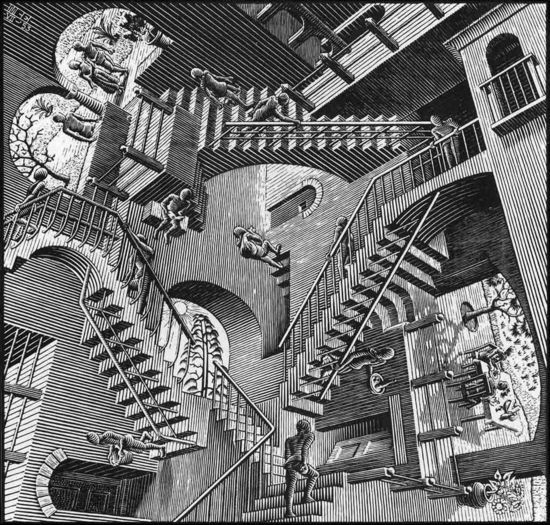
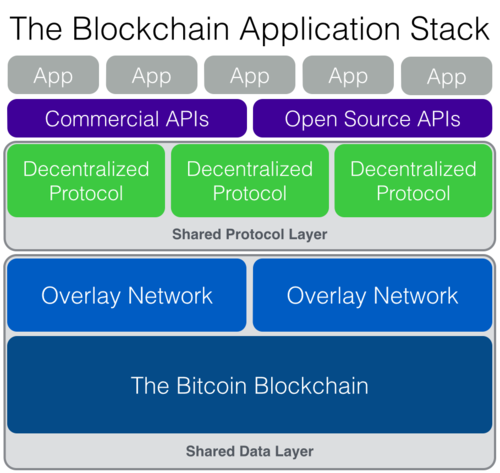
把覆盖网络和区块链结合起来会发挥出更大效应

2014-12-23 18:15:00



　　编者按：接上一篇《未来十年，Blockchain会如何互联网世界？》，Joel Monegro沿着结构图继续探讨区块链思维方式的未来：d.com/photo/2014/021e24e7218937d972dbcbdb8cfd6a7e.jpeg

　　想像一下，如果有一个全球统一的数据库，或者一个各种全球数据库的集合，那会怎样？而这就是“共享数据层”背后的基本想法。诚如其名，“共享的数据层”就是一个数据存储的层级，它是去中心化的，并向所有人开放。



　　去中心化就是说没有任何单个实体、个人或公司拥有这个数据库，它是由全世界的计算机来维持的。

　　开放意味着任何个人、公司或应用都无需许可就能使用，而你的个人数据是加密的，你可以允许一些应用接入你的个人数据，但是它们并不拥有这些数据，而且任何时候你都可以取消，或者使用它们竞争对手的产品。

　　只要你把“覆盖网络（Overlay Networks）”和“区块链”结合起来，以上这些都是可能的。

**在区块链上存储数据**

　　2013年，比特币协议里引进了一个新功能：创建一种名叫OP\_RETURN的交易，你可以嵌入40比特的小数据进入。最初，这个功能旨在把情 境信息加入比特币交易里，比如配送信息等。而更具创造性的用法是，创造最小量的交易（0.00000001 BTC加上交易费），并且嵌入任何你想放进去的信息。

　　因为区块链在时间戳和分布式一致性（distributed consensus）上很有优势，你可以利用它在信息不可逆上的优势来永久保存记录。“分布式一致性”是说，网络中的大多数节点都认同某条信息为真，在比特币中就是指交易信息和交易发生的时间。

　　40比特并不多，而且通常约束条件会激发更多的创造力。利用这个功能的第一个有趣的应用就是“Proof Of Existence”，它可以为任何文件创建一个散列（hash），也就是不同于其他所有文件的身份认证ID，并且它放入区块链中。而后，通过比较区块链 里的散列和你手头的文件的散列，你可以用那个交易的时间戳和存储在其中的散列，来证明那个时点上某个文件确实存在。只要二者匹配，你就有了明证。

　　另一个更加以顾客为导向的应用就是Blocksign，它的电子签名服务和Docusign与Hellosign类似，就是在区块链中利用同样的技术来存储签名文件。

　　上面两个例子都很有趣，但这只是对OP\_RETURN的牛刀小试而已。已经有越来越多的开发者想出更聪明的办法来利用好这40个比特了。

**区块链的短板**

　　比特币生态系统里的很多成员开始担忧，过度使用OP\_RETURN来存储数据的弊端。比如说最多的担忧就是：矿工费用越来越高，用无用的信息来鼓吹区块链，以及确认交易的时间很长等等。

　　你可以使用最小量的比特币交易来存储信息，但是你依然需要付费给矿工，是矿工们承担确认信息和录入区块链的工作。当然最低的费用是0.0001 BTC，或者低于0.04美元。看起来这费用并不多，但是费用会随比特币价格升高，而且记录很多条信息（比如每天5亿条推特）那费用就相当高了。还有些人 感觉，以存储非交易信息来创造最小量交易，会给整个网路带来不必要的压力，还会膨胀区块链。最后，需要10分钟的时间来确认一次交易并录入区块链，这个速 度不足以满足现代应用的需求。

　　以上这些担忧都是合理的，而传统的解决办法就是，fork并创造新的加密货币或协议，从而加快确认速度、扩大存储量等。但是，很多团队开发出很 多创造性办法，利用“覆盖网络”，并节约使用区块链来做更重要的事。我相信这才是正道，而这种方式以前也很有效地解决各种问题，诚如 Chris Dixon前不久发的Twitter里说的：

　　Many people tried to fork IP, TCP,HTTP, SMTP, etc but turned out it was better to build on top. Same with BTC.

**覆盖网络**

　　覆盖网络是一个系统，它可以用附加功能来扩展或补充区块链，比如存储某些类型的数据甚至文件。它与区块链加起来就构成了“共享数据层”。

　　最初，开发者会fork比特币协议来支持一些功能，并用自身的区块链来发布替代的加密货币（altcoin）。但越来越明显的是，在比特币区块链基础上建构的优势更多，比如你可以从它显著的流动性和网络效应里获益，而在新的加密货币及其区块链里你就得不到。

　　“覆盖网络”是一个很宽泛的词，其中大多数系统还在涌现，而且它们一定会有各种不同的结构。不管它们采用何种形式，它们的共同点就是：它们与比特币区块链连在一起，并且是去中心化和开放的。

　　利用比特币网络是一种很有效的方式来开发你自己的货币和协议，而你不需要创建你自己的区块链。Counterparty和Mastercoin 就是现成的例子，Counterparty的协议文件很好地解释了它的运作原理和它与比特币的联系。根本说来，尽管Counterparty有自己的货币 （XCP），而每一个XCP交易都是由少量的BTC来支持的。Mastercoin和它也大体相似。

　　另一个方法就是Blockstream开发的“侧链”，它的基本思想就是，从理论上来说，侧链允许开发者自己的加密货币和区块链，但与altcoin不同的是，它们可以和比特币自由转换，并从比特币的流动性中获益。

　　还很难说侧链是否会成功，但是Blockstream获得的2100万美元种子投资会让它有公平发展的机会。如果你感兴趣，可以读读Blockstream的白皮书，对侧链系统有一个深度解释。

　　一个新案例就是Factom，它是一个“区块链数据层”，可以用来加密和实时审计大批量的记录。Factom是一个拥有节点的独立网络，可以利 用分布式哈希表来存储数据。这个方式对有些应用有很多用途，但对于其他很多应用则不适用，不过你可以它为例来创造其他重叠网络。

**个人数据的所有权和安全性**

　　你存储在Dropbox里的信息是加密的，但是Dropbox也拥有你的密码，它也可以进入你的文件，只要哪天Dropbox被黑了，就会危及你的数据。

　　但是在区块链这一层里，用户数据的模型是反过来的：不是由第三方保护你的数据和密码，而是整个网络保护你的数据和密码。任何人未经允许都不能获 得，你可以完全掌控。各种应用就变成了在你数据之上的界面，通过同一个协议，不同的app可以交互。就像你可以用Gmail邮箱给你用Yahoo邮箱的朋 友写邮件一样，你也可以不用下载同样的app就能读到你朋友po的信息。

　　这并不是说用户是否想要这样，而是说，当用户想这样做的时候他们能否做到。大多数人选择让第三方保管自己的密码，就像他们用Coinbase。但是只要你要求，Coinbase也会交回你的密码，并且你可以用其他服务，而你的账本完好无损。

　　我会继续写文章探讨这个结构图。