大家好，区块链 双花相信很多的网友都不是很明白，包括区块链 双花攻击也是一样，不过没有关系，接下来就来为大家分享关于区块链 双花和区块链 双花攻击的一些知识点，大家可以关注收藏，免得下次来找不到哦，下面我们开始吧！

本文目录

最近“区块链”成了热词，“区块链”为什么这么火？

区块链由于在信息保真、去中心化、算法信任等方面的技术革新，受到追捧，但技术总归要落地才能体现价值，在真实环境下，区块链的一些特性还是要妥协，总体而言，这是一个值得期待的技术

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。

区块链最近比较火，到底是什么技术？现在已经有哪些应用？

谢邀，正好刚刚看到了关于区块链的解释，搬过来分享一下。

举个简单的例子，假如你们家里有个账本，让你来记账。在以前，就是爸爸妈妈把工资交给你，让你记到账本上。中间万一你贪吃，想买点好吃的，可能账本上的记录会少十几块，然后你想买个手机，账本上就少记录几千块。这只是举一个例子，我相信小时候大家都想从爸爸妈妈的口袋里拿点钱来花。

有了分布式账本后，上述说的问题就不会有了，因为你在记账，你爸爸也在记账，你妈妈也在记账，他们都能看到总账，你不能改，爸爸妈妈也不能改，这样想买烟抽的爸爸和想贪吃的你都没办法啦。

区块链本质上是一个去中心化的分布式账本，其本身是一系列使用密码学而产生的互相关联的数据块，每一个数据块中包含了多条经比特币的网络交易有效确认的信息。

再来解释一下，什么是去中心化。

我们首先思考这样一个问题，你要在网上买一本书，交易流程是什么？

第一步：你下单之后把钱打给了支付宝。

第二步：支付宝收款后通知卖家可以发货了。

第三步：卖家收到通知后给你发货。

第四步：你收到货之后很满意，于是确认收货。

第五步：支付宝收到了你的通知并打钱给卖家。

在这个过程中，虽然你是在和卖家交易，但是整个交易都是围绕支付宝展开。因此，如果支付宝系统出了问题，比如天上降下来一块陨石，把支付宝的服务器全砸了，或者由于全球经济危机支付宝倒闭了，无奈的支付宝只好淡然地表示不存在这笔交易，那么这笔交易就会以失败告终，到时候买家卖家就会纠缠不清，双方无法自证。

模拟一个区块链小城市

为了说明去中心化的区块链是如何运行的，我们先把整个去中心化的分布式结构简化为一个极端的情况来探究。我们假设有一个去中心化的小城市，在这个城市里有5个可爱活泼的小伙伴，他们互相借钱的时候，是这么干的：

假设B向A借了1块钱，这个时候，城市里的人怎么办呢？A在人群中大喊：“我是A，我借给了B1块钱！”B也在人群中大喊：“我是B，A借给了我1块钱！”

此时城市里的其他人C、D、E都听到了这些消息，他们拿出了手中的小账本并默默记下：“某年某月某日，A借给了B1块钱。”

当我们把一个去中心化的模型极度简化之后，我们就会发现，在这个只有5个人的城市中，已经建立了一个去中心化的系统，这个系统不需要银行，也不需要支付宝。这个模型不需要信任关系，也不需要一个拥有公信力的组织。

当分布式结构中的每个人都记账的时候，篡改账本是不可行的。比如B突然不认账了：“我不欠A的1块钱！”这个时候，人民群众C或D或E就会站出来说：“不对，我的账本上明明记录了你在某年某月某日向了A借了1块钱，并且没有查到你还款的记录。”

说到这里，你有没有发现一个问题，在这个模型中，所谓的1块钱根本不重要，也没有人在意，“1块钱”已经变成了一个变量，它可以被替换成任何概念，只要大家承认这是一个有价值的东西即可。

比如A在这个城市中大喊一声：“我创造了一个巴拉拉能量！”城市中的其他人都听见了，于是大家纷纷在自己的小本子上记下“某人有一个巴拉拉能量”，大家甚至不用知道巴拉拉能量是什么，A竟然真的有了一个巴拉拉能量。

A还能干什么呢？A可以再大喊一声：“我给了B一个巴拉拉能量。”只要城市中的B、C、D、E，即城市里的所有人都承认了这个交易，那么这个交易就真的成立了，虽然现实生活中并没有巴拉拉能量。

这个区块链小城市模型中存在着几个问题：

问题一：凭什么帮你记账？

凭什么你对着天空大喊一声，别人就要帮你记账，别人的时间不要钱吗？别人的小本子不要钱吗？于是，为了让大家都帮我记账，我增加了一条新的规则，我决定给第一个听到我喊话并且将其记录在小本子上的人奖励。奖励机制也很简单，第一个听到我喊话并记录下来的人，可以得到一个巴拉拉能量的奖励。

这个巴拉拉能量不是白给的，是对你劳动的报酬，就像打工可以挣钱一样，你帮我记账，整个系统都会给你报酬。你要做的事情，有这样几点：

首先，你要抢在所有人之前听到了我的喊话并记在了自己的小本子上；

记录之后，你还要马上告诉整个城市里的人——这句话我记录完了，你们再记录也没有用了，别人就会放弃这笔赚钱的生意；

与此同时，你还要做一件事，就是给自己的记录加一个独一无二的编号，然后把记录和编号一起喊出来，于是，下一个人再记录的时候，就会带着这个记录和独一无二的编号继续下去。

在这条新的规则开始实行之后，一定会有这样一些人，他们为了得到巴拉拉能量，开始屏气监听周围发出的各种声音，只为了能在第一时间记下一条新的记录。

这个时候，对区块链有所了解的读者是不是想到了这样的名词——“比特币挖矿”。没错，这就是比特币挖矿的简单说明。

关于比特币挖矿的话题，知乎用户“玲珑邪僧”的一篇文章举过一个更生动的例子，大致是这样的：单身男士们要找女朋友，“国民岳母”说，我有好多肤白貌美、乖巧可爱的女儿，这样吧，我给你们出一个旷世难题，解出一个就给你们其中一个姑娘的微信号。

于是，单身男士们疯狂竞争，想破脑袋去解这道旷世难题。只要其中一位单身男士解出一道题，就立马得意扬扬地昭告天下，示威全部单身男士，这个姑娘的微信号是我的啦，先到先得，你们放弃吧。其他单身男士虽然已经算到一半了，但是没有办法，速度不够快啊，只好立马去解下一道题。

同时，首个成功破解旷世难题的幸运的单身男士不仅不用付一二十万元的彩礼，被其才华征服的“国民岳母”还会给这位单身男士一笔巨额财产做嫁妆，也就是比特币挖矿中的比特币奖励。

问题二：分叉问题听谁的？

在这一段的论述中，我们引用了知乎用户“汪乐–LaiW3n”的说法。在这个广阔的小城市里，一定还会存在这样的问题，B和C几乎同时记录完了，于是同时向天空大喊了一声，“这个编号89757的巴拉拉能量归我了”。

但是，由于这个城市太广阔了，有的人会认为这个编号89757的巴拉拉能量归B，也有的人认为这个编号89757的巴拉拉能量归C，但是编号89757的巴拉拉能量只有一个啊，只有一个人能得到，怎么办呢？一人一半？当然是不可能的，这个时候我们会采用更原始简单的规则来解决，谁长听谁的。

在不加任何限制条件的情况下，这件事件会发展成这样：一部分人认为这句话是B说的，在听到这句话之后开始记账，之后他们所做的所有事情都是基于B有了编号89757的巴拉拉

能量这个事实，并且随着这个信息一次次地传下去，这条信息链会越来越长；而另外一群认为C先说这句话的人，也会按照这样的趋势发展。

这下事情严重了，原本是一条唯一的、编号顺序严谨的总信息链，在B和C喊出“这个编号89757的巴拉拉能量归我了”这句话之后，硬生生地分叉了！这还得了，要是这种情况延续下去，每个人手里的账本都变得不一样了，而且根本没法确定哪个是真的！

为了解决这个问题，小城市又追加了新的区块链规则，记录的时候必须顶格写，而且要保证，中心在离田字格上边缘0.89757毫米的位置上，于是，每个人写字的时候都要拿刻度尺量好之后再写，这非常困难，每个人的记录需要5分钟才能完成。

因此，写这句话所用的时间变得不同了。所以只要有人高喊“我写完了！那句话是某某某写的”，其他正在写这句话的人便会停笔，然后在小本子上重新开始写“那句话是某某某写的，上一句的编号是×××”。

问题三：双花问题

双花问题是指一笔数字现金在交易中被重复使用的现象。

如果我同时向B和C都喊了一句，我给你一个巴拉拉能量，怎么办呢？巴拉拉能量只有一个，如何保证一个巴拉拉能量在实际的交易中只被支付了一次呢？

我们以比特币为例，中本聪在《比特币白皮书》第五小节中是这样说的，运行比特币网络的步骤如下：

1.新的交易向全网进行广播；

2.每一个节点都将收到的交易信息纳入一个区块中；

3.每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

4.当一个节点找到了一个工作量证明，它就向全网进行广播；

5.当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才

认同该区块的有效性；

6.其他节点表示他们接受该区块，而接受的方法则是跟随在该区块的末尾，制造新的区块以延长该链条，并将该区块的随机散列值视为新区块的随机散列值。

也就是说，交易发生的一刻起，比特币的交易数据就被盖上了时间戳；而当这笔交易数据被打包到一个区块中后，就算完成了一次确认；在连续进行6次确认之后，这笔交易就不可逆转了；在比特币中，每一次确认都需要“解决一个复杂的难题”，也就是说每一次确认都需要一定的时间。

在这种情况下，当我试图于把一笔资金进行两次支付交易的时候，因为确认时间较长，后一笔交易想要与前一笔交易同时得到确认几乎是不可能的，而这笔资金在第一次交易确认有效后，第二次交易时就无法得到确认。区块链的全网记账需要在整个网络中达成共识，双花问题是无法产生的。

区块链技术怎么保证支付的安全？

为了解决丢失秘钥和黑客偷窃私人信息的问题，OAS区块链团队将推出（公有链+私有链）的技术，保证了客户的区块链支付安全的需求，如果黑客盗取用户的密钥转移了用户的资金，则用户可以通过申诉，仲裁员通过判断可以取消异常的交易内容，这个团队主要是提供这些服务平台，中介主机托管服务，?ERC20–智能合约，ERC721–资源的共享和交易等，最大限度的保证了区块链支付的安全，也保障了用户的权益。

OK，关于区块链 双花和区块链
双花攻击的内容到此结束了，希望对大家有所帮助。