huobi.com-专业&quot/&quot；比特币交易平台：比特币私钥和钱包地址的关系。要理解&quot/&quot；t&quot/teach/_blank&quot；比特币交易部分你需要掌握很多密码学知识：公钥、私钥、哈希、对称加密、非对称加密、签名等。所以普通用户最关心的是哪些需要用户小心保管，哪些可以&#039；不能向外界泄露，哪些可以公开？接下来，让&#039；让我们从钱包的地址生成开始。。第一代地址。首先，使用随机数生成器生成一个&quot私钥&quot。一般来说，这是一个256位的字符串。有了这串字符，你就可以在相应的&quot钱包地址&quot，所以一定要好好保管。。2.然后是&quot私钥&quot被算法处理，然后&quot公钥&quot已生成。它是一种椭圆曲线算法，相应的&quot公钥&quot可以从已知的&quot私钥&quot。然而，如果你知道一个&quot公钥&quot，你可以&#039；不要计算&quot私钥&quot反过来。这也是保证比特币安全性的算法基础。。3.与SHA256一样，它也是一种哈希算法。&quot公钥哈希&quot可以从&quot公钥&quot。同样，反过来也是不可行的。4.将一个字节的地址版本号连接到&quot公钥哈希&quot，然后对其执行两次SHA256操作。，取结果的前4个字节作为&quot公钥哈希&quot把连接放在最后。

5。用BASE58对上一步的结果进行编码，得到&quot钱包地址&quot。比特币地址设置为从数字1开始。。示例：私钥、公钥和钱包地址之间的关系在上述五个步骤中，只有&quotBASE58编码具有相应的可逆算法(即&quotBASE58解码&quot)，而其他算法是不可逆的，所以它们之间的关系可以表示为如图所示。显然我们可以使用&quot私钥&quot。"如果你有一个比特币私钥，你就有一个比特币公钥哈希&quot和&quot钱包地址&quot可以通过互易运算转换，所以是等价的。交易&quot私钥&quot用于通过()对比特币钱包地址之间的传输进行签名。。交易数据由&quot私钥&quot钱转到的钱包的，也就是你负责的话，只能在私钥对应的钱包地址上花比特币。"私钥&quot。整个交易过程如下：1。如你所见。交易数据包括&quot转账金额&quot和&quot转移钱包地址&quot，但是从交易开始，光靠这些数据肯定是不够的。其中一个可以&#039；Idon’我无法证明银行里的钱转移钱包地址&quot是他们的。所以你需要用&quot私钥&quot来证明你是货币的主人。。2.生成&quot钱包流出公钥&quot。该过程与生成&quot钱包地址&quot。

3。我们必须加上&quot翻转签名&quot和&quot转出公钥&quot到原始交易数据生成合法交易，这样我们就可以广播到比特币网络而私钥在比特币钱包里是看不到的。，以便成功完成转出。在&quot公钥&quot用于验证签名是否广播到比特币网络，比特币网络上的每个节点都会检查交易数据。最重要的部分是签名的验证。如果验证结果正确，比特币将成功从&quot转移钱包地址&quot到&quot转移钱包地址&quot。内容：1。如果一个&quot钱包地址&quot不向其他人寄钱&quot钱包地址&quot，那么它的&quot公钥&quot不会暴露。第二，生成私钥到公钥()的算

法是不可逆的。所以即使&quot公钥&quot被暴露，相应的&quot私钥&quot无法破解。破解难度往往取决于生成算法。功能。就目前的计算机计算能力而言，比特币钱包可以&#039；我看不到私钥，它还远未完成。三个。私钥用于生成公钥和钱包地址。，也用于签署交易。因此，拥有一个&quot私钥&quot对应一个钱包地址，意味着有全权操作这个钱包地址上的所有比特币。第四，私钥的备份方式可以多种多样。比如在QT钱包客户端。通过在wallet文件菜单中选择备份wallet.dat文件，wallet上的所有私钥都存储在一个文件中。中间

这种方式需要注意的细节是，钱包转账超过100次后，如果发起新的转账，需要再次备份。。这是因为QT钱包中的零钱机制。如果是SPV轻钱包，往往不会出现这种问题。您只需要备份一次私钥。5.为钱包设置的密码和钱包的私钥不是一个概念。你钱包的密码相当于重新加密了你钱包上的所有私钥。。在wallet.dat文件中，无法窥探其中包含的许多私钥的长度。但是，手动设置密码通常不太安全。除非是非常复杂的密码，一般都是可以暴力破解的。是还是那句话？&quot私钥&quot是比特币钱包里最基本最重要的东西，绝对不能随便泄露。本文只讨论标准P2PKH的交易模式，P2SH不在讨论范围内。

Ethos是一个简单易用的采矿系统。，为矿业提供教程软件和矿机评估交易信息，用数字货币对比计算各种矿业利润，介绍矿业工具和矿业网站的最新消息。