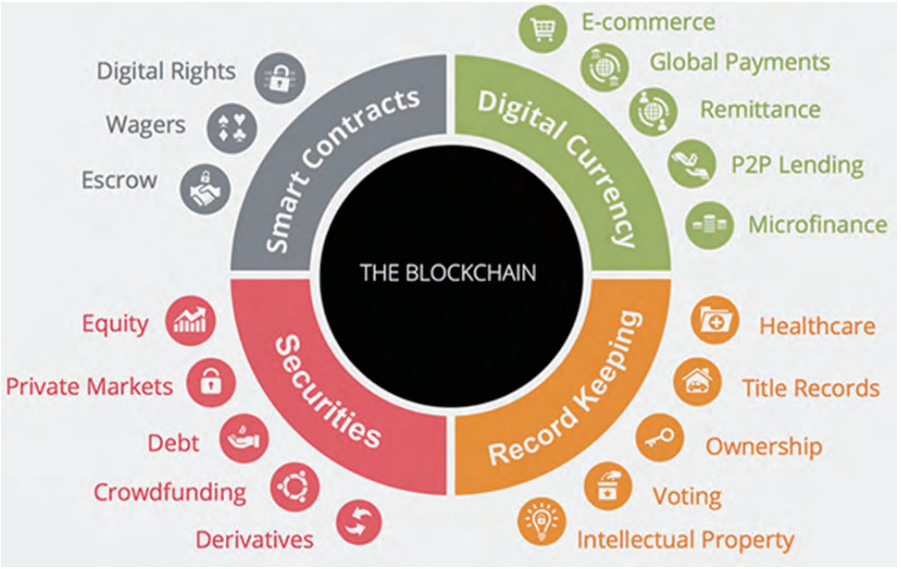
徐义吉

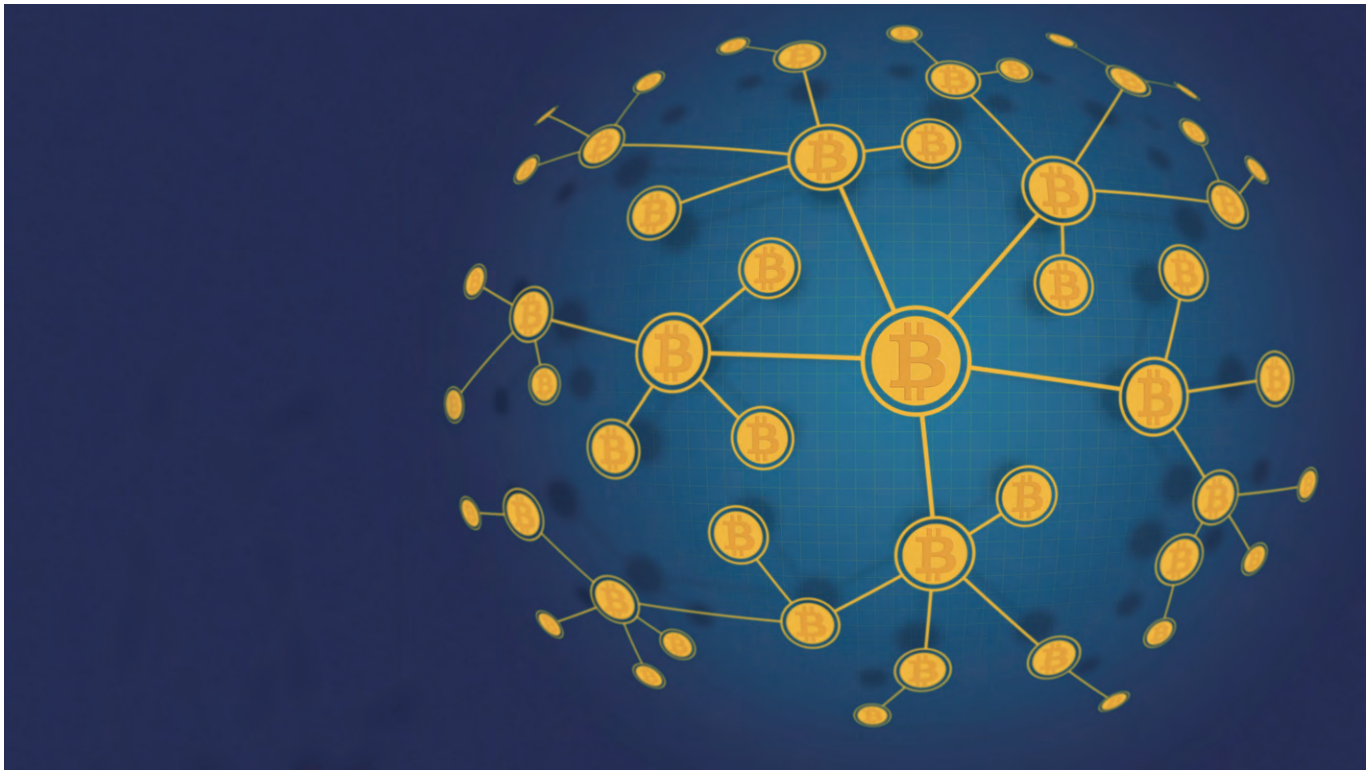
行业早期参与及贡献者，参与发起创办了“小蚁区块链”和“GemPay/竞付宝”项目。2013年开始发起“比特创业营”及数场比特币/区块链大型国际峰会，擅长区块链商业模式及产品创新，利用区块链作为底层架构的研究者。

文 徐义吉

毋庸置疑，区块链技术已经成为当前的热门话题和创新领域，除了很多来自比特币领域的极客和创业团队以外，也日益引发很多大机构的热切关注和深入参与布局。简言之，比特币的具体实现方式就是区块链技术诞生地，作为一种分布式共享账本，有着可靠、透明、可追踪、不可更改及数字资产化等特点。如下图所示，区块链的应用研究当前主要集中在诸如智能合约、数字货币、记录存证和数字证券化等领域。

与此同时，区块链技术和思想带来了大量的讨论和争鸣，面对很多人对于去中心化思想在区块链技术中是非必要条件的想法，笔者会在下文中重点讨论，提出一些自己的观点，进一步梳理出关于区块链技术为何产生及应用场景的看法和思路。





去中心化思想是非信任机制的产物

提到区块链技术，我们有必要回到区块链最初的诞生地，即从“比特币的出现”来看这个事情。在中本聪的论文里面，比特币最初试图解决的是多重支付或双重支付，即“双花”的问题，就是一笔钱花了超过一次以上。面对“双花”问题，传统系统的解决思路是依靠一套授权机制（中心化的权威）来层层管理和授权每次的转账和交易，这一点大家可以看现今的银行体系。

中心化的授权机制即是一种信任机制，即默认管理人都是尽责和完善的，其中可能发生的问题我这里不赘述了。然而中本聪设计的比特币采用了不同的思路，采用一种节点之间的共识，即彻底非信任机制来解决问题，当一笔交易被越来越多的节点记录确认后，“双花”的风险即无限趋近于零。在非信任机制里面，每一个节点都是平等的，没有任何特权存在，神奇的是在足够多的节点确认账本交易之后，产生了比特币系统自身的信用价值。从非信任机制的起点出发，中本聪或者说比特币无意中诠释了本来较为空洞的去中心化思想的一种实现。

在中本聪的论文里面，区块链技术其实就是对于这种非信任机制电子现金系统的具体实现。区块链本质上也是一些技术的组合实现方式，包括非对称加密、点对点网络和块链式数据结构等。从集合角度来看，去中心化思想是非信任机制的超集，非信任机制是区块链技术的超集。

最大程度博弈是去中心化思想的表现

在非信任机制里面博弈是非常重要且必要的，还是拿比特币来说，存在用户、矿工及开发者的持续动态博弈环境。通过挖矿POW机制来激励矿工们维护系统和记录交易，通过开源社区的方式来监督并且规范开发者的开发更新，通过自愿交易手续费的方式让用户更为有效地使用比特币平台。比特币没有想过要成为世界银行，作为一种具有颠覆式创新精神的网络电子现金系统来说，其主要目的已经实现，其网络及处理性能不足其实并非重点。

这种博弈体系是区别于传统系统的精髓所在，即是否承认平等博弈和无特权结构，如有特权结构，即使刚开始哪怕是一点权力也会影响博弈结构，导致整个系统变味，从而一步步走向中心化控制的老路。因为人们总是倾向于使用权力达到更加快速且高效的结果，姑且不问动机如何。强调区块链中的中心化要素即特权的情况可能是危险的。因为在责任不清晰的情况下，特权往往和利益关联且无法约束。曾经轰动一时的DAO项目，融资1亿多美元，其失败很大程度上是参与者选择性地逃避了“责权利”中的责，模糊了权，过分追逐利的结果。

我们看到，很大一部分人对于区块链技术持有一种工具化使用的态度，存在夸大区块链及智能合约的技术特点，而不太重视区块链应用模式的去中心化本质的情况。如果仅仅是工具化使用，还是否属于区块链应用的范畴？这个值得思考。笔者看来，区块链的工具化特点应该是其广义化的定义。而结合非信任机制的去中心化、开放、平等及博弈特点的区块链应用应该是其狭义化的定义。

区块链是一种开放式的场景应用

很显然，如果承认区块链系统是一种去中心化、非信任、基于博弈的体系，所产生的应用就应该是一种基于开放式场景的应用。进一步来说，第一是数据层面的开放，第二是共识层面的开放。区块链技术真正的魅力是在去中心化思想下，基于共识机制的开放式全网数据存储&处理能力。基本上联盟链和私有链都会涉及一定程度上数据及共识的不开放，这是引入特权造成的结果，其造成的进一步影响还有待观察。

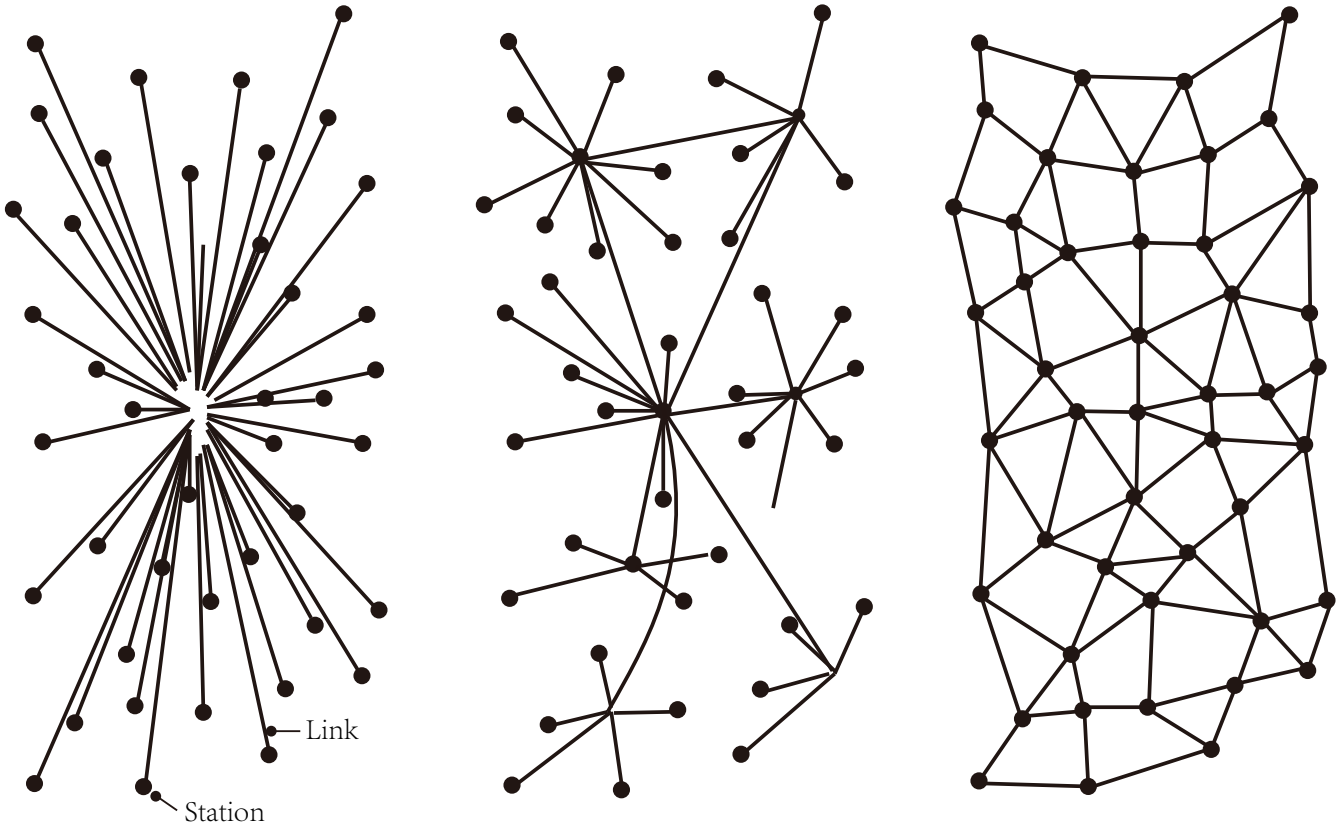
不得不再提一下比特币，某种角度来说，它是区块链应用的第一个范例。由于本质上是一种相对较简单的账本结构，有着固定的简单输入输出格式（记账）。但是今后是否所有区块链即有这种简单结构，笔者认为并不尽然。区块链的成功还需要面对以下问题：

第一个是输入、输出的问题。很多复杂场景下我们会面对更多的情况和变量，其实所谓的“智能合约”即是一种有判断条件的输入、输出机制。一旦输入源和输入内容更为复杂多样，其中必然面对更为复杂的博弈情况。

第二个是数据存储和处理的问题。比特币当前平均每10分钟生成接近1M大小区块，平均每秒处理交易的能力还在个位数徘徊。即使这样运行至今全网账本已经超过80G，如果要进一步发挥区块链的作用，所有数据不可能都放在链内，必须要有诸如“区块链数据中心”（Blockchain Data Center）等，通过侧链校验的方式来存储链外数据。同时，由于节点设备、网络带宽和共识机制限制，当前的处理能力也是严重不足，无法解决大规模数据实时并发处理需求。

笔者在谷歌搜索引擎反作弊小组工作多年，畅想一下，当所有的广告信息数据不再局限于一家公司，而是在一定保护隐私机制下的开放式数据体系，接受大家的共同维护和监督，是否平台还有作恶的可能？如果群体的共识算力POW能够进一步用于解决一直困扰广告系统的点击欺诈等问题，那该有多美好！

如果承认区块链系统是一种去中心化、非信任、基于博弈的体系，所产生的应用就应该是一种基于开放式场景的应用



CENTRALIZED
(A)

DECENTRALIZED
(B)

DISTRBUTED
(C)

实践出真知的思考

虽然当前区块链创新和创业已然变成热门话题，但还是在发展初期，离不开大家的不断实践与试错，同时结合各方观点的争论及总结，把技术、产品、商业模式一步步走踏实。区块链技术不是空中阁楼，只有在实践中才会有更进一步的反馈和进步。

关于共识机制的选择与优化，这方面有一定的思考空间。当前主要有POW（基于算力）和POS（基于权益）两种共识机制，并各有利弊，这里不做进一步展开，同时也有一些基于存储或者响应等共识机制。由于共识机制是维护区块链系统的根本保证，所以值得做出进一步探索、优化和提升的努力。

关于联盟或私有链的特权机制，纯工具型的私有链在这里不做讨论，因为只是一个内部系统而已。如果是联盟链或者引入一定博弈机制的私有链，其中的特权机制如何引入才不破坏区块链体系原来的完整和有效性，这个也值得讨论。

关于去中心化的终极形态，当前谈论的去中心化，是允许一些小的中心化节点存在的，未来是彻底的分布式体系？去中心化是中间状态还是终极状态？如果大家认为未来是分布式应用的天下，那么去中心化就是中间状态，很多尝试不是太超前而是做得还不够。如果去中心化是终极状态，这个显然并不可能。

相对其他的技术来看，区块链技术是如此令人着迷，从早期的极客到现在金融大咖都纷纷加入。其中很重要的一点是区块链技术是有灵魂的，这个灵魂或者说指导思想就是去中心化思想，或者又叫自由主义、奥派经济学等，有其一套较为完整的意识形态，而且具有对现有系统底层颠覆创新的潜力，着实令人激动，同时也激励大家勇于开拓及探索，结合一定的理论和实践突破，真正为区块链的长足发展和进步打下一个坚实的基础。E