其真实我们的日常生活中，我们曾经听说过双重支付的效果，就比如说，一些黑心的房东或是中介在卖房子的时分，同时和两团体签合同，又大约是一团体只需一万块钱，但它同时许愿了两团体会给对方一万块钱。在比特币的系统中也会出现诸如此类的双重支付的效果，而针对这些效果，比特币也想象了一套特地的进攻机制，它会对买卖音讯提到的余额中止检查。那么比特币双重支付是什么意义?

比特币双重支付是什么意义

首先，电子货币具有一个一般的效果：电子货币不同于现金纸币，其可以随意的中止复制。也就是说一个电子币可以复制多份，然后停止屡次支付运用。我们把这个效果成为双重支付(double-spend)。

双重支付成绩又称为“双花”问题，即运用货币的数字特性用“同一笔钱”完成两次大约屡次支付。在激进的金融和货币体系中，由于金钱货币是物理实体，具有客观独一具有的属性，所以可以防止双重支付的状况。但在其他的电子货币系统中，则需求可信的第三方管理机构提供保证。区块链技术则在去中心化的零碎中不借助任何第三方机构而只经过火布式节点之间的相互考证和共识机制，有效地处置了双重支付问题，在音讯传输的同时完成了价值转移。

区块链技术经过区块链接形成的时间戳技术加上考证比特币能否满意UTXO(未破费买卖)和数字签名，有效防止了双重支付的问题。假定有人用同一笔UTXO结构了两笔付给不同买卖方的买卖，则比特币客户端只会转发最先被侦听到的那个。矿工会选择将那笔交易包入未来区块，当其中一笔交易所在的区块后有5个链接的区块，这笔交易曾经取得了6次确认。在比特币区块链上，一般的做法是6次确认后基本上该比特币被双花的概率很小。依照中本聪在比特币白皮书中的计算，6次确认后双花的概率大约在0.024%。

双重支付的处置方法

问题1：如何检查余额?

比如网络收到了一条消息：A转给B 十个比特币。

此时全网会下载比特币区块链一切的消息，追溯A的一切历史交易记载。假定区块链交易信息显现，A的余额足以支持这次10个BTC的交易，那么这条信息会被全网所接受，否则不会被接受。

问题2:假定同时支付给两团体，以哪条交易记载为准?

比方A向全网广播：转10个比特币给B，但同时他又发了一条，转10个比特币给C，而此时A的总余额只需10个。该哪条交易记载为准呢?

这时，有些人会先收到A给B十个比特币的消息，他们检查余额之后会自动疏忽另外一条消息;十分，那些先收到A给C十个比特币消息的人，在检查余额之后也会自动疏忽另外一条消息。

不论接收到的是哪条交易信息，接下去，网络上的矿工都会对自己收到的消息停止打包，计算区块当中所包括的随机数，也就是挖矿，第一个计算出随机数的矿工，就会将这个区块放到主链当中，这条交易记载也就会被全网招认。假设放入主链的交易信息是A转给B十个比特币，那么B将会取得这些比特币，另外一边的矿工也就自动中止计算了;假设放入主链的交易信息是A转给C十个比特币，那么C将会获得这些比特币。

上文的方式就是币圈子汇游网小编关于比特币双重支付是什么以及比特币双重支付应当怎样处置这两个问题的精细解答。做一个冗杂的总结的话，就是比特币区块链在防止双重支付问题上，首先会检查一切的交易记载，追溯交易信息，然后在确保余额准确的状况下，那些先被放入主链的交易信息将会被全网接受。经过了这么多年的展开，往常比特币的机制也在逐渐被完美，目前比特币所面临的最大的问题就是区块容量的问题，所以目前比特币展开的十万火急就是扩容。