

其实区块链 双花的判别的问题并不复杂，但是又很多的朋友都不太了解区块链双花的解决办法，因此呢，今天小编就来为大家分享区块链 双花的判别的一些知识，希望可以帮助到大家，下面我们一起来看看这个问题的分析吧！

本文目录

1. [什么是“区块链”？](#)
2. [互联网区块链项目是什么](#)
3. [区块链会是第三代互联网吗？](#)
4. [什么是区块链？](#)

什么是“区块链”？

我不是计算机技术专家，以下对区块链的介绍来自阅读和专家朋友的评论，仅供参考。

如果要用一个词来解释区块链，那就是：分布式记账。

要理解一下这个词是什么意思，就需要先理解，传统的记账都是有一个中心的。比如银行，你从银行存款取款，通过银行借钱给别人，都是以银行为中心，所有这些交易都建立在银行的信用之上。那如果银行耍赖呢？或者更严重，国家耍赖呢？国民党在统治中国大陆的末期滥发金圆券，以及魏玛德国和津巴布韦的恶性通货膨胀，搞得货币没有卫生纸值钱，都是非常著名的例子。

金圆券

区块链针对的，就是这个问题。他们认为，去中心化的记账才是不可修改，不可抵赖的。怎么实现去中心化记账？基本的思想是，所有的用户都存储下所有的交易记录，通过数学方法，让非法修改账本变得非常困难。这样一来，就保证了账本的可靠性。

具体而言，所有用户通过穷举随机数变量，第一个得到特定要求哈希函数值（Hash）的用户将有权记账该轮交易，并获得对应的比特币奖励。以数据块（block）的形式进行传输，并以末端追加的方式将数据块连成链状（chain），因而叫做区块链（blockchain）。

听了介绍，你也许会感到这种思想很有意思，但并不像宣传得那样激动人心，那样有革命性。你的感觉是对的。实际上，区块链的基本逻辑就有些绕不过去的问题。

例如，目前完整的比特币公共账本大小已经超过150G，并以每年数十G的速度快速递增——仅仅为了支持500万用户每年3000万笔交易。如果有朝一日其处理量与目前的支付宝比肩，那每年比特币账本的大小将增加超过500T。这相当于把支付宝服务器的存储数据在所有用户的个人电脑上进行备份，——你会觉得这是个好主意吗？

又如，在传统的银行体系中，如果你把密码丢了，并没有什么了不起，向系统及时申报就是了，你的财富不会消失。但在区块链体系中，如果你把密码丢了，那么这就是个巨大的麻烦，你的货币就找不回来了。不开心？意不意外？

互联网区块链项目是什么

区块链是一个基于共识机制、去中心化的公开数据库。共识机制是指在分布式系统中保证数据一致性的算法；去中心化是指参与区块链的所有节点都是权力对等的，没有高低之分，同时也指所有人都可以平等自由地参与区块链网络，唯一的限制就是个人自己的选择；公开数据库则意味着所有人都可以看到过往的区块和交易，这也保证了无法造假和改写。基于以上特性，可以总结得出：区块链由许多对等的节点组成，通过共识算法保证区块数据和交易数据的一致性，从而形成一个统一的分布式账本。

从价值层面来看，区块链是一个价值互联网，用于传递价值。目前的互联网仅用来传递消息，但是还不能可靠地传递价值；而比特币区块链却可以在全球范围内自由地传递比特币，并且能够保证不被双花、不被冒用。从这个角度来说，区块链是记录价值、传递消息和价值本身转移的一个可信账本。这里要提一下区块链在维基百科上的官方定义：一个区块链是一个基于比特币协议的不需要许可的分布式数据库，它维护了一个持续增长的不可篡改的数据记录列表，即使对于该数据库节点的运营者们也是如此。

区块链会是第三代互联网吗？

最早的网络是模拟通讯网络，主要是解决了电报的数字交流，电话的语音交流，传真的图像交流，但是视屏电话，始终由于模拟带宽的限制没有腾飞。这时候，还是只能进行相对简单的日常和工作信息交流。然后是数字通讯网络，同时实现了基于TCP / IP的包交换协议，从而有了今天无处不在的互联网和移动互联网。最早的互联网，也是只能进行一些静态信息的交流。之后，慢慢有了动态信息，交互式 and 实时读写。但是，大量的信息在网上移动，很多的都没有给生产者带来价值，而是给中间商带来了巨大的利润。Google，百度，采集和索引网上的内容，然后给用户提供查找服务，赚得盘满钵满，而内容的生产者并没有得到应有的价值回报。同理，Facebook，腾讯的社交网络。于是，时代召唤第三代网络，价值互联网。这时

，随着比特币在2009年的诞生，区块链作为后面的价值网络，应运而生。价值的首要前提是需要确定资产的所有者。这就是区块链解决的第一个问题，确权。首先，区块链应用密码学，利用公钥私钥机制，保障了只有通过私钥签名的资产才能使用唯一的公钥才能验证，那么，一个人只要用私钥对自己的资产签名，那么别的人就不能再声明对此资产的所有权了，而且也不能被篡改，因为别人没有他的私钥。那么，对于某个资产的签名，保证了某人对资产的唯一所有权，理论和算法上证明了。其次，区块链应用了分布式共识机制，保障了声明所有权的时间顺序，只有有了时间顺序，才有保障在同时有多人声明的情况下，第一个声明的人才是某资产的真正唯一拥有者。实现的机制是，先由一个节点收集在某一段时间内的声明顺序，然后由大量的其它节点来见证和验证，如果大部分节点都认可了，那么这个声明的顺序就被公认和确定了。有没有发现，还是基于的大多数认可的民主机制。最后，通过链式结构，加密哈希和分布式账本，保障了历史的所有权长期存在，不可更改。这些历史的所有权记录，是经过大部分群体认可的，所以是可信的。也就是说，当初声明的时候，大多数都听到了，见证了，想否认都不大可能了。通过这些方式，区块链能够确权了，不可否认的确定谁拥有什么。那么，接下来需要解决价值的另一个前提是安全可靠的交换。价值是在供需中体现出来的，没有交换，就没有价值。区块链是如何解决可靠的交换的呢？首先，还是应用密码学，所有者通过提供签名验证才能释放自己的资产，转移给另外的人。另外的人拿到资产后，也只能通过自己私钥验证的签名才能将资产转移给别人。这样，就保障了转移的一方确实拥有相应的资产。被转移的一方确实收到了相应的资产才能继续转移。这样，就保障了资产是所有者在交换。其次，贯彻“Code is Law”的思想，采用脚本和智能合约的技术，保障交易只能在符合条件的情况下，才能真正发生。如果条件不能满足，那么相应的交易就会失败，等于什么都没有发生。这种自动化的交易机制，除了人，让机器人和系统也能参与到交易中来。再次，还是通过共识的机制给交易确定了顺序，从而解决了数字货币或是数字资产的“双花”问题。交易顺序一旦确定，同一笔资产，哪个交易先发生，哪个后发生，一目了然。这样，先发生的确定，后发生的就无效了，这样，保障了不会有双花发生。最后，一个交易的确认，也是需要大多数的确认和共识，并且记录在案，不能更改。所有的历史交易都记录在案，随时可以查询。有了“确权”和“交换”，价值就能完成了。而区块链正是解决了这两个问题，才成为了第三代互联网价值互联网的基石，让价值互联网成为可能和现实。有了价值互联网，以后的想象空间就大了去了，这也是为啥各大公司，各个国家都不可忽视区块链技术和可能带来的变革。

什么是区块链？

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。

关于区块链

双花的判别，区块链双花的解决办法的介绍到此结束，希望对大家有所帮助。