

33 | 区块链技术架构：区块链到底能做什么？

2020-02-07 李智慧

后端技术面试38讲

[进入课程 >](#)



讲述：李智慧

时长 13:45 大小 11.03M



在我的职业生涯中，我经历过各种各样的技术创新，见识过各种技术狂热的风潮，也看过各种技术挫折，但从来没有一种技术能像区块链技术这样跌宕起伏，具有戏剧性，吸引了各色人等。

区块链为什么能吸引这么多的关注？它到底能做什么？它的技术原理是什么？又为何如此曲折？

让我们从区块链的起源——比特币说起。



比特币与区块链原理

2008 年 11 月，由中本聪设计、开发的比特币正式上线运行。我们现在都知道，比特币是一种加密数字货币。价格最高的时候，每个比特币可兑换近两万美金。一个看不见、摸不着的数字货币为什么能得到这么多的拥护，被炒到这么高的价格？

让我们继续追溯到传统的货币发行与交易系统。

传统的货币，也就是我们日常使用的钞票，是由各个国家的中央银行发行的。中央银行根据市场需求决定投放的货币数量，但是很多时候为了刺激经济发展，中央银行通常会额外多投放一些货币，这样就会出现钱越来越不值钱的情况，即通货膨胀。甚至有的时候，某些政府为了弥补自己的债务，恶意超发货币，有的国家甚至发行过面额为 50 万亿的钞票，导致了恶性通货膨胀。

于是就有人想，能不能发行一种数量有限、不会膨胀的数字货币，通过互联网在全球范围内使用呢？其实发行数字货币容易，但是得到大家的认可很难，而且货币在使用的时候，如何进行交易记账是个大问题。

传统上如果通过互联网进行交易转账，必须通过银行或者支付宝这样的第三方进行交易记账。但是通过互联网发行的数字货币必然得不到法定货币的地位，也就不会被银行等官方机构认可。如果没有受信任的官方机构记账，又如何完成交易呢？

所以比特币数字货币首先要解决的问题就是交易记账。比特币的主要思路是，构建一个**无中心、去信任的分布式记账系统**。这个记账系统和传统的银行记账不同，银行的账本由银行自己管理，银行是记账的中心，而比特币则允许任何人参与记账，没有中心，**完全分布式的**。

此外，传统的银行中心记账必须有个前提，就是交易者都相信银行，信任银行不会伪造、篡改交易。但是任何人都可以参与记账的比特币不可能得到大家的信任，所以这个记账系统必须从设计上实现**去信任**，也就是不需要信任记账者的身份，却可以信任这个人记的账。

这些不合常理，听起来就难度重重的要求，正是通过**区块链技术**实现的。

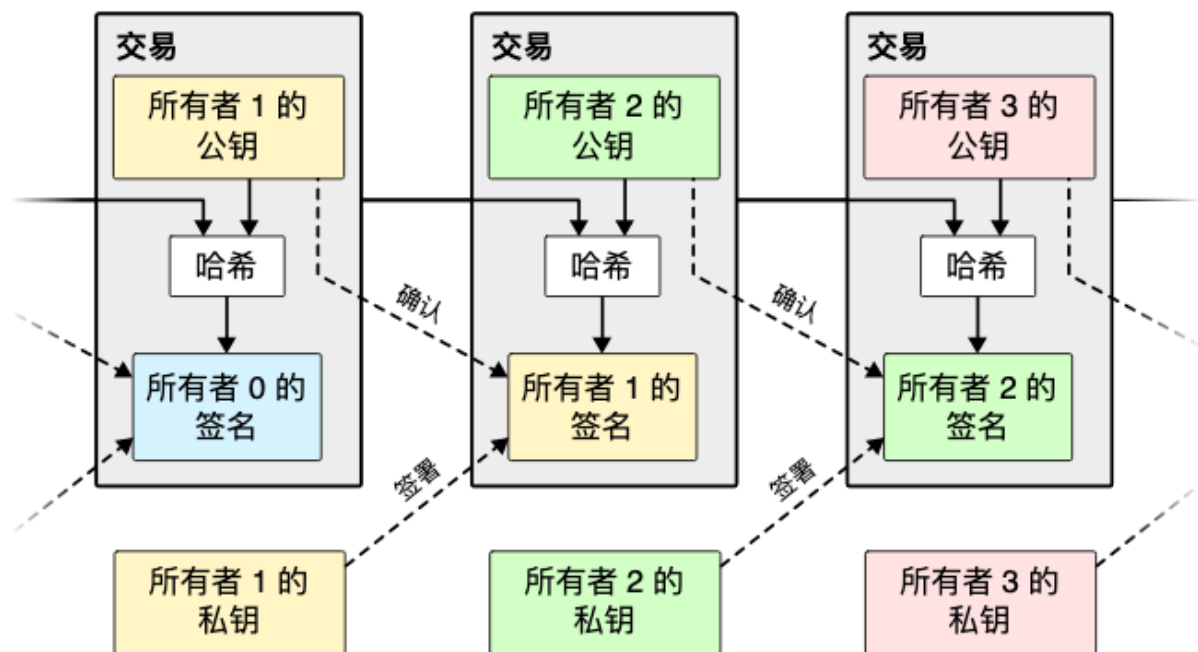
交易

首先，在比特币的交易系统中，所有**交易**的参与者都有一个**钱包地址**，事实上，这个钱包地址正是**非对称加密算法**中的**公钥**。非对称加密算法我在第 30 篇，安全性架构一篇讲过。进

行交易的时候，交易的发起者需要将要交易的数字货币（一个 hash 值）和交易的接受方用自己的钱包**私钥**进行**签名**。

记账者可以使用发起者的公钥对签名进行验证，保证交易是真正发起者提交的，而不是其他人伪造的交易。

如下图：



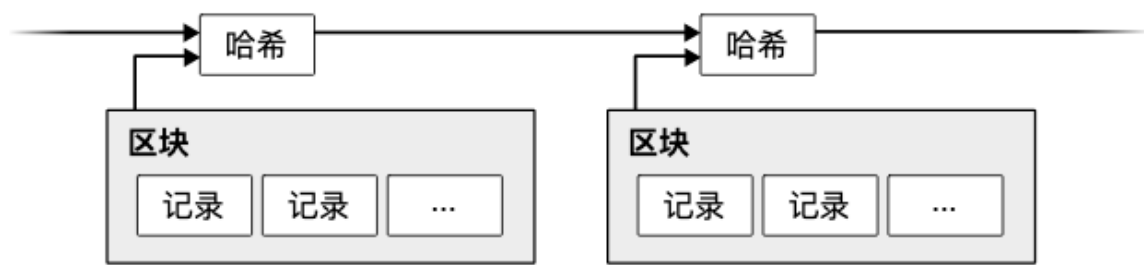
区块链

交易签名只能保证交易不是他人伪造的，却不能阻止交易的发起者自己进行**多重交易**，即交易的发起者将一个比特币同时转账给两个人，也就是所谓的**双花**。

比特币的解决方案是，记账者在收到若干交易后，会将这些交易打包在一起，形成一个区块（block）。区块必须严格按照顺序产生，因此最新一个区块的记账者可以根据区块顺序得到此前所有的区块。这样，记账者就可以检查所有区块中的交易数据，是否有双花发生。

至于如何保证区块的严格顺序，比特币的做法是，在每个区块的头部记录他的前一个区块，也就是前驱**区块的 hash 值**，这样所有的区块就构成了一个链。我们知道，单向链表是有严格顺序的。

通过 hash 值链起来的区块就是所谓的**区块链**，如下图：



工作量证明

区块链的严格顺序不但可以避免双花，还可使**历史交易难以被篡改**。如果有记账者试图修改一笔过去区块中记录的交易，必然需要改变这个交易所在区块的 hash 值，这样就会导致下一个区块头部记录的前驱区块 hash 值和它不匹配，区块链就断掉了。

为了不让区块链断裂，篡改交易的记账者还必须要修改下一个区块的前驱 hash 值，而每个区块的 hash 值是根据所有交易信息和区块头部的其他信息（包括记录的前驱区块 hash 值）计算出来的。下一个区块记录的前驱 hash 值改变，必然导致下一个区块的 hash 需要重算。以此类推，也就是需要重算从篡改交易起的所有区块 hash 值。

重算所有区块的 hash 值虽然麻烦，但如果篡改交易能获得巨大的收益，就一定会有人去干。我前面说过，区块链是去信任的，即不需要信任记账者，却可以相信他记的账。因此，区块链必须在设计上保证记账者几乎无法重算出所有区块的 hash 值。

比特币的解决方案就是**工作量证明**，比特币要求计算出来的区块 hash 值必须具有一定的难度，比如 hash 值的前几位必须是 0。具体做法是在区块头部引入一个随机数 nonce 值，记账者通过修改这个 nonce 值，不断碰撞计算区块 hash 值，直到算出的 hash 值满足难度要求。

因此，计算 hash 值不但需要大量的计算资源，GPU 或者专用的芯片，还需要大量的电力支撑这样大规模的计算，在比特币最火爆的时候，计算 hash 值需要消耗的电量大约相当于一个中等规模的国家消耗的电量。

在这样的资源消耗要求下，重算所有区块的 hash 值几乎是不可能的，因此，比特币历史交易难以被篡改。这里用了“几乎”这个词，是因为如果有人控制了比特币超过半数的计算资

源，确实可以进行交易篡改，即所谓的 **51% 攻击**。但是这种攻击将会导致比特币崩溃，而能控制这么多计算资源的记账者一定是比特币主要的受益者，他没有必要攻击自己。

矿工

前面讲到，比特币的交易通过区块链进行记账，而记账需要花费巨大的计算资源和电力，那为什么还有人愿意投入这么多资源去为比特币记账呢？

事实上，比特币系统为每个计算出区块 hash 的记账者赠送一定数量的比特币。这个赠送不是交易，而是凭空从系统中产生的，这其实就是比特币的发行机制。记账者为了得到这些比特币，愿意投入资源计算区块 hash 值。

由于计算出 hash 就可以得到比特币，计算 hash 值的过程也被形象地称作“挖矿”，相对应的，进行 hash 计算的记账者被称作矿工，而用来计算 hash 值的机器被称作矿机。

当“矿工们”为了争夺比特币，争相加入“挖矿”大军时，比特币区块链就变成一个**分布式账本**了。这里的分布式有两层含义：“矿工”记账时需要进行交易检查，所以需要记录从第一个区块开始的、完整的区块链，也就是说，完整的账本分布在所有的矿工的机器上；此外，每个区块是由不同矿工挖出来的，也就是说，每次交易的记账权也是分布的。

比特币虽然取得巨大的成功，但一直没有得到主流国家的官方支持。但是比特币使用的区块链技术却得到越来越多的认可，在企业甚至政府部门间的合作领域里，得到了越来越多的应用。

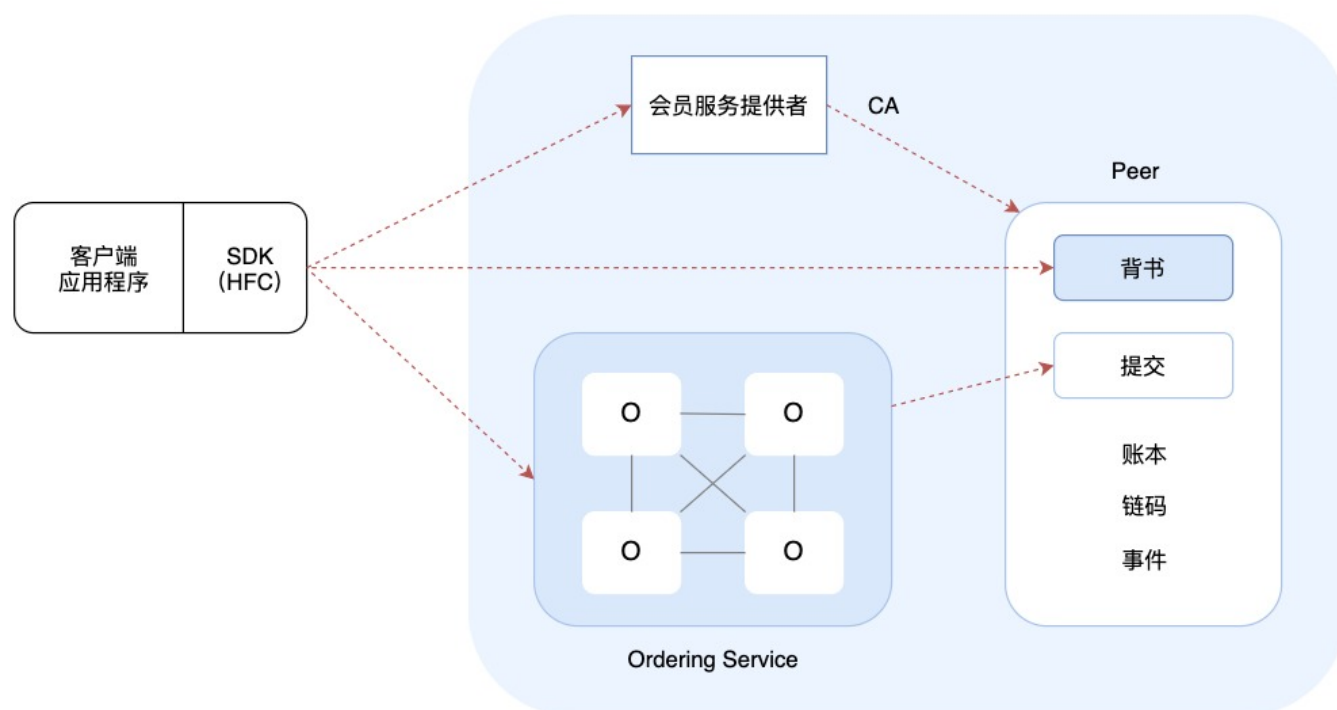
联盟链与区块链的企业级应用

比特币应用的区块链场景也叫做公链，因为这个区块链对所有人都是公开的。除此之外，还有一种区块链应用场景，被称作**联盟链**。

联盟链是由多个组织共同发起，只有组织成员才能访问的区块链，因此有时候也被称作**许可型区块链**。传统上，交易必须依赖一个中心进行，不同的组织之间进行交易，必须依赖银行这个中心进行转账。那么银行之间如何进行转账呢？没错，也需要依赖一个中心，国内的银行间进行转账，必须通过中国人民银行清算中心。

跨国的银行间进行转账则必须依赖一个国际的清算中心，这个中心既是跨国转账的瓶颈，又拿走了转账手续费的大头。所以当区块链技术出现以后，因为区块链的一个特点是去中心，各家银行就在想：银行之间能不能用区块链记账，而不需要这个清算中心呢？最初的联盟链技术就是由银行推动发展的。

目前比较知名的联盟链技术是 IBM 主导的 Hyperledger Fabric。主要架构如下：



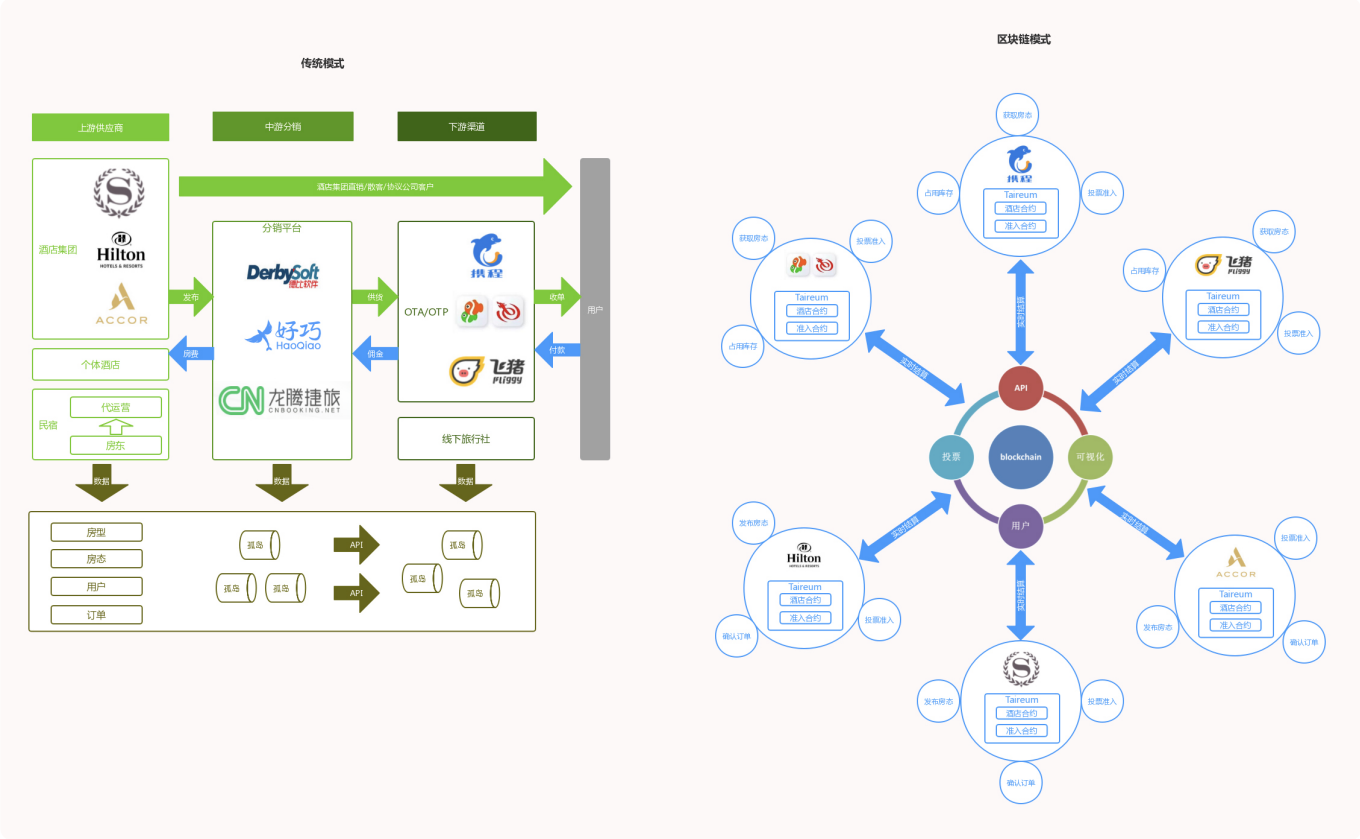
Peer 节点负责对交易进行背书签名，Ordering 节点负责打包区块，Peer 节点会从 Ordering 节点同步数据，记录完整的区块链。而所有这些服务器节点的角色、权限都需要 CA 节点进行认证，只有经过授权的服务器才能加入区块链。

最近两年，随着区块链技术的火爆，联盟链技术也开始从银行扩展到互联网金融领域，甚至非金融领域。2018 年支付宝香港和菲律宾一家互联网金融企业通过区块链进行了跨国转账，而香港和菲律宾的外汇管理局也作为联盟成员加入了区块链，使得**转账和监管在同一个系统中完成**。

在互联网 OTA（在线旅行代理）领域，酒店房间在线销售是一块非常大的业务，但是一家酒店不可能对接所有的 OTA 网站，而一家 OTA 网站也不可能获得所有的酒店资源，于是就催生了第三方的酒店分销平台，这个平台负责对接所有的酒店，酒店房间通过该平台对外分销，而 OTA 网站通过该平台查找酒店房间以及预定房间。

于是这个平台就成为一个全行业不得不依赖的中心，一方面产生了巨大的瓶颈风险，另一方面酒店和 OTA 也不得不给这个中心支付高昂的手续费。

事实上，我们可以利用联盟链技术，将酒店和 OTA 企业通过区块链技术关联起来，酒店通过区块链发布房间信息，而 OTA 通过区块链查找房间信息以及预订房间。如下图所示，左边是传统的酒店分销模式，右边是基于区块链的酒店分销模式。



上面讲到的 Hyperledger 联盟链技术部署和应用都比较复杂。目前在区块链领域，社区资源比较丰富，更为易用，也更被广泛接受的区块链技术是以太坊。但是以太坊是一个公链技术，不符合联盟链受许可才能加入的要求，因此，我和一些小伙伴对以太坊进行了重构，使其符合联盟链的技术要求，你可以点击 [源码地址](#) 看一下，也可以看看 [相关文档](#)。

如果你感兴趣的话，欢迎你参与开发与应用落地。

小结

应该说，区块链能吸引到这么多的关注，产生这么大影响，和加密数字货币的炒作是分不开的。正因为数字货币的炒作，才使得区块链技术吸引了大量的资源，更多的人才投入研发区块链相关技术，区块链技术进步与应用也吸引了大量的关注。

但是数字货币的投机属性又使得人们对区块链技术抱有急功近利的想法，希望区块链技术能快速带来回报。

在我看来，**互联网技术的快速发展是生产力革命**，使得生产力数以十倍、百倍的增加。而**区块链技术是生产关系革命**，传统上，所有的交易和合作都必须依赖法律以及信任。而法律的成本非常高，很多场合无法支撑起用法律背书的成本；而跨组织，特别是互为竞争对手的组织之间又不可能产生信任。**区块链的出现，使得低成本，去信任的跨组织合作成为可能**，将重构组织间的关系，这个关系既包括企业间的关系，也包括政府和企业间的关系，还有政府部门间的关系。

互联网使得这个世界变得更加扁平，信息流动更加快速，但无法弥合这个世界割裂的各种关系，而区块链可以打通各种关系，将这个世界更加紧密联系在一起，使全人类成为真正的命运共同体。

思考题

今天我讲了一下区块链技术，它虽然火爆，但仍然处在发展之中。你能想到的利用区块链技术的场景有哪些呢？

欢迎你在评论区写下你的思考，也欢迎把这篇文章分享给你的朋友或者同事，一起交流一下。

点击参加 21 天打卡计划 

搞定后端技术基础



扫一扫参与小程序话题



新版升级：点击「 请朋友读」，20位好友免费读，邀请订阅更有**现金**奖励。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 32 | AI与物联网架构：从智能引擎到物联网平台

下一篇 答疑 | 互联网需要解决的技术问题是什么？

精选留言 (5)

 写留言



丁丁历险记

2020-02-07

假如武汉的肺炎可以基于区块链来去记录和追踪政府那些科学家的每一项决策，我觉得文明就开始了。



2



小美

2020-02-10

老师比特币是怎么发行的呢，怎么保证发行总数不增加，不通货膨胀

作者回复：这块因为篇幅原因没写  具体是这样的：

最早的时候，每挖出一个区块奖励矿工50个比特币，然后每四年奖励减半，当比特币总数达到2100万个时候，停止奖励。矿工靠交易手续费维持挖矿记账。

也就是说，比特币代码控制发行总数，最多2100万个。



蓝魔、

2020-02-09

在抗击 2019 新型冠状病毒(2019-nCoV)的斗争中，众多热心人积极参与公益捐助活动。由于公益活动信息管理意识和技术手段落后，捐助活动信息的传递经常出现混乱，信任危机频繁发生。这既伤害了捐助者的善心，也为慈善组织带来不必要的麻烦。可以通过区块链技术搭建捐赠服务平台来提供信任服务。

展开 ∨

作者回复: 



你的美

2020-02-08

老师好请教个观点：联盟链是针对加入组织的企业而创立（目的只是做为交易转账方便吗），这对早期的企业信息安全是好，但区块链技术是针对每个人都有发生的交易，而研发的加密数字货币，那联盟链的技术发展最终会不会兼并每个人都拥有公钥的以太坊技术呢，我觉得这样的区块链技术才是完善的对吗？

展开 ∨



號國技醬

2020-02-07

好像懂了，又好像没懂，脑子笨，准备多研读几遍

展开 ∨

