比特币与拜占庭将军问题

[**He1l\_Q**](http://www.8btc.com/author/71)**2013-11-07 08:49 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**26**](http://www.8btc.com/bitcoin-and-the-byzantine-generals-problem#comment)**25856**

每次我向那些不熟悉比特币的人解释比特币的独特之处的时候，我都会用会计学上的总账和拜占庭将军问题来帮助讲解。此文就是帮助讲解的内容，有了此文我就可以把链接发给小伙伴们，而不需要每次都重新打一大堆字了。



首先，不要把比特币当成一种货币，而是一个总账。它是个电子总账，网络上的每一个参与者的电脑都会有一份总账的备份，并且所有的备份都是在实时的持续的更新、对账、以及同步着。每一个参与者都能在这本总帐里记上一笔，这一笔记录着一定数量的币从一个参与者那里被发送到另一个参与者那里，并且每一条这样的记录都接着就实时的广播到网络了，所以在每一台电脑上的每一分份拷贝都是几乎同时更新的，并且所有的总账拷贝都保持着同步。这本公开的分布式的总账的官方叫法是“[区块链](https://en.bitcoin.it/wiki/Blockchain)（blockchain）”，并且它使用了[BT技术](https://en.wikipedia.org/wiki/BitTorrent)以保证所有的拷贝都是同步的。

你还可以把比特币当作一个对于在分布式系统领域的[一个复杂的算法难题](https://en.wikipedia.org/wiki/Consensus_(computer_science))的通用解决方法，这个难题俗称“拜占庭容错”、“拜占庭将军问题”、或者“两军问题”。

这一问题的趣味非正式表述如下：想象一下，在拜占庭时代有一个墙高壁厚的城邦，拜占庭，高墙之内是它的邻居想象不到之多的财富。它被其他10个城邦所环绕，这10个城邦也很富饶，但和拜占庭相比就微不足道了。它的十个邻居都觊觎拜占庭的财富，并希望侵略并占领它。

但是，拜占庭的防御是如此的强大，没有一个相邻的城邦能够成功入侵。任何单个城邦的入侵行动都会失败，而入侵者的军队也会被歼灭，使得其自身容易遭到其他九个城邦的入侵和劫掠。这十个城邦之间也互相觊觎对方的财富并持续互相对抗着。而且，拜占庭的防御如此之强，十个邻居的一半以上同时进攻才能攻破它。

也就是说，如果六个或者更多的相邻敌军一起进攻，他们就会成功并获得拜占庭的财富。然而，如果其中有一个或者更多背叛了其他人，答应一起入侵但在其他人进攻的时候又不干了，也就导致只有五支或者更少的军队在同时进攻，那么所有的进攻军队都会被歼灭，并随后被其他的（包括背叛他们的那（几）个）邻居所劫掠。这是一个由不互相信任的各方构成的网络，但他们又必须一起努力以完成共同的使命。

而且，是个邻居之间通讯和协调统计时间的唯一途径是通过骑马在他们之间传递信息。他们不能聚在一个地方开个会（所有的王都不互相信任他们的安全在自己的城堡或者军队范围之外能够得到保障）。然而，他们可以在任意时间以任意频率派出任意数量的信使到任意的对方。每条信息都包含类似如下的内容：“我将在第四天的6点钟进攻，你愿意加入吗？”。

如果收信人同意了，他们就会在原信上附上一份签名了的/认证了的/盖了图章的/验证了的回应，然后把新合并了的信息的拷贝再次发送给九个邻居，要求他们也如此这样做。最后的目标是，通过在原始信息链上盖上他们所有十个人的图章，让他们在时间上达成共识。最后的结果是，会有一个盖有十个同意同一时间的图章信息链，可能还会有一些被抛弃了的包含部分但不是全部图章的信息链。

但是，问题在于如果每个城邦向其他九个城邦派出一名信使，那么就是十个城邦每个派出了九名信使，也就是在任何一个时间又总计90次的传输，并且每个城市分别收到九个信息，可能每一封都写着不同的进攻时间。除此以外，部分城邦会答应超过一个的攻击时间，故意背叛发起人，所以他们将重新广播超过一条的信息链。这个系统迅速变质成不可信的信息和攻击时间相互矛盾的纠结体。

比特币通过对这个系统做出一个简单的（事后看是简单的）修改解决了这个问题，它为发送信息加入了成本，这降低了信息传递的速率，并加入了一个随机元素以保证在一个时间只有一个城邦可以进行广播。它加入的成本是“工作量证明”，并且它是基于计算一个随机哈希算法的。哈希是一种算法，它唯一做的事情就是获得一些输入然后进行计算，并得到遗传64位的随机数字和字母的字符串，就像这个：

d70298566aa2f1a66d892dc31fedce6147b5bf509e28d29627078d9a01a8f86b

在比特币的世界中，输入数据包括了到当前时间点的整个总账（区块链）。并且尽管单个哈希值用现在的计算机可以几乎即时的计算出来，但只有一个前13个字符是0的哈希值结果可以被比特币系统接受成为“工作量证明”。这样一个13个0的哈希值是极其不可能与罕见的，并且在当前需要花费整个比特币网络大约10分钟的时间来找到一个。在一台网络中的机器随机的找到一个有效哈希值之前，上十亿个的无效值会被计算出来，这就是减慢信息传递速率并使得整个系统可用的“工作量证明”。下面是一个例子：

f51d0199c4a6d9f6da230b579d850698dff6f695b47d868cc1165c0ce74df5e1

d70298566aa2f1a66d892dc31fedce6147b5bf509e28d29627078d9a01a8f86b

119c506ceaa18a973a5dbcfbf23253bc970114edd1063bd1288fbba468dcb7f8

在找到一个有效值之前，成百万上亿个更多的类似上面这样的字符串被计算出来。。。

000000000000084b6550604bf21ad8a955b945a0f78c3408c5002af3cdcc14f5

那台发现下一个有效哈希值的机器（或者说在我们类比中的城邦），把所有的之前的信息放到一起，附上它自己的，以及它的签名/印章/诸如此类，并向网络中的其他机器广播出去。只要其他网络中的机器接收到并验证通过了这个13个0的哈希值和附着在上面的信息，他们就会停止他们当下的计算，使用新的信息更新他们的总账拷贝，然后把新更新的总账/区块链作为哈希算法的输入，再次开始计算哈希值。哈希计算竞赛从一个新的开始点重新开始。如此这般，网络持续同步着，所有网络上的电脑都使用着同一版本的总账。

与此同时，每一次成功找到有效哈希值以及区块链更新的间隔大概是10分钟（这是故意的，算法难度每两周调整一次以保证网络一直需要花费10分钟来找到一个有效的哈希值）。在那10分钟以内，网络上的参与者发送信息并完成交易，并且因为网络上的每一条机器都是使用同一个总账，所有的这些交易和信息都会进入遍布全网的每一份总账拷贝。当区块链更新并在全网同步之后，所有的在之前的10分钟内进入区块链的交易也被更新并同步了。因此分散的交易记录是在所有的参与者之间进行对账和同步的。

最后，在个人向网络输入一笔交易的时候，他们使用内嵌在比特币客户端的标准公钥加密工具来同时他们的私钥以及接收者的公钥来为这笔交易签名。这对应于拜占庭将军问题中他们用来签名和验证消息时使用的“印章”。因此，哈希计算速率的限制，加上公钥加密，使得一个不可信网络变成了一个可信的网络，使得所有参与者可以在某些事情上达成一致（比如说攻击时间、或者一系列的交易、域名记录、政治投票系统、或者任何其他的需要分布式协议的地方）。

这里是比特币为何如此特别的关键：它代表了一个对于一个困难的算法上的难题的解决方案，这一解决方案在一系列的历史事件发生之前是不可能的，这些事件有：

1. 互联网的创造
2. 公钥加密算法的发明
3. 点对点Bitorrent(BT)协议的发明。BT协议最开始是开发来用于在网络上的相对小的用户子集之间共享许多文件的，但比特币用它来在所有用户之间共享单个文件。
4. 人们意识到，在系统中添加一个简单的时间延迟，同时使用公钥加密算法以验证每笔交易，可以解决这个问题。

如果说一些最棒的想法在事后看来是很简单的，那么上述的第四点就完全符合条件，尽管整个项目是站在了巨人的肩膀上的。

最后，这一对于拜占庭将军问题的解决方案，可以推广到任何核心问题是在分布式网络上缺乏信任的领域。如我们已经提到乐的，人们正在为互联网建设一个[分布式的域名系统](https://dot-bit.org/Main_Page)，以及为政治选举建设分布式的投票系统（还没有网站）。如果人们认为单纯的文件分享搅乱了这个世界，那么比特币解决方案和协议才刚刚打开洪水的闸门。