
有很多朋友都问过我一个问题，什么是区块链？以前也断断续续地讲过一些区块链的内容，集中性不太强，今天干脆我们单独讲一讲区块链，把它讲透。然后您就会明白，区块链和各种数字资产，加密货币其实是两回事。一些打着区块链旗号的乱七八糟的概念和理财产品也就骗不了你了。

首先我们明确一个概念，区块链就是一个工具，它本身没有任何价值，也无所谓好坏，就像一个锄头，单独往那一放，产生不了什么价值。但是你用锄头耕作，种菜，种出来的菜有价值。一些加密数字资产，比如比特币，它是利用了区块链这个工具，产出的一个产品，这个产品在很多人心中有价值。很多人认同比特币，那比特币在他们眼里就有价值。但是我们要搞清楚，比特币是个产品，这个产品是用区块链这个工具生产出来的。这是两回事，不要搞混了。

那么区块链究竟是一个什么样的工具呢？从本质上来讲，它就是一个数据库。不过这个数据库有点特殊，它是一个分布式的，去中心化的数据库。

说到这儿，可能有些朋友就开始蒙圈了，“我连数据库都搞不清楚，你还来个分布式去中心化的数据库，叫我怎么理解？”，不着急，我慢慢说您就明白了。

数据库在我们的生活中很常见，即使您没学过相关的知识，您应该也知道它是个什么东西。它是存储处理各种数据用的。大到一个国家的人口经济环境数据，中到各省市，大公司，企事业单位的各种报表，小到老百姓居家过日子，你都离不开数据库。你就是开个小店，进多少货，卖多少钱你还得统计统计呢，对吧。我们就用最

简单的例子，老百姓居家过日子记个账，来跟您形象地说明区块链到底是个什么东西。

比如说张三，以前过日子糊里糊涂，挣多少钱，花到哪儿了，从来没有个数，日子过得是一塌糊涂。后来高人指点，说你这样不行，你得学会记账，搞清楚你的收入支出，然后你就能量入为出，过日子要学会计划。张三一听有道理，那就记账吧。

张三一个月收入5000，张三媳妇收入5000，另外还有一些其它的收入2000，张三一家一个月收入12000。支出，房贷3500，物业水电通信费1000，衣服化妆品什么的支出2000，吃饭支出1500，等等等等，这一项一项支出一个月总计10000，张三一家每月能结余2000。

张三一看，这挺好，我每月收入支出一目了然，哪些钱该花的这没办法，哪些钱不该花的我也知道了，下次注意节省一点。慢慢每月我能结余出3000块钱，一年36000。过两年就可以换辆车了。这就叫记账，张三用来记账的笔记本就叫数据库，写在笔记本上的各项收入支出的数字就是数据库里的数据。

数据库我们解释清楚了，就这么简单。那什么是分布式去中心化的数据库呢？其实也简单，那就是张三媳妇也记账。

张三一个人记账，这叫中心化，只有一个数据库。哪天张三的笔记本被火烧了，数据库就没了。现在张三媳妇也记账，这就有了两个数据库，两个中心。两个数据库里的数据一模一样，这就叫分布式去中心化，即使有一天，张三的笔记本被火烧了，张三媳妇的笔记本还在啊，数据不会丢失。这就是分布式去中心化的好处，数据是安全的，它没有一个唯一的中心，谁的数据丢了都无所谓。

现在又出现了一个新的问题，两个人都记账，以谁的为准呢？如果两个人记录的数据都一样，那没有问题，这两个账本都是对的。万一出现差错呢？以谁的为准，这就不好说了。

为了防止唠嗑唠稀碎，我们还是用这个例子接着往下说。刚才说了张三媳妇也记账，那我们就说说张三媳妇为什么要记账。

张三开始记账了，张三媳妇就起疑心了。平常吊儿郎当一个人，突然开始记账了。大白天的老母猪上树了，这里边一定有鬼。是不是惦记着回头跟我离婚分家产呢？不行，我也得记账，免得到时家里有多少钱我都说不清楚。于是，张三媳妇也开始记账了。

过一段时间，张三发现媳妇也在记账，就问她，你记账干什么呢？

媳妇也爽快，我怀疑你记账是想以后和我离婚分家产，那我也得记，免得到时我连家里有多少钱都说不清。

张三一听哭笑不得，媳妇你想多了，我记账是为了把咱们的日子过好。不过你记账我也不反对，咱俩这叫分布式去中心化记账，数据更安全。你也体会一下，什么叫不当家不知柴米贵。

这一解释，张三媳妇心里的石头放下了，原来这死鬼不是为了跟我离婚啊，那就好。不过万一咱俩有一个记错了，过一段时间都忘了，那这个账以谁的为准呢？

张三一听，对啊，以谁的为准呢？干脆这样，咱爸咱妈四位老人都闲着没事，也请他们帮我们记账，这就多了四个账本，六个账本总不能都错了。以大多数记录相同的为准，怎么样？但有一点啊，你的那点怀疑可不能跟爸妈讲，如果老人误以为咱俩要离婚记账，非把咱俩的腿打折了不可。

于是，六个账本一同记账，为了方便对账，张三全家约定，每天的收支记到一张纸上，一天一张纸。这张纸我们可以把它叫做一个区块，一天天的，一个区块接着一个区块记下去，连到一起就叫做区块链。

这个例子接地气吧，它就能把区块链解释得清清楚楚。六个账本，同时记录张三一家的收支情况，每天的记录打包成一个区块，这就是区块链。

区块链我们再总结一下，第一，它是个数据库，记录的是张三一家的收支情况。第二，它是去中心的，六个账本，没有一个是唯一的，六个账本里的数据如果相同，都是有效的。第三，它是分布式的，六个账本在六个人手里，不可能同时被毁，数据是绝对安全的。

另外就是数据的纠错问题，区块链的纠错原则就是以大多数为准，只要结果，不论对错。大多数原则怎么理解呢？还是张三一家的例子。

张三全家每星期对一次账，六个人拿着六个账本坐在一起对账，如果说张三的账本里一个区块，比如5月1日一笔支出是100元，但是其它五个账本里记录的都是120元，那以其它五本的记录为准，张三5月1日这个区块的记录必须改过来，而且张三5月1日以后的区块全部作废，必须改成与其它五个账本的区块一致，否则张三的账本都给你废了，你这个账本没人承认。张三心想我比窦娥还冤，这笔钱是我亲手花出去的，就是100元啊。那也不行，大多数人记录的都是120，那就是120，不是也是。这就是区块链的纠错机制。遵循大多数原则。

如果说张三媳妇的数据也错了，张三媳妇5月2日的区块有一笔数据不对，那么张三

媳妇5月2号的区块数据包括以后的区块全部作废，必须改成和大多数人一样的。

当然我们说张三冤枉不是指区块链的纠错机制不对啊，你反过来想，如果有人恶意篡改数据呢？他改少数账本的可能性高呢，还是改大多数账本的可能性高呢？答案是显而易见的，能够同时把大多数账本的数据都篡改了，这个可能性基本不存在。所以，区块链的纠错机制其实保障的是数据的不可篡改性。

比特币圈里有个说法，如果你掌握了全网51%的算力，那就完全掌握了比特币，你想怎么改就怎么改，就是这个道理。我给张三转账十个比特币，你完全可以改成转给你，同样是有效的，全网的矿机都承认这个结果，因为你就是大多数嘛。那我和张三就傻了，傻了也不管用啊，区块链就是这样，只承认大多数的结果，不论对错的。我拿出什么证据都不管用。

有朋友可能要问啊，那这种现象可能出现吗？理论上可能，但实际上基本不可能，全网的算力越大，越不可能。但是历史上也确实出现过这种可能性。

有一年，比特大陆曾经掌控过比特币全网百分之四十几的算力，离百分之五十一很近了，比特大陆一统计，发现已经掌控了这么强大的算力，把自己吓坏了。赶紧发声明，自愿退出一部分算力，承诺尽快退到百分之三十以下，甚至更低。有朋友可能奇怪，为什么不控制比特币呢？为什么要自愿退出呢？原因很简单，如果比特大陆真的控制了比特币，那谁还跟你玩呢？比特币就会一文不值，比特大陆手里的矿机立马成废铁。所以，没有人愿意去控制比特币，也控制不了。这个例子其实也说明了区块链的数据不可篡改性。一旦你有能力篡改数据了，也就没人跟你玩了。

说到这儿，您应该已经完全理解区块链了，它就是一个数据库，一个很纯粹的工具而已，本身无所谓好坏，它可以实现数据的安全和不可篡改性，这些优点使得区块链的应用越来越广泛。一些重要的数据，也在使用区块链技术，目的就是为了安全和不可篡改。举个例子，2018年3月，非洲的塞拉利昂总统选举使用了区块链技术，为什么呢？因为各个党派之间互相不信任。投票结果没人相信，没办法了。那咱们使用区块链吧，这个数据可是改不了的。这也是区块链的应用，不是说一提起区块链，就意味着数字货币，它们不是一回事。

现在市面上，打着区块链旗号的各种产品层出不穷，但是你真正理解了区块链，你就会发现，大多数的所谓区块链概念的产品都是骗子。希望这期节目能给大家提供一些帮助。