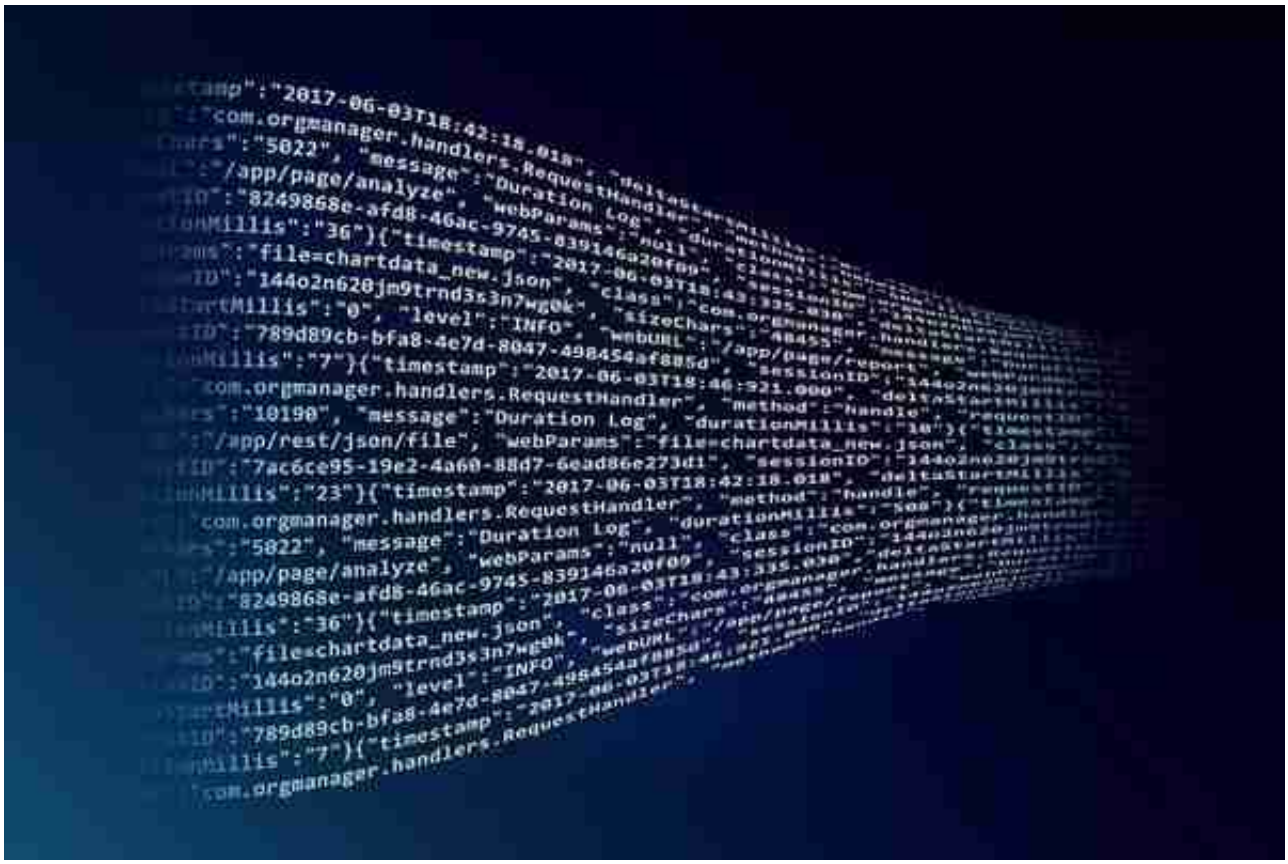
去中心化（Decentralization）是区块链最重要的技术特点之一，也是其最具争议的概念之一。许多对于区块链的迷思与误解，都与对去中心化的认知不清有关。因此，在本周 DeepHash 专栏，创新工场执行董事、分布式系统专家王嘉平从他在知乎上对一个提问的回答开始，进而一连串地思考了去中心化这一概念，包含去中心化后是否又会出现新的中心？怎么看待新的中心出现？区块链什么可以去中心化？什么不能去中心化？以及加密货币挖不挖矿对去中心化与否可能产生什么影响？最后他将相关思考写成本文，内容深入浅出，穿透问题本质，相信也能让许多读者改变对区块链技术的看法。



2016 到 2018 年间，币圈造就了一种吹牛就可以圈钱的商业模式，所有上天入地能想到被吹的都拿来用上了。不论经济逻辑、无论趋势方向、无论时间窗口。

“去中心化” 就是其中一个被吹上天的概念。区块链作为分布式网络系统的一类，其去中心化是一个技术指标，有非常明确的定义，仅指代特定技术栈层级中的一些特性。但却被某些人偷换概念，拿来在社会的各个层面进行意淫和吹嘘，有说可以改变生产关系的，有说社会治理的，有说分配制度的当然这种搞法也不长久。

有人问，有了区块链技术之后，会不会形成新的中心？答案是会的，一定会有新的中心。但问题的根本并不在此，而是在于新的中心对公平和效率有没有伤害？有什么样的伤害？无论在技术层面，还是更广义的社会层面，中心化或去中心化只是组

织方式的一种形式、一种手段、和一种方法，并不意味着绝对的好与坏。

区块链作为一种新型技术，是去中心化网络系统，但这是技术概念。这个概念和大众关心的去中心化，其实根本不是一回事儿。对于大众关心的中心化问题，权力/控制力的集中，资源/财富的集中，区块链提供了一些工具，缓解一些中心化带来的问题。但区块链更多的是限制中心化的坏处，约束新的中心作恶的可能性，而不是消灭中心。

文明各个层面出现中心化是必然的，而一代一代的新技术，并不是消灭中心，而是有些增强了中心的能力和范畴，比如人工智能和互联网技术，另一些则是约束了中心的作恶可能，比如密码学技术和互联网技术。(不是笔误，互联网技术两边都占了...)

中心化现在常常被大家看成是一个不好的东西，殊不知我们人类文明可以从动物界脱颖而出，直到发展成现在的高度，都是得益于中心化，得益于其不断扩大的规模，得益于其不断提高的能力。这个好处能成立的本质原因是生产力有限，我们需要中心化来提高效率，减少摩擦，将为数不多的生产力充分发挥出来。

当我们需要生产力发挥到极致的时候，中心化的优势就尤为明显，例如战争时期。中心化的本质是为了效率，但是到了某一天，效率不再是瓶颈的时候，中心化的负面问题便凸显出来了，中心化对公平伤害便被大家更多地关注了。

但问题是，中心化是不是一定会伤害到公平呢？其实未必，包括区块链在内的去中心化应用，都试图在给出这样一个答案，用底层架构的去中心技术，来约束其上可能出现的业务中心、权力中心、资源中心等，对公平性带来的伤害。也许区块链的答案依旧不够理想，但是可能会比之前要好很多。

当然，公平可能是个很模糊的概念，每个人心中有不同的解读。在我这里的讨论中，我暂且框定一个具体的和商业活动有关的定义，以避免误解。我这里用这样的标准来衡量公平，即旧的中心有没有、或者有多少超越规则之外的控制力、影响力和竞争手段可以去扼杀和阻止新的中心的产生。

中心的出现是必然

在人类文明出现之前，整个自然生态系统大体上是去中心化的，所有生物面对自然规则是被动地适应环境。在社会性生物出现之后，群体集中给很多种群带来了生存的优势，其中也包括人类的祖先。人类出现后则有了一些本质的变化。原始技术的出现让人类开始部分地理解自然规律，并利用这些规律逐步大规模主动改造环境。技术的演进，生产力的发展，人类总体就是相对于自然生态系统中的一个中心，一

个无与伦比的强大中心。

在地球上，不再可能有任何一个生物种群可以作为新的中心而出现，对自然生态系统而言，人类已经将公平抹杀殆尽，残存的也只有偶尔的施舍。即动物保护之类的。而游说者的论点也是为了维护生物多样性，为了生态环境的鲁棒和稳定，说到底还是为了我们人类自身的利益。

人类能走到今天这样的中心，本质上是因为生物种群之间生产力发展的巨大差异。文明的发展速度远超生物进化的速度，人类成为第一个解锁文明科技树的种群以来，瞬间用几千年的时间，秒杀了其他生物积累了几亿年的生存优势，而成为了生态系统的中心，并且彻底扼杀了其他生物种群成为新的中心的可能。

同样在商业环境中，也是一样的故事。不同个体，不同团队或公司之间发展的差异性，是每次技术更替时出现中心的本质原因。这个差异越大，发展速度越快，出现的中心就会越快，越强大。

互联网的中心化和去中心化

TCP/IP 以及路由寻径是互联网的根基，这是彻底的去中心化架构的技术。所以这项技术突破了不同的国家政体和意识形态，连接了我们整个世界。这是通讯去中心化架构的伟大胜利，当然成事的不仅仅是这个技术特性，也和那个时期的经济全球化进程这个时间窗口契合。伴随那一次技术更替，其上的商业便有了新的规则和测度。这是花了好长时间大家才弄清楚的。一开始也有很多人像如今区块链萌芽时期一样，将技术理念无限拔高到社会的层面、制度的层面、生产关系和人类组织方式等等。

互联网的去中心化是通讯的去中心化，且仅此而已。在通讯之上，从域名系统、CA 证书中心、Web Server，一切都是中心化的技术架构，最后到现在的云计算和 CDN，又将中心化的技术架构推向了极致。

我们看看这最终导致了什么结果？互联网的通讯资格没有壁垒，谁都可以在互联网上提供内容和服务。所以初期这是一个非常扁平化、非常分散的世界。那么问题来了，用户需要从中找到自己要的东西，就会非常困难。与之对应的，那就是搜索。因为中心化的索引，可以高效地发现用户希望找到的内容。同时，这个业务是具备规模效应的，更多地索引，更多地被使用，可以找得更全，找得更准。这样，第一个扎实的中心出现了。

搜索巨头可以扼杀和阻止其他新的中心出现吗？可以，但没有超越规则的手段。正因为互联网的底层通讯架构是去中心化的，即使 Google 占据了很大的用户流量比

例，也无法在通讯层面狙击其它新型的互联网服务，即使和运营商勾结也还是会相当困难，并且极易被发现。所以，当 Google 意识到社交服务的重要性的时候，搜索巨头的地位并不能帮它打赢这场竞争，最终败在 FB 的先发优势面前。虽然 FB 可以抵御 Google Plus 那种同质化的竞争，但是面对异质竞争，其自身的社交巨头地位也同样助益不大，无法阻拦来自移动互联网的新的中心，如 Snap。

而另一方面，互联网在通讯架构之上是中心化，直接导致了用户的行为和数据及其用户之间的社交关系，虽然都是用户贡献的，但是全部垄断在这些巨头手中，并且是这些公司盈利模式的核心，竞争力的根基。平台有绝对的控制力阻拦用户将自己的数据搬去一个新的平台，和这些相关的领域，没有新的中心出现。新的中心需要在服务和体验上有绝对的优势，以至于用户愿意在这个新的平台上面从零开始。

去中心化应用，并不是有了区块链才有的，当然我这里并不是指基于 Smart Contract 的 Dapp。一个经典的例子就是
Bittorrent，曾经占据互联网一半流量以上（2006）。

自 DHT 之后（磁力链接），Bittorrent 成为一个彻底的去中心化的内容发布和下载工具，这个工具形成的网络不被任何人控制，没有数据垄断、没有直接的隐私问题，不过用户关心的是我可以更快更方便地下载电影。最后那个同名的公司失败了，Bittorrent 究其根本，只是一个工具，0 运维成本，完全社区化运作。在那个时代，这样的服务提供方式，无法建立有效的盈利模式，开发团队无以为继，最终连创始人也失去信心。

区块链的去中心化和中心化

基于互联网，区块链的去中心化天生具备通讯的去中心化，然后又基于点对点的网络架构，所以用户的访问方式和接入网络的方式也是去中心化的。然后区块链还去中心化了用户的账户体系、用户的行为，和数据流转与存储，另外就是业务逻辑的执行过程。而最后一点正是区块链真正的核心价值，详细可以参考这篇〈区块链到底有什么了不起〉

然而，区块链能做到的去中心化，仅限于此。除了这些部分，很不幸，其它方面依旧是中心化的。

首先，最大的中心化部分是业务逻辑的制定，也就是项目方。数字货币需要集中交易，才能尽可能汇聚流动性；PoW
共识中矿工需要规模化运营才能拿到更便宜的电，更便宜的矿机或者显卡；PoS
共识中用户需要汇聚资产给大的验证者才有相对平稳的收益（这个道理和 PoW 矿池的作用雷同），这些都是显而易见的中心。区块链的技术和生态架构一直在演化

，相信之后还可能有更多成为中心的角色。但是这些中心都将受到底层区块链去中心架构的约束，未必是为所欲为。

项目方是中心化的，但是并没有太多作恶的机会，也没有超越规则的竞争手段来打击其他的项目方。这个约束得益于，区块链不可篡改的核心特性。要注意，区块链不可篡改的关键是业务规则和逻辑不可篡改，而并不是账簿。

很多中心化服务的套路都是先用非常优待的规则骗取用户入坑，然后渐渐修改规则，甚至还不易被发现，同时还利用数据的垄断特性，绑架用户。这样的事情，要在区块链平台上的项目里头实施就会困难很多，至少一定无法不被发现。

中心化的数字货币交易所，就是个大问题。中心化数字货币交易所是一个中心化的互联网应用，其本质和区块链毫无关系。区块链在其中仅仅是充当了支付手段，是投资者进场和离场的途径。不过这个去中心化的支付手段，绕开了传统的受监管金融体系，使得数字货币交易所有顽强的生命力。

中心化数字货币交易所应该问题蛮多的，不过这个方面我不是专家，只能拍拍脑袋猜猜。小则可以抢先交易，歧视性撮合，大则可以凭空增发操纵市场，在 K 线图上涂鸦。（各位交易所大人，我只是说可能，您的交易所一定是好的，公正的，高效的！）有些甚至很容易实施，并且不被发现。当然现在有个小小的趋势，就是去中心化交易所，至少将清算在链上完成，避免了凭空增发的可能性。

共识算法的头部聚集

听起来不可思议，作为区块链这样一种去中心化技术的核心，共识算法对待其参与者却不是平均的（当然，公平和平均是两码事儿）。在 permissionless 系统中，要保障出块权分配不受女巫攻击（Sybil Attack），共识算法在逻辑上需要按照参与者的某种权重来等比分配出块的机会。这种权重通常源自于某种稀缺资源，在 PoW 系统中，这个权重是算力；在 PoS 系统中，这个权重通常是资产抵押的数量。也就是说，出块权是同某种稀缺资源相锚定的，否则将无法抵御女巫攻击。

值得提一下的是，所有的拜占庭算法（BFT/pBFT）都不是完整的 permissionless 共识算法。因为 BFT 类算法，本质上是要 permission 的，仅限于委员会成员。所以为了构造完整的 permissionless 共识算法，所有类 BFT 算法都有一个前置的算法，周期性的选择一个委员会出来，例如用 VRF（可验证随机函数）。

不客气的讲，这其实就是一个 hack，不过还算合理。而这个委员会的选择过程也

不是对所有参与者机会均等的，也是机会和抵押数量成正比，才能抵御女巫攻击。当然也可以看到有些白皮书，采用机会平均的选择，加上所有参与者定量抵押、后验罚款的方式。在外部做空机制和高倍杠杆存在的情况下，这类算法是完全无法保障安全性的。

正是因为对这种稀缺资源的依赖性，无论 PoW 还是 PoS
都会出现出块权的头部聚集，当然两者头部聚集的角色不一样。PoW 的情况大家已经看到了，算力会向大矿场和矿池聚集。只要这种算力具备高度粘性，这种聚集，未必是中心化的。这里说的高度粘性算力，指的是 Bitcoin 那种由 ASIC 芯片加速挖矿计算的算力。由于部署这种算力的设备不具备通用型，那么矿工一旦投资建设这种算力，那么这个算力是无法抽调用在其它链上的。这就是所谓的粘性。

例如 51% 攻击，在矿工具备粘性的情况下，其实这并不是主要问题。用双花攻击来获利，对有粘性的矿工来说是一个杀鸡取卵的事情。因为一个头部矿场如果发起 51% 攻击，那多半这个链是要废了，以后也没得挖了，挖矿设备就要变成废铁了。所以这里的粘性指的是矿工对矿机和矿场的不可转移投资。

从这个意义上来说，采用 Anti-ASIC
算法的链，是在作死，这将使得矿工采用通用设备进行挖矿（例如 GPU），把本来不可转移投资变成了可转移投资，矿工就可能具备了干一票走人的动机。如果大家认为这是一种中心化，可以扩展阅读，吴忌寒总前阵子的观点（注 1）。

PoW
采用链外的力量来保护链的安全以及链上的资产，是一种更为安全的做法。而 PoS 是用链上的资产来保护链上的资产，这种自己维护自己的方式，用陆奇总的话来说则是 drink its own pee。

我们具体看看，PoS 情况下，会发生怎么样的聚集。由于 Stake 是出块权，那么大家会愿意出借手中的币给大型的验证者，以获得出块奖励，而且越大型验证者出块奖励会越平稳，收益体验更好。那个这个大型的验证者会是谁呢？以现在的整个生态来看，只有两种中心化的数字货币交易所，或者是超大用户规模的钱包。无论是哪个，都比算力聚集更为糟糕。Stake 的聚集直接导致了一种不良的治理结构，交易所将又是运动员又是裁判。同时数字资产相对于矿机来说是更具流动性的投资，PoS 主链的验证者将更不具粘性更为投机。

说到这里，很明显我是站在 PoW 这边的。从安全角度来说，只有 PoW 是真正的 permissionless 共识算法。因为这个算法太纯粹了，太简单了，直接达到 51% 的防御壁垒，所以大家很少听到 PoW
被改进，唯一一次实质性改进是为了抵御自私挖矿的 Ghost

Protocol，那也只是针对高分叉率的情况下的特殊处理。

越是简单的算法，出现安全问题的可能性就越少。反观 BFT 类算法，就复杂得多，各种变种也多，安全性有待长期运行的考验。至于 PoW 费电，大家看看大型矿场都建在哪里，用的是哪里的电，就会明白，PoW 更多的是更好地利用了产能过剩的电，而不是浪费了更多的电。近期也有很多 Staking 经济的声音，但其实这个事情和共识算法本身没有直接关系，无论 PoW 还是 PoS 的链，都能够实现和运行基于 Staking 经济模型和激励机制。

区块链可以去中心化什么？不能去中心化什么？

可以看到一个有意思的地方，区块链的去中心化底层是有一定能力主动约束上层业务的，这将有可能让这新一代的平台上的业务，虽然具备中心，但是中心的作恶可能被大大约束，从而兼顾效率和公平。也正是因为这个原因，之前互联网的运营手段和商业模式，在区块链上很可能无法奏效。正如，互联网无法延续软件时代的运营手段和商业模式一样。

区块链不是万能药，更高社会层面的中心化，本来就不仅仅是技术能解决的问题，二八原则永远会在。但是中间有些层面是能够被区块链彻底去中心化的，从而使得其上出现的新的中心不那么能为所欲为，尤其是现在互联网中的那些中心化部分，如搜索，如社交。当然现在的区块链还远没有能力承载这样大体量的业务，但是有朝一日，会的。