

币圈难题之：比特币在区块链上的交易是如何进行的？在日常生活中，“交易”本质上就是指资产所有权的转移。因此比特币交易，实际上也可以称之为是，记录在区块链当中的比特币所有权的转移。简单来说就是一个地址向另一个地址转账的过程。

在这个过程中，我们需要使用到私钥和公钥，来确认比特币的所有权以及对交易进行签名。私钥是通过安全算法随机生成的一个字符串，通过私钥可以推导出公钥，拥有私钥的人就拥有对比特币的支配权。

通常情况下，交易发起方创建了一笔交易之后，他将使用私钥对这笔交易进行签名，这个签名表示比特币所有者对交易的许可，同时也确保了交易发生后不会被他人修。

随后，这笔交易将被广播到整个比特币网络中，等待确认；当矿工接收到这些交易请求之后，将通过计算哈希值来争取记账权，然后将交易打包成一个区块，并上传到整个区块链当中；当整个网络中有超过六个节点对这些交易进行确认之后，比特币的转账过程就完成了。

交易完成后，比特币接收方将获得这笔资金的所有权。用一句话来概括，比特币交易就是“经过签名运算，表达价值转移的过程”。它们都通过比特币网络进行传输，由矿工节点验证并打包到区块，然后永久保存在区块链上。关于比特币和区块链的题外话：前两年“币圈”被炒作了一整年，经过时间的沉淀和行业的变迁，区块链成为了一个新的炒作热点，一方面有着国际上比特币和区块链猫的先例作为价格支撑，另一方面采用区块链的公司又可以加上高新技术概念股炒作，在中国“资产荒”的大背景下，区块链概念股也就具备了格外良好的炒作意义。