大家好,今天小编来为大家解答以下的问题，关于区块链与证券ppt，区块链与证券监管ppt这个很多人还不知道，现在让我们一起来看看吧！

本文目录

区块链是什么？如何看待区块链？

谢谢悟空问答的邀请！

长久关注我的网友都知道我对区块链和比特币的观点，正好看到钱塘号的一篇文章，和我的观点一致，且分析得非常精准，就借用其中部分内容小结一下吧。

1、区块链是一种鸡肋技术

人类社会任何技术的发明应用，本质都是为了提高社会的生产效率。而所谓区块链技术本质不过是几种早已成熟的技术的大杂烩，冗余且十分低效，除了提高了洗钱和诈骗的效率以外，对人类社会的进步毫无贡献。

2、不是蠢就是坏的区块链媒体

空气币和区块链的造富神话，让区块链自媒体也开始迎风乱扭。一群群根本不知道区块链为何物的妖魔鬼怪纷纷进驻区块链自媒体战场，开始大放厥词胡编乱造。

现在搞区块链的每个人其实都想去掉现有的中心，让自己变成中心，这是人性使然，不管人类社会发展到什么程度，人性的贪婪永远不会改变。区块链的谎言就像“没有中间商赚差价”一样，本质都是想把其它中间商都干掉，让自己成为最大的中间商。

区块链技术淋漓尽致地展现了人与人失去了信任之后社会所需要付出的高昂代价，当既有信托机制崩溃的时候，阴谋家和野心家以及诈骗犯又是如何趁虚而入，疯狂收割的。

总之，任何东西，但凡只要和区块，链，分，分布式，记账，加密，验证，可追溯等等这些个关键词沾到哪怕一点点，这些所谓的区块链媒体人就会像狗闻到了屎了

一样疯狂地把区块链概念往上套。

下面再借用巴菲特谈比特币延伸一下。

因为符合上述定义的、以比特币为代表的原教旨区块链技术，是反效率的，从经济学角度来说，不但不是一种帕累托改进，甚至还可以说是一种帕累托倒退。

5月5日，“股神”巴菲特在他领导的伯克希尔哈撒韦公司股东大会期间表示，比特币是一种“赌博设备”，不生产任何实质性的东西。他说，比特币“不生产，不和你对话，什么都不做。它就像一个海贝壳或者什么东西，那对我来说不是一种投资。”

巴菲特说，比特币有一点有限的用处，那些和欺诈活动有关。比如我揪一颗纽扣就可以当token，然后出价1000美元卖给你，看今天之内能不能涨到2000美元。

巴菲特表示，比特币有一点有限的用处，那些和欺诈活动有关。它们和很多骗局联系在一起，已经消失了。这方面有非常多的损失。

和我之前反复强调的对比特币的观点完全一致……

点到为止吧。

你对这个问题有什么更好的意见吗？欢迎在下方留言讨论！

区块链到底是什么？小白注意哪些？

区块链是什么

区块链本质上是一个去中心化数据库。是一种分布式数据存储，点对点传输，共识机制，加密算法等计算机技术的新型应用模式。

举个例子：

比如说小明找大康借一百块钱，但大康怕他赖账，于是就找来村长做公证，并记录下这笔账，这个就叫中心化。但如果，你不找村长，直接拿个喇叭在村里大喊“我大康借给小明一百块钱！请大家记在账本里”，这个就叫去中心化。

以前村长德高望重，掌握全村的账本，大家都把钱存在他这里，这是过去大家对中心化的信任。现在，大家都担心村长会偷偷挪用大家的钱，怎么办呢？于是大家就

给每个人都发了一本账本，任何人之间转账都通过大喇叭发布消息，收到消息后，每个人都在自家的账本上记下这笔交易，这就叫去中心化。有了分布式账本，即使老孔或老周家的账本丢了也没关系，因为老朱、老杨等其他家都有账本。

区块链有什么特点：

去中心化：因为区块链的去中心化，它可以帮助点对点交易，因此，无论你是在交易还是交换资金，都无需第三方的批准。区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除了自成一体的区块链本身，通过分布式核算和存储，各个节点实现了信息自我验证、传递和管理。去中心化是区块链最突出最本质的特征。

开放性：区块链技术基础是开源的，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。开放性比较少被提到，但它也很重要，甚至可以说开放性是去中心化特性的保证之一。

安全：不受任何人或实体的控制，数据在多台计算机上完整复制（分发），攻击者无单一的入口点。只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据，这使区块链本身变得相对安全，避免了主观人为的数据变更。

不可篡改：信息通过密码学技术进行加密，一旦进入区块链，任何信息都无法更改。

匿名性：除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。区块链的匿名性特点，在一定程度上很好地保护了用户的隐私。但是区块链的匿名性也颇具争议，因为它在人们交易、隐私方面起到了重要的保护作用，也为一些违法犯罪行为提供了“保护伞”。

区块链应用领域

金融领域

区块链在国际汇兑、信用证、股权登记和证券交易所等金融领域有着潜在的巨大应用价值。将区块链技术应用在金融行业中，能够省去第三方中介环节，实现点对点的直接对接，从而在大大降低成本的同时，快速完成交易支付。

首先是因为区块链的去中心化特性带来的优势。在传统的金融机构，如银行，老王想给小张转一笔钱，他需要先通过中心机构银行的确认才能把钱转到小张手中，而

在区块链网络中，老王不需要通过银行就能把钱转给小张，这不仅提高了交易的效率，还在一定程度上节约了交易的成本。

目前火爆的defi，就是去中心化金融，虽然现在还在初始阶段，各方面都还不够成熟，但相比2017年的1-C-0空气，已经有了一定的落地。

物联网和物流领域

区块链在物联网和物流领域也可以天然结合。通过区块链可以降低物流成本，追溯物品的生产和运送过程，并且提高供应链管理的效率。将物流和供应链行业带入现代化将在全球范围内产生广泛影响。通过降低整体成本并允许物流流程中的实体与更多的个体代理商合作，整个物流将会有全面的改进。这些效率的提高最终将导致在流程的每个阶段节省成本。该领域被认为是区块链一个很有前景的应用方向。

公共服务领域

区块链在公共管理、能源、交通等领域都与民众的生产生活息息相关，但是这些领域的中心化特质也带来了一些问题，可以用区块链来改造。比如，对于普通企业来说，往往最难的就是去政府部门办事，不但需要各种证明文件，而且还需要跑多个部门，不同的部门要求还不一样。主要原因就是原先各个政府部门的数据都是孤立的，彼此不共享，但如果都能在信息高度安全的基础上“上链”，数据实现共享，则办事人就能实现只需在一个部门内解决多数问题。因为所有办事流程交付给智能合约后，后面就可以自动处理并流转，所谓“一网通办”并不再是梦想。

数字版权领域

通过区块链技术，可以对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，也可作为司法取证中的技术性保障。拿一首歌曲来说，如果原作人申请了该歌曲的版权，但是由于中心化机构存在存储不安全、不公开透明以及易被利益驱使的缺陷，版权可能被他人进行篡改，这样很可能损害了歌曲原创者的权益，而如果说该歌曲的数字信息及版权信息记录在了区块链上，借助区块链的公开透明以及防篡改性等优势，就能很好地避免版权信息被恶意篡改的情况发生了。

保险领域

在保险理赔方面，保险机构负责资金归集、投资、理赔，往往管理和运营成本较高。通过智能合约的应用，既无需投保人申请，也无需保险公司批准，只要触发理赔

条件，实现保单自动理赔。未来区块链作为保险行业重要的基础设施及工具，将与云计算、大数据、人工智能、物联网等众多新兴技术融合，实现更多的保险行业创新应用，构建创新型、平台式的保险服务创新生态体系。在区块链的推动下，未来将出现开放保险。利用区块链技术的开放性，将可改变传统保险业中的“信息孤岛”情况。另外，区块链未来也可提升保险互信、成就保险普惠。

区块链的应用前景巨大，将彻底革新现有价值传递体系在民生的各个领域，未来在区块链都会应用的到，可以想象的是，当社会的各个领域广泛用上了区块链，它将成为信息时代的重要基础设施，能解决很多当前令我们头疼的事儿。

区块链的龙头股有哪些？

整理了4个区块链的企业参考。

1、恒生电子

公司于2016年以400万美元投资智能合约公司Symbiont。Symbiont是用于发行和交易区块链智能证券的平台，专注于私募股权市场和企业债券市场。目前已有几项应用落地，包括安联保险重灾掉期保险系统、与Vanguard合作将区块链用于ABS的发行和交易等。

恒生电子是一家从事金融、证券软件开发的企业。2016年6月1日，金融区块链合作联盟深圳成立，恒生电子是25个发起成员之一，运用区块链技术实现基于联盟链的数字票据系统。目前，恒生电子的区块链技术已进入测试阶段。恒生电子FTCU联盟链的基础服务已推出，支持合同链、私募股权链等业务场景的接入。目前，FTCU联盟链的基础服务已完成技术研发。

值得注意的是，恒生电子在2016年的营业收入为21.7亿元，同比下跌2.49%；净利润为1829.14万元，同比下跌95.97%。恒生电子2017年三季报显示，营业收入为16.5亿元，同比增长23.41%；净利润为2.89亿元，同比增长41.15%。

2、四方精创

四方精创是一家为银行提供IT服务外包的企业。2017年2月28日，四方精创与IBM开展项目合作，并签署了《业务合作协议》，运用云计算技术及设计思考，进行区块链技术应用研究。四方精创也是中国首个区块链联盟“金链盟”联合发起人。

四方精创2016年的毛利率为50.28%，处于同行业首位。2014年-2016年四方精创研发费用占总营收比率一直处于上升态势，并且在2016年行业内排名第一，达到1

8.27%。四方精创在2017年三季度的营业收入为3.31亿元，同比增长40.29%；净利润为5399.99万元，同比增长30.68%。

3、赢时胜

2017年8月，公司联合光大银行、泰达宏利基金、英大基金等合作研发的国内首个基于区块链技术的泛资管阳光链正式上线。参与各方从2016年即开始多方布局，组建团队，发挥各自资源优势，力促上述泛资管阳光链成功上线。该泛资管阳光链，不仅实现了管理人和托管人信息共享，还可实时可审计、可监督以及可监管，解决了泛资管行业的痛点。

赢时胜也是金融区块链合作联盟深圳25个发起成员之一。赢时胜致力于为金融机构及其高端客户的资产管理业务和托管业务提供整体信息化建设解决方案的应用软件及增值服务提供商。金融加密、信息技术、算法等可用于区块链上。

2017年三季报显示，赢时胜的营业收入为1.17亿元，同比增长16.15%；净利润为3335.1万元，同比增长222.54%。

4、广电运通

广电运通是一家提供货币处理设备及系统解决方案的企业。

2017年7月14日，广电运通在投资者互动平台上表示，公司积极与银行等机构进行交流，探索业务场景上的应用，已针对区块链技术在金融领域、数字资产等方面的应用展开研发工作。在9月11日，公司再次表示已针对区块链技术在金融领域、数字资产等方面的应用展开研发工作，未来不排除继续加大投入力度。

广电运通的股价自2017年12月初开始震荡上涨，但上涨幅度均不大，直至1月10日，盘中直线拉升涨停。2017年三季报显示，广电运通的营业收入为24.33亿元，同比下跌6.4%；净利润为6.58亿元，同比增长29.79%。

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。

关于区块链与证券ppt的内容到此结束，希望对大家有所帮助。