去中心化的含义

一. 引言

在密码学货币的世界里，很少有词语像“decentralized”一样，既令人心潮澎湃，引发经久不衰的传播，同时又那么困惑。一方面，去中心化被当成区块链（尤其是工作量证明系统）最重要的成果；另一方面，也有人认为工作量证明并没有（甚至是不可能）实现去中心化，因为出现了大型矿池和强势的挖矿设备制造商。

本文第二部分将探讨现有文献中对“去中心化”概念的探讨；第三部分将提出我认为的“去中心化”概念；第四部分将讨论“去中心化”与“免信任（trustless）”之间的关联；第五部分将给出全文的结论。

二. 文献

Vitalik 在文章 *The Meaning of Decentralization* [1] 中提到，我们至少应从三个层面判断一个系统的属性：架构层（由多少计算机组成，可以容忍多少节点崩溃）、政治层（有多少人实际上控制这个系统）以及逻辑层（整个系统像一个单点还是一个集群）。Vitalik 认为如此方可涵盖各式各样的系统（如法律系统、公司）。此外，他还举出了去中心化会带来的几大优点：容错性、抗攻击性、抗勾结性。但是，为使这种定义成为一种有指导意义的学说，我们必须追问几个问题：（1）不同层面的去中心化定义是否足够清晰；举例而言，究竟应当以矿池的数量还是以参与治理的团体数量来评判政治层的去中心化呢？（2）不同层面的去中心化是否明确导向可欲价值的实现；比如，架构层的去中心化会必然产生出抗攻击性吗，逻辑层的去中心化会产生什么价值，还是基本没有价值呢？（Vitalik 其实回答了这个问题。他认为多数情况下逻辑层的中心化是好事，但也有人认为，在网络环境较差等条件下，逻辑层的去中心化是好事。）

Chris Dixon 的文章 *Whe decentralization matters* [2] 亦是常常被引用的一篇文章，在该文中，Chris 认为去中心化的价值在于以之为基础的创新活动不会被武断地遏止，在此，Chris 并没有明确定义“去中心化”（他甚至把维基百科也当成是去中心化的例子，因为其中的内容生产不是被有意组织起来的，而是自然生发出来的），但是可以意识到，要实现他的目标，Vitalik 意义上的架构层和政治层去中心化是必须的。

Tonny Sheng 是另外一位集中讨论“去中心化”含义的作者 [3]。他尤为反对使用节点数量来衡量去中心化程度，他认为包括上述两位作者在内，许多人对“去中心化”一词的探讨是有意义的，但仍没有解决根本的问题。他认为，最好还是别用“去中心化”这样模糊的词语了，应该探讨更清楚描述“抗审查性”的概念。

我相信读者已经意识到了，上述几位作者的探讨基本上没有涉及系统中不同节点的差别（Tonny Sheng 本来是最应该讨论这一点的作者，因为他探讨的案例是 EOS）。虽然这只是视角的选择，但我更愿意从节点开始分析，而不是概览整个系统。此外，上述几位作者的结论实践意义稍弱：我们并不能从中知道，为了让一个系统变得更加去中心化，我们可以做哪些改进工作。

三. ”去中心化“与系统的寿命

一如所有的写作者都是站在前人的肩膀上，我在本节中写下的观念受到了 StopAndDecrypt [4] 和杰出的区块链工程师 Jan [5] 的启发，尤其是后者。我可以毫不犹豫地承认：这些原创观念的贡献应归功于 Jan，我只是把它写下来而已。

迄今为止，大多数文献都在讨论分布式共识机制的意义、矿池对系统安全性的影响等，但鲜少有人讨论过这样一个问题：有寿命的节点，如何可能组成一个永生的系统？一个区块链系统固然能对外部攻击有一定防御能力，但内部的溃败呢？如果这个系统并不能长期存续，所谓的价值储存岂不也是泡影？

1. 背景

并不是所有类型的阶段都对分布式系统的健康和存续有意义：轻节点只从全节点处获取信息，对系统没有贡献；全节点（保存了所有链数据并独立完成所有验证工作的节点）则通过验证工作构筑了对无效交易和无效区块的防线。全节点可以是或者不是出块节点，出块节点（尤其是矿池）对网络的贡献与全节点的贡献不是同一种。

但是，人们必须投入计算机资源才能产生全节点，在当前的语境下，这些资源包括：计算能力（广义上的计算能力，而不是 Hashrate，用于验证）、硬盘、网络带宽以及内存。并且，此种投入不是一次性的投入，而是在链生长的过程中，不断变化的持续投入。举例而言，去年今日，运行全节点需要占用的内存，与今日需要占用的未必相同；去年一年产生的链数据大小，与今年产生的连数据大小未必相同。绝大多数情况下，上述四种资源要求中至少有一项会因区块链的普及而提高，比如因待打包的交易增多而产生更高的内存占用；增加区块大小也会要求更多带宽。

那么问题来了，如果有某些项的要求提高得太快，会出现什么情况呢？无法满足要求得计算机会发现自己无法同步最新区块，或者经常性地落后于最新区块，最后死亡——从网络中消失。节点是有寿命的。运营者主动退出、无法再满足资源要求，乃至是硬件损坏，都可以是节点死亡得原因。

2. 定义及其解释

因此，我在这里提供一种“去中心化”的定义，它将满足（1）足够清晰，价值指向明确；（2）具有实践意义；两种属性：当某个区块链系统在运行中的某个时间内产生的所有资源要求增量，均低于技术发展所产生的资源增量，则这个系统具备“去中心化”属性。举例来说，若某年的技术进步使硬盘空间可以增加 120MB，网络带宽增加了 10MB/S，计算能力上升了 1GHz，内存增加了 20 MB；与此同时，若某区块链系统在该年中产生的链数据小于 120MB，带宽要求上升了 5MB/S，计算能力要求增加不到 1GHz，内存占用的增量小于 10MB；那么，该系统是去中心化的。符合去中心化定义的系统必定能够：假设人们的偏好不变，随时间推移拥有越来越多的全节点，因为全节点的相对成本变得越来越低。而不符合该定义的系统，将在链自然生长的过程中加速全节点死亡。

此处需要解释的是：（1）不需要考虑全节点初始化需要的资源数量，因为只要在增量上满足条件，“去中心化”与其价值追求（即网络中拥有更多全节点）之间的关系便不会被打破；（2）也许有人会认为，可以使用“资源投入与个人收入占比一定的条件下产生的资源增量”来代替“技术发展产生的资源增量”，我认为这样替代也是合适的，只不过计量上可能稍微复杂一些；之所以使用“技术发展产生的资源增量”，是因为想到了摩尔定律，如此一来，可供的资源增量便不难计量；（3）使用“小于”而不是“低于其 1/2”并没有特别明确的理由，换言之，可以把它视为一个心态问题——我并不介意有工程师对此要求更严苛一些；只要满足“小于”这个条件，上述价值便可产生出来；（4）之所以假设人们的偏好不变，是为了这个定义的实用性：毫无疑问，如果人们的偏好会改变（这当然是实情），达成上述价值所需的条件（即所需资源的增量与实际产生的资源增量之间的关系）会变得更严或者更松，但我认为一位工程师实在没有理由断定人们的偏好会往哪个方向变动，即便可以预期这样一个系统会促进经济发展因而改变人们的偏好，也不是一个理论上的理由；再说一遍，我并不介意有些人对此要求更高一些；（5）我同样不怀疑，这样的定义忽略了许多细节，比如，也许，内存也许不仅有大小的区别，还有类型的区别（我不懂硬件），但添加这些条件不会改变其中的逻辑：所需资源增量小于可供资源增量；这也是为什么我认为可以提出这个定义；（6）终极而言，考虑全节点而不考虑出块节点，是因为全节点才对网络安全性有决定意义，是全节点的存在约束了出块节点的行为，而不是相反，具体缘由可见 Jan 的雄文 *Don't Trust. Verify.* [5]；显然，只有 100 份账本的货币，和拥有 1000 份账本的，即便名义上是同一种，实际上也不是同一种。

3. 该定义的不可消除性

众所周知，现在有公开是开始考虑全节点的激励问题。当前，在比特币和以太坊网络中，运行全节点是没有直接收益的；虽然部署全节点是应用开发和服务提供商业务中的一环，但在大多数情况下，运行全节点是自发行为，没有收益。但全节点又确实是有意义的，因此有人设想为运行全节点提供经济激励，来增加全节点数量，提升网络安全性（相应地，本文提出的“去中心化”概念要求会变低甚至不再存在，因为不再依赖自发的部署行为）。

在此我想挑战一下此种观念，我认为这并不能解决问题。因为，一旦要为运行全节点提供激励，就免不了要创建一套新的账本，用来度量、记录全节点的贡献并分发收益，这一套账本也需要传输、计算和存储，那么让谁来存储和计算这份账本呢？即便你可以说，就让这些全节点自己来承担呗，他们也确实需要投入额外的资源，这部分额外的资源又是没有得到定价的；如此而已，不可穷尽。实际上，这个结论就隐藏在当前出块节点及其内涵中：出块节点必须是一个全节点，但他们是因为出块而获得奖励，不是因为验证而获得奖励；一旦矿池模式出现，就会有许多节点从网络中消失，退化为运算设备；当人们发现提供其它资源（及其组合）也可以获得奖励，很可能又会有新一层类似矿池的层级出现，而那些原本的全节点也退化为计算设备或者硬盘设备，那些与新型矿池运行同一种客户端软件的节点仍然不能得到奖励。

如果说对全节点的激励并不内置在协议层，而变成是比如说全节点向轻节点一对一收费，那么就跟当前的状态没有区别了——当前的矿池也是这样做的：运行全节点，向矿工收费。

综上，我在此证明的是：一个公共账本系统中总会有一部分资源是没有得到系统本身的定价的，试图为其定价会要求投入另一些不能得到系统定价的资源，因此一样会存在未得到支付的资源提供者，一样会面临所需资源增加的问题，一样会存在“中心化”与“去中心化”的区别，一样要面对链生长对这部分节点的影响问题。

总而言之，我认为“去中心化”是公链中一个不可取消的元概念，内在的原因是出块和验证在公共账本系统中的不同角色；而这个概念捕捉的是节点寿命与公链存续之间的关系。因为节点是有寿命的，一个公链系统必须是去中心化的，否则便会不断枯萎。就像个体与自身所处文化的关系一样，个体毫无疑问为文化的生发和延续做出了贡献，而文化若不断使个体的处境变得更加艰难，这种文化早晚会崩溃。有肉身的个体能组成长生的文化，在于文化真的能让他们过得更好。

四. “Decentralized”与“Trustless”的关系

“Trustless（免信任）”是“Decentralized”的必要条件。

免信任的含义是：在任何时刻，验证系统当前状态的形式正确性（correctness）无需对某个有形实体的信任，而只需要对某一系列抽象规则的知识。这些规则为判定 correctness 确定了一些不依赖于对第三方信任的标准。此外，因关键的历史事件而产生的区块检查点（如创世块以及 The DAO 硬分叉）与“系统是否免信任”无关。这些检查点只是协助人们选择他们愿意选择的链，而不影响系统的属性。至于如何将检查点的存在及其意义公示出来则更像是一个治理问题。换言之，免信任解决的不是“你在哪条链上”的问题，而是“你所在的这条链（不管叫什么）的属性”问题。

因此，如果一个系统不是免信任的，那么人们不需要也不会（有的时候也许不被允许）去运行全节点，讨论“系统是不是去中心化”也就没意义了。而一个系统即便实现了免信任，也未必就实现了去中心化。

五. 结论

我认为，一个具有实践意义的“去中心化”概念回答的不是一个系统在功能提供方面的问题，而是一个免信任的系统与外在于这个系统的其它资源供应系统之间的关系问题。符合该定义的系统可预期拥有更多全节点，最终实现系统本身的长期存续。

---

[1]: https://ethfans.org/posts/the-meaning-of-decentralization

[2]: https://medium.com/s/story/why-decentralization-matters-5e3f79f7638e

[3]: https://orange.xyz/p/207

[4]: https://hackernoon.com/the-ethereum-blockchain-size-has-exceeded-1tb-and-yes-its-an-issue-2b650b5f4f62

[5]: https://orange.xyz/p/186