公钥密码系统分为三部分：公钥、私钥和加解密算法。公钥密码系统的公钥和算法是公开的(这也是公钥密码系统名字的来源)，私钥是保密的。针对不同的目的，可以选择使用公钥还是私钥进行加密。然后用相应的私钥或公钥解密它。公钥密码系统的主要功能如下：

加解密功能

签名验证功能

密钥协商功能

。

在比特币系统中我们的公钥加密创建了一个密钥对来控制比特币的获取。密钥对包括一个私钥和一个由其派生的唯一公钥。公钥用于接收比特币，私钥用于支付比特币时签署交易。公钥和私钥之间的数学关系以便私钥可以用于生成特定消息的签名。这种签名可以验证公钥，而不会泄露私钥。在支付比特币时，比特币的当前拥有者需要在交易中提交自己的公钥和签名(每笔交易的签名不同，但都来自同一个私钥)。。比特币网络中的每一个人都可以通过提交的公钥和签名进行验证，确认交易是否有效，也就是确认付款人在那一刻拥有交易比特币的所有权。

私钥其实就是一个随机选出的数字而已。对一个比特币地址内所有资金的控制取决于对相应私钥的所有权和控制权。在比特币交易中，私钥用于生成支付比特币所需的签名，以证明资金的所有权。私钥必须永远保密，因为一旦泄露给第三方。相当于这个私钥保护下的比特币也被交出来了。私钥也必须备份，防止意外丢失，因为私钥一旦丢失，将很难恢复，其保护的比特币也将永远丢失。

这个随机数是怎么选出来的？？一般用随机函数发生器来实现，这里就不详细描述了。

在上图中，我们已经看到了比特币账户(地址)(私钥—

公钥—

比特币地址)的一般生成过程，这里我们将详细描述其生成细节。。比特币账户生成过程中应用了两个密码哈希函数，一个是SHA256，一个是RIPEMD160。下图是比特币地址(账户)的生成过程：

随机数生成器生成一个256bit的随机数，该随机数用作账户的私钥。

比特币使用椭圆曲线签名算法(ECDSA)对数据进行签名和验证，具体使用secp256k1曲线。。相应的公钥可以通过ECC乘法来计算。

散列公钥两次，以获得公钥的散列值。

对该对进行双重哈希运算，取前4个字节作为校验码。

对该对执行base58编码以获得地址。

其他前缀的含义如下：

类别

版本前缀(十六进制)

Base58格式

比特币地址

Paytothescripthashaddress

0x05

3

Bitcointestnetworkaddress

0x6F

m或n

私钥wif(钱包导入格式)

0x80

5(无压缩)，K或L(压缩格式)

BIP38加密私钥

0x0142

6P

bip32扩展公钥

0x0488b21e

xpub

使用base58编码格式对地址进行编码，主要是为了方便使用和识别。

Wallet是为用户提供交互界面的应用程序。。钱包控制用户访问，管理密钥和地址，跟踪余额，以及创建和签署交易。其中，最核心的功能是保存私钥。一旦私钥泄露或遗忘，比特币就会被盗或丢失。

你钱包里有比特币吗？钱包里只有钥匙。没有比特币。

那我的比特币呢？你拥有的比特币，其实是你所有账户地址未使用的交易输出。钱包会监控输出到你的公钥地址，比如A给你转1个比特币，B给你转9个比特币。，而你还没有&#039；t目前把它们转给别人，钱包计算出你目前有10个比特币。当你需要花比特币给别人转账时，你构造一个交易，用你未使用的交易输出作为输入，作为接收方输出&#039；的账户地址，并设置转账金额、自己的公钥信息等。再交易签名(私钥签名)确认后，发送到比特币网络确认，转账完成。

以上是dadaQQ.com&#039；的详细描述什么是比特币私钥，账户和钱包。更多比特币私钥、账户、钱包知识分享，请关注Coinmaster其他相关文章！

本站提醒投资有风险，入市需谨慎。此内容不作为投资理财建议。

标签：比特币比特币私钥比特币账户比特币钱包