大家好，感谢邀请，今天来为大家分享一下淘宝 区块链的问题，以及和淘宝区块链应用的一些困惑，大家要是还不太明白的话，也没有关系，因为接下来将为大家分享，希望可以帮助到大家，解决大家的问题，下面就开始吧！

本文目录

到底什么是区块链，怎么解释才能让老百姓都能明白？

先说结论：“中本聪”利用区块链技术，巧妙地解决了账本同步和信息不重复的问题，这就使得去中心化账本的理想最终得以实现。

去中心化的理想（理解区块链的前提）

区块链原本是一种基于互联网的信息编码、传输、加密、解密、验证技术，但在我看来，现在已经上升到了一种“去中心化”的理念，本质上是一种理念上的革新。而比特币就是这种理念的一个具体应用。打个比方来说，区块链就相当于电子商务，你想想二十年前，有几个人搞得懂什么是电子商务，它本质上也是一种理念，只不过这种理念必须要借助一定的技术手段来实现。而比特币就相当于淘宝网，是电子商务的一个具体应用。

所以，我们要理解什么是区块链，必须要先理解什么是“去中心化”。

我举两个例子来帮助你理解：

第一个例子是从网上下载电影。最早的时候，我们下载电影都是到一些知名的电影下载网站上去下载。这些网站会把电影文件存放在一台或者一组服务器上，大家都访问某台服务器下载影片。这就叫中心化。

在这个游戏规则中，电影网站的服务器就是中心，每一个下载电影的人只不过是这个中心拉出来的线而已。中心化的游戏中，玩家的地位是不平等的，网站主占据绝对强势地位，他想让你下载就下载，想给你限速就限速。后来，一种去中心化的下载模式出现了，这就是BT下载，也叫P2P（peertopeer）下载，现在我们一般讲到P2P指的都是那种个人借贷的网站，但是最初的概念是从BT下载来的，P2P就是个人到个人，点到点。

BT下载的原理与电影网站完全不同，影片并不是存在某个服务器上的，而是大家互相从网络上的每一个人那里去下载这个影片的一小部分，最后拼成一个完整的文件。在这个游戏中，所有玩家的地位是完全平等的，任何一个玩家可以随时离场、随时加入，只要这个游戏还有人在玩，整个游戏就能够正常运行，没有人拥有特别的权力。这就叫去中心化。

第二个例子就是我们每天都在使用的银行卡或者支付宝这些人民币支付手段，现金我们先抛开不谈。我们用无现金的方式支付人民币买东西，就是一个中心化的游戏，它的中心有好多级，比如说，支付宝的服务器是第一级中心，支付宝资金的托管银行工商银行、中信银行的服务器就是第二级中心，这些银行的再上一级中心就是央行人民银行的服务器。

在这个游戏中，不同级别玩家的权力、地位是不平等的，最大的Boss当然是央行，它甚至能发行货币，它的权力可以大到分分钟就把我们的钱全部抢光，很简单，它只要突然增发货币就可以了，物价突然上涨100倍，我们的钱就等于被抢光了。

那货币游戏能不能像下载一样也去中心化呢？也是可以的，比特币系统就是这样一个去中心化的货币游戏系统，你可以把它看成是一个大型的货币实验。

比特币的游戏规则是这么玩儿的，就两条核心规则。

第一，它的货币发行不是由某个机构说了算，而是公开一套算法，每算出一个符合要求的数字，就相当于挖到了若干个比特币。谁都可以去算，绝对公平，谁也做不了弊，因为算法本质上就是一个个数字去凑，凑出一个算一个。

第二，比特币的交易信息不是记在某一台服务器上的，而是所有参与这个游戏的玩家电脑中一人一份，同步记录，这种交易记录在理论上几乎是无法篡改的。这就是去中心化账本。这样一来，所有游戏玩家的地位和权力就完全平等了，几乎没有任何一个玩家是特殊的。为什么要加上“几乎”两个字呢，因为，毕竟能够有能力挖比特币的那些矿主还是有点特殊的，但这种特殊性并不是太大，而且矿主也没有任何壁垒，只要你买得起好电脑，谁都可以当矿主。

不得不说，比特币的这个设计非常之妙，妙不可言，他的发明人，神秘的“中本聪”确实是颗大葱。

理解了去中心化，你就等于理解了区块链，一个真正的区块链项目就是通过合理的游戏规则设计辅以信息技术，来践行去中心化理念的项目。比特币系统就是去中心化理念和区块链技术的一个优秀示范项目。不夸张地说，我觉得这是一场互联网的理念革命，是人类的又一次平等化革命，上一次是打破了人与人之间在身份地位上

的不平等，这一次是打破了游戏规则本身的不平等。正因为这样，所以区块链才能激发人们如此大的热情，这是一个听上去可以颠覆一切旧规则的新生事物。

然而，我这里话锋一转，在我看来，比特币系统并不是一个成功的区块链应用，它是一个天生的残废。我为什么这么说呢？因为，从我前面介绍的比特币两条核心游戏规则就知道，它有以下这些天生的缺陷：

第一，比特币客户端软件需要巨大无比的存储空间，因为每一个节点都必须要记录下从比特币系统诞生的第一天起所有的交易记录，截止2018年2月，这个交易记录文件已经有147GB那么大了，而且只会增加不会减少。

第二，为了防止有人作弊，比特币系统有一套很复杂的游戏规则来确保交易记录是真实的，这样就导致每一笔交易的确认时间一般需要一个小时，甚至几天。你想想吧，如果用比特币去街边买杯奶茶，会是什么情况。

第三，最多只有2100万枚比特币，而且，无论有多少人在挖矿，系统规则决定了平均每10分钟才能产出若干枚比特币（2018年是12.5枚）。我想起了那句话：人民群众日益增长的比特币需求与比特币总量不充分之间的矛盾。

但是，比特币不能代表区块链，区块链也不是比特币。区块链在未来可以有哪些应用呢？

实际上，区块链解决的核心问题是信任问题，大家想一下，所有的金融机构，例如银行、保险、券商等等，让他们赖以生存的根本是信用。我们之所以会放心地买股票、买期货、买纸黄金，那都是因为我们信任充当交易中介的机构，而这些交易中介就是金融活动的中心，我们宁愿为此付出一定的手续费、交易费，金融机构也因此挣得盆满钵满。

但是，当区块链在人们的观念上和技术上都成熟后，这种中心化的金融机构是有可能被颠覆掉的，因为我们可以利用区块链的理念和技术来改写游戏规则，让所有的金融产品交易都不再需要一个中心，而全部都以点对点的方式完成，并且从理论上能够保证信用问题。到了那时，银行还需不需要我不知道，因为银行可能还会涉及到更复杂的国家利益问题。但是，一定会有很多商业金融机构受到区块链的冲击。再比如，公证也是一个典型的中心化的贩卖信用的机构，区块链完全可以实现对公证行业的改写。

更新：

首先，请记住：比特币不是区块链，它只是区块链技术的一个具体应用。

好，我们接下来往下说。

到此为止，我们去中心化账本的理想只实现了一半，并没完全实现，为什么呢？因为还有两个重大的问题没有解决：

第一个问题：账本同步问题。比特币网络中有那么多台电脑，一条交易信息发送出来的时候，当然不可能所有的电脑都开机，必然有一些处于离线状态，开了电脑也未必开着比特币客户端，所以总有一些电脑无法立刻收到这条信息。这样就会导致不同电脑上的记录不同步，到底以谁的电脑记录为准呢？

第二个问题：如何防止同一个比特币被重复使用呢？假如有一个黑客，他只有1个比特币，但是他却同时把这个比特币付给A和B（虽然理论上无法真正的同时，但可以做到间隔时间极短），于是他就会在网络上广播两条信息，一条是支付给A的信息，一条是支付给B的信息，因为网速的关系，必然有的电脑先收到了信息1，有的电脑先收到了信息2，这就产生了矛盾，如何确定哪一条信息是有效的呢？

为了解决上面这两个难题，“区块链”技术横空出世——真正让中本聪一战成名的技术。

再次强调：比特币不是区块链，它只是区块链技术的一个具体应用。

接下来，让我一步步为你揭开区块链技术的面纱。

为什么要叫“区块链”？

因为中本聪把这个账本设计成了由一个个“信息包”首尾相连而成的长链，每一个“信息包”被称为一个“区块”，这些区块每一个都有唯一的编号（在比特币系统中，编号被称为高度（height）），这些编号就是自然数1、2、3、4……一直往下排，不允许跳跃，也不允许中断和重复。

下面讲解区块的具体规则：

第一个区块当然是由区块链的发明人“中本聪”亲自创建的，那是北京时间2009年1月4日，在芬兰赫尔辛基的一台小型服务器上，第一个区块诞生了，这也被称作“创世区块”。在这个区块上，包含的主要信息是：

创世区块

中间那段话是“中本聪”刻在第一个区块上的纪念，从第2个区块开始，以后每一

个区块都必须严格按照比特币系统的规则来创建。区块的规则是：

区块规则

区块链所有的奥妙就在尾巴上加的这个随机数上，因为它实在太奥妙，让我等凡夫俗子只能大呼过瘾，所以后面我就把它称为“奥数”，以方便讲解。

“中本聪”规定：这个新区块的数字指纹（一个256位的二进制数）的前72位必须全部为0。

回忆一下我们前面介绍过的数字指纹的知识。因为SHA算出来的指纹是毫无规律可循的一个数字，所以，想要满足“中本聪”的这个变态规定，唯一的办法就只能凭运气凑“奥数”，从0开始不断地去常试，直到满足要求为止。这就是一个纯粹的概率问题。我们来算一下要满足这个要求的概率是多大。

因为二进制数，每一位只有两种可能性，0或者1，所以，凑出一个奥数的可能性是2的72次方分之一，也就是1/4722366482869645213696。这个数字已经大到看花眼了吧，它大约就是4.7万亿亿分之一。换句话说呢，就是平均要进行4.7万亿亿次SHA计算，才可能得到一个“奥数”，你可见每一个“奥数”的金贵。

最巧妙的是，“奥数”并不是某一个方程的解，解出一个少一个，因为每一个区块的字符串都不同，所以，每一次寻找奥数都需要从0开始，任何一个数字都有可能成为新的奥数，完全没有规律可循。

一旦成功找到了一个奥数，就获得了一次记账权力，可以给账本上新增加一个区块。那么，为什么要花时间找奥数，去给账本记账呢？因为好处实在太大了。

比特币系统规定，每成功增加一个区块，这台记账的电脑（实际上是某个账号）就能获得12.5个比特币的奖励（截止到2018年2月时的奖金额），以及这个区块中所有交易的手续费，总额取决于交易频繁程度（平均约2比特币）。这样一来，相当于每找到一个奥数，可以获得14.5个比特币奖励，按照2018年2月的比特币市场价，相当于12万美元。这么丰厚的奖励，自然就会吸引大量的电脑愿意去抢夺记账权。

寻找奥数就是抢记账权，抢记账权也就是挖比特币。因此，寻找奥数也被形象地称为“挖矿”。挖矿的电脑就叫“矿机”，一个装满矿机的房间当然就可以叫“矿厂”了嘛，矿厂的主人就是“矿主”，他们是比特币江湖中的弄潮儿。

但是，我需要给你解释一下挖矿的难度，让你打消去挖矿的冲动。个人电脑的运算

速度大约是每秒可以进行60万次SHA计算，也就意味着，一台个人电脑需要花一千万年才有可能凑出一个奥数。当然，这是一种概率计算，我不能从理论上排除某人的人品超新星爆发，算了一次奥数就中了4万亿亿分之一概率的奖。但我还是想劝你不要相信自己是耶稣转世，你没有那个命。

我给你看看人家专业的矿厂是怎样的：

图:一个中等规模矿厂（图片来源：百度图片搜索）

这只是一个中等规模的矿厂，大规模的矿厂据说有几万甚至几十万台矿机同时运行。我在《看看新闻》2017年6月17日的一个新闻中看到，记者拜访了一座位于中国四川的矿厂，根据报道：这个矿厂有5000多台矿机的规模，平均每天耗电超过20万度，当地的电价是3毛/度，一天光是电费就6万多元，平均每天可以挖出大约50个比特币，一年左右回本，之后能做到20%左右的利润。

不过我觉得这个报道中的数据前后矛盾，我查了一下，比特币当时的市场价是大约2500美金/个，美元兑人民币的汇率大约是6.8，所以，每天的收入大约是85万人民币，一年的收入大约3.1亿元，一台矿机的成本均价是1-2万元，矿厂的矿机总成本是5000万-1亿元，再算上电费等，一年起码2亿的利润。我想，在充分市场竞争下，出现这种暴利的可能性很低。所以，不是记者搞错了，就是被采访对象在吹牛不打草稿。由于比特币的价格和全网算力的波动很大，所以投资比特币矿厂很难做长期预测，不确定因素太多。

图：看看新闻报道的位于四川的某矿厂（图片来源：《看看新闻》官网）

根据我们前面掌握的比特币知识，50个比特币，相当于找到了4个奥数，抢到了4次记账权。目前，整个比特币网络的所有矿机加起来的总算力能达到的水平，大约平均每10分钟可以找到一个奥数，也就意味着平均每10分钟生成一个新的区块。当然，这个10分钟是一个平均数，快一点的话3、4分钟生成一个区块，慢一点的话15分钟左右。

正因为奥数太难找，每个区块平均要10分钟才能生成一个，所以就能基本解决我在本章开头提出的第一个问题“如何同步账本？”，只要有个3、4分钟的时间，足以让所有在线的电脑同步到这个区块了，那些不在线的电脑或者第一次运行客户端的电脑，上线以后必须要先做一件事情，就是从相邻的节点上获取最新的账本。

请注意，我用了“基本解决”这个词，也就意味着，并没有完全解决账本同步的问题。这是因为总会有极小的概率两台矿机恰好同时（只要在网络上所有在线的节点没有完成区块链同步之前都可以算同时）找到奥数，也就意味着同时抢到了记账权

。因为矿机实在太多了，这样的小概率事件时不时也会发生一次。同时抢到记账权的矿机都会将自己生成的新区块广播到比特币网络中。

遇到这种情况，比特币系统怎么处理呢？

在这种情况下，相当于网络上的其他节点收到了两个合法的新区块，因为网络节点的地域分布不同，所以，不同的节点收到这两个新区块的先后次序就会不同。此时，所有的节点会暂时保留两个新区块，并且把区块链做一个临时的分叉，如下图所示：

（图片来源：自绘）

接下去，比特币网络中必然又会有其中一个节点（矿机）抢到了记账权，这时该节点就会将生成的最新区块接到其中的一个分支上，那到底是接到新区块1上还是2上呢？系统规则是：这个节点先收到哪个区块，就接到哪个区块上，同时放弃另一个区块，然后全网广播，如下图所示：

（图片来源：自绘）

比特币网络上的所有节点在收到最新的区块链后，只要发现其中一个分支比另外一个分支多2个区块了，就立即也放弃那个短的分支，总之，比特币网络永远只承认更长的那条分支。你可能会想，那如果小概率事件再次发生，在区块链第一次分叉后，又同时产生了两个新区块，而恰好两个新区块产生在两个不同的分支上，这时候，其他节点收到的区块链还是两个一样长的分支，那怎么办？很好办。还是同样的规则，只要分支一样长就暂时保留，直到出现两个分支不一样长时，就放弃短于2个区块的，保留长的。那个被放弃的分支中所有交易和比特币奖励都会被判定为无效。

因为有了这个临时分叉的规则，所以，比特币玩家在完成一笔交易后，不能立即认为这笔交易是成功的，有可能会被取消，必须要等到一定数量的新区块生成后，如果交易依然没有被取消，这才能放心地认为交易成功了。那到底要等到多少个新区块产生才能放心呢？按照概率来说的话，小额交易有这么三个新区块产生就够了，但是大额交易的话，为了更保险，一般认为是等到6个新区块产生，就足以放心了。前面说过，每个区块产生的平均时间是10分钟，也就意味着，一笔大额交易需要1个小时左右才能确认交易成功。

但是小额交易确认的时间往往会更长，甚至长达好几天。听到这个你可能会有点儿糊涂，刚才不是还说小额交易一般只要三个新区块产生就够了吗？怎么确认时间反而会更长呢？比特币网络刚刚诞生的头几年，确实不会出现这样的怪事，但是这几

年随着交易量的猛增，就会出现这种怪事了。

为什么？先回忆一下每个区块的规则：

区块规则

你的交易记录要被写到区块链上，有一个前提：矿工将你的这笔交易记录打包到这个区块上。你可能想问：为什么会不打包？难道系统规则还允许不打包吗？打包成功了不是还要给矿工交税吗？矿工好不容易抢到一次记账权，怎么会有钱不赚呢？

是的，允许不打包。原因不是矿工不想赚钱，而是“不可抗力”，关键问题是每一个区块允许存储的数据量有限。中本聪当初设计比特币系统时，规定了每一个区块最大只能是1MB，一条交易记录大概是0.25K，那么一个区块最多可以储存4000多条交易记录，如果在一个新区块产生的时段中，发生的交易请求超过了4000条，那就肯定存不下了。我们可以算算，这个量大概是一个怎样的交易频率。每个区块的平均产生时间是10分钟，也就意味着，平均每秒钟的交易量如果超过7条，那么就一定会出现排队等待打包的交易记录了。这个交易频率实在很低，要知道支付宝一秒钟大约要处理上万笔交易。这一秒钟七笔交易对于全球来说，实在是太不够用了。

一般来说，大额交易优先打包，小额交易，手续费越高的交易越优先打包，打包规则矿工有一定的自主权。比特币交易手续费的规则比较复杂，不同的矿工收得还不一样，不是三言两语能说清。但有一点可能会让你感到诧异，越是大额的交易反而收费越低，甚至免费。交易额越小反而费率越高。这是因为，交易手续费除了鼓励矿工挖矿，还有一个非常重要的功能，就是防止有人恶意发布大量的小额交易造成信息拥堵。

现在，比特币交易滞留是非常普遍的现象，很多小额交易甚至等上好几天都确认不了，因此，很多人不惜附加很高的交易手续费来让矿工提前替他们打包。

好了，讲到这里，有关区块链的核心原理就讲完了，关键要记住，“中本聪”利用区块链技术，巧妙地解决了账本同步和信息不重复的问题，这就使得去中心化账本的理想最终得以实现。

学习知识，我认为最佳的方式就是带着问题学习，在学习过程中，先掌握知识的主干，如果还有兴趣，再去了解那些枝枝杈杈。

区块链是什么意思？

区块链，通俗来讲，就是一种记账方式，即分布式账本。什么是分布式账本呢？

下面我举个例子来说明。从前，有一个村庄，村民买卖交易的记录，由村长一个人用一个账本记录下来。这种记账方式有很多弊端。有一天，一场大火把村长家烧了，账本没有了。这样大家的交易记录全毁掉了。后来，村民想出一个办法，就是大家都记账，也就是每一个人都有一个账本，记录全村所有的交易记录。这样即使丢了一本，其它人还有，因为每一本账本记录都是一样的。

这种记账方式就是分布式记账，去中心化，是人类记录方式的一个创新，人类记账方式从原始社会末期用结绳子到刻在龟背，甲骨上，到了宋代出现了纸质账本。到现在互联网，用计算机储存式记账。以前这些所有记账方式都是中心化。但是区块链这种分布式记账方式就是去中心化。

现在比特币就是这种记账方式，比特币所有的交易记录大约有一百多G也就是一个电脑硬盘就可以装完全球这么多人交易记录。大家想一下，全球有多少个人矿工安装了比特币程序，就算有一台计算机硬盘被毁坏也，也不影响交易记录的缺失，因为有千千万万台机算机还保存有交易记录。

这种就是区块链1.0，比特币是区块链的底层技术。后来有了区块链2.0，也就是智能合约，以太坊就是一种智能合约。也许大家不明白什么叫智能合约，我举个例子，张三借本四一百元，约定一个月后还，如果不还，将会从张三钱成中强制性扣这一百元。大家都同意后，将这个合约写入区块链，一个月后如果张三不还李四的100元，那合同到期，强制执行。智能合约，不可篡改，可追溯。

区块链和虚拟币相伴，正因为有虚拟币让更多的人认识区块链，区块链的应用目前还在萌芽阶段，各个正在加大投入区块链研究。目前还没有进行商用，估计未来三五年十年内开始商用了。

用区块链技术是否可以打造一个新的淘宝网？

按我个人的理解，用区块链是一个创新的技术打造淘宝，肯定是非常好的，首先区块链的技术，它是去中心化，数据任何人都不能都不能篡改的，可以让每个人的信任度提高，以后就不要第三方担保

TB上的淘金币有没有可能未来成为虚拟货币之一关联区块链？??？

应该不可能，淘金币类似游戏币的一种虚拟消费币。只可以在淘宝天猫平台使用，主要由商家充值，为了获取流量的工具。流通于商家、平台跟顾客之间，其实现在很多商家开始大量放弃淘金币服务了。据了解主要原因是淘金币流量规矩不合理。

END，本文到此结束，如果可以帮助到大家，还望关注本站哦！