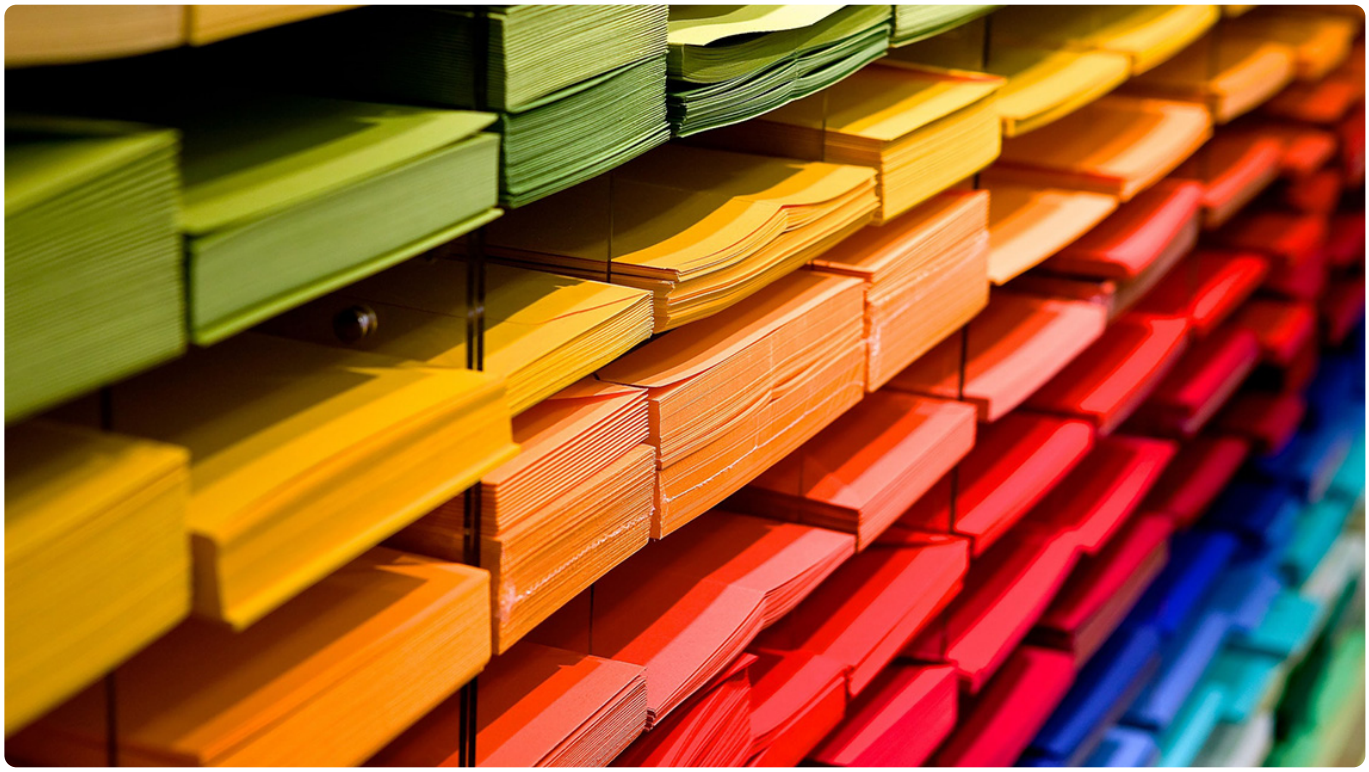
第2讲 | 区块链到底是怎么运行的?

2018-03-28 陈浩

深入浅出区块链 进入课程 >



讲述：黄洲君
时长 12:09 大小 5.57M

上一次，我们聊到了区块链的概念及整个行业的发展过程，今天我想稍微深入一下，尽可能通俗地介绍一下：区块链到底是如何运行的?

这一篇文章我将以比特币区块链为例来进行讲解，理由有两个：

1. 由于区块链发展到目前阶段，各个技术方向都有长足的发展，那么为了方便你理解，我在这里介绍最简单、最容易理解的□比特币区块链；
2. 由于大部分区块链都是以比特币区块链为基础进行扩充的，所以首先了解比特币区块链有助于其他项目区块链的后续学习。

中心化记账的问题

首先，我们借鉴了一个区块链描述中的经典情景来模拟中心化记账。

假设有一个有百户居民的村子，其中有一位德高望重的村长，村长有一个儿子。村民们都把钱存到村长家，村长负责记账。比如，张三用 1000 买了李四家的牛，村长就把张三名下的存款减去 1000，李四家加上 1000。听起来是不是很像银行的操作?

对，我们就是先从中心化的银行记账开始聊起。村民都相信村长，才愿意把钱存到村长家，他们相信村长不会作恶。

可惜好景不长，老村长由于操劳过度，驾鹤西去了。新上任的村长儿子铁蛋很是聪明，但也有个毛病，就是粗心大意。他不但经常算错账，一次还被人偷改了账单。

不过，幸好村民自己都有记账，但是由于铁蛋每次错账后都要和别人核对半天，导致村民对新村长的记账能力十分不满。

时间就这么过着，然而最可怕的事情还是发生了，铁蛋的老婆竟然私下篡改账本，给铁蛋七大姑八大姨的余额全部偷偷加了好多，终于有一天事情暴露，村民们气冲冲地跑到铁蛋家里讨说法，于是一片混乱。

这时候有个叫中本聪的人站了出来，他说他设计了一套系统，可以不依赖任何人记账，于是，众人开始将目光集中到他的身上。

1. 公开记账

中本聪说他的系统稍微麻烦一点，需要干三件事儿。

1. 每家每户都派发一只信鸽。这就是 P2P 网络，是一个点对点的分布式网络，如果不好理解，你先不用理会，我会在后面讲到。
2. 每家每户都发一个特殊的印章和一个扫描器。这个扫描器有两个功效，一是识别他人的交易是否真实有效，二是识别这个交易是不是自己账号的，□同时识别并解锁未花费的余额。这就是非对称加密。
3. 每家每户可以参与记账，不过不再记余额，而是记交易本身的内容。这就是区块链中的交易，这个“交易”对应的英文单词是“Transaction”，这是个专有名词，专指一笔账，不同于金融交易的 Trade。

这三条总体来说其实是干一件事情，就是：

每家每户都记账，账簿上不再记载每户村民的余额，而只记载每一笔 Transaction，即记载每一笔交易的付款人、收款人和付款金额。

那么问题就来了：如果每户都记账，肯定每户的账都不统一啊，你记你的，我记我的，最后不全乱了么?

这个时候需要大家统一账本，保证大家的账本都是一致的。因为记录的交易是全村所有人有序产生的，所以这就需要有一个广播机制。这个广播机制，我先卖个关子，后面再讲。

中本聪说，其实很简单，我们现在先把全村所有人的资产都加起来。还真巧了，刚好 100 万。

中本聪接着说：“只要账簿的初始状态确定，并且每一笔交易可靠并按照物理时间自然记录，并且只加不改不删，这样，当前每户持有多少资产是可以推算出来的。”

中本聪说我现在把我的印章给你们看，这个印章很特殊，盖的章有两块标记，第一块是一个可以识别的标记，比如我往纸上一敲，可识别的标记是 1MsTg2。

这就是你们的代号，由于我们账本是公开的，使用真实姓名会很危险，所以你们记账的交易单上收款人、付款人都填这个码，不用写姓名。你的扫描器和你的印章生成的代号是关联的，有且仅有持有对应扫描器的人才能花费金额，这一步即为“解开交易”。

刚刚说印章有两块，这第二块内容配合这个扫描器才能看，肉眼看则都是乱码，扫描器一扫就知道第二块内容是否有效，这一步也就是“交易验证”。

并且所有交易大家都能接收，都能看到，但却解不开印章乱码部分的内容，仅仅收款方才能解开，因为你的扫描器和你印章生成的代号是关联的，有且仅有持有对应扫描器的人才能解开交易。

以上就是区块链中“公开记账”的过程。“公开记账”就是全网所有人都可以随时查看一套账本，然后按照规则透明公开地进行记账。

2. 创建创世区块

创世区块是我们生成全村公开账本的第一笔交易的第一个信封，好比一篇文章总得有个开头一样。

于是乎，中本聪说我先生成第一个 Transaction，这个交易单的付款人为空，收款人是村长，付款金额是 100 万，因为是创世区块，产出多少个是可以随意规定的，由于我们上面统计了全村的账目情况，所以我就写了 100 万，待会儿付款给村长以后，我们可以按照原来的账本给大家发送对应的金额过去。

好了，我们有了第一笔交易，第一个信封也已经做好了。现在让村长把信封传给张三，张三复印一份，然后传给李四，李四继续传下去，一传十，十传百，直到传给全村人，这个步骤也就是“同步区块”，也就是全网都拿到这个信封，以及信封里面的 Transaction。

3. 交易

由于上一节我们的创世区块把 100 万交给了村长，那么我们假设张三在村长那里的存款余额是 10 万，这时候村长要根据原来的旧账本，把这 10 万发送给张三，然后把旧账本上的账划掉。下面我们讨论一下如何构造这笔交易。

中本聪开始教村长写交易单，把 100 万分成两部分，第一部分 10 万，收款人是张三；第二部分是 90 万，收款人是自己；这样一个 Transaction 就做成啦。

前面我们说了，不能直接写名字，要写代号，这个代号也就是你的钱包地址，我们需要把收款人写名字的地方，让收款人拿出自己印章，把代号读出来，然后告诉村长即可。

100 万　10 万，张三
　　90 万，自己

村长写好 Transaction 以后，还需要拿出自己的印章，在 Transaction 上盖章，这个盖章的过程也就相当于区块链中的签名。这个章，全村人都可以拿扫描器扫一下验证是否有效，即验证付款人的章是否有效。

100 万　10 万，张三的印章（1s25vR）
　　90 万，村长的印章（13gYip）

就这样，村长一共写了 10 份 Transaction，分别代表了发送给不同人的交易，张三一笔 10 万，李四一笔 1 万，等等。

4. 打包 Transaction （挖矿）

现在我们有了 Transaction，但是还需要东西把 Transaction 装起来，我们用一个特殊的信封把 Transaction 装起来，这个信封就是区块链中的“区块”，这个封装过程就是“打包交易”。

为什么要封装起来呢？是为了让打包交易的人能够在信封上署名，表示这次打包是由某某某打包的，其次全村的交易可能非常多，需要装配标号，方便大家查询。

我们看到上述的 Transaction 虽然已经生成，但是有个问题，就是没有规定谁有权利把 Transaction 封装到信封里。

我们在开篇的故事中看到了中心化操作肯定是不行的，假设在全村人中，这时候如何筛选出这些打包的人呢？

中本聪这时候说了，由于我们村的人口增长，100 万未来可能不够，我们暂定 150 万，那多余的 50 万，我们就当奖励给这些装信封的人了，当然不能一次性给，谁装一次信封就领 3 个币。

这时候大家伙儿来劲了呀，只要装信封就能够领钱了，我们在这里把符合条件的人称作“矿工”。

但是中本聪又说了，要获得这个装信封的权利，是有条件的。我给大家出一个难题，谁先解出这个难题的答案，谁就有权利把 Transaction 装到一个信封中，并且要在此信封上盖上自己的章。

这个难题是这样的，它有两大特性，第一是容易验证，第二是计算过程非常复杂。

例如，有种棋牌类游戏叫作“24 点”，玩法就是给出任意 4 个整数，通过整数运算得到 24，比如现在给出 2、9、1、5 四个数，答案是（5-2）*（9-1）= 24。当然，本处仅是举例，“24 点”游戏的答案空间非常小，□是远远不够生成信封的。

答案非常好验证，但是计算过程是一个尝试的过程，需要耗费大量的精力。而在真实的比特币中，采用的是寻找符合条件的目标哈希，这也就是比特币矿工所做的事情。

好了，这时候大家开始计算给出的难题，刚好李四第一个计算出来，那么这次装信封的操作就由李四完成，李四把 10 份 Transaction 装到信封中，也就是打包 Transaction，并且要

在信封背面写上一个信封的□摘要信息。

比如上一个信封中的第一个交易是什么、信封封面长什么样，最后要在信封上盖上章，也就是“签名”，矿工签名的目的是为了领币，也就是 Coinbase 交易。

以上过程在区块链领域称作“打包 Transaction”，也就是大名鼎鼎的“挖矿”。

5. 广播交易

来说说上文提到的广播交易，广播是为了让全村人知道当前时刻你产生了一笔 Transaction，或者是你装好了一个信封。

广播的内容分两种，一种是广播 Transaction，一种是广播信封。第一种广播是意味着还有未被打包的 Transaction，而第二种广播信封则意味着这个 Transaction 已经被某个矿工确认。

收到了广播的通知后，大家先验证信封上难题的答案是否正确，这样便可以验证出信封是否被伪造，接着验里面的每笔交易，最后还要验证信封背面的内容，即上一个信封的摘要是否正确。因为上一个信封大家都已经确认，所以这样可以极大地规避作弊的可能。如果觉得没问题，就可以存入本地数据库中了。

□至此，全村人的记账问题就差不多解决啦。

总结

今天我用非常浅显的例子与你聊了比特币区块链，其中包括区块链中公开记账、创建创世区块、交易、打包 Transaction、广播交易的几个步骤。

因为篇幅所限，□在表述上可能会有不精确的部分，但是大体意思是相通的，相信读完文本，你已经对区块链的原理有了一个大致的了解。

你也可以针对每个模块进行扩展，比方更换矿工的计算方法，可以推导出 PoS 共识机制，不知道你还能想到哪些扩展呢？欢迎留言探讨。

感谢你的收听，我们下次再见。

本文叙述模式参考链接：
http://www.8btc.com/bitcoin-story?_t=1520884553

上一篇 第1讲 | 到底什么才是区块链?

下一篇 第3讲 | 浅说区块链共识机制

精选留言 (61)

写留言

蜡蜡 置顶
2018-03-29

27

陈老师，您好，非常精彩的讲解了比特币到底是怎么运行的，个人对比特币运行的整理与思考如下，欢迎讨论：
步骤1：召集全村每家每户， 一起共同记账。
1）高薪招聘记录账本人员： 人人都可以参与，只要每次谁记录的最快又最准，每次可以拿到丰厚的报酬。...

展开

良辰美景
2018-03-28

27

作者你好，我读了几遍，仍然还是不太明白，有如下问题，希望能给解答一下：
假如现在有A村民（有50万）与B村民，A转账10万给B
文章说需要在这个交易上写的信息如下：
10万，B章
40万，A章...

展开

作者回复: 1. 不需要的。村民A如果有50万，转移过程由村民A盖章即可，其实这更像咱们的实体纸币，纸币100在花费的时候，现场确认是你掏出来的就行。钞票本身的面额就是50万，不需要检查的。
2. 村民C是无法解开交易的，扫描器和章是一对的。扫描器其实有两个功用，一个是可以验证别人的章是否有效，第二是识别属于自己的交易。
3. 是的，存在每个村民的家（本地持久化存储）中。快速理解就是每个村民家中都有一套日志型的账本，有点像数据库的binlog，是无状态的。每家收下的所有信封连在一起就是重演历史交易
4. 账单是全冗余的，所有节点都保存了副本。节点数量是开放的，动态变化的。
5. 一个区块是由大小上限的，比特币的上限为1MB一个块，曾经出现了网络拥堵的情况。上万TPS的区块链系统是由的，不过从架构上看更中心化一点。这个我们会再后续文章有详细讲解

near
2018-03-28

14

请问老师：例子中说拿出50万奖励封装信封的人，当这50万奖励用完以后，后续产生的交易信息由谁来封装信封呢?

陈建斌红了...
2018-03-28

9

怎么广播，难道每个节点要保留所有其他节点的ip地址吗

展开

作者回复: 是的。仅保存临近节点，临近节点接力

teletime
2018-03-28

8

这样记帐的话，随着时间推移，总帐无限增大，每次计算一个帐户的当前余额，要追溯的历史链越来越多，效率能撑住？

LuDi
2018-03-29

7

配一些图来说明的话，会让读者更容易理解呢？

展开

作者回复: 谢谢建议，到深入讲解模块会配图的。

ync
2018-03-29

5

作者您好，阅读后我收获很多，但有个问题不太清楚：交易为什么不记用户余额？不记得话每次交易都要翻老帐，当用户量和交易量上去的话效率会不会很低？

展开

作者回复: 你好。
区块链有两种记账模式，第一种是我们正在举例讲解的utxo模型，另外一种是你说的记余额模式。交易效率不会低的，但是会影响同步效率。
utxo是无状态的，余额是有状态的。后面utxo一文我们会有详细讲解这两者。

胡敏
2018-03-29

5

我理解 打包交易 的的前提是有交易，如果交易量不足，哪些所谓矿工为啥可以一直挖矿呢

作者回复: 交易笔数至少会有一笔。这一笔叫做铸币交易。又称coinbase。这种区块我们叫做空块。属于正常情况

Corey
2018-03-29

4

（1）矿工打包交易时，计算出目标哈希，是怎么实现易于验证的？

（2）全网有没有可能，同时超过2个矿工同时计算出目标哈希，如果出现这种情况，网络是怎么处理的?
（3）目前btc使用1M，bch使用8M，扩容可以提高交易量，带来的问题有 带宽、存储、计算，但是目前btc也基本都是专业人士在挖，扩容还带来了其他什么问题吗？...
展开

作者回复: 1. 简单来说，就是所有人把这位矿工的计算原结果再计算一次。如果符合前n位是0就证明是有效的
2. 网络不存在绝对的同时。这种情况再观察下一个块的产生，如果其中某一条链“长度”大于另外一条，则废弃短链。这种情况的概率叫做孤块率，越低越好
3. 扩容之争有很多备选方案，比特币社区争论了很久，导致社区分歧才有了bch。专业矿机的产生不是扩容导致的，扩容后续我们也会讲。
4. 不是必须

ytl
2018-04-03

3

如果两个矿工差不多时间解除难题，都暂时认为自己获得奖励，区块链产生自然分叉。通过竞争，几个区块后只有一条链最长，所有矿工都追随最长链。前面以为自己得到奖励的矿工并没有真正得到奖励。
展开

作者回复: 嗯嗯，我们理解一致。“最长”其实是难度累计最大，而不是高度。

万历十五年
2018-05-27

2

1.数字签名主要解决了“谁干了什么”的问题
2.打包主要解决了“篡改”问题，使篡改成本变高

羽惑飞
2018-04-02

2

50万被旷工挖完后谁来打包?
展开

石标
2018-04-01

2

你好，请问挖矿的奖励谁来付？

展开

作者回复: 系统凭空产生的，所以叫挖矿。

Andy
2018-03-29

2

老师你好，非常感谢你的精彩内容呈现，关于你提到的总帐户约定为100万，矿工交易费备用金为50万。我有个疑问，比如像比特币平台，它是怎样约一个总交易帐户数额，以及交易打包矿工费用的预备数量？我理解是像目前比特币每天都会产生交易，这样每天就会支付交易的费用，这不是会导致备用金一直在递减吗？最终直到备用金为0后，怎样又重新调整那备用金帐本金额呢？谢谢！

展开

作者回复: 你好。100万相当于发行总量上限。矿工收到的手续费可以再流入市场。并没有消失。所以总量恒定。目前比特币交易平台是中心化的。是链下交易记录。后续咱们有文专门讲交易平台

鸿飞
2018-03-29

2

老师费心了，这么复杂的知识放到一个故事里面了，赞

展开

小颜
2018-03-29

2

老师我问下，比如A给B转帐10块，交易方是A(A的代码替换)，收款方为B(B的代码)，那请问A是怎么知道B的代码的

feiandyta...
2018-03-28

2

为什么一个交易记录有两个收款人？应该是一个收款人和一个付款人才对吧？

展开

纯洁的憎恶

2018-08-16

1

分布式存储，每一个节点可以通过接收广播，获取所有节点的交易信息并存储，但只能通过个人秘钥查询本节点为收款方的交易。写入一笔交易时，收款人要把自己的代号告诉付款人，有付款人写入交易信息，并签名（用于辨别真伪）。每一个节点都存有其他所有节点的签名，只是非自己的签名不可见，用于自动验证系统中发生的每一次交易的真实性。

展开

泡泡

2018-06-08

1

“为什么要封装起来呢？是为了让打包交易的人能够在信封上署名，表示这次打包是由某某某打包的”这句话没有逻辑性吧。为什么要装起来，是因为要让装起来的人写是他装起来的，那他为什么要装起来，不装不就不用写了吗？

展开

作者回复: 为了获取奖励哦，不写就没法发奖励。coinbase

王志波

2018-04-08

1

需要解答的问题是由谁来产生呢？负责打包的矿工吗？还是分布式网络中的某个节点？

作者回复: 都是对等的，任何人都可以成为矿工，其次也是网络中的某个节点。