


我们在接收和发送比特币时都会用到比特币地址，它是一个由数字和字母组成的字符串。在交易的过程中，它通常以收款方的形式出现，那么比特币地址和密钥之间有什么关系？比特币是建立在密码学基础之上的，因此其地址也是匿名的，不包含所有者的任何信息。中本聪利用了椭圆曲线算法先产生比特币的私钥和公钥，然后将公钥的值再经过一系列数字签名运算就得出了我们所使用的比特币地址。在这里，私钥用来声明用户对比特币的所有权，由私钥可以推导出公钥，反之则不行。 

在实际的交易过程中，我们通常使用比特币钱包的接收界面直接生成比特币地址。在转账时可以手动输入接收方的转账地址，也可以通过扫描接收方地址二维码完成交易。像Blockchain之类的加密货币钱包，通常在用户接收到一笔汇款之后就更改一次比特币地址，目的在于鼓励用户使用新地址交易，以提高匿名性，当然同一个钱包的所有旧地址都依旧可用。比特币地址和密钥之间有什么关系？上面就是关于这个问题的相关内容，希望能给大家起到参考作用。