

区块链：创造信任的机器



英国《经济学人》周刊2015年10月31日的封面文章

比特币有着一个**不好的名声**。这种去中心化的数字货币，由一个庞大的计算机网络所支撑，因其价值波动较大，支持者们的热情和它脱离方向的应用，如敲诈勒索，暗网集市上购买毒品、雇佣打手，比特币的声名因而显得有些狼藉。

这是不公平的。一比特币的价值已经相当稳定，今年大部分时候，也都维持在了250美元。监管机构和金融机构们的怀疑，已经让位给了热情（欧洲联盟最近承认它为货币）。但是，最为不公平的是，比特币的阴暗形象，使得人们忽视了“区块链”的巨大潜力，这种奠定了比特币的基础技术。**这一创新所承载的意义延伸，远远超出了加密货币。**区块链让人们在互不信任，并没有中立中央机构的情况下，能够做到互相协作。**简单地说，它是一台创造信任的机器。**

区块链的食物链

想要了解区块链系统的能力，以及它们能够做的事情，区分开大众常混淆的三件事，是非常重要的，它们分别为比特币这种货币，支撑比特币的特定区块链，以及总体的区块链概念。打个有用的比喻，Napster，这家运行于1999年的公司，正是p2p文件共享服务的开拓者，但它却是非法的，它提供了数以百万计免费的音乐曲目服务。Napster公司本身被迅速关闭处理了，但它启发了很多其他的p2p服务。当然，当前也有许多的p2p服务，被用于盗版音乐和电影。尽管p2p技术的来历不明，但它也找到了合法的用途，例如Skype和Spotify这样的互联网创业公司，开了先路。同样的，这也发生在了比特币的身上。

区块链是一个更为有效的技术，它在本质上，是一个共享、可信的公共总账，任何人都可以对它进行核查，但不存在一个单一的用户可以对它进行控制。在区块链系统中的参与者们，会共同维持总账的更新：它只能按照严格的规则和共识来进行修改。比特币的区块链总账防止了双花的发生，不断跟踪着交易。这也使得没有中央银行的货币，成为了可能。

区块链也是密码学意外成果的最新例证。数学加密被用于浓缩原始片信息，转换成一个码，被称为一个哈希散列。任何企图篡改任何部分的区块链，都是会立即暴露的，因为新的哈希与旧的是不匹配的。这样一门科学，能让信息保持机密性（对于加密消息、在线购物以及银行而言，是重要的），自相矛盾的是，它也是开放式交易的一种工具。

比特币本身可能会永远限于一个好奇型的事物。然而，区块链则有着许多其他的用途，因为它满足了可信赖记录的需求，这对于每一种类型的交易来说，是重要的。现在，已有数十家创业公司希望利用区块链技术，无论是在比特币区块链上做文章，还是创建自己的新区块链（见文章）。

当前存在的想法，例如制造经济的防篡改公共数据库（土地登记），比方说（洪都拉斯和希腊对此有兴趣）；或奢侈品和艺术品的所有权登记。文档可以通过嵌入有关它们的信息，然后存放到公链上，你也不需要公证员为它提供担保。金融服务公司正在考虑使用区块链，作为记录谁拥有了什么的方式，而不是通过一系列的内部总账记录。一个值得信赖的私有总账，可以省去核对每笔交易对手方的需求，它速度快，并且最大限度地减少了错误。桑坦德银行估计，到2022年，它每年可能至多为银行们省去200亿美元的费用。目前，已有25家银行加入了一家区块链创业公司所创建的区块链联盟，称为 R3 CEV，一起制定共同的标准，此外，纳斯达克也即将开始利用这项技术，用于记录私营企业的证券交易。

这些新的区块链，不需要像比特币那样的方式进行工作。它们之中有许多，可以调整自己的模型，例如，寻找“挖矿”（支付参与者新产生的比特币，作为它们维护总账而提供的算力的回报）过程的替代型维护方式。一些行业的审查参与者们，可能会选择加入一条私链，因为他们需要的安全性并不高。区块链还可以实现商业规则，例如交易只当两方或多方认可时才会发生，或者另一笔交易已首先完成。正如Napster和p2p技术，一个聪明的想法正在被修改与完善。在这个过程中，它正迅速地摆脱比特币阴暗的声誉。

区块上的新链

区块链的传播，不利于“诚信商业”中的任何人（中央机构和官僚机构，如银行、结算所和政府主管部门），即使一些银行和政府正在探索利用这项新技术，其他人也会反对它。不过，考虑到政府和银行近年来下放了信任，**作为一种可创造更多监督和透明度的方式，可能也并不是什么坏事。**

在早期阶段，拟定区块链监管法将是一个错误：p2p技术的历史告诉我们，这项技术的全部潜力要变得清晰，还需要几年的时间。在此期间，监管机构应放开他们的双手，或想办法在现有框架内制定新的办法，而不是过于死板地冒险扼杀这种快速发展的想法。

共享式公共总账的概念，听起来可能没那么革命性，也并不性感。但复式簿记和股份制公司也同样如此。而区块链，就像它们一样，正在经历一个明显世俗的过程，但它有潜力改变人们和企业如何合作的方式。比特币狂热分子已被纯自由意志给迷住了，即数字货币能够超越任何央行的这种理想。真正的创新不是数字货币本身，而是铸造出它们的信任机器，而它的希望远远不仅如此。