链滴

什么是 {:) 区块链　　？

作者：ibut

原文链接：https://ld246.com/article/1516712385436

来源网站：链滴

区块链（blockchain）是眼下的大热门，新闻媒体大量报道，宣称它将创造未来。
HP 社区也即将推出 B3T 社区合约 Token。借此东风我们一起来了解一下！</
>
<h2 id="一-区块链的本质--">一、区块链的本质**</h2>
区块链是什么？一句话，它是一种特殊的分布式数据库。
首先，区块链的主要作用是储存信息。任何需要保存的信息，都可以写入区块链，也可以从里面读取
所以它是数据库。
其次，任何人都可以架设服务器，加入区块链网络，成为一个节点。区块链的世界里面，没有中
节点，每个节点都是平等的，都保存着整个数据库。你可以向任何一个节点，写入/读取数据，因为
有节点最后都会同步，保证区块链一致。
<h2 id="二-区块链的最大特点--">二、区块链的最大特点**</h2>
分布式数据库并非新发明，市场上早有此类产品。但是，区块链有一个革命性特点。
区块链没有管理员，它是彻底无中心的。其他的数据库都有管理员，但是区块链没有。如果有人
对区块链添加审核，也实现不了，因为它的设计目标就是防止出现居于中心地位的管理当局。
正是因为无法管理，区块链才能做到无法被控制。否则一旦大公司大集团控制了管理权，他们就
控制整个平台，其他使用者就都必须听命于他们了。
但是，没有了管理员，人人都可以往里面写入数据，怎么才能保证数据是可信的呢？被坏人改了
么办？请接着往下读，这就是区块链奇妙的地方。
<h2 id="三-区块--">三、区块**</h2>
区块链由一个个区块（block）组成。区块很像数据库的记录，每次写入数据，就是创建一个区
。
每个区块包含两个部分。
<blockquote>

区块头（Head）：记录当前区块的元信息
区块体（Body）：实际数据

</blockquote>
区块头包含了当前区块的多项元信息。
<blockquote>

生成时间
实际数据（即区块体）的 Hash
上一个区块的 Hash
...

</blockquote>
这里，你需要理解什么叫 <a href="https://ld246.com/forward?goto=https%3A%2F
2Fbaike.baidu.com%2Fitem%2F%25E5%2593%2588%25E5%25B8%258C%25E5%2580%25BC"
target="_blank" rel="nofollow ugc">Hash，这是理解区块链必需的
所谓 Hash 就是计算机可以对任意内容，计算出一个长度相同的特征值。区块链的 Hash 长度是
56 位，这就是说，不管原始内容是什么，最后都会计算出一个 256 位的二进制数字。而且可以保证
只要原始内容不同，对应的 Hash 一定是不同的。
举例来说，字符串 123 的 Hash 是 a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0（十六进
），转成二进制就是 256 位，而且只有 123 能得到这个 Hash。
因此，就有两个重要的推论。

推论 1：每个区块的 Hash 都是不一样的，可以通过 Hash 标识区块。

推论 2：如果区块的内容变了，它的 Hash 一定会改变。

<h2 id="四-Hash-的不可修改性">四、Hash 的不可修改性</h2>
区块与 Hash 是一一对应的，每个区块的 Hash 都是针对"区块头"（Head）计算的。
Hash = SHA256(区块头)
上面就是区块 Hash 的计算公式，Hash 由区块头唯一决定，SHA256 是区块链的 Hash 算法。
前面说过，区块头包含很多内容，其中有当前区块体的 Hash（注意是"区块体"的 Hash，而不整个区块），还有上一个区块的 Hash。这意味着，如果当前区块的内容变了，或者上一个区块的 Hash 变了，一定会引起当前区块的 Hash 改变。
这一点对区块链有重大意义。如果有人修改了一个区块，该区块的 Hash 就变了。为了让后面的块还能连到它，该人必须同时修改后面所有的区块，否则被改掉的区块就脱离区块链了。由于后面要到的原因，Hash 的计算很耗时，同时修改多个区块几乎不可能发生，除非有人掌握了全网 51% 以上计算能力。
正是通过这种联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法被篡改。这就像历一样，发生了就是发生了，从此再无法改变。
每个区块都连着上一个区块，这也是"区块链"这个名字的由来。
<h2 id="五-采矿">五、采矿</h2>
由于必须保证节点之间的同步，所以新区块的添加速度不能太快。试想一下，你刚刚同步了一个块，准备基于它生成下一个区块，但这时别的节点又有新区块生成，你不得不放弃做了一半的计算，次去同步。因为每个区块的后面，只能跟着一个区块，你永远只能在最新区块的后面，生成下一个区。所以，你别无选择，一听到信号，就必须立刻同步。
所以，区块链的发明者中本聪（这是假名，真实身份至今未知）故意让添加新区块，变得很困难他的设计是，平均每 10 分钟，全网才能生成一个新区块，一小时也就六个。
这种产出速度不是通过命令达成的，而是故意设置了海量的计算。也就是说，只有通过极其大量计算，才能得到当前区块的有效 Hash，从而把新区块添加到区块链。由于计算量太大，所以快不起。
这个过程就叫做采矿（mining），因为计算有效 Hash 的难度，好比在全世界的沙子里面，找一粒符合条件的沙子。计算 Hash 的机器就叫做矿机，操作矿机的人就叫做矿工。
<h2 id="六-难度系数">六、难度系数</h2>
读到这里，你可能会有一个疑问，人们都说采矿很难，可是采矿不就是用计算机算出一个 Hash，这正是计算机的强项啊，怎么会变得很难，迟迟算不出来呢？
原来不是任意一个 Hash 都可以，只有满足条件的 Hash 才会被区块链接受。这个条件特别苛刻使得绝大部分 Hash 都不满足要求，必须重算。
原来，区块头包含一个难度系数（difficulty），这个值决定了计算 Hash 的难度。举例来说，第00000 个区块的难度系数是 14484.16236122。
区块链协议规定，使用一个常量除以难度系数，可以得到目标值（target）。显然，难度系数越，目标值就越小。
Hash 的有效性跟目标值密切相关，只有小于目标值的 Hash 才是有效的，否则 Hash 无效，必重算。由于目标值非常小，Hash 小于该值的机会极其渺茫，可能计算 10 亿次，才算中一次。这就采矿如此之慢的根本原因。
区块头里面还有一个 Nonce 值，记录了 Hash 重算的次数。第 100000 个区块的 Nonce 值是 <ode>274148111</code>，即计算了 2.74 亿次，才得到了一个有效的 Hash，该区块才能加入区链。
<h2 id="七-区块链的分叉">七、区块链的分叉</h2>
即使区块链是可靠的，现在还有一个问题没有解决：如果两个人同时向区块链写入数据，也就是，同时有两个区块加入，因为它们都连着前一个区块，就形成了分叉。这时应该采纳哪一个区块呢？
<img src="https://ld246.com/images/img-loading.svg" alt="imagepng" data-src="https:/b3logfile.com/file/2018/01/31542b53b60648eba76f62428cd920f1_image.png?imageView2/2interlace/1/format/jpg">
现在的规则是，新节点总是采用最长的那条区块链。如果区块链有分叉，将看哪个分支在分叉点面，先达到 6 个新区块（称为"六次确认"）。按照 10 分钟一个区块计算，一小时就可以确认。
<img src="https://ld246.com/images/img-loading.svg" alt="imagepng" data-src="https:/b3logfile.com/file/2018/01/3329760e99f542cdae41523b84a4e3e1_image.png?imageView2/2interlace/1/format/jpg">

由于新区块的生成速度由计算能力决定，所以这条规则就是说，拥有大多数计算能力的那条分支就是正宗的比特链。
<h2 id="八-总结">八、总结</h2>
区块链作为无人管理的分布式数据库，从 2009 年开始已经运行了 8 年，没有出现大的问题。这明它是可行的。
但是，为了保证数据的可靠性，区块链也有自己的代价。一是效率，数据写入区块链，最少要等十分钟，所有节点都同步数据，则需要更多的时间；二是能耗，区块的生成需要矿工进行无数无意义计算，这是非常耗费能源的。
因此，区块链的适用场景，其实非常有限。
<blockquote>

不存在所有成员都信任的管理当局
写入的数据不要求实时使用
挖矿的收益能够弥补本身的成本

</blockquote>
如果无法满足上述的条件，那么传统的数据库是更好的解决方案。
目前，区块链最大的应用场景（可能也是唯一的应用场景），就是以比特币为代表的加密货币。
转自：阮峰的网络日志