区块链及数字货币中双花问题是什么意思？提到双花问题，很多投资者都可以说是一脸懵圈，甚至有部分投资者都没有提说过双花问题，其实币圈一直都有双花攻击的案例，比如说2018年曾经发生了比特币黄金的双花攻击，只不过大多数投资者都不太关注这方面的新闻，因而自然也就不会去了解双花问题是什么意思，那么，区块链及数字货币中双花问题到底是什么意思呢？下面小编就给大家通俗的讲解一下区块链及数字货币中双花问题是什么意思？】

因数字货币是二进制的代码，是可以复制的数据，存在一笔数字资产被重复使用的情况，这就是所谓的“双花”。一笔资产可以花两次甚至花多次。

我们知道作为中心化的支付平台第三方是保留交易总账来保证每笔数字现金只会被花掉一次;而作为去中心化的区块链里数字资产，双花问题是如何出现的呢?

先假设一个场景

场景1：诈骗者使用数字货币购买数字产品如买一本电子书，价格为1个EOS。他先将EOS发送给店家，假设这笔交易是tx1;然后同时将相同数量EOS发给自己另外一个钱包地址，称这笔交易为tx2。店家网站程序检测到交易tx1后，觉得没有问题，程序自动发电子书过去;但因交易tx1和交易tx2是相冲突，矿工只会在一个时间点打包一个交易，万一不小心都打包了，其他节点矿工会验证并拒绝这个区块打包成功，所以如果交易tx2打包成功了，交易tx1会作废，这种情况下，诈骗者成功双花了EOS，即买到了电子书，也收回了自己的EOS。

解决办法：这种场景下的双花比较好解决，店家网站程序自动发电子书前，先让区块确认交易，至少一个区块交易，而只有被至少一个区块确认过的交易，就会盖上时间戳且之前从未存在过，才被认为交易的有效性。目前比特币的交易要被6个区块确认才算安全有效可靠，以避免孤立区块的情况;EOS的充值确认在币安里是需要至少32个区块确认数。

另外一种场景，假设诈骗者是矿池或矿工。

场景2：诈骗者矿工先构造交易tx1和tx2，tx1的手续费很低，将tx1发给商家买电子书，但是交易tx2隐藏起来不广播，只保存在自己的区块内。因为tx1的手续费太低，所以其他节点矿工们不想打包;而tx2被隐藏起来了，所以区块链浏览器是不可能发现有相冲突的交易，商家也就不可能发现。当商家认为是正常的交易一旦发货了，诈骗者矿工就会在自己挖到的区块打包进去，这个时候广播这个区块，全网所有的节点就会发现tx1是非法的了，直接作废掉，商家就收不到币了。

解决办法：想防御这类双花攻击就要依赖其他矿池矿工的协作。因为诈骗构造的tx2交易是不会被广播的，是以直接打包进诈骗矿池挖到的区块才会被其他矿池发现。如果其他矿池如果针对这种包含了延迟出现交易(tx2)的区块进行孤立，那这个诈骗矿池的这个块就白挖了，损失区块奖励，这是非常惨的事。具体的设定可以是矿池将超出一定时间，比如10秒内，都没有见到的交易(tx2)，却包含在最新的区块里，则直接孤立掉这个块，在这个块的前一个高度上挖矿。

如果执行这种孤立政策的算力超过51%，那基本上就没有矿池敢发起这一类隐藏交易(tx2)来攻击零确认交易了。

首先，要检查这笔钱是不是没有被花费过。方法是查看你的这笔交易的来源是否在UTXO(未花费交易列表)中。不需要追溯到挖矿挖出的Coinbase交易。

然后要看你提交的交易里有没有包含有效鉴权。如果这笔钱之前是通过P2PKH交易付给你的，那就是看交易里有没有这笔钱所在地址的对应私钥的签名。P2SH、P2MS类型的交易的鉴权规则类似。

如果你用同一笔UTXO构造了两笔分别付给A和B的交易。那么bitcoin-core客户端的规则(截止2016.2)是只转发先侦听到的那个。但至于哪笔交易会被包含进未来区块，则取决于矿工。

矿工的挖矿程序一般是定制开发的，矿工可以自主任意选择这两笔交易里的一笔。比如有的矿工会选择先看到的交易，有的矿工会选择交易手续费更高的那个。

当这两笔相矛盾的交易中的一笔被写入区块链，并且深度达到6后(6个确认后)，可以认为这笔交易获得了最终的确认。等待6个确认的情况下，比特币是几乎绝对不可能被双花的。一个确认都不等待，则有相当的可能被双花攻击。通常，3个确认已经相当安全。

其实避免数字货币的双花问题，主要就是交易成功后的区块确认数，比特币的区块确认数达到6就非常安全，双花问题基本上不可能出现，除非矿池的算力超过50%了，就可以为所欲为，双花在这种情况下算蝇头小利，强制分叉获利远远大于双花获利，另外判断交易是否合理，不仅仅是矿池节点，任何一个核心节点都会进行。即查询历史区块链，判断交易的输出是否不大于输入。

以上就是DaDaqq.com区块链及数字货币中双花问题是什么意思 如何防范双花问题的详细内容，更多关于双花问题是什么意思的资料请关注币大师其它相关文章！

Tag：区块链 数字货币 双花问题