

区块链技术的火热，加上虚拟货币比特币疯涨，让人们越来越熟知这一新兴领域，很多人也开始跃跃欲试。但虚拟货币及区块链中很多概念及细节，让人似懂非懂。基于资金安全考虑，很多人都会选择观望和犹豫。OK，这里给大家讲一讲虚拟货币钱包，类比银行卡，期望打消大家的一些疑虑，若能帮到大家，将是不二最开心不过之事。

虚拟货币（本文以下都已比特币为例）对绝大多数人来说都是比较陌生的，说起钱包，更是有些糊涂，下面就展开来说比特币钱包相关的最最基础的两点：地址、私钥。

银行的账号和密码

大家都能理解，自己的钱，都是保存在银行。而对钱的支配（存、取、转、兑），都通过银行账号和密码来执行。大家去银行开户，使用身份证登记，并通过系统验证真伪后，会给开通一个全国唯一的银行账号。最关键的，随着银行账户的开通，会要求你设置密码：查询密码和交易密码。这个账号和密码，就是你对自己存放在银行里的钱执行操作的凭证。如果你要给别人汇款，填写别人的银行账号（姓名、卡号、开户行）、汇款金额、取款密码，就可以完成汇款交易。收钱时，只用高速别人你的银行账号（姓名、卡号、开户行），别人就可以打钱过来。

即使是你的银行卡遗失了，只要密码不被人知道，捡到也拿不走你的钱。这时，补办一张卡，原卡作废，你账户的钱仍然是你的。这里也很好理解，你的钱不是存在银行卡里，而是在银行里。

这里也可以看出，银行卡密码的重要性，要绝对妥善保管好。



地址和私钥

比特币钱包怎么理解

银行账号（卡号）、密码，我们可以记在脑子里，也可以记在本子上。比特币的私钥、地址，都是一些计算机符号，而且这些符号有着严格的技术标准、算法和函数。存放和管理地址、私钥，打包交易和发送交易的工具，接收交易完成后信息的工具，这些，我们统称为比特币钱包。钱包可以是一个软件程序或一个APP，也可以由互联网平台提供线上钱包。

最简单最常用的，比如Bitcoin Core钱包，可以下载后安装在自己的电脑上。安装完成，就可以打开钱包，生成地址和私钥。其中有一个文件wallet.dat，这里面存放着你的私钥（银行密码）。不多说，wallet.dat这个文件一定要保护好，同时还要对这个文件进行加密，进一步提高安全性。很简单，别人拿到了你的私钥，就可以把你的比特币全部转走，关键是你还没法报警，报警也没有（比特币可是匿名交易的，不像银行账户，全部实名）。

为了私钥安全，有一个很好方案：在一台永远不上线的电脑上安装比特币钱包软件，然后生成地址和私钥。这时候你的私钥是完全没有接触过互联网的。这个离线生

成的地址，也是可以接受比特币的。通过私钥签名构造交易包，也可以在这个离线电脑是进行了。构造完毕后，在把交易包拷贝出去，在另外一台联网电脑广播确认。这种方式被称为离线钱包，也叫冷钱包。是最安全的存储比特币的方式之一。

钱包里面有没有比特币？这可不同我们口袋里的钱包，里面还有点现金。比特币钱包，仅仅存放的是地址和私钥，你自己的真正的比特币，是存放在比特币网络中（区块链的链条上），就跟你的钱在银行，自己只掌握这账号和密码。