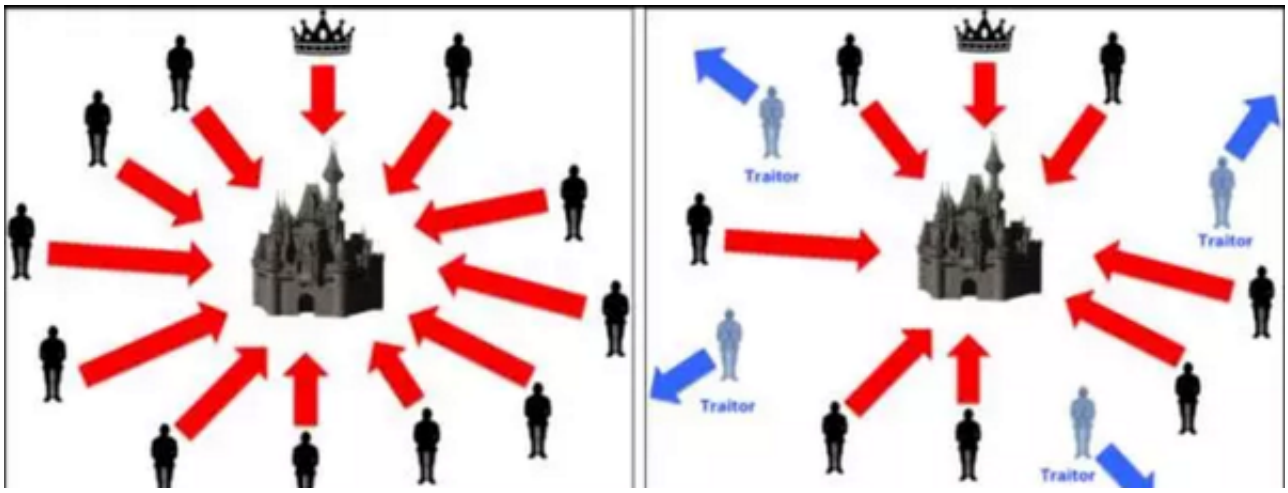

好了让&#039；s想象一下，一群拜占庭将军想要攻打一座城市，他们将面临两个不同的问题：每个将军和他的军队在地理上相距甚远，因此集中指挥是不可行的，这使得协同作战变得极其困难。。被攻击的城市有一支庞大的军队，他们取胜的唯一方法就是所有人同时攻击。为了使合作成功，城堡左侧的军队派了一名信使给城堡右侧的军队带去了一条信息&quot周三袭击&quot。然而假设右边的军队没有准备好进攻，并要求信使带回一条消息&quot不，攻击星期五&quot。而信使需要通过穿越被攻的城市返回左路军，那么问题就来了。这个可怜的信使可能会发生很多事情。例如他可能被俘虏了，泄露了信息，或者被被攻击的城市杀死了，被替换了。这会导致军队获得被篡改的信息，从而使作战计划无法达成一致而失败。上述例子对区块链有明显的借鉴意义。区块链是一个巨大的网络。你如何信任他们？如果要从钱包里给某人发4个以太币，如何保证网络中的某人不会篡改信息，把4个以太币换成40个？中本聪发明了工作量证明机制来绕过拜占庭式的一般问题。。其运作原理是：假设左路军要发出&quot周一袭击&quot对于正确的军队，他们需要执行以下步骤：首先，他们将添加一个&quotnonce&quot初始文本，可以是任意随机的十六进制值。然后，他们用&quotnonce&quot添加并得到一个结果。假设他们决定仅在哈希结果的前五位数字为零时共享信息。如果散列结果满足条件，他们将让信使带着散列结果的信息出发。否则他们将继续随机改变nonce的值，直到他们得到想要的结果。这个过程不仅冗长耗时，而且占用大量计算能力。如果敌人抓住信使并试图篡改信息，根据哈希函数的特性，哈希结果将发生巨大变化。。如果城市右边的将军们看到这个消息没有&#039；t以指定数量的零开始，那么他们将停止攻击。但是，这里可能有一个漏洞。哈希函数不是100%无冲突的。所以，如果城里的敌人得到了信息并篡改了它。并且通过不断地改变nonce值，我们得到从指定数量的零开始的结果。我们做什么呢虽然极其耗时，但还是可行的。鉴于这种情况，将军们可以借助人数的力量。假设，如果不是左边的一个将军给右边的一个将军发消息。取而代之的是，左边有三个将军给右边的将军发消息。为了达到上述目的，他们可以自己制作信息，然后对积累的信息进行哈希处理。然后，在将nonce值添加到散列结果之后，再次执行散列。这次他们想生成一条以六个零开头的消息

。显然，这将非常耗时。但这一次，如果信使被城市俘获，敌人篡改信息并找到与结果匹配的nonce值将需要无限长的时间，这可能会持续数年。例如将军派多个使者，那么城池可能会在计算中被攻毁。右边的将军要做的事情很简单。他们只需要将之前给他们的正确的nonce值添加到信息中，散列它，然后检查结果是否匹配。。散列一个字符串是非常容易的。那么，从本质上来说，工作量证明的过程就是：寻找满足hash目标的nonce值是一个非常困难和耗时的过程。但是，要验证结果中是否有邪恶的行为是非常简单的。