08 | 共识（下）：区块链领域的两类常用算法

2021-08-06 赵铭

《说透区块链》 课程介绍 >

讲述：赵铭
时长 13:24 大小 12.29M

你好，我是赵铭。

在上一讲中，我们通过对拜占庭将军问题的描述及推演，引出了分布式共识的基础知识，也论证了区块链共识的必要性。而这一讲，我将为你梳理区块链中常用到的共识算法。

说起对区块链共识最初的认知，我们几乎都能想到比特币中的 PoW，也就是工作量证明算法。

其实它只是众多区块链共识算法中的一个，虽然现在区块链领域中有很多种类的共识算法，但总的来说可以分为两类，一类是联盟链中用到的拜占庭容错算法，而另一类就是公链中用到的类似于 PoW、PoS 之类的算法，而我更愿意将它们统称为激励共识算法。

因为是两类共识，理解起来肯定有差异，但是我们却可以从上一讲故事里提取共识的基础要点来进行对比分析。我大致总结了三个要点。

1. 由谁来生产区块？因为区块链是去中心化网络，节点间权利与义务是对等的，因此在任意一个时刻，任何节点都可以生产区块。但是以谁的为准呢？这是我们在理解区块链共识时需要首先搞清楚的问题。

2.**什么时刻可以达成共识？**分布式共识其实也蕴含一个前提，那就是需要在有限的时间内达成各节点间区块一致。如果共识过程无限期，那么共识本身就不成立了。

3.**有多少节点参与了共识？**通过对拜占庭将军问题的解析，我们知道共识的达成跟叛徒的数量息息相关，不同的共识对于叛徒的容忍程度是不一样的，我们常听到的少数服从多数，51% 攻击等等说的就是这一点。

只要按照以上这三点思考和推演，我们理解共识就会显得比较容易。接下来，我就带你分别梳理一番。

拜占庭容错共识

所谓拜占庭容错共识，其实就是直接超脱于拜占庭将军问题的工程实践。

在上一讲的描述中，我们其实已经通过图例说明了达成一次共识需要哪些步骤保证，拜占庭容错共识就是将这些步骤通过缜密论证推理后形成的实践。而其中最著名的成果就是《实用拜占庭容错》算法，简称 PBFT。

这个算法解释起来很深奥，但是如果我们只看示意图，其实与我前面画的 A 将军共识示意图并没有什么太大的不同，都遵循相同的逻辑。只不过我们只是故事的推演，而 PBFT 却能实实在在用在真实场景中。

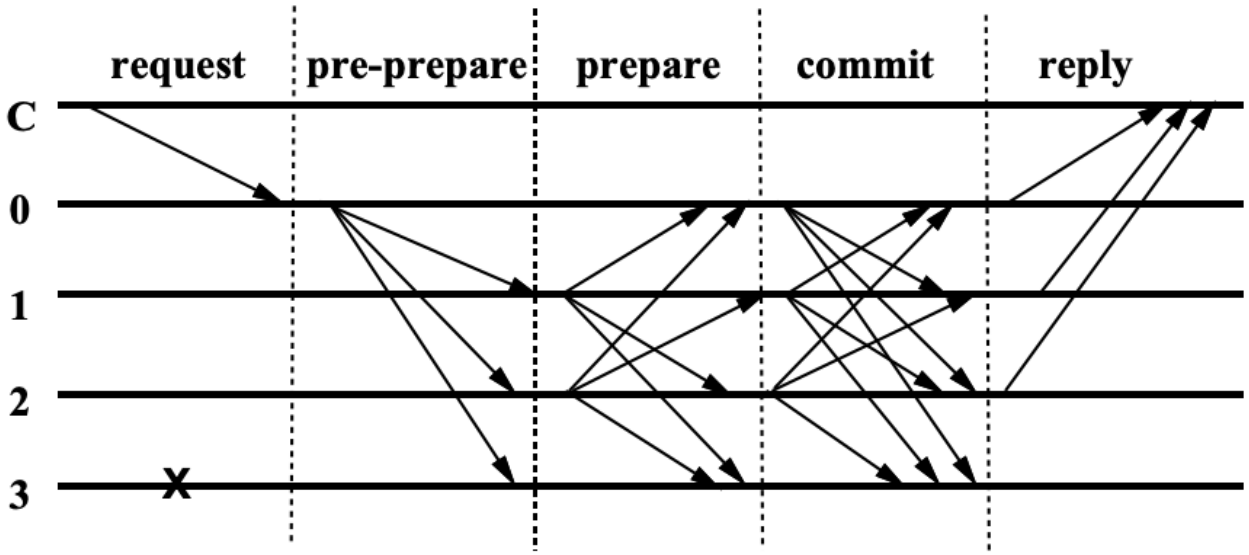

Figure 1: Normal Case Operation

PBFT示意图，来源于PBFT论文

从图中我们可以看到一个 request 被提交到 0 节点，再通过 0 节点发送给其他参与方节点，随之展开共识后续的流程。在 PBFT 中，节点被赋予主节点与从节点这两个角色，request 都从主节点发起，一次共识有且只有一个 request 存在。图中的 0 就是 request 的发起者，所以 0 是主节点。

如果从区块链角度来看，0 就是区块的生产者，且针对当前区块的共识并不存在潜在的竞争区块，也就是说在拜占庭容错共识中，主节点具有绝对的话语权。

当然，为了防止主节点作恶，节点角色是可以动态进行切换的，其他节点通过共识的结果可以推断出主节点是否是诚实节点，一旦主节点不是，则可以发起投票剥夺主节点的权利，这样就保证了系统的正常运行。

我们再从时间的角度来分析一下共识的流程，从图中可以发现，PBFT 将共识信息的流转划分成 3 步，每一步都包含着多次的信息广播通信。通信虽然需要时间，但是只要能走完整个流程，就代表着共识可以达成，而且一旦达成就不再改变，可以说拜占庭容错共识是**强一致共识协议**。

你可能对此有点疑问，如果遇上节点间网络通信中断，那共识不就不能够在有限时间内完成了吗？这个问题，如果我们换个角度来看，其实非常容易理解。

网络中断的节点其实可以算做一种作恶节点，虽然它的恶并不是有意的，但确实阻碍了共识的达成。而依据上一讲的结论，只要这个共识网络中作恶节点的数量并未超过总节点数的 1/3，共识依旧可以达成。就比如图中的节点 3，可以看作是因为网络问题，它并未响应任何其他节点的请求，但因为其他节点都是诚实节点，少数服从多数，这次的共识依旧成立。

另一方面，我们已经知道一次共识的达成，PBFT 需要进行多次的网络通信，而图中还仅表示的是只有 4 个节点的情形，如果将节点数进一步扩展，通信的要求就会指数级增加，因此它并不适用于有大量节点参与的场景。

这个问题也并不仅仅是 PBFT 才存在，而是任何类 BFT 的共识算法都要面临的共同问题，虽然它们或多或少都在 PBFT 的基础上作出了改进，但面临像比特币以太坊这类拥有大量节点的公链网络时，基本都束手无策。

所以，BFT 类的共识算法主要是链圈在推动，大多是用在联盟链中，因为联盟链主要参与对象是企业，有准入机制的存在，一条链的参与方不会很多也很少存在动态增删节点的情形，可以说**联盟链与拜占庭容错共识是天生一对**。

激励共识

然而，如果我们将目光转向公链网络，就会发现事情变得有些棘手了。比特币、以太坊等公链与联盟链除了拥有一致的区块链基本思想，其他方面可谓千差万别。

所谓公链，就代表着这是一个公开的、任何人、任何机构都可以**随时随地**参与的区块链网络。随时意味着网络中的节点可以任意的上线或者下线，不受任何约束。而随地意味着你可以在世界的任何地方启动节点，不管你是在珠穆朗玛峰，还是在亚马逊丛林，只要有网络，就没有人可以限制你的加入。

那在这样苛刻的分布式系统中，该如何保持节点间数据的一致呢？我以 PoW，工作量证明算法为例为你解析这类算法。

因为公链网络是公开的，没有任何人可以干涉别的节点，所以任意一个节点的动作都可以看作是网络的缩影，那任意一个节点可以生产区块也就意味着网络中所有节点都可以。那同一时刻肯定存在多个候选区块，这给共识的达成造成了不小的困难。

那中本聪干脆这样规定，虽然每个节点都可以独立的将自己一段时间内搜集到的交易打包成区块，但是你创建的区块必须满足一定的条件，否则就算区块被全网广播了，也是一个错误的区块，其他节点会拒绝接受，也就是说无法达成共识。

而这个条件就是利用哈希算法计算区块哈希，使得区块哈希以 N 个 0 开头，N 的多少取决于当前网络区块增长的速度，是一个动态调整的值。这样一来，**PoW 就限制了一段时间内网络中区块提案的个数。**

当然虽然增加了难度，但并不能保证在一个公开的网络中，不会有多个节点同时计算出满足约束条件的区块，并向外扩散。而且就算区块创建的时间有先后顺序的差别，但网络扩散是无序随机广播的，谁也保证不了谁会被先收到，极有可能一些节点收到了满足条件的区块 A，而另一些节点收到满足条件的区块 B，那到底以谁的为准呢？

这时候骚操作来了，区块链是区块通过区块哈希前后关联形成的链式结构，中本聪规定，**比特币网络允许有多条区块链存在，但只认同节点能接收到的最长的那条区块链是全网络共识的链**，其余短的区块链都是无效链。

这也就意味着，节点当前所累积的最长链可能并不是最终的结果，在某个时刻它可能收到比节点本地存储更长的链，此时节点就应该切换区块链，否则有很大概率它所维系的区块链并不是全网络共识的结果。

通过以上分析，可以发现在 PoW 共识中，并不存在对某一区块共识结果的实时确认，因为随时都有可能被其他更长链上的竞争区块替换掉。

通过这两条规定，比特币巧妙解决了如何在分布式系统中达成共识的问题。与拜占庭容错共识相比，在无节点角色区分的情况下降低了区块提案的个数，同时将一致性从强一致性放宽到最终一致性，虽然效率有所下降，但却达到了相同的效果。

这里我们还可以顺便从共识的角度，分析一下怎样保证比特币的不可篡改特性。作恶者如果想篡改区块，其目标就是要计算出满足条件的替代区块，并使得该区块所在的链成为全网中最长的区块链。

而区块哈希的计算几乎没有捷径可走，必须老老实实计算，这就要求作恶者必须拥有占比全网总的计算资源的绝大部分，才能有机会将自己篡改的区块链变成全网路中最长的链，

因为你在篡改的同时，被大多数节点认可的最长的链，它也在不断地向前延伸。

此消彼长，归根到底，**对比特币网络的篡改，实质是对计算资源（算力）的争夺，谁拥有更多的计算资源，谁的话语权就大，这也就是我们通常听到的 51% 攻击。**

而其他激励共识算法也遵循相同的道理，比如 PoS，权益证明算法，谁拥有更多的权益，就更有机会去争夺下一个区块的提案权。再比如 DPoS，委托权益证明算法，个人的力量是有限的，但是如果把很多人手中的权益集中起来，就可以以一种联合代表的形式参与到对区块的共识当中。与 PoW 相比，无非是减少了对计算资源的浪费，但本质并无差别。

最后，我还想谈谈激励共识算法中的激励。公链是公开的网络，可以看作是一个小型的社会，所有的参与方都是基于一个共同的目标，参与到社会的建设中，但这必须需要付出一定的成本，比如 PoW 共识的成本就是对计算资源的消耗、对电能的消耗。

如果没有激励，参与者的成本无从分担，就无法保证区块链生态的平稳发展。通过激励机制，使得各参与节点能摒弃信任中介，建立一种无组织、自协作的新型生产关系网络，并以此来吸引更多节点加入，共同维持区块链的正常运转。

总结

区块链中对共识的实现是有差异的，但是其底层逻辑是一致的。在联盟链的实现中，共识基本遵循了拜占庭容错共识算法的思路，这也与联盟链的应用场景有关。

而公链网络因其开放特性，并不十分契合拜占庭容错共识，但却创新性地引入了基于激励的共识算法系列。这不仅体现了对拜占庭容错共识的简化，还革命性地引入了社会治理思想，通过调动节点的参与积极性，共同推动区块链网络的繁荣。

自此，我通过 5 讲内容讲解了区块链中最常用到的四种基础技术，区块链节点把将一段时间内通过点对点网络收集到的交易集合，通过区块这种形式打包在一起，并前后通过区块哈希进行关联，形成一条由哈希构成的链式结构，通过达成区块的共识，在去中心网络中保持各节点状态一致。

1.拜占庭容错共识将节点进行角色划分。经过有限次数的网络通信，可在有限时间内达成共识。但随节点数增多，效率下降，因此仅适用于联盟链。

2.PoW在保证公链网络节点公开进出的基础上，降低了节点间候选区块提案数量，让网络可以达成最终一致性。

3.公链共识引入激励机制，结合社会治理思想，构建了一种无组织、自协作的新型生产关系网络。

说透区块链

赵铭 | 区块链服务平台资深架构师

讨论

你能否通过这 4 讲的内容，将区块链的三大特性与四种技术基础之间的对应关系，用你个人的理解通俗地概括出来呢？

扩展阅读

实用拜占庭容错共识算法是理论付诸实践的一次伟大尝试，建议你抽空啃一啃这篇论文，对你了解共识算法有很大帮助。

工作量证明与权益证明是公链网络中最常用到的共识算法，其他算法都是在其基础上衍生而来，通过这两篇文章你可以了解更多的知识。

关于区块链中的激励问题，我推荐你阅读中国人民银行数字货币研究所所长姚前写的这篇文章。

欢迎你在留言区跟我互动，主动思考、积极交流会让你更有收获。如果这一讲对你有帮助，也欢迎你把今天的内容分享给自己的朋友、同事。

上一篇 07 | 共识（上）：拜占廷将军也讲少数服从多数？

下一篇 09 | 智能合约：虚拟与现实的价值锚定载体

精选留言 (4)

写留言

Joeswooddd
2021-08-08

老师，我对51%算力攻击有些疑问，我的理解是通过累计大量的算力形成矿池，51%的算力能更快的产生区块，篡改者产生区块的速度大于其他人的速度，通过自己产生的长链在节点广播中代替其他节点中的短链，是这样的吗？

作者回复: 对的，是这样的。

三儿
2021-08-07

原文中“而这个条件就是利用哈希算法计算区块哈希，使得区块哈希以 N 个 0 开头，N 的多少取决于当前网络区块增长的速度，是一个动态调整的值。这样一来，PoW 就限制了一段时间内网络中区块提案的个数” 是不是像区块链POW本身的调节机制，像TCP/IP协议栈中的拥塞控制？

展开

作者回复: 你好，这个确实是可以这么类比看的。主要就是为了保证出块速度的绝对时间间隔，防止比特币挖矿奖励在很短的时间内被挖出，因为这样从长远看不利于生态的发展。

高鹏0409

2021-08-06

为什么规定最长的哪个链是共识的呢？如果本来是分支的链很短，后来追上来了呢？

作者回复: 为什么要规定：这是为了约束共识的一致性。就是要让参与者知道什么情况算是达成共识。就比如摇骰子，规定大数赢，那相比5,6是赢的。但是如果规定小数赢，那5就赢。类似的道理吧。

短链追上：这就是我后面提到的了，节点当前所累积的最长链可能并不是最终的结果，在某个时刻它可能收到比节点本地存储更长的链，此时节点就应该切换区块链。

1

漂泊的小飘

2021-08-06

老师，这个课程后面会不会给我们一个思路或者代码去实现一个简单联盟链呢？

作者回复: 你好，不会的。这门课程的定位是给所有专业背景同学看的区块链通识课，提代码的话就有些偏科了。

但我后面会提到推荐的联盟链实现