假期福利! 经典O'Reilly图书免费送, 搞懂DApp生态就靠它了!

原创

区块链大本营 于 2019-05-02 18:00:00 发布 2537 收藏

本文链接：https://blog.csdn.net/Blockchain_lemon/article/details/89838752

来源 | 《去中心化应用·区块链技术概述》

作者 | Siraj Raval

译者 | 吴海星

编辑 | 乔治

出品 | 区块链大本营（blockchain_camp）

#文末参与话题讨论，免费获取纸质书籍一本😜

区块链这个领域很容易把人搞糊涂。似乎有数不清的创业公司、新币种、意识形态和流行语层出不穷，很难把它们全都弄清楚。

根据 Melanie Swan 的《区块链：新经济蓝图及导读》一书和其他人的观点，可以把这个领域细分成三类：区块链 1.0 是“货币”；区块链 2.0 加上了合约（股票、债券、金融资产）；区块链 3.0 超出了纯粹的金融领域，涵盖了治理和健康之类的应用（Dapp）。

本文将探讨这三类区块链靠什么来推进。

作为一名 Dapp 开发者，你只需要知道一点：那些能让你的 Dapp 变得安全、健壮、可盈利的工具。本文将会描述蓬勃发展的 Dapp 生态系统，也就是非常容易制作 Dapp 的生态系统。我还会讨论制作 Dapp 所需的技术，以及目前最可行的方式是什么。

一直以来，Web 应用中有四个概念是处在集中控制领域中的：身份标识、财富、数据和计算。其中每一个都要对服务提供商有充分的信任，然而这种信任却有可能遭到背叛。最近，在分布式系统中出现了一些新技术，让用户可以控制这些事情。接下来就让我们研究一下这些创新。

去中心化数据

对我来说，这是最重要的概念。现在，我们放心大胆地把自己的数据交给“服务栈”，心甘情愿地用自己的数据换取他们提供的免费服务，甚至会因为委托他们存储数据而支付费用。但是实际上，只要用户免费把数据给他们，他们就能靠这些数据把存储数据的钱赚出来。我们相信提供商不会滥用我们的数据，也不会把数据卖给那些我们不愿意向其暴露这些数据的人。

然而现实是，我们知道，只要把数据委托给一个集中式实体，这份信任就可能会被辜负。Amazon 的 Web 服务、Google 云端硬盘、Dropbox 以及其他任何一家“云”服务提供商，尽管有着分布式的计算后台，但所有权都是集中的。

另外，随着机器人和自动化技术的急速扩张，全球经济正从以劳动力为基础快速迈向以信息化为基础，数据将变成价值的主要形态。尽管人类的劳动力跟机器人没法比，但在数据上却可以一较高下——这是利用对世界的独特看法而分析出来的数据，是通过五种感官处理过的输出。我们不仅要拥有数据，还要在日新月异的世界中掌握其所有权。

那该怎么解决这个问题呢？怎么把数据以一种去中心化的方式存储，让你独自拥有自己的数据？这个问题至少已经得到了 10 年的深入研究，并且已经由几方提出了一个解决方案。理想的方案应该是提供一种去中心化的数据存储方式，它要足够健壮，并且尽可能不需要依靠信任保护数据。

1、方案1：把数据直接存放在比特币的区块链中

这种方法比较幼稚。它确实把数据去中心化了，因为每个人都有一份存储数据的区块链副本，但谁也不能修改数据。数据当然会用 SHA-256 加密，每个有钱包的人都会存储一份数据副本，但只有掌握了私钥的你能够访问。不过比特币的区块链不适合用来处理大量数据！区块链的设计目标是存储简单的交易日志，这个任务它完成得很好。但即便是只存储交易日志，区块链的规模在过去这几年就已经超过了 38 GB，下载一次可能要花上几天时间。

核心开发人员一直密切关注着扩展性和区块链膨胀问题。在你把数据上传到区块链之后，比特币矿工只能免费存储你的数据，他们得到的报酬根本不足以负担支出的成本，所以也就没有了继续维护比特币网络的动机。

专门用一个放宽大小限制的区块链来单独存放额外的数据怎么样？即便用另一种“加密货币”作为报酬支付给为你存储数据的矿工，这种办法还是不行。因为区块链会疯狂增长，任何想要使用这种“货币”的人都要下载超级大的钱包。仅仅几个用户存储一些图片就会使其臃肿不堪，更何况我们即将步入 PB 级数据都很平常的时代。要获得健壮的去中心化数据存储，不管从短期还是长期来看，都不能把数据存在区块链中。

2、方案2：把数据存放在分布式散列表中

分布式散列表（DHT）在过去 10 年里得到了广泛采用。它们不仅分发数据副本，还包含查找数据的索引函数，可以确保弹性。像 KaZaA、Napster 和 Gnutella 这些早期的 P2P 文件共享程序用的都是自己的 DHT，去中心化程度各不相同。一些用中心追踪器来监测所有数据的移动，一些（比如 Napster）有所有数据都要通过的中心源，它们都有单一失效点（出于法律原因）。

真正把 DHT 发扬光大的是 BitTorrent，它现在仍然有 3 亿多用户。尽管有去中心化的数据存储（BitTorrent 主干 DHT），BitTorrent 仍然要靠中心追踪器（比如海盗湾）来监测网络。海盗湾这样的网站会由于法律原因被定期关闭，所以即便 BitTorrent 有数据弹性，还是会有一些失效点。

如果我们用 BitTorrent 的 DHT 存放 Dapp 的数据，是不是很好？ BitTorrent 不仅提供了去中心化数据存储，还提供了一种数据分发协议，通过在种子用户和吸血用户之间设置对抗性策略使带宽的利用率达到最大化。

BitTorrent 的数据传输协议甚至比 Web 的还要快，因此它成了通过 Web 传输大型数据集（如高清电影）的主流方法。但用 BitTorrent 存储数据也有问题，各个节点没有长期为你保存数据的动力。在 BitTorrent 网络中，需求越旺盛的文件优先级越高，所以只有在获得人们的需要时，你的数据才会一直被复制并留在网络中。

然而在声誉良好的中心服务器上，比如 Amazon 的 Web 服务之中，即便只有你一个人用，数据也会一直放在那里。为了保护自己的声誉，他们只能依照合约保存好数据，不会因为没有其他人使用而不再保存。

首先，我们要的不仅仅是 DHT 的去中心化存储能力和 BitTorrent 的文件传输速度——我们还想要持久保存数据。因此，必须以某种方式激励节点存储数据。另外，我们需要保证指向数据的链接不会挂掉。互联网最初的提案中就有一条是链接的永久性。

这个想法源自上都（今内蒙古锡林郭勒盟正蓝旗境内）项目（Project Xanadu），在其所描绘的 Web 中，每个链接都有两个方向：一端指向目标，一端指向它的源头。也就是说，内容的创建者总能获得创建数据的认定，因为所有链接都会链回到他们。然而这样的 Web 始终没能出现，所以我们现在用的是基于 HTTP 的 Web，伴随我们长大、让我们因熟悉而喜欢的也是单向链接。

有没有哪个系统实现了这些功能呢？有，它叫星际文件系统。这个开源项目目前仍处于 Alpha 阶段。我非常喜欢 IPFS，并且是其协议的早期贡献者之一。它的创建者 Juan Benet 曾经花了 5 年时间思考数据存储问题，并最终付诸行动，发布了 IPFS 科学论文来阐述所有的想法。我用了几个月的时间来了解这个系统和他的思想框架，思考为什么 IPFS 比其他方案好。目前，我觉得它最有可能成为最有价值的数据存储方案。

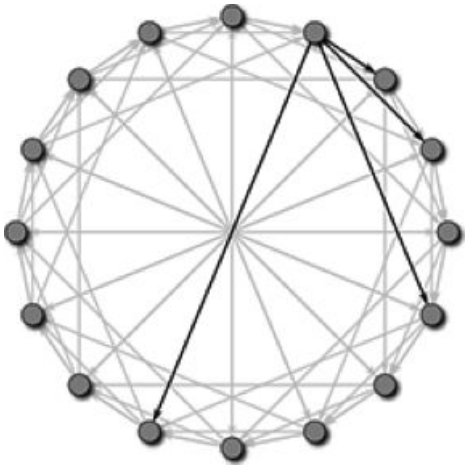
IPFS 致力于帮我们发展出一个永久的、去中心化的 Web，一个永远不会有死链的 Web，一个数据不再由单一实体控制的 Web。下载好 IPFS 客户端后，用户能用它向网络上添加任何数据，然后会得到一个散列值。之后，用户就可以用这个散列值访问对应的数据了。

跟基于 IP 寻址的 Web 不同，IPFS 是一个内容寻址系统。在 IP 寻址系统中，如果命名服务器失效，它的所有数据也会失效。内容寻址的寻址数据则高效得多，因为用它访问数据不需要依赖单个服务器的运行。从一个内容地址请求数据时，得到数据的速度要比从 IP 地址请求数据更快，因为它会根据内容地址路由到离你最近的数据副本。

从后端来看它是什么样的？

IPFS 用 DHT 保存数据。它基于流行的 Kademlia DHT，还借鉴了 Chord 和 BitTorrent 的 DHT。用户上传到 IPFS 的数据会被复制到几个节点上，所以即便某个节点失效了，数据依然可以访问得到。除此之外，就像 BitTorrent 一样，需要某份数据的节点越多，数据的弹性就越大，因为所有下载那份数据的节点都会分享它们持有的副本。

Chord 的顶级功能是它的 DHT 圈，它会创建和弦（chord），并将相互靠近的和弦扩展为更大的和弦，从而使 DHT 查询在全局节点内最大化。这样，网络全局看起来就像一系列不断增大的和弦，而查询将会得益于其效率，在必要的地方进行和弦之间的跳跃。



和弦

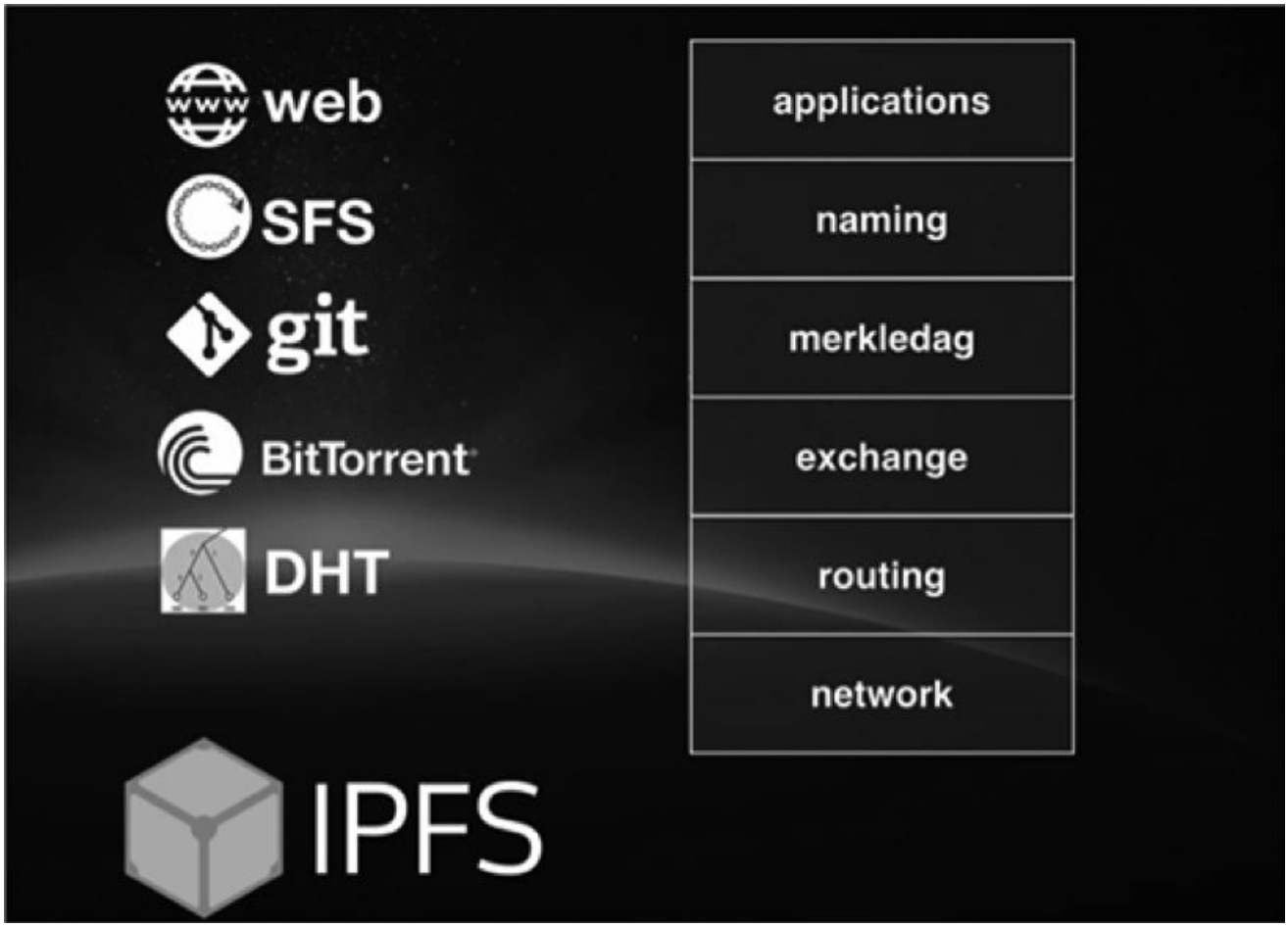
现在，像 Amazon 和 Google 这样的集中式服务提供商都有遍布全球的数据中心，用户可以自行选择用哪个数据中心来接收和路由自己的数据，但服务一般都会自动帮你选好。即便跟遍布全球的数据中心比，类似 Chord DHT 这样的系统还是有优势的：它们可以提供一种特有的办法，用多个节点来提升数据的传输效率。

IPFS 用 merkleDAG 作为 DHT 的结构，让用户在需要时找到数据，merkleDAG 是一种简单灵活的数据结构，你可以把它理解成一系列相互连接的节点。说得具体一点，就是一个有向无环图（DAG）。merkleDAG 看起来可能像一个链表或一棵树。往 DHT 上添加数据时，系统会生成一个 SHA-256 多重公钥-私钥对，然后把它们两个都交给用户。开发人员可以通过编程将散列值链在一起，形成他们自己的微 merkleDAG。

一定要注意，IPFS 中的所有数据会形成同一个包含所有节点的泛 merkleDAG。IPFS 上的所有数据都是公开的，所以用户要自己负责数据的加密。私钥除了可以用来访问数据，还能证明所有权。

IPFS 受到了 BitTorrent 的启发——数据传输速度，为了寻找用于分享数据的同伴而采用的对抗机制。IPFS 团队相信 Web 也应该采用这种工作方式。举个例子，如果一所大学里整个班的学生都跟 Facebook 的中心服务器上请求同一个视频，就会占用很多不必要的带宽，还会产生很多不必要的数据冗余。如果图片就在附近，他们没必要向那么远的服务器发起请求。

在内容寻址系统中，如果知道所需数据的内容地址，就可以从最近的地方获取。节点间的数据分享不需要中心来协调。它跟 BitTorrent 一样，采用了 HTTP Web 所用的服务器 - 客户端架构，并且也做成了分布式的。



IPFS

IPFS是如何在BitTorrent上进行改进的

IPFS 有个姊妹协议，叫作“文件币”。“文件币”用于支付给矿工（存储数据的节点），它采用了一种称为 BitSwap 的新型“价值换数据”机制。“加密货币”在这里发挥了作用：它的价值转移很快，并且允许根据每个相关字节的存储进行微支付。“文件币”目前仍在开发当中，但 IPFS 已经可以使用了。

IPFS 命令现在是免费的，矿工存储数据完全出于他们对网络的热爱。最终，所有的上传和下载都会需要“文件币”。“文件币”很有可能成为直接建立在比特币区块链上的“资产”，因此用户可以用比特币“购买”存储空间。

除了上面这些，IPFS 还借鉴了 Git 管理所有数据版本的版本控制模型。Git 用 DAG 为数据版本建模，IPFS 用其作为整个系统的结构。用户能看到数据的版本历史（或者任何已经获得解密访问权限的数据）。

因此，IPFS 是 Git、DHT、SFS、BitTorrent 和比特币的集大成者，用这些系统最优秀的思想创建了一个去中心化数据存储网络。IPFS 希望有朝一日能将 Web 的 HTTP:// 协议换成 IPFS://，但它们也能协同工作。在谈到具体实现时，我会详细介绍几种方法。

IPFS 是经过深思熟虑的去中心化存储解决方案。尽管这一领域还有其他表现不错的竞争对手，但它是最健壮的，优于所有的“加密货币”项目。下面来看一下其他方案。

以太坊：以太坊致力于构建一个通用（图灵完备）的区块链计算语言，包括去中心化存储。他们的工作重心是确保 DAO（他们指的是“民主自治组织”）的安全，存储则放在了次要位置（写本书时）。

StorJ：它已经预先开采了很多 StorJ 币，并做了一些漂亮的设计。它的设计很整洁，在奥斯汀黑客马拉松上赢得了胜利，而且看起来开发小组的人也知道自己在讲什么。然而不管怎样，在黑客马拉松结束了一年多之后，它还是个雾件。

Maidsafe：与跟以太坊一样，想做的事情有很多。他们没有使用工作证明，目标是为计算、存储和“货币”创建一个去中心化平台。他们已经在这个平台上工作了 6 年，但看起来还没得到足够多的关注。

去中心化财富

比特币是第一个成功的去中心化财富存储。在比特币之前，通过 Web 传输价值时需要一个可信的第三方提供商（银行）。比特币实现了去中心化价值传输，满足了 Dapp 内部对去中心化支付的需求。

那些“山寨币”怎么样？莱特币、狗狗币、点点币、暗黑币和肯伊币怎么样？山寨币一般是从比特币的源码中分化出来的，添加了一些由于种种原因被比特币的核心开发人员拒绝采纳的功能。比如说，莱特币创建者想要提高支付速度，于是复制了比特币的代码，添加了一些加速代码。莱特币就由此诞生了。

莱特币的市值相当大，至少已经在“加密货币”前五名的位置上待了一年。莱特币是极少数出于好意（更快的支付速度）的币种之一。大多数山寨币就不一样了：如果不是让搞笑成为其支撑资金的模因（比如狗狗币），就是玩了“吸引散户接盘”的套路。

山寨币的思想是，人们可以创建一种新币，给它贴上标签，然后通过媒体曝光来哄抬它的价格（肯伊币）。他们鼓吹说这个“加密货币”将来会非常值钱，早期买入的投资者都会大赚一笔。

这个新币的价格一旦高到一定程度，创建人就会把它全部卖掉，换成更稳定、更长久的货币，比如法定货币。这是山寨币圈子里的常见套路，明显会对“加密货币”的生态系统造成极其恶劣的影响。

首先，这些山寨币会玷污“加密货币”的名声，让潜在的投资者变得越来越谨慎。其次，它们在毫无必要地与比特币区块链争抢市场份额，却不能带来丝毫真正的价值。这反过来又会损害比特币的价值，而且所有将比特币作为最常用“加密货币”的系统也都会深受其害。

当然，比特币使用的是工作量证明方案。也就是说，网络中的每台挖矿机都必须生成一个反映其计算力的计算证明，并负责处理事务。作为回报，挖矿机会得到比特币，作为它们维护网络的报酬。“加密货币”界的一些人觉得工作量证明消耗的能源太多了，并且只是防范女巫攻击的短期方案，所以在共识机制上展开了大量的研究。

工作量证明用了大量计算力，并且挖矿机维护网络所消耗的电力成本高达 1500 多万美元。如果能找到更好的网络维护方法，就不用这么浪费了。有两种工作量证明的替代方案比较受欢迎，分别是权益证明和代理式权益证明。

尽管在比特币之后进行了大量的共识机制研究，比如权益证明，但目前还没有什么能像工作量证明那样抵抗得住女巫攻击。虽然计算昂贵，但目前来看没有比它更好的选择了。比特币网络上的投资已经超过 30 亿美元，有难以计数的创业公司、投资人、媒体和零售商接受了比特币。它有先发优势，并且已经通过 5 年多的奋斗在一些国家或机构中赢得了认可。

我们不需要重新开始。即便发现了优于工作量证明的共识机制，也应该让比特币的核心开发人员实现它，而不是交给某个山寨币。这样整个社区才能更快前进。

有些人可能会说这是“比特币最高主义”。反对者认为比特币最高主义者一直在鼓吹比特币的先发优势，并且认为他们为了保护自己在比特币网络上的投资，坚决反对任何竞争者出现。比特币最高主义的负面影响就是，不管多么有价值，任何不在比特币协议范围内的想法都会被迅速淘汰，得不到社区应有的认可，相关工作也会停滞不前。

这个问题有个两全其美的解决办法：侧链提案。

该提案基于 Adam Back 与人合作的一篇论文 。

https://blockstream.com/wp-content/uploads/2014/10/sidechains.pdf

Adam Back 是工作量证明的发明者，中本聪曾在其关于比特币的论文中提到过他。

https://bitcoin.org/bitcoin.pdf

这个提案源于一个想法：要测试共识机制以及任何关于“加密货币”的新想法，开发人员必须创建比特币区块链的分支，做一个全新的山寨币来验证其假设。

这对比特币没什么好处，并且对开发人员而言，要发起一个新的区块链是很困难的。巴克团队提出的解决方案是通过代码让比特币在主链（比特币区块链）和侧链之间自由切换。也就是说可以创建一个全新的区块链，并很容易地将它作为比特币区块链的侧链。你无须发起自己的挖矿网络，就能得到比特币工作量证明的安全保障。

那些已经有“加密货币”投资经验（拥有比特币）的人会成为你的潜在客户群，因为他们可以直接使用自己手里的比特币。最后，在两个链之间发送比特币不需要任何转换。双向侧链现在正在开发，很快就会发布。

比特币区块链是相对安全的区块链，因为世界上所有超级计算机的计算力加在一起也不如它多，所以它对女巫攻击的防御能力也是最强的。从头开始发起一个工作量证明区块链非常困难，因为早期的计算资源太少了，攻击者很容易凑够 51% 的计算力从而接管整个网络。

除此之外，开发人员应该专心构建用户需要的去中心化应用程序——这已经是个很有挑战性的任务了，不应该再分散精力去从头开始发起一个区块链。如果你想试验共识机制或者实现一些新的“加密货币”技术，侧链可以帮你。

如果你并不想实现新的“加密货币”技术，而是只想为自己的去中心化应用程序发行一个“内部货币”，该怎么办呢？如果要让这种“货币”可以跟随网络一起增值，允许用户访问稀缺资源，并且激励他们一起扩大网络，该怎么办呢？这样的话，你无须创建新的（侧）链，只要直接在比特币上创建一种资产就可以了。尽管在这种情况下也有好几种选择，但我会选择彩币。

Counterparty

Counterparty 是比特币 2.0 的协议，让用户创建和管理资产、制定拍卖、出价，甚至在比特币上创建图灵完备的合约。听起来是不是很棒？但问题是 Counterparty 把这些有趣的特性全都放到了协议中。它不是模块化的，没有分层按顺序排好。

在比特币区块链上发行资产并允许用户用比特币轻松传输是个很好的想法，但它们却跟股息功能合并到了一起。分配股息是个挺好的小特性，但却是 Counterparty 内部的操作，不是用本地比特币追踪资产。所有的事情都被迫揉进了一个过度雕饰的协议中。

举个例子，投注就是在资产上添加了一个具有实验性、挑战性的特性。更好的做法是，构建简单的几层，每层都完成一件事情。模块化是优秀软件的标志。虽然 Counterparty 的野心很大，却根本没有做到模块化。

假设有一个协议类库市场，所有协议类库都会相互竞争，无疑是最优秀的最终胜出。可以想象一下，如果所有类库都令人绝望地交织在一个包里，你要么把它们都装上，要么一个也不装。这简直就是一场噩梦，而这恰恰就是 Counterparty 要迫使你做的事情。

Counterparty 中有一个 XCP“货币”。这是一个令人迷惑不解的元素，没有人想要它。如果你想用 Counterparty 的 API 构建一个应用币，就要应对 XCP 以及所有转换操作。如果要创建资产，不管它是什么类型的，都需要销毁 0.5 个 XCP（按当前价格计算要超过 1 美元）。XCP“货币”的供应是固定的，并且因为只要有人发行新的资产就要销毁“货币”，所以它的“货币”总量一直在减少。

在使用 Counterparty 的某些特性时需要用到 XCP 让开发人员觉得很烦。这意味着你得一直盯着牌价（XCP/BTC）。虽然有平台在追踪这一价格，并且能跟所有市场一样提供实时报价及流动性需求，但说真的，这有什么意义？你只不过要给你的应用创建一个“内部货币”，为什么要应付这么多麻烦事？这基本上就是一个没必要去跨越的巨大障碍。因此，这是个糟糕的主意。

Counterparty 一直在更新其客户端，那些依赖它的 API 的人，比如 Gems 应用，因此得到了一个混合的结果。因为没有模块化，所以如果出现 bug，一切都会马上崩溃。总而言之，Counterparty 过于集中式管理了。好在我们还有更好的选择（彩币），它们提供了必要的模块化和去中心化，也无须使用额外的“货币”。

Hyperledger

Hyperledger 相信自己是“代币无关”的，即允许发行者不用基于底层货币来发行新币种：既不需要比特币，也不需要法定货币，更不需要其他任何山寨币。它在理论上是健全的，但在实践中却不是，因为它靠的是一个籍籍无名的共识机制。在这一领域有很多研究，然而还没有哪个能够证明自己足以跟工作量证明相抗衡。

有种办法可以轻易切断任何一个区块链 2.0 项目发出的噪声，那就是深入探究它们的共识机制。如果没有使用工作量证明，或者不是基于比特币的，就看看它们的市场份额有多大，再看看出现过多少次安全漏洞。我每次这么做都会发现安全漏洞。下表汇总了这一领域的各种信仰，其制作者是 Meher Roy。

信仰/投注	平台机会	增量风险	优点
一级	不适用	不适用	不适用
代币不可知论	超总账、Eris、Codius、瑞波币 / 恒星币	缺乏身份标识和私钥管理的方案因最终用户控制交易而导致的监管不确定性平台特有的缺陷，如弱共识算法	适用于所有资产，包括平价货币、股票和“加密货币”可以复制由“加密货币”社区率先开发的所有应用程序与现有法规相对兼容
“加密货币”最高主义	比特币、以太坊、嫩薄荷、卵石币、瑞波币 / 恒星币（部分）等	对于新的价值形式，改变社会惯性需要大量的网络效应拥有稳健货币政策和共识方法，交易速度快，并且具有可伸缩性的系统出现较晚	对传统银行体系不满意的细分市场是一个现成的市场当前有重大的公共利益
比特币最高主义	侧链	那些比比特币强，能够改善网络维护成本、交易速度和可扩展性的新技术	比特币显著的先发优势
超比特币	不适用	被证明是幻想	无

“加密货币”的政治信仰

代币不可知论是一套强有力的观点，但我相信比特币可以跟现有的金融系统合作。我们已经度过了比特币的蜜月期，同时也意识到，不管银行系统多么老旧，它在世界上确实有一席之地。

图灵完备的智能合约怎么样？这是在 Dapp 中创建去中心化支付系统时不可缺少的金融工具中的第二部分。以太坊团队在这方面取得了最大的成功，但他们还有更大的野心。以太坊要创建一个图灵完备的区块链、一个去中心化存储网络、一个去中心化通信协议、一个运行以太坊 Dapp 的新型浏览器，以及一种编写以太坊 Dapp 的新型脚本语言。

我们稍微退一步来看。一个团队不能、也不应该想要单独完成所有这些想法，毕竟每个想法都是公司量级的。以太坊筹集了很多资金，也获得了很多关注，但是就算有创始人 Vitalik Buterin 的聪明才智，也不能指望其创造出下一代比特币。就像比特币协议的首席开发者 Gavin Andresen 所说，他们将来要么被安全问题搞得焦头烂额、疲于应付，要么会大规模缩减其区块链。

图灵完备的脚本语言是个好主意，你可以用它做任何想做的事。比特币的脚本语言特意做了限制，以防止无限循环这种恶意脚本出现（无论是出于恶意还是无能）。Gavin Andresen 说以太坊的大部分目标都可以用比特币实现，而且核心开发人员已经开始动手实现其中一些特性了。

从务实的角度来讲，要想让人们使用你的 Dapp，最简单的办法就是确保这个 Dapp 能用他们已有的“货币”，而目前份额最大的就是比特币。所以，你应该在比特币或者侧链上发行一种彩币，因为侧链基本上就是带有额外特性的比特币，比如更快的交易速度。

去中心化身份标识

身份标识的概念已经被人们争论了几个世纪。到了互联网时代，这个词有了全新的意义。什么是身份标识？谁拥有身份标识？在互联网上应该如何看待身份标识？

由于密码学最近的发展，很多解决方案都已经“假定有了一个公钥基础设施”。基本上，如果人们愿意安全地存储一个私钥，身份标识就变成去中心化的了。只有那些有密钥的人才能访问它。BitAuth 是一个现成的好例子。

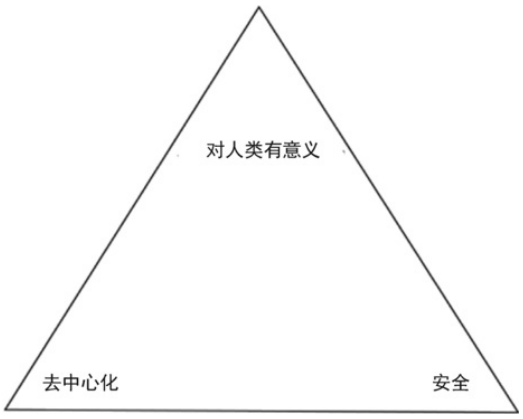
BitAuth 用比特币现有的技术创建一个使用 secp256k1 的公-私钥对。不需密码就可以进行跨 Web 服务的认证。它会给你一个系统识别码（SIN），也就是公钥的散列值。它用签名防止中间人（MITM）攻击，用随机数防止重放攻击。你的私钥永远不会暴露给服务器，你可以安全可靠地保管好它。身份标识是去中心化的，所以不需要把它交给一个可信的第三方，而是可以自己保管。

另外还有一些合并互联网身份标识的尝试，都取得了不同程度的成功。其中最值得注意的就是 OpenID 协议。OpenID 是一个利用 HTTP、SSL 和 URI 等已有 Web 协议的去中心化身份标识协议。它的核心思想是，身份标识已经像碎片一样分散在 Web 上了，通过使用 OpenID 协议，用户可以将现有的 URI 传输到一个账号中，而这个账号在所有 OpenID 支持的网站上都可以用。

OpenID 将服务提供商需要存储身份标识的需求进行了抽象，让你可以只用可信的存储源，然后将身份标识带到多个提供商那里。在身份标识合并的尝试中，OpenID 是目前来看最成功的一个：Google、Yahoo! 和 Twitter 都已经是 OpenID 的提供商了。

这种方式很好：我们无须重复注册就可以将自己的身份标识带到各个网站上，也就不需要一次次地重复输入身份信息了。这样不仅更方便，我们也不会因为要把身份标识数据存储在新的服务上而提心吊胆。不过 OpenID 仍然有潜在的安全隐患，因为你还是要把自己的数据托付给这些服务提供商中的一个。

这个问题又被称为 Zooko 三角，名称币旨在帮我们解决这个问题。



Zooko 三角

Zooko 三角是一种猜想。它指出，在一个按某种协议给出名称的系统中，只能实现其希望达成的三个特性（对人类有意义、去中心化、安全）中的两个。OpenID 实现了安全性和对人类有意义。名称币做了补充，添加了去中心化。名称币基本上是一个第三方身份标识提供商，由区块链作为你和请求身份标识的服务之间的中介。名称币的区块链是比特币区块链的早期分支之一，它的价值已经经过了时间的检验。

大多数山寨币都已经烟消云散了，名称币能留下来是因为只有它补足了 Zooko 三角。用户可以向名称币的区块链发送一条交易来注册自己的名称——他的名称会嵌在交易中，放在命名空间 /id 下。当用户发送交易时，如果是唯一的（之前没有人发过），名称币就把它存下来，否则不存。

也就是说，只要人们能想到名称，命名空间就可以存。尽管这样用户可以创建和选择自己（人类易读）的标识，但由于人类易读的短语是有限的，这也是个问题。标识的分段确实有用，因为在新服务中，用户可以从新的命名空间中选择身份标识。

换句话说，这是个折中方案：让一个通用的身份标识提供商补足 Zooko 三角是一项重要创新，但命名空间是有限的。不过域名注册也是这样的。现在是 ICANN 控制着域名注册，这是一个得到美国商务部支持的集中式组织。名称币由于提供 .bit 域名的注册而大受欢迎，变成了相对于 ICANN 的去中心化选择。Chrome 或 Firefox 之类的常规浏览器无法访问这些 .bit 域名。要进行访问，目前只能通过 .bit web 代理，或者下载插件。随着 .bit 越来越受欢迎，浏览器可能会对该协议提供原生支持。

大多数人不需要创建 .bit 域名，因为那会增加不必要的麻烦，让用户需要安装额外的软件或通过代理才能访问你的网站。在名称币区块链中注册一个用户名相当容易。只需要将一些比特币换成名称币，下载钱包，然后就可以注册你的用户名了。

但如何登录到名称币区块链中呢？认证和授权的工作机制是怎样的？最近创建的 NameID 是个两全其美的方案：用户可以用自己的名称币 /id 登录到 OpenID 支持的所有网站中。这样，名称币终于可以无障碍地进入主流 app 市场了。

不过，将身份标识去中心化的代价是什么？好吧，其代价跟把数据用 IPFS 去中心化，把财富用比特币去中心化一样：用户必须保管好自己的私钥。对于黑客来说这没什么，他们喜欢去中心化和保护隐私。当涉及在互联网上使用正确的工具这一话题时，他们是最理想的人群。在追求所用工具的高效和完美上，黑客们会为自己天生的驱动力而自豪。他们用 GPG 加密通信，用 Tor 客户端来防御自己的浏览历史。

对他们来说，为了去中心化额外存储些私钥完全没问题。但主流人群呢？他们真的关心这些吗？我觉得他们并不是特别关心隐私和去中心化。再考虑到计算机安全知识的平均水准，公平地说，我觉得大多数人都不能或者不愿意安全地保管加密密钥。迄今为止最大的比特币应用 Coinbase 在市场上的成功就是明证。Coinbase 跟去中心化是对立的：它是比特币银行。它提供了保管私钥的服务。

很多比特币社区反对任何形式的集中，一些人甚至连 BitTorrent 追踪器这种轻微的集中都不想碰。真正的问题是：你愿意在多大程度上去中心化你的软件？想去中心化域名并让用户保管三组不同的密钥吗？这个问题的答案取决于你的受众群，以及去中心化带来的收益是否值得你这么做。

比如提到“去中心化的 Dropbox”这个 Dropbox 的竞争对手时，答案可能是肯定的。如果有竞争对手能承诺在保证安全的前提下将数据去中心化，我敢打赌，肯定有足够多的人认为有充足的理由来安全地保管好一个私钥，以便让这样的系统工作。

即便那些人真的不想保管，也会有商家跟进，提供存储即服务的业务。必须承认，即便用了这么长时间的比特币，我也还是在用 Coinbase 的服务保管我的比特币。我只是不想因为持有比特币而提心吊胆地害怕自己的电脑被黑！我之所以更相信 Coinbase，是因为他们持有很多用户的资产，CEO 看起来也值得信任（至少比 Mt.Gox 的 Mark Karpelès 可信），并且其背后的两个投资商（安德森·霍洛维茨和联合广场风险投资公司）也很可靠。

我认为，我们不需要创建完全没有信任关系的系统，而是应该创建更可信的系统。我喜欢一个关于火车的例子。假设有一列从旧金山开往洛杉矶的火车突然撞车了。如果火车的控制权集中在调度员手里，我们就知道谁应当承担责任（调度员）。如果火车的控制权分散到了每个乘客手里，则无法追究每个人的责任，也很难找到那个坏人。

去中心化本身没什么好的，必须在明确的目的下和真实的用例中才能体现其优势。Dapp 可以有不同的去中心化程度，这要取决于它们各自的用例。毫无疑问，如果要创建一个组织秘密活动的应用，那就应该是去中心化的 Dapp。如果要创建一个想得到广泛认可的社交网络，用 .bit 做域名很可能并不是什么好主意。

如果你用了一个把数据存储在 IPFS 上的 Dapp，并且它还用比特币区块链上的彩币发行了自有“货币”，那么你很可能也会用 NameID 存储用户的身份标识。这里可能会有三组密钥合并到某种本地或者第三方的密钥库中，让用户可以访问并使用你的软件。

去中心化计算

我们已经介绍了数据、财富和身份标识的去中心化存储，那么计算呢？我们能把 Web 应用程序直接存放在 IPFS 上并运行它吗？好吧，既可以也不可以。IPFS 只是一个文件系统，跟其他所有的文件系统一样，在它上面运行和显示静态网站完全没问题。

但对于我们现在称为后台系统的动态应用程序而言，则需要一个编译和运行环境，比如 Node.js 和 Ruby on Rails —— IPFS 不行。因此，虽然可以把应用程序的数据存放在 IPFS 上，也还要考虑要把源码放在什么地方。

为此，我们有两个选择。

第一是把数据保存在 IPFS 上，把源码托管在传统的虚拟机（VM）提供商那里，比如 Heroku。VM 模拟了特定的计算机系统，其操作是基于（假想或真实的）计算机功能和架构的。VM 的实现可能涉及特殊的软件、硬件及两者的组合。Heroku 是非常流行的平台即服务（PaaS）提供商，让用户非常轻松就能用上 VM。虚拟机上可以运行 Go 和 Node.js 等代码写成的动态后台系统，还可以用 MongoDB 这样的内部托管的数据库来存储数据。

如果把源码放在 Heroku 上，数据放在 IPFS 上，那么用户仍然会相信数据是属于他们的，你没有把数据卖出去赚钱。但他们不能保证在服务器上运行的代码就是你开源的代码。除了无法验证，这还意味着有中心失效点（Heroku）。

第二种办法是把数据保存在 IPFS 上，把源码部署到构建于 IPFS 之上的去中心化 VM 上。有这样的东西吗？最接近的项目是 astralboot。这基本上是一个 golang 服务器，只是它直接从 IPFS 上拉取文件，并且允许你运行基于 IPFS 的 Debian 环境。也就是说如果你在 astralboot 上部署了一个动态应用程序，它是搭建在 IPFS 上的，你只需要在 astralboot 上的 Linux 环境中配置出特定的环境。

另一个选择是以太坊自己的 EVM（以太坊虚拟机）。以太坊的区块链跟比特币区块链有很多不同：有不同的块时间，图灵完备的合约，并且它是一个去中心化状态机。我认为它虽然是 VM，但并不完整，最起码肯定不是大多数开发人员想要的那种 VM。

在今天的软件市场上，几乎一定要从第三方那里请求数据。在这一领域有很多竞争者，他们专注于数据利基市场，为你提供指向其他服务的 API。与其每次都做重复性的工作来为你的应用创建可信的数据源，还不如直接用第三方的 API。以太坊 EVM 的问题是无法获取区块链之外的数据，除非数据提供者已经在自己的服务器里设置好了智能合约，能够跟以太坊协作。

这对于作为 Oracle（可信的联合数据源）的新 API 来说是好事，但对于已有服务来说却不太妙。以太坊区块链和比特币区块链都不能从外部请求数据。这种不便是故意实行的安全限制。如果能从区块链里调用 API，黑客有可能用各种数据请求逃脱区块链，最终结果就是造成网络膨胀。所以单独将区块链当作完整的 VM 来用不是个好主意。

另外一个项目是 Go-circuit，会创建在机器集群上运行实例的小型服务进程。它们形成了一个流畅的高效弹性网络，来自任何一台机器的分布式进程都可以协调同步。这是一个为 Go 程序准备的分布式运行时，还集成了 Docker。如果你的项目用的是 Go 语言，那它很棒，否则的话它对你来说就没什么用。

所有这些关于去中心化计算的讨论都提出了一个问题：如果计算是个市场会怎么样？想象在一个网络中，真正有用的工作量证明计算是在侧链中，像网格币和素数币之类的一些币种已经在这么做了。但它们对用户决定的新计算来说是不可用的（以可验证的方式），它们是基于造币者需要的现有计算的。我们需要的是 Dapp 开发者能够通过易于访问的接口部署代码的 P2P 去中心化计算。

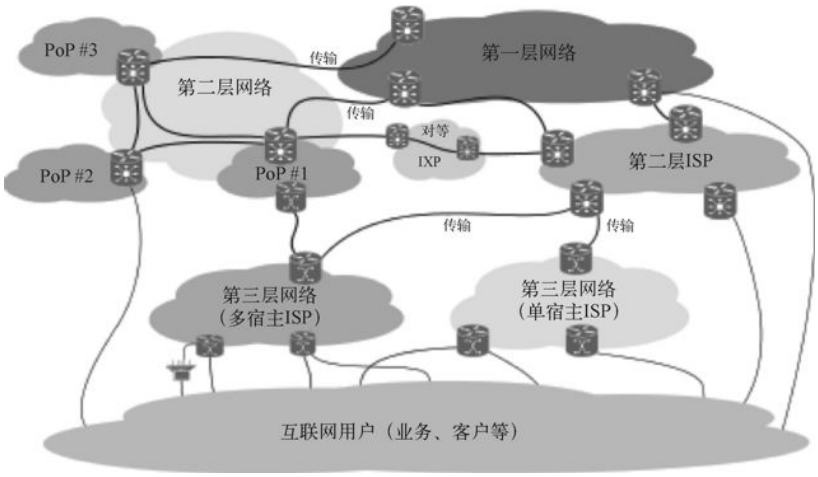
我们想要的网络有自己的计算币，Dapp 开发人员会为了计算他们的代码而向挖矿机、计算引擎支付费用。随着用户量的增长，网络的价值会不断增长，从而带动计算币的价值跟着增长。这是加密研究的一个领域，所以我相信，肯定有像 astralboot 这样的产品在加紧研发中，它们是以最快方式做原型的希望。

如果你觉得 astralboot 太难配置，也还有 Heroku 可以用。如果 Heroku 失效了，而你的代码是开源的，那么任何人都可以把它重新上传到新的服务器上，访问那些放在 IPFS 上永久的、用户拥有的、可公开验证的数据。如果计算市场成为现实，你就可以直接从浏览器上运行动态应用程序了，就像现在运行在 Web 的域主机上一样。

去中心化带宽

之前已经讨论过 Dapp 中能去中心化的 4 个重点了：**数据、财富、身份标识和计算**。我们还谈到了域名注册，不过在大多数情况下都没有这个必要。接下来我们要讨论去中心化带宽。

对于大多数用户而言，ISP 在你和互联网之间充当网关的角色。有些 ISP 跨越国家，作为中央中枢把人们连接起来。此外，ISP 还解决了“最后一公里”问题，把终端用户连接到更快、容量更大的互联网“主干网”上。“最后一公里”只是电信行业用来指代电信网络最后一层分支的词语，它将通信连接送到散客那里。真正直达客户的是互联网网线。



互联网

AT&T 和 Comcast 之类的 ISP 靠为我们提供互联网接入来获利，因为现在除了 ISP，我们没有别的选择。其缺点是，这些集中式网关也是中心失效点。政府可以根据需要关掉它们。ISP 还必须遵守当地的法律，创建不允许用户访问的 IP 黑名单。

这全都管用，因为现在还没有什么能取代它，不过有其他选择已经开始出现了。最新的例子是 iOS 上的 FireChat，这款应用是由一个叫作开放花园的公司创建的。FireChat 利用 iOS 的多端连接特性，实现手机之间点对点的直接对话。它不需要 ISP。FireChat 是网状网络应用程序的范例。网状网络是标准的集中式互联网的去中心化版。在网状网络中，用户不需要通过中心网关来访问站点。他们可以直接连接到最近的路由器上，一般就是附近的电脑。

现在有很多已经投入使用的网状网络。西班牙有世界上最大的网状网络之一，那里有超过 50 000 人需要访问互联网，却没有 ISP 为他们提供网络接入。在纽约遭遇飓风期间，网线断掉的情况下，网状网络被用于传递宝贵的救援信息。

在旧金山也有大量的“暗”网，只对其所创建的秘密社团内部的访客开放。网状网络一般无法访问常规互联网及其中的数据。如果环中没有隧道，就无法访问到正常的网状网络。只有通过隧道到网状网络的来回切换才能建立起隧道。现在还没有主流硬件厂商能够支持这两项工作同时进行，但你可以借助开放花园和 CJDNS 这样的项目来使用混合网络。

这要稍微难一点，因为除了软件，还涉及硬件的变更。路由器应该有能力同时访问两个网络，这样就能从常规互联网中拉取数据并用在网状网络中，从而让它不能被关掉。

尽管去中心化带宽值得拥有，但只有在互联网审查和 Web 访问被阻断的情况下才有这个必要。我觉得如果大范围出现这种情况，现实需求将会把去中心化带宽变成主流选择。使用区块链，我们能让其他计算设备取代 ISP 成为网关。他们能通过用“加密货币”路由数据和带宽证明来获取报酬。

就像“加密货币”能将计算和数据存储的 P2P 市场变成现实一样，“加密货币”也能促成带宽分享。“加密货币”能在集中式力量存在的地方培育出市场。这些市场可能是计算、存储、带宽，以及任何能想象到的“真实”和“人造”的稀缺资源。我们将会看到，经济变得越来越依赖于信息。随着所有基于劳动力的事情慢慢被自动化吞噬，数据市场极有可能慢慢变成最大的市场。

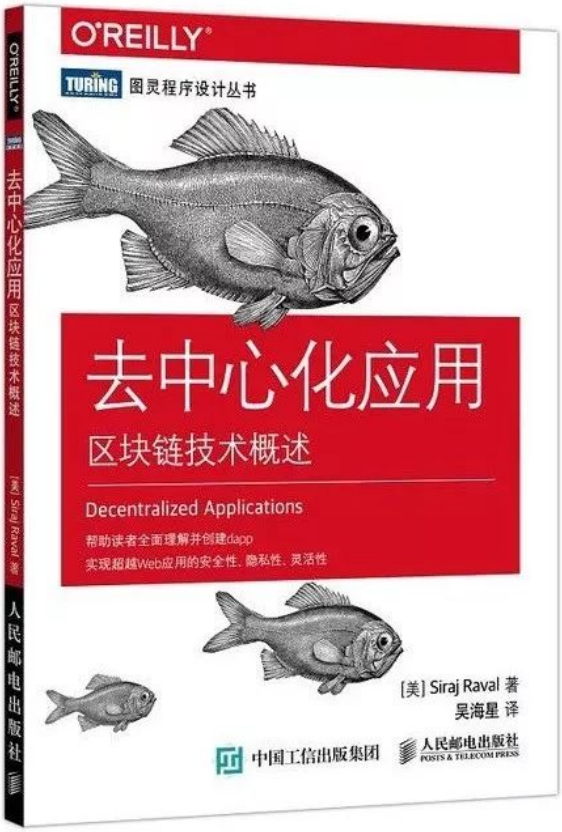
以上，分别讨论了去中心化数据、去中心化财富、去中心化身份标识、去中心化计算、去中心化带宽，当然，还有很多其他应用场景没有涉及。

对于以上作者描述的场景，你赞同吗？**拿福利之外，也留言告诉营长吧！**

本期话题：**如果可以，你最想开发一款怎样的DApp？**说出你的理由（50字以上）。

请在文末畅所欲言，营长将从精选留言用户中抽取5位幸运读者，免费送书一本！

截止时间5月4日中午12点！



感谢人民邮电出版社的大力支持

16岁保送北大、麻省理工博士、

EOS黑客松全球总决赛前三名

5月8日晚，精彩技术公开课与您不见不散！

推荐阅读：

太可怕了！五一外出还敢连Wi-Fi？

精华篇 | 王嘉平：突破不可能三角「异步共识组Monoxide」（附PPT）

不改变比特币，如何扩容？

20k~80k，蚂蚁金服等大厂招人啦！想赶上这波人才荒，你要掌握这些...

《互联网人叹气图鉴》

硬核粉丝 | 清华双胞胎“YCY Dance Now”杀进超越杯编程大赛决赛

异构计算=未来？一文带你秒懂3大主流异构

他说：当一个程序员决定告别996，什么都有可能发生！

老铁在看了吗？？