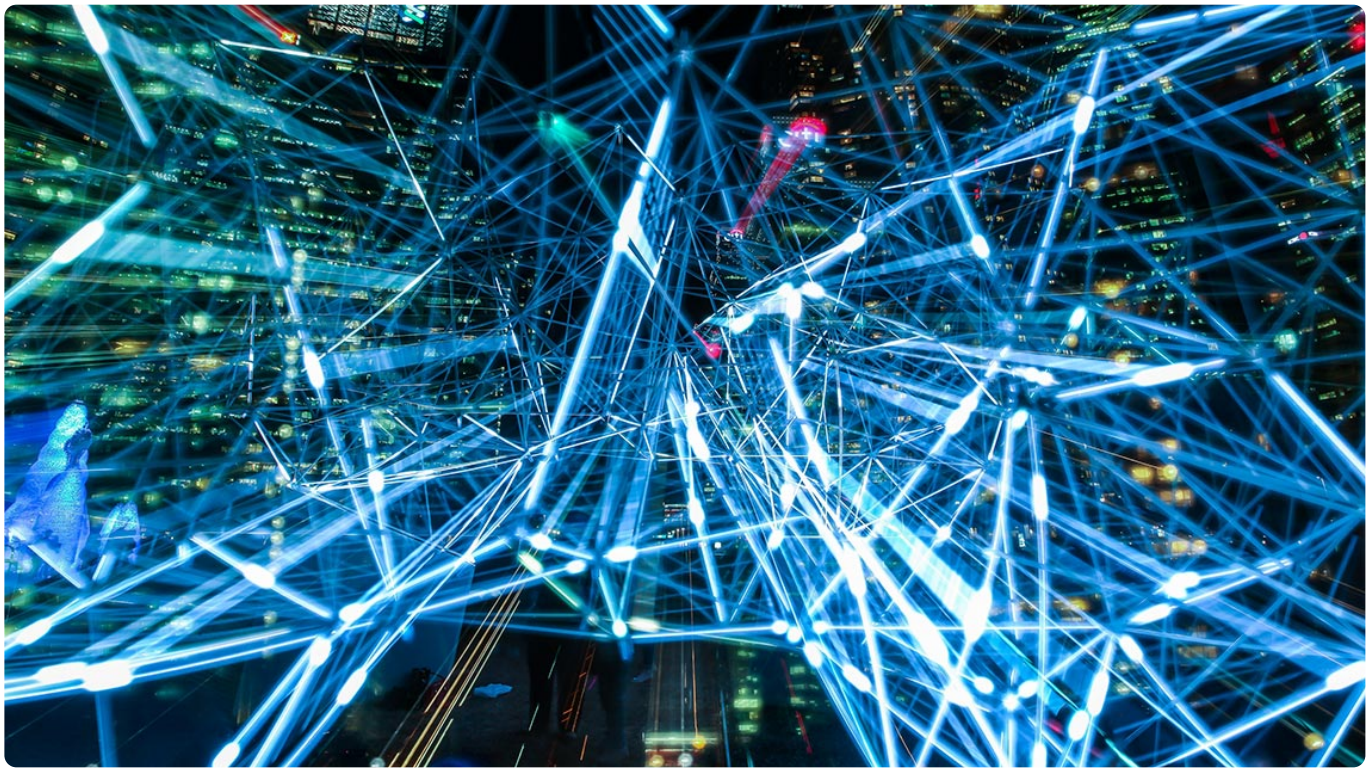
第3讲 | 浅说区块链共识机制

2018-03-30 陈浩

深入浅出区块链

进入课程 >



讲述：黄洲君

时长 09:43　大小 5.58M

我在第 2 讲“区块链到底是怎么运行的”一文中，提到了“打包 Transaction”和“广播交易”这两个概念，因为概述的原因，当时只带着你走了一遍过程。其实，以上谈到的两个内容正是区块链最核心的技术内容之一：共识机制。

区块链发展至今，已经形成了各种不同类型的共识机制，在今天的文章中，我们就展开聊一聊区块链共识机制到底是什么，以及区块链的共识过程到底是怎样的。

分布式系统的经典问题： 拜占庭将军问题

拜占庭将军问题其实是虚构出来的一个故事，是为了方便通俗地介绍分布式系统所面临的难题。这里我仅作一个简短的说明，你可以在中文社区找到更丰富的通俗解释材料。

为了避免重复，我们换一种表述形式，还是以上一次的村子为例，假设随着村子和人口的发展，大村子演变成了十一个小村子并分散在各地，各地的通信只能靠信鸽进行。

大家约定了每年都会举办一个相亲大会，至于谁能举办，每年轮流从两个备选村子，A 村和 B 村中选择一个，然后大家投票，票数多者可以赢得举办权。

由于地图很大，任何一个村子的投票都无法靠一只信鸽传输到每个村子，必须靠一个中继村子代为传输，这也就意味着有中继村子可以读到其他村子的投票信息。

那么，如何防止下面两个问题的出现呢?

1. 投票者的“精分”，这里所谓的“精分”是指某个村子的投票行为不一致，发送给第一个村子的投票消息为“投票给 A”，而发送给第二个村子的投票消息却为“投票给 B”。
2. 中继村子作弊，即篡改上一村的投票消息。

上面讨论的问题我们可以认为是简化的 “拜占庭将军问题”（完整的拜占庭将军问题还有将军 - 副官模型，如果感兴趣的话，你可以自行阅读）。

我们回头再看区块链。区块链本质上也是分布式系统的一种，其共识机制也是为了上述问题而提出的解决方案。

什么是区块链共识机制?

共识机制是区块链是核心的组成要素之一，它决定了区块链的业务吞吐量、交易速度、不可篡改性、准入门槛等等，是最为关键的技术要素之一。

要理解区块链共识机制，首先就需要理解区块链共识机制到底解决了什么问题。

共识机制主要解决了两个问题：

1. 谁有权利；
2. 作弊问题。

上一次我们构造了一个中心化记账的场景，在这个场景下，记账问题其实可以简化为大家信任中心记账者即可。

然而在分布式记账的场景下，问题更为复杂。首先，大家面临的最大问题是谁有权利记账，其次是如何避免记账者作弊。毕竟，谁都有权利记账，也就意味着谁都有可能作弊。

以上两部分共同构成了区块链共识机制。

另外补充一点，在比特币社区，“共识”（consensus）这个词已经跳出了技术的范畴。通常人们在表述一个比特币上的问题时，共识的内涵还包括比特币的使用者、开发者、矿工来达成□社区共识的部分，所以“共识”这个词在区块链领域还有些“民主”的味道，不单单是技术领域的“共识”。

最经典的入门型共识机制：PoW 工作量证明

PoW （Proof of Work）工作量证明可以解决上述的两个问题，

在上一篇文章中，其实我们已经悄悄讲解了一点 PoW 共识机制，你还记得上文提到的“24 点”那个游戏吗？“24 点”其实是尽可能随机地选取系统中任意的节点来规避作弊者，这个方案的实践其实就是 PoW 共识机制。

产生记账者的随机性其实来自于谁最先计算出 24 点的答案，这个问题可以简化成谁拥有的计算资源更多，谁就拥有整个系统的最大概率的记账权。一旦这个概率超过一半以上，那么这个系统就有一定的中心化风险。

如何理解上面一段话呢？

举个例子，李四家发明了一种算盘，可以快速计算 24 点答案，比起其他人掰手指头，李四家总是有很大的概率拿下记账权，换句话说，也就是李四和全村其他所有人竞争，相当于算盘对全村其他人手指头的竞争。

如果算盘足够强大，就能有一半的概率获得记账权，那么李四个人的诚实性，就成为了系统的唯一破绽。

比如李四在第一次记账时篡改部分交易，第二次还是他记账，还继续篡改交易，那么两次修改如果自洽的话，是可以形成假账的，这就是所谓的中心化风险。

所以在 PoW 这种机制中，计算资源（又称算力）是决定记账权的唯一因素。与之对应的，便是计算难度。

计算难度又称作挖矿难度，计算难度是区块链为了控制产生答案的速度，比如平均 10 分钟就有一个答案产生，平均 2 分钟一个答案产生。

在上述场景中，因为李四有了算盘，强大的计算资源突然加入以后，肯定会让整个系统的□产生答案的速度变快很多，作为系统本身会自适应，将难度提升，降低□答案产生的速度。

上面介绍了这么多，其实是想引出另外一个问题，PoW 到底是如何避免作弊者的呢？答案就是计算资源（算力）。

设想，如果一个作弊者想篡改信封里面的交易，首先得获得记账权，也就是装信封的权利。

而影响记账权的唯一因素只有计算资源（算力）的大小，如果想篡改交易，只能投入大量的计算资源与整个系统中其他所有人进行对抗，这是十分困难的，尤其在整个系统有一定基础计算资源（算力）的情况下。

PoW 中一个有趣的设计是激励机制，在 PoW 共识机制下，我们假设所有参与者都是理性的，理性的意思就是单纯逐利，不考虑家庭、爱好等其他因素。有了理性的前提，PoW 共识机制会给每个诚实的记账者予以奖励，这个设计可以抗击作弊收益的问题。

怎么进行抗击的呢？整个过程是这样的，理性的人如果作弊、篡改账本肯定需要投入成本，也就是计算资源，收益是篡改账本获得的收益减去投入成本，这个收益往往小于诚实计算所获得的收益。所以，作弊者在作弊过程中投入的计算资源过大，反而得不偿失。

PoW 工作量证明的补充：解决双花攻击

上面给出了一个结论，我们说作弊的收益往往小于诚实计算的收益。这一点其实对应到区块链领域有个著名的问题：双花攻击（double-spending）。

双花攻击是指一个代币被花费了两次，这在任意的区块链系统中是不被允许的。如果避免了双花问题，基本就能避免上述作弊中收益过大的问题，因为攻击者首先要窃取到你的私钥，同时又能控制了你的计算资源（算力）。

为了方便分析，我们回到上一篇中广播交易的那一节。那一节中我介绍了广播的内容分为两种，第一种是 Transaction，第二种是区块，也就是信封。

第一种又被称为未确认的 Transaction，第二种信封中所有的交易被称作已确认的 Transaction。

所有记账节点都会遵循以下两条规则：

规则一：一个代币如果已经被花费，那么会被标记成已花费，如果再次接收到这个代币被花费的请求，那么记账节点会拒绝打包这笔交易；

规则二：如果同时接收到两个信封，这两个信封中装的两笔交易出现了一个代币被花费了两次的情况，这种情况也就是我们所说的分叉（Fork），那么选择挖矿难度比较大的那个信封。

规则一避免了未确认的交易出现双花，规则二基本避免已经确认的交易中（信封中）的双花问题。

假设作弊者的计算资源（算力）占整个系统的 30%，那么连续两次获得记账权的概率是 9%，看起来作弊的可能性还是挺高的，如果是连续 6 次获得记账权呢？概率直降到万分之七。

在比特币中，这个 6 也就是 6 次确认，表示连续 6 个块过去了，如果我的交易没有被双花的话，那么它被篡改的可能性将越来越小，最后变得几乎不可能被篡改。这也是区块链不可被篡改说法的由来。

试想，如果任何作弊者花了大量的成本获取了系统 30% 的计算资源（算力），最后只有万分之七的概率获得篡改的可能性，比起作弊，还不如诚实记账的收益高。

总结

好了，今天带你了解了区块链的共识机制，也顺便浅谈了拜占庭将军问题，介绍了区块链的入门共识机制 PoW，它其实也是目前区块链领域使用最广泛，应用最成熟的共识机制。

最后，还涉及了一部分 PoW 工作量证明的补充：解决双花攻击。由于篇幅所限，我们将在技术篇详细讲解 PoW、PoS、DPoS 等共识机制。

那么，亲爱的读者，你觉得 PoW 共识机制和其他分布式一致性算法有什么不同吗？欢迎给我留言，一起讨论。

感谢你的收听，我们下期再见。

上一篇 第2讲 | 区块链到底是怎么运行的?

下一篇 第4讲 | 区块链的应用类型

精选留言 (38)

写留言

阿痕
2018-03-30

12

PoW算法的特色是结合了经济学上理性人的假说，发明了激励机制，让做好人的奖励大于做坏人的获利。但我觉得比特币每4年递减的特点可能会导致这个天平被打破，比特币奖励越来越少，而比特币总量越来越多，是否意味着某一天可能作恶的收益要大于做好人的收益呢?

作者回复: 1. 可能的，不过这个周期非常长，临界点可能在这个世纪末，但由于不确定因素非常多，多因素综合，例如到时比特币100万美金一个，即使低收益只要可以覆盖成本即可，而且作弊是概率的，只有期望值。所以足够的时间会发现新的算法来修正PoW，或切换其他共识
2. 比特币的总量是恒定的

Alexcsl
2018-03-30

6

关于双花问题，如果双花交易同时出现在两个区块中，那应该根据挖矿难度的大小，自动舍弃一个区块，保证只有一次花费被确认。这和算力，连续六次记账的概率有什么关系呢？是因为进行双花攻击的时候，是把两笔交易记在同一个区块里，一旦由另一个节点进行merkel树检验，会发现异常，必须由攻击节点连续记录六个区块么？还请老师解惑

展开

作者回复: 已在其他回复中回答。

酱了个油
2018-03-30

5

对六次确认的描述比较困惑...

展开

finch
2018-03-30

5

pow跟一般分布式算法的区别在于，pow是有激励机制，并且作弊是要有代价的，代价与激励之间的博弈使得比特币过得安全。个人见解。

静。安
2018-03-31

3

老师作为一个软件开发人员区块链技术应该向什么方向学习呢，还有前景问题，望老师解惑，谢谢！

作者回复: 1. 公链开发。偏底层
2. 区块链应用开发。 偏智能合约

两个都需要区块链基础知识作为支撑，先打好基础，再找方向o(=•ω < =)ρ⌒☆。

4Neutrino
2018-05-25

2

老师好，有点疑问，算力强大的单位，就算难度提升了，那他挖矿成功的概率还是高啊？这似乎没有解决中心化问题吗

作者回复: 问题是这些算力有没有进入门槛，如果没有，普通人也可以介入，那么就是公平的，算力中心化的威胁只有51%攻击，实际上达到51%，矿工的攻击动机也是不足的，因为很容易被发现，攻击成功会造成用户流失，短期收益很高，但是断了自己的长期财路，矿工一般不会选择攻击。所以问题就演变成攻击是否可以被公众感知。

TaoLEE
2018-05-01

2

为什么说共识机制有"民主性"?

展开

作者回复: 共识机制狭义上指分布式一致性，实际上也可以拓展到区块链治理共识。

昊
2018-03-31

2

你好，请教一个问题，比特币中的币和对应区块链的区块是一个东西吗，如果不是，那币具体是什么

作者回复: 币是业务逻辑，区块是技术逻辑。币是网站积分，区块是数据库的表。

席彬
2018-03-30

2

陈浩老师好，有两个问题请教
1双花攻击中后一个区块如何验证前一个区块是否“作弊”
2区块链产生分叉后，新产生的区块如何“选择”加入哪一个分支

展开

作者回复: 你好。

1. 每一笔交易记录都是有前向输入的，如果已经被花费过，则状态已经变更为已花费，再次话费

共识验证的代码会检验不过，拒绝被打包。这个我曾经在比特币上干过，修改本地节点代码后发起攻击，交易不会被打包，除非全球的矿池同时重启，也是概率会成功，仅限未被确认的交易。

2. 通俗说法叫做所有节点跟随最长的一条分叉链，共识代码规定的。专业的说法叫做“难度”累积最大的一条链。

Qiubh
2018-05-05

1

每一个区块里都保存着所有的交易信息吗？还是说要获取所有交易信息需要一直往上遍历？

作者回复: 后者。

123456
2018-04-12

1

老师，您好，请教一下：看了文章和您在讨论区的一些回复，还是没搞明白挖矿和比特币的关系，您打的比喻：挖矿产生的区块相当于数据库，而比特币相当于积分，这个怎么理解呢？这是说比特币是写在对应区块的一笔交易记录吗？还有是不是每产生一个区块就会派发一个比特币？比特币归属怎么来记录呢？每个区块里边是不是可以无限追加交易记录？我这还没入门，希望老师赐教哈

展开

作者回复: 1. 积分记录在数据库的表中，谁有权利创建新表，谁就能获得积分。
2. 比特币是表中有效的未花费记录
3. 一个区块就是一张新表，表可以哈希后串起来
4. 不是无限的，有区块容量限制

Hollis
2018-04-03

1

我有个问题想问下：

工作量证明的题是谁出的？如何保证节点收到的题是一样的？

展开

作者回复: 细节我们会在深入技术一章中讲。
每次难题都是基于当前全网的状态和上个区块作为输入，所以每个人得到的难题都一样。

yhkang
2018-03-31

1

每次打包交易，节点都需要检查创世区块以来的所有区块才能确定交易发送方是否有足够的余额吗?

作者回复: 不用，像链条一样，一个套一个，所以只需要验上一个。

酱了个油
2018-03-30

1

分布式存储的一致性的算法并不判断数据真伪的问题，不具备防篡改的能力，抛出备份数据，它维护的是仅一套数据，它本身是中心化系统的一部分，与区块链有本质区别。存储方式上来看，更像“只存储数据为主的cdn”。

展开

蜡蜡
2018-03-30

1

陈老师，您好，认真看了五遍，还是不太懂共识机制和工作量证明的原理。望陈老师指点:
共识机制是为了全网形成形成正确的共识:
1）原文易被篡改;
2）收信人无法验证原文是否被篡改;
其中工作量证明相当于去猜福利彩票双色球的中奖号码：你只要趴在桌上写啊写，就一...

展开

作者回复: 原交易不被篡改是由非对称加密保证的，这里说的共识是大家达成一致记录，不被扰乱的过程。
工作量证明与彩票，可以这么理解。重点是中奖之后的逻辑。

少
2018-03-30

1

有个问题我一直没弄懂，就是每个代币交易过之后就会被标志为已花费，那么在交易市场“比特币”等代币可以反复的被交易，这好像是矛盾的。是不是“交易”和“花费”的概念不同还是收到的代币和支出的代币不是同一个代币？

> 作者回复: 货币是同质的。如果你用纸币，你一定不关心这张纸币是哪里来的，你钱包里的纸币已经经过千万人之手了也说不定，还依然在交易。
> 花费是动作，交易是描述一件事情的记录。中文的交易都对应trade, tansaction。概念上是不同的，交易市场是trade。后面我们讲数字货币交易所会详细剖析

学习
2019-04-27

看了头几篇，作者表达不够清晰、不够通俗，术语太多，逻辑漏洞也多，关键地方不讲透，让人困惑重重。
看着令人累觉不爱。

展开

朱秀芹
2019-03-24

老师，你好。请问对确认交易的双花会产生分叉我有些疑惑。首先，确认下概念，确认的交易是否是指交易放在了区块里，但是还未经过信封确认未放到区块链里。其次，如果我的首先假设成功的话，那么一个区块中会有多个交易，就因为这个区块中包含了双花的交易，我就放弃这个交易，那么这个区块中的其他交易怎么处理？还会处于游离状态，被打包到新区块吗？最后，多个区块里面的交易是否会重复？比如我打包了交易1和交易2，...

展开

Awumbuk
2018-11-18

老师你好，为什么信封中装的两笔交易会出现一个代币被花费了两次的情况？

展开

Happy
2018-10-09

大佬您好 所謂一個区块被打包 需要6次确认 是判断拥有6次记账权？还是什么意思 ， 所谓的6次确认是怎么确认的 谢谢

作者回复: 一次确认就代表已经刚刚被打包进区块，两次确认就代表又产生了一个新块引用这个区块，链式引用，引用越多就代表被篡改的可能性越小，6个确认是在概率上认定为基本不可能被篡改了，所以6次只是一个建议，由用户自己选择的，当前比特币网络很稳定，一般1~2就可以认定有效，以太坊一般是12个。