

数字货币钱包知识如何选择最适合自己的门罗钱包？本文将谈谈门罗币的接收、存放和发送的实用技巧。一开始我们会接触到一些门罗钱包和软件相关的关键概念和术语。后来我们会教你如何使用门罗币的官方免费开源软件CLI:命令行界面(CLI)和图形用户界面(GUI)。

什么是钱包？

在您收到门罗币之前，您必须计划好门罗币的接收和存放地点。这时候你需要一个钱包来存放和消费门罗币。你的钞票(比如欧元和美元)可以存放在各种实体钱包里。类似地你也有各种各样的门罗钱包可供选择和转移资金。

钱包会帮你处理那些复杂的加密过程，所以你不用使用钱包不需要任何高深的数学知识。你只需要注意你的种子代码和地址。学习如何使用钱包的功能。至于公钥私钥等钱包背后的技术细节，我们将在第5章开始涉及。

您的门罗种子代码是一系列秘密数字，您的钱包使用这些数字来查找和消费您的门罗硬币。为了方便起见这串数字被转换成12~25个短语，就像藏宝图一样，可以帮助你区块链找到你的资产。因此，您必须非常小心地生成和保存您的种子代码。请不要不要在像咖啡店这样的公共场所设置钱包。因为关键信息可能会被别人或者摄像头记录下来。以电子方式存储种子密码(例如在文本文件或电子邮件中)也很危险，因为恶意软件或服务可能会窃取它并拿走您的Monroe硬币。

种子代码生成地址让你接受门罗硬币。就像你的电子邮件地址一样，你和想给你发东西的人分享。大多数钱包有两种形式显示你的地址：一串字母和数字；二维码。你可以以任何形式与他人分享你的地址。

如果你的Monroe钱包的物理部件损坏了，你只需要将种子代码引入一个新的钱包就可以恢复它。只要持有种子代码，就可以随时获得资产。如果您丢失了种子代码，您将永远失去这些资产。。你可能知道密码丢失后，可以通过管理员重新创建。但是种子码不是密码，没有人知道你的种子码，没有人可以不依靠种子码把你的资金转到新账户。

大多数软件会建议你在初始化钱包时记录种子代码。但是有些软件没有这样的提示，所以一定要主动完成这一步，确认备份功能。请从一开始就这样做，否则一次损坏就会造成永久的资产损失。

图2.1:钱包的主要功能是存储种子码、生成地址、查看资产余额和发送交易。

## 选择最适合自己的钱包

在这一节，你会接触到很多不同的钱包。

通常情况下，你将大部分法定货币资产(如欧元或美元)存放在银行或保险柜中，只随身携带部分现金以备日常使用。类似地很多人也选择使用两种互补类型的钱包来存放加密的钱：方便的热钱包，存放少量日常使用的钱；更安全的冷钱包，用于长期或大额资金存储。

市场上有不同的存储方案。它们在便利性、隐私性和安全性方面是不同的。你的需求决定了最适合你的钱包。接下来，让&#039；让我们来看看这些钱包如何以不同的方式存储种子密码。

### 软件和移动钱包

软件钱包(桌面或移动)非常方便。很多门罗用户在手机上安装热钱包，用于日常支付。最佳做法是随身携带等同于日常现金的加密货币。因为软件钱包将种子代码存储在您的设备中。一旦你的设备中毒或安装了键盘记录器，你的门罗硬币就会被盗。

图2.2a和2.2b:Android上的手机钱包Monerujo和iOS上的蛋糕钱包

### 硬件钱包

硬件钱包是一种具有保密钱包功能的硬件设备。，与手机或电脑断开后完全隔离。硬件钱包有一个匹配的屏幕来显示你的种子代码和交易信息，没有必要将这些信息发送到外部设备。

虽然硬件钱包不如软件钱包方便。但是他们很安全！即使您怀疑或确认设备已被恶意软件感染，您仍然可以使用硬件钱包从该设备发起交易，因为您的种子密钥存储在硬件钱包中，并以非常安全的方式受到保护。现在Monroe社区正在开发他们的第一个开源硬件钱包：Kastelo。

图2.3:梦露&#039；开源硬件钱包Kastelo

### 纸质钱包

如果你没有；不要经常转移你的门罗硬币，那么纸钱包是一种成本非常低的存储方式。你只需要把你需要的信息(公开的或私人的)打印在纸上。。因为你的种子代码只存储在纸上，你不；不需要担心暴露于病毒或数据。但是纸质钱包不适合频繁的资金转账，因为你每次都要把纸上的信息输入到设备里。

图2.4：纸钱包是门罗密钥的纸质备份。确保没有其他人可以访问此信息。

## Web钱包

您可以通过第三方提供的网页登录您的Monroe钱包。这些在线钱包极其方便，但却以牺牲安全性和隐私为代价。有两种网络钱包。核心区别在于，作为用户，你知道还是不知道；我不知道你的种子代码。

第一种web钱包是把你的资金存放在自己的账户里，只给你提供一个账户名和密码登录(注：你在交易所的钱包也是一样)。实际上你不；拥有此帐户的种子代码，因此您可以；不要控制你的个人资金。你必须信任为你保管资金的机构。因为他们本质上提供的是银行服务，所以你必须非常谨慎。无论是意外还是盗窃，他们都可能随时损失你的资金。。一旦他们的网站被关闭，你的账户密码就沒用了，因为你可以；没有种子代码，你无法控制自己的资金。

第二个web钱包把种子代码和资金都掌握在自己手里。。一个设计良好的钱包，如MyMonero(mymonero)您可以安全地访问您的帐户，而无需将您的种子密码发送给第三方。因为您的种子密码没有存储在设备和服务提供商中，所以每次您登录时，您必须输入它。这种类型的网络钱包(相对而言)更安全，因为第三方不控制你的资金。它们只是为你的浏览器提供一个与你的账户交互的接口。即使这种类型的钱包网站不再可访问，您也可以在其他钱包中输入种子密码。，再次访问您的帐户。

虽然网络钱包使用起来非常方便，但以上两者都不建议作为长期存储或大额资产存储的选择。两者都在安全性上有所欠缺(需要信任第三方/需要在浏览器中频繁输入种子密码)。，并且在隐私性方面也有所牺牲。

图2.5:MyMonero交互界面

## 冷钱包

“冷钱包”是纸质钱包和其他离线存储方式的统称。例如，只有

在需要加密货币时才启动并连接到互联网的电脑或手机。 ，是电子冷钱包。该设备可以使用任何操作系统，但一定要采用高标准的安全措施(如防火墙、杀毒软件和只访问/使用你信任的网站/软件)。seed机密语言存储在计算机上，因此请尽量确保它是“孤立”尽可能。

图2.6:冷钱包是指专门用于存储和汇出加密货币的设备。上面运行MonroeCLI的电脑就是一个冷冰冰的钱包。

## 门罗钱包链接

无论你选择哪个钱包。请务必使用来源可靠的经过审查的软件，因为有无数的钓鱼软件和欺诈钱包！如果你在恶意钱包里输入了种子码，不知不觉中你的门罗币已经不见了。

以下包含社区开发或信任的一些开源钱包的下载地址。

lightwallet:Monerujo-cakewalletMonerujo—Android-MyMonero.comonios-Web,desktop,AndroidandiOS

官方软件：图形用户界面(GUI)—Windows、Mac、Linux命令行界面(CLI)—Windows、Mac、Linux

## 连接到远程节点(可选)

如果您希望缩短同步时间并减少磁盘空间的占用，那么您可以选择连接到远程节点，而不在设备上保存完整的区块链。大多数钱包，例如上面提到的轻型钱包，都被自动设置为连接到默认的远程节点。。如果您想要手动设置远程节点，可以使用社区网站node.moneroworld.com上的资源(端口/端口18089)。

节点是指那些已经下载了完整的区块链的计算机。他们还可以帮助其他用户同步钱包和中继交易。运行本地全节点不仅是保护隐私的首选，还可以通过共享全节点帮助他人维护网络安全。如果你不#039；不想下载整个节点，或者想快速使用Monroewallet。然后你可以选择一个方便的远程节点连接方式。

运行节点不等同于挖掘。挖掘过程是资源密集型的，我们将在第4章讨论这个主题。只要区块链同步完成，运行本地节点不会占用太多CPU或网络资源。