比特币如何达成共识 - 最长链的选择

2017-12-07 | 2018-01-10 | 比特币

比特币没有中心机构，几乎所有的完整节点都有一份公共总帐本，那么大家如何达成共识：确认哪一份才是公认权威的总账本呢?

为什么要遵守协议

这其实是一个经济问题，在经济活动中的每个人都是自私自利的，追求的是利益的最大化，一个节点工作量只有在其他的节点认同其是有效的（打包的新区块，其他的节点只有验证通过才会加入到区块链中，并在网络上传播），才能够过得收益，
而只有遵守规则才会得到其他的节点认同。
因此，基于逐利，节点就会自发的遵守协议。共识就是数以万计的独立节点遵守了简单的规则（通过异步交互）自发形成的。

> 共识：共同遵守的协议规范

去中心化共识

在工作量证明一篇，我们了解通过工作量证明来竞争记账，权威的总帐本是怎么达到共识的，没有完全说清楚，今天补上，
实际上，比特币的共识由所有节点的4个**独立过程**相互作用而产生：

1. 每个节点（挖矿节点）依据标准对每个交易进行独立验证
2. 挖矿节点通过完成工作量证明，将交易记录独立打包进新区块
3. 每个节点独立的对新区块进行校验并组装进区块链
4. 每个节点对区块链进行独立选择，在工作量证明机制下选择累计工作量最大的区块链

共识最终目的是保证比特币不停的在工作量最大的区块链上运转，工作量最大的区块链就是权威的公共总帐本。

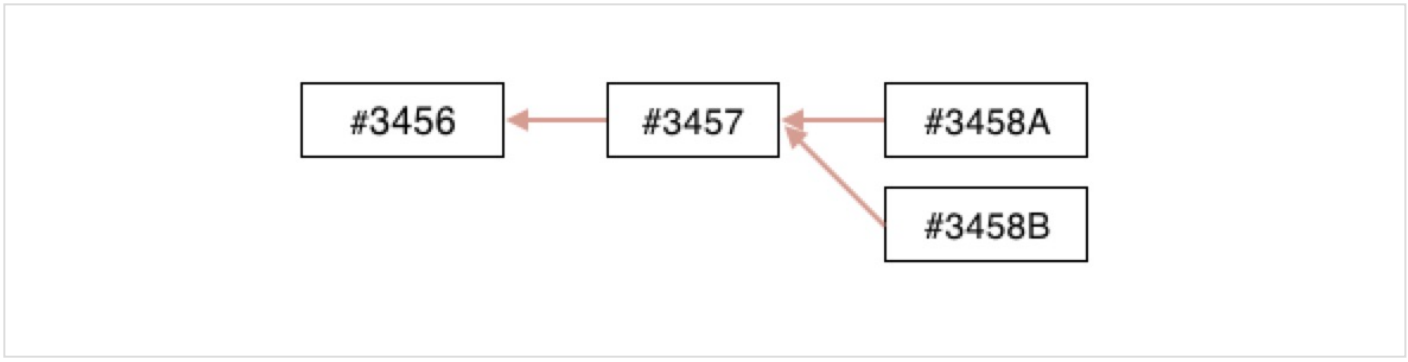
第1 2 3步在比特币如何挖矿-工作量证明一篇有提到过，下面着重讲第4步。

最长链的选择

先来一个定义，把累计了最多难度的区块链。在一般情况下，也是包含最多区块的那个链称为**主链**
每一个（挖矿）节点总是选择并尝试延长主链。

分叉

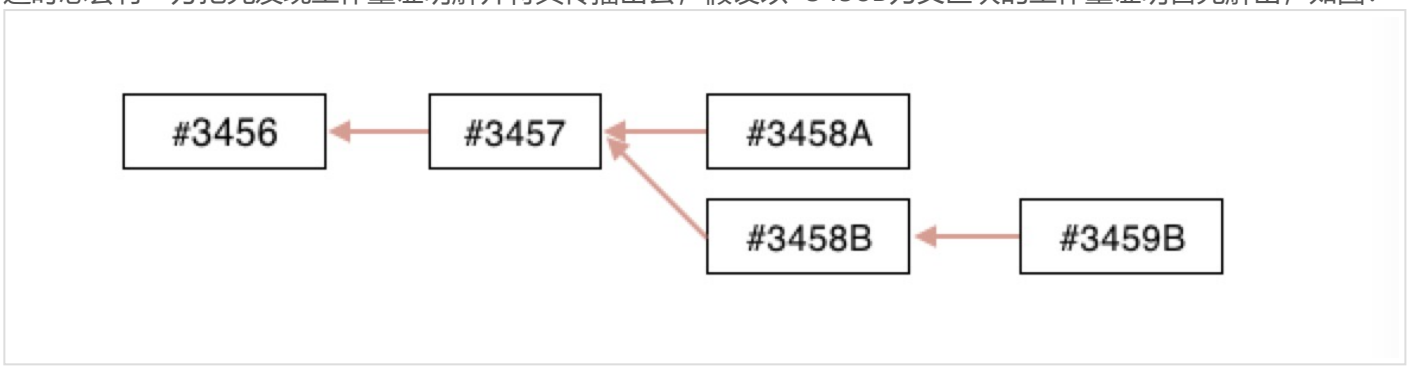
当有两名矿工在几乎在相同的时间内，各自都算得了工作量证明解，便立即传播自己的“获胜”区块到网络中，先是传播给邻近的节点而后传播到整个网络。每个收到有效区块的节点都会将其并入并延长区块链。
当这个两个区块传播时，一些节点首先收到#3458A, 一些节点首先收到#3458B，这两个候选区块（通常这两个候选区块会包含几乎相同的交易）都是主链的延伸，分叉就会产生，这时分叉出有竞争关系的两条链，如图：



两个块都收到的节点，会把其中有更多工作量的一条会继续作为主链，另一条作为**备用链**保存（保存是因为备用链将来可能会超过主链难度称为新主链）。

分叉解决

收到#3458A的（挖矿）节点，会立刻以这个区块为父区块来产生新的候选区块，并尝试寻找这个候选区块的工作量证明解。同样地，接受#3458B区块的节点会以这个区块为链的顶点开始生成新块，延长这个链（下面称为B链）。
这时总会有一方抢先发现工作量证明解并将其传播出去，假设以#3458B为父区块的工作量证明首先解出，如图：



当原本以#3458A为父区块求解的节点在收到#3458B, #3459B之后，会立刻将B链作为主链（因为#3458A为顶点的链已经不是最长链了）继续挖矿。

> 节点也有可能先收到#3459B，再收到#3458B，收到#3459B时，会被认为是“孤块“（因为还找不到#3459B的父块#3458B）保存在孤块池中，一旦收到父块#3458B时，节点就会将孤块从孤块池中取出，并且连接到它的父区块，让它作为区块链的一部分。

比特币将区块间隔设计为10分钟，是在更快速的交易确认和更低的分叉概率间作出的妥协。更短的区块产生间隔会让交易确认更快地完成，也会导致更加频繁地区块链分叉。与之相对地，长的间隔会减少分叉数量，却会导致更长的确认时间。