



图一（来自Andreas M. Antonopoulos 的《精通比特币》）

1、私钥：是对一个比特币地址拥有取钱权限的代表，掌握了私钥就掌握了其对应比特币地址上的所有生杀大权。私钥可以算出公钥，公钥可以再算出比特币地址。每次交易的时候，付款方必须出具私钥，以及私钥产生的签名，每次交易签名不同，但是由同一个私钥产生。

2、公钥：是和私钥成对出现的，公钥可以算出比特币地址，因此可以作为拥有这个比特币地址的凭证。

3、比特币地址：如果说区块链是一个账本，比特币地址就是其中的账号。

4、钱包分为很多种，冷钱包、热钱包、硬件钱包、脑钱包、纸钱包等等，一看这些概念我就会犯晕，我觉得我们不需要搞懂那么多。我们只要搞懂应用场景，手机端还是PC端的，而且我觉得我们只会用到轻钱包，那种储存全部交易的全量钱包太恐怖了。如果你真不放心，就把这个钱包安装在平时不怎么上网的终端上，防止黑客盗用就好。

（二）、钱包实战

钱包以不同的协议又分为比特币钱包、以太坊钱包、EOS钱包等。

1、比特币钱包可以在比特币官网上找bitcoin.org，有很多钱包客户端厂商可选。

点击“创建钱包”，给钱包取名字和密码。千万千万注意：自己记住密码，imtoken不会记住你的密码，忘记密码不能被找回！！所以忘记密码就等于丢失了钱包里

的所有货币！！因此，强烈建议设置一个密码提示信息，以防自己的健忘症。

为什么不能被找回？这个也是对你自己负责，因为如果有存储或重置功能就容易密码泄露。



接下来我们要备份钱包，钱包备份是为了在程序被删除或手机被盗等等情况下恢复钱包设置用的。有两种方式：备份助记词或备份keystore。



而keystore是类似上图的一串。大家可以备份这个keystore，删除钱包后，用这个keystore将钱包恢复。几次练习，就可以把钱包玩熟了。

至此，钱包完成创建，在自己的钱包页，点击地址栏右侧



(三) 从交易所提币到钱包

点击我的资产：



输入之前钱包导出的地址：



会显示转账页面：



按下一步后输入密码即可转账。

结尾：以上介绍了数字货币钱包的基础应用方法，钱包现在还可以看数字货币行情、行业讯息等，基本上拥有一个数字货币钱包是币圈的标配，甚至为了保险起见，很多人会将数字资产分开储存在不同的几个钱包内。另外欢迎关注我们的公众号，实时更新关于pc.exchange交易平台的最新信息，并有更多区块链小白教程分享。

pc.exchange