

# 去中心化的未来

作者:Roberto Capodieci, 时间:  
2021 年 10 月

在本篇贴文中，我将探讨去中心化和区块链。首先，从我们大家都熟悉的一点说起……

我们都经历过狂热的首次币发行 (ICO)。也听说过类似于下文的初创企业宣传语：“我们是一家以客户为中心的**组织**，通过利用设计思维实现物联网、云计算、大数据、机器学习和人工智能的价值，推动区块链相关企业的数字化变革。”

也许你会好奇这些企业是做什么的，结果是又一款代币：“我们发布了一款叫做 DecibelCoin 的新代币。它的工作原理是什么？你只要对着麦克风大声喊就能赚钱……它是一个……准备好听双关语了吗？它是一种声音投资。”我们为这个笑话做一个 NFT（非同质代币），把它放在交易平台“OpenSea”上卖。

我们来看看如何做到这一点，才能更好地理解未来的方向。我们生活在所谓的信息时代（亦称“计算机时代”或“数字化时代”）。人类经历了石器时代、青铜器时代……没错，从人类起源说起……科技从铁器时代开始发展。我不是说穴居人制造微芯片，而是一些基础技术持续演进导致了几千年后的工业革命。

工业革命分为多个阶段（对开发者而言，我们谈的是数组的数组）：第一次工业革命基于运用于机械化生产的蒸汽动力，第二次工业革命基于运用于实现大批量生产的电力，第三次工业革命基于运用于智能化生产的电子技术。

如今我们正在经历所谓的“第四次工业革命”，但我更愿意称之为“信息时代”，它立足于用于服务和产品的数据与信息。信息时代也可划分为多个阶段（再次以开发者为例，我们谈的是数组的数组的数组）：在初始阶段，模拟内容开始以数字格式储存和共享；在第二阶段，该数字内容可通过网络发送和共享，并最终出现在互联网上；在第三阶段，个人与企业通过互联网出售和提供服务；最后，在刚刚开始的四阶段，社区与社区之间互相提供这些产品与服务，即去中心化阶段。

言归正传。

去中心化系统的协议很快会开始取代当前互联网上主流的集中式网络服务协议。应用不会连接至部分中央提供者的 API，而是直接与对等网络交互，我们将向去中心化互联网迈进一步。当我们连接至全球网状网络的一个随机热点，而不是有效充当计算机与互联网其余部分之间中间人角色的 ISP 时，那么即便是作为基础设施的互联网，最终也将去中心化。

去中心化的工具有多种，区块链是当前使用的重要技术之一。众所周知，虽然比特币的优势让区块链概念进入人们眼帘，但它只是对等网络上运行的众多去中心化服务之一。区块链的采用

没有止步于加密货币用例。这是因为区块链协议是开放的，任何人均可在该协议上实现、复制和修改，最重要的是优化。请注意，我们讨论的是底层区块链平台，而非在此基础上开发的应用程序。下文引用了 Coinbase 联合创始人弗雷德·埃尔萨姆 (Fred Ehrsam) 的一段话：

区块链是数字有机体。它如同生物有机体通过其 DNA 的变化而成长一样，区块链协议通过其代码的变化而发展。和生物有机体一样，能够存活下来且茁壮成长的区块链项目最具适应性。

发展演进势在必行。

大多数区块链技术、共识机制和交易类型均考虑了加密货币。进一步深挖就到了区块链如何保障安全的核心，在非加密货币相关用例中采用或当管理的所有权价值高于区块链内部经济价值时，会使这些平台变得脆弱且容易遭到攻击。简言之，在攻击成本的投资回报率使攻击成为可能之前，区块链是安全的。

举例说明，利用当前共识机制，那些管理的所有权价值显著高于区块链自身市值（比如仓单等所有权凭证）的区块链，以及用于去中心化数据管理，对加密货币无实际需求（比如医疗记录等文件流）的区块链容易遭受攻击。

为了去中心化并真正实现分散管理，区块链不应有管理员、中央控制器或机构，甚至没有具影响力和充满魅力的领导。在区块链中，每位用户拥有并控制其数据。区块链取缔相信第三方的需求，所有发生过的事情、发生时间和确实发生过的保证均有密码证明，遵循区块链核心软件中硬编码的协议规则。不遵循规则的交易不被处理。假如我没有 10 个比特币，就无法发送。

必须将区块链视作去中心化系统，该系统配备加密保护数据转换的工具。区块链令数字资产的稀缺性，甚至单一性成为可能，这在十年前的数字世界是不可能的。此外，区块链还使得就某数据的当前状态达成共识成为可能，而无需依靠任何第三方告诉我们该数据的当前状态是什么。

在不久的将来，区块链有可能从根本上改变我们共享信息、买卖物品以及彼此之间和与机构之间互动的方式。我们将利用区块链证明自己的身份，甚至验证所吃的食物到药物等一切事物的真实性。最重要的是，人们拥有并控制属于自己的数据。

我们都知道，隐层技术（比如数据库）往往是用户最难理解的，因为看不到它们！区块链也遇到了此问题。由于与据称使用加密货币从事的非法活动经常存在负相关，这让该技术的采用变得更糟。积极正面的叙述是加快区块链采用并取得必要信任所必需的，从而让该技术被多个行业所接受。

此外，“区块链”正如新兴的云计算、大数据或 AI 一样：太多人将其用作一个流行词，甚至不知道他们说的是什么。区块链应用于解决实际问题，但遗憾的是，人们常常出于营销目的，将其强行塞进无实际需求的项目。

一个真正有效的去中心化系统不存在集中式所有权或控制点，因为它属于运行其 P2P 网络节点的人们。公司创建真正的去中心化系统并将其移交给公众，不保留系统的任何控制权。此外，也许拥有该系统经济的一大部分。节点应用程序代码掌握在开源社区手中，整个项目是公开的。

一旦系统公开且系统代码开源，则该项目真正实现了去中心化：支持项目融资的公众成员直接对开源社区完成的开发流程做贡献。运行系统对等网络中某节点的成员通过运行该网络、创造集体价值和强化系统，对该系统本身作出贡献。他们应该从用户活动中获利。

当用户为 P2P 网络中消费的服务付款时，这些款项应分给 P2P 节点所有者。事实上，节点操作员必须就处理能力和运行其节点所耗成本获得补偿。当前机制仅奖励创建新区块的账户，网络的其余部分仍未得到补偿。正确的做法则相反：惩罚本应创建区块却没有创建的账户！

请注意：我并不是说企业不应该有利用去中心化服务获利的办法或机会！到现在为止，我谈的是底层，区块链平台本身需要真正的去中心化。

在开放式公有链上创建的去中心化应用程序可以有中心控制点、管理账户、用户等级和具体货币化方法。从混合应用(仅将区块链用于其部分流程)开始到 DAO(完全在区块链上运行的应用程序)，这是一个待实施和正在实施的服务世界。

其中大多数去中心化系统将取代现有的在线服务和应用程序，但其他系统是新的，如果没有一个用于运行的去中心化平台，它们将永远没有存在的机会。区块链及更广泛的去中心化带来了巨大机会，我们在部署新项目时必须聚焦并加以利用。我给大家讲一则故事，本人认为这是近代史上错过的最大去中心化机遇之一。

我们都知道 Torrent 吧？不知道？肯定没有人做过这种事，Torrent 是一个网络对等协议，最常用于下载盗版电影与音乐。Torrent 具有去中心化性质，原因是它是一个对等网络，也是首个当局无法关闭的文件共享系统。Torrent 是当今区块链的基础。（如果运行稳定的协议）区块链无法关闭。

在本文末尾，我将履行承诺讲述一则有趣的小故事。标题：“音乐与电影行业失去的机遇”

消费者一直购买音乐和电影。(更多罪犯)为家人和朋友拷贝音乐磁带和 VHS 录像带。该行为被人们所容忍，原因是复制版音频和视频质量降低，让复制链变得很短。

回到文章开头：随着我们进入信息时代的第一阶段，内容变得数字化，人们开始复制 CD 和 DVD。此时质量尚未降低，

电子版与原件质量一样好。因此，人们对电子版的容忍度低很多。然而，情况开始变得糟糕。

进入信息时代的第二阶段时，紧随而来的是巨大惊吓、尖叫、人们在音乐与电影行业办公室走廊上绝望地奔跑、管理层抓掉了头发（我猜测），现在可以从互联网上复制数字内容。音乐和电影行业游说政府关闭用于交易盗版内容的任何网站、论坛和在线文件存储工具。Napster 最后一个倒下。音乐行业对他们提起诉讼，Napster 收到禁令，被勒令于 2001 年 7 月关闭服务器。

Torrent 随之而生：一个无法直接关停的对等网络。由于 P2P 软件盗版也很猖獗，音乐与电影行业现在联合软件行业游说政府逮捕最终用户，并称他们为“盗版者”。根据美国法律规定，知识产权侵权可能导致最高被处 5 年监禁和 25 万美元罚金。这是复制一份的惩罚。复制一首歌或一部电影记为侵权一次，非法下载 MSWindows 意味着其中每个应用程序均构成一次侵权：计算器应用、记事本应用等。

青少年仅因为从 Torrent 下载盗版软件最终被判多次无期徒刑。音乐、电影和软件行业的这一举动是否成功遏制了 P2P 盗版行为？没有。他们是否获得公众的同情？没有。他们太专注于和假想的敌人战斗（如果不理解此类比，请阅读塞万提斯·萨维德拉所著的小说《堂吉珂德》），我认为他们错过了一个良机。

即，通过甚至不需要他们管理或付费的网络，在地球上每一个地方（从大城市到边远国家的最小乡村）销售其制作的内容的可能性。他们要做的仅仅是通过 Torrent DRM 锁定内容分享、提供免费预览以及解锁 DRM 的付费途径。虽然曾经面临完美的冲浪潮头，但他们却错过了。

几年后，随着比特币与区块链的出现，被扰乱的行业并非音乐和电影行业，而是全球金融业。我很高兴这次的反应有所不同，正如我们所看到的，金融行业创新获得了支持。

让我们一起举棹扬帆弄潮头，那里有无数机遇，未来任重道远！