什么是拜占庭将军问题

2018-02-05 | 2018-07-16 | 比特币

接触区块链的同学，多少都听说过拜占庭将军问题，经常看到或听到某某区块链使用某某算法解决了拜占庭将军问题，那么究竟什么是拜占庭将军问题呢?

什么是拜占庭将军问题

也被称为“拜占庭容错”、“拜占庭将军问题”。
拜占庭将军问题是Leslie Lamport（2013年的图灵讲得主）用来为描述**分布式系统一致性问题**（Distributed Consensus）在论文中抽象出来一个著名的例子。

这个例子大意是这样的:

拜占庭帝国想要进攻一个强大的敌人，为此派出了10支军队去包围这个敌人。这个敌人虽不比拜占庭帝国，但也足以抵御5支常规拜占庭军队的同时袭击。这10支军队在分开的包围状态下同时攻击。他们任一支军队单独进攻都毫无胜算，除非有至少6支军队（一半以上）同时袭击才能攻下敌国。他们分散在敌国的四周，依靠通信兵骑马相互通信来协商进攻意向及进攻时间。困扰这些将军的问题是，他们不确定他们中是否有叛徒，叛徒可能擅自变更进攻意向或者进攻时间。在这种状态下，拜占庭将军们才能保证有多于6支军队在同一时间一起发起进攻，从而赢取战斗?

> 拜占庭将军问题中并不去考虑通信兵是否会被截获或无法传达信息等问题，即消息传递的信道绝无问题。Lamport已经证明了在消息可能丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。所以，在研究拜占庭将军问题的时候，已经假定了信道是没有问题的.

问题分析

单从上面的说明可能无法理解这个问题的复杂性，我们来简单分析一下:

1. 先看在没有叛徒情况下，假如一个将军A提一个进攻提议（如：明日下午1点进攻，你愿意加入吗？）由通信兵通信分别告诉其他的将军，如果幸运中的幸运，他收到了其他6位将军以上的同意，发起进攻。如果不幸，其他的将军也在此时发出不同的进攻提议（如：明日下午2点、3点进攻，你愿意加入吗？），由于时间上的差异，不同的将军收到（并认可）的进攻提议可能是不一样的，这是可能出现A提议有3个支持者，B提议有4个支持者，C提议有2个支持者等等。

2. 再加一点复杂性，在有叛徒情况下，一个叛徒会向不同的将军发出不同的进攻提议（通知A明日下午1点进攻， 通知B明日下午2点进攻等等），一个叛徒也会可能同意多个进攻提议（即同意下午1点进攻又同意下午2点进攻）。

   > 叛徒发送前后不一致的进攻提议，被称为“拜占庭错误”，而能够处理拜占庭错误的这种容错性称为「Byzantine fault tolerance」，简称为BFT。

相信大家已经可以明白这个问题的复杂性了。

中本聪的解决方案

在出现比特币之前，解决分布式系统一致性问题主要是Lamport提出的Paxos算法或其衍生算法。Paxos类算法仅适用于中心化的分布式系统，这样的系统的没有不诚实的节点（不会发送虚假错误消息，但允许出现网络不通或宕

机出现的消息延迟）。

中本聪在比特币中创造性的引入了“工作量证明（POW : Proof of Work）”来解决这个问题，有兴趣可进一步阅读工作量证明。
通过工作量证明就增加了发送信息的成本，降低节点发送消息速率，这样就以保证在一个时间只有一个节点(或是很少)在进行广播，同时在广播时会附上自己的签名。
这个过程就像一位将军A在向其他的将军（B、C、D...）发起一个进攻提议一样，将军B、C、D...看到将军A签过名的进攻提议书，如果是诚实的将军就会立刻同意进攻提议，而不会发起自己新的进攻提议。

以上就是比特币网络中是单个区块（账本）达成共识的方法（取得一致性）。

理解了单个区块取得一致性的方法，那么整个区块链（总账本）如果达成一致也好理解。
我们稍微把将军问题改一下：假设攻下一个城堡需要多次的进攻，每次进攻的提议必须基于之前最多次数的胜利进攻下提出的（只有这样敌方已有损失最大，我方进攻胜利的可能性就更大），这样约定之后，将军A在收到进攻提议时，就会检查一下这个提议是不是基于最多的胜利提出的，如果不是（基于最多的胜利）将军A就不会同意这样的提议，如果是的，将军A就会把这次提议记下来。

这就是比特币网络最长链选择。

经济学分析

工作量证明其实相当于提高了做叛徒（发布虚假区块）的成本，在工作量证明下，只有第一个完成证明的节点才能广播区块，竞争难度非常大，需要很高的算力，如果不成功其算力就白白的耗费了（算力是需要成本的），如果有这样的算力作为诚实的节点，同样也可以获得很大的收益（这就是矿工所作的工作），这也实际就不会有做叛徒的动机，整个系统也因此而更稳定。

很多人批评工作量证明造成巨大的电力浪费，促使人们去探索新的解决一致性（共识）问题的机制：权益证明机制（POS: Proof of Stake）是一个代表。在拜占庭将军问题的角度来看，它同样提高了做叛徒的成本，因为账户需要首先持有大量余额才能有更多的几率广播区块，POS不是本文重点，以后在讲。

> 共识算法的核心就是解决拜占庭将军问题（分布式网络一致性问题）。