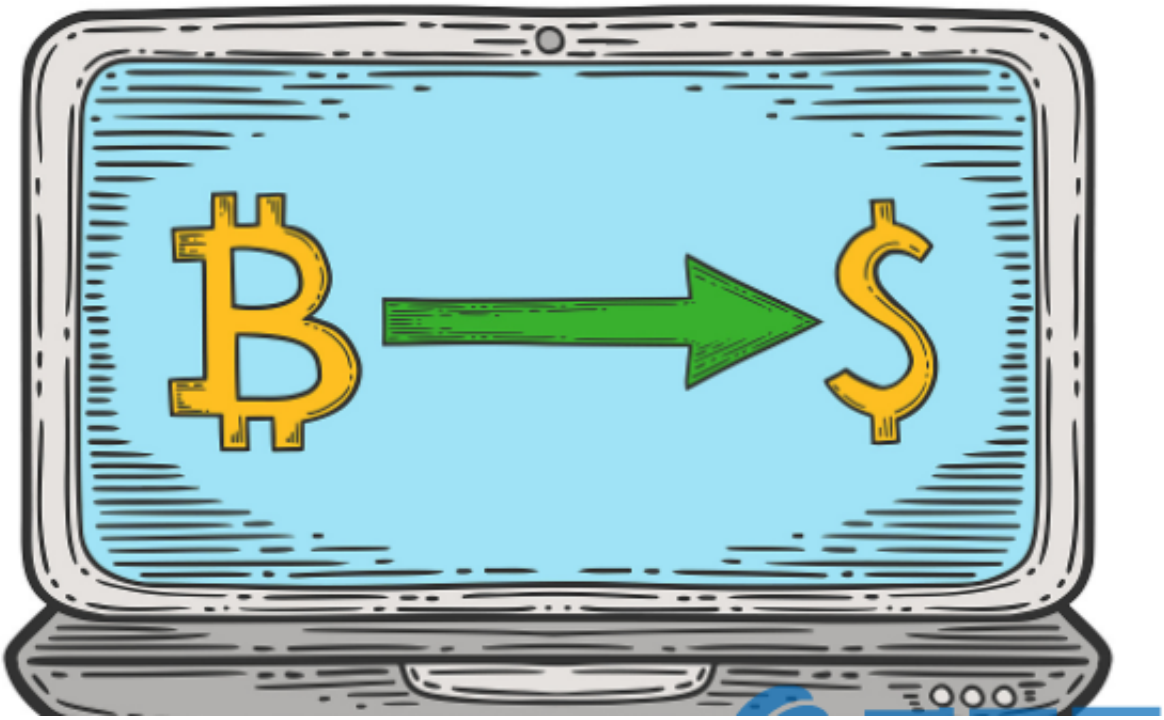
如何防止一个比特币被使用两次？作为一个去中心化的点对点电子现金系统，比特币区块链主要依靠UTXO和时间戳来处理&#039；双花&#039；问题。双花&#039；指同一笔款项支付两次的情况，即重复支付。

作为一个去中心化的点对点电子现金系统，比特币区块链主要依靠UTXO(未用交易输出)和时间戳来处理&#039；双花&#039；。当比特币交易被创建并广播到区块链网络时，每个节点(比特币交易参与者)将验证该交易。，看事务的输出是否存在于UTX0(未用事务输出)，即&#039；未用交易输出&#039；



如果A拥有的1BTC被证明是an&#039未使用的事务输出&#039；如果他把1BTC同时转给Bl和B2，挖矿节点会选择性记录一笔交易，可能是最先收到的，也可能手续费更高。

如果这两个事务被挖掘节点先后接收，那么根据时间戳，先接收的事务将验证成功，后接收的事务将失败，因为事务输入在UTX0中不存在。

如果两个挖掘节点记录了两个事务&#039；从A到B1&#039还有&#039；从A到B2&#039；同时，并且这两个交易分别被证明是合法的，那么这两个挖掘节点会把自己挖到的新块广播到全网。

此时，链将分支。其他参与挖掘的节点会随机选择一条链继续挖掘。哪个链最先产生新的块，就会成为目前最长的链，记录在最长链上的事务最终会被认证为成功，

而记录在另一个链上的事务则不会被认证。

如果一笔交易创建后没有记录在块中，则确认为0；如果记录在块中，则确认为1。为了防止恶意制造最长的链条为&#039；双花&#039；建议等待6个新块生成，即&#039；6确认&#039；在完成交易之前。