如果您对使用比特币、以太坊、莱特币或目前市场上超过 1,500 种硬币和代币中的任何其他虚拟硬币感兴趣，您将需要一个钱包。如果您是加密货币新手，本指南是您了解什么是加密货币钱包、它们如何工作以及最适合您的捷径。

什么是加密钱包以及它与普通钱包有何不同

加密货币钱包或只是一个钱包是一种软件程序，可让您访问您拥有的所有加密货币，并允许您管理您的资产、存储、接收和发送硬币。

一些钱包被设计为只存放一种类型的硬币，而另一些钱包则支持多种硬币，如果您不想将自己限制在单一资产中，这将非常方便。一些钱包还有其他功能，例如检查您选择的法定货币的实时汇率。

加密货币钱包与标准的“袖珍”钱包根本不同，因为那里根本没有硬币。实际上，数字硬币根本不存储在任何地方，因为它们实际上并不存在。相反，我们将交易记录存储在区块链，并且加密货币钱包可以与这些区块链进行交互和分析，以让您对您的资产进行操作。它看起来更像是一个带有数字密钥的网上银行。

我的钥匙在哪里？

每个加密钱包都有一个公钥和一个私钥。

公钥
是另一种加密误称，因为它不是密钥而是钱包地址。这就像其他人用来向您的钱包发送硬币的银行帐号。

私钥是您的数字签名和密码小盒的 PIN
码的组合。它用于访问钱包并管理与其相关的资金。

私钥是一串字母和数字，随机生成并以您的钱包支持的格式加密。您不必深入了解如何创建私钥的技术细节，请确保将其保存在一个秘密且安全的地方。任何获得你私钥的人都可以打开你的钱包并拿走你的钱。此外，如果您丢失或忘记了钥匙，您将失去金钱。永远。无论。没有钥匙，没有钱。记住这一点，小心你的钥匙。

从技术上讲，当有人向您发送比特币或任何其他类型的虚拟货币时，他们会将硬币的所有权分配给您的钱包地址。因此，交易归结为区块链上的记录和几个加密货币钱包中的余额变化。没有实际的硬币交换，因为这些硬币也仅以数字形式存在。

丢失的钥匙剧情

来自 Newport 的 IT 工作者 James Howells 被称为一个丢弃 7,500 个比特币的人。那家伙事故盟友用他的私钥扔掉了一个旧硬盘。

现在，获得价值超过 5000 万美元的硬币的途径被掩埋在数千吨的垃圾填埋场在纽波特 Pillgwenlly 的一个废物回收中心。

什么是热的，什么不是

加密货币钱包可以是热的也可以是冷的，这取决于它们是否连接到互联网。

热钱包始终在线，这使得它们的安全性降低，但更加灵活、快速和用户友好。只要您有连接到互联网的设备，它们就可以让您即时访问您的数字资产，无论您身在何处。但是这种舒适是有代价的：它们本质上是不安全的，并且由于不断的互联网访问而容易被盗。有时您甚至无法控制钱包的安全性，因为这取决于您的钱包服务提供商的做法。热钱包就像一个皮包：它非常适合用来支付小额现金来支付您的日常开支，但您不会把所有的积蓄都放在那里。这是一个理想的解决方案，可以随时保留您想要的少量加密货币。

冷钱包是具有强大安全性和改进的防盗保护的已禁用物理设备。当您需要进行交易时，您可以将它们插入计算机，然后回到线下世界的安全。它们几乎是防黑客的，您只需要确保它没有被盗、被破坏或破坏。冷钱包是您长期持有的保险库或保险箱的加密货币替代品。它们最适合用于存储您不打算在最近的将来花费的大量加密货币。

加密货币钱包的类型

有五种广泛类型的加密货币钱包。每个都有其优点和缺点，并提供不同级别的安全性。在这里，它们是桌面、移动、在线、硬件和纸质钱包。

任何钱包都只是存储公共地址和私钥组合的一种方式，但许多公司开发了多种软件解决方案来改善用户体验并提供服务于特定目的的附加功能。

1) 桌面钱包

桌面钱包是您下载并安装在计算机或笔记本电脑上的软件程序。它们易于安装并且可用于所有操作系统，尽管其中一些只能在特定操作系统上使用。大多数桌面钱包在安装时都会为您提供助记词。这是一长串单词，用于存储钱包恢复所需的信息。如果重新安装，您将需要它来访问您的钱包。因此，将助记词保存在安全的地方，

远离窥探是至关重要的。

好处：
桌面钱包提供了高级别的安全性，因为它们只能从安装它们的计算机上访问。您的钱包安全是您的责任。您不必依赖其他人来保护您的钱包免受外部威胁。此外，桌面钱包通常具有丰富的功能并提供额外的工具和功能。大多数加密货币都有为其硬币创建的桌面钱包。

缺点：由于您的计算机或笔记本电脑已连接到 Internet，您的您的数字资产可能会成为病毒和恶意软件的受害者。如果您的计算机被黑客入侵或感染病毒，您可能会丢失虚拟货币。因此，如果您想确保您的硬币安全无虞，则必须使用防病毒、反恶意软件和良好的防火墙。

桌面钱包示例

出埃及记是方便使用的桌面钱包简单的界面; 非常适合那些刚刚开始加密之旅的人。出埃及记允许保持比特币和一些山寨币，包括以太坊、莱特币和达世币。它适用于 Mac、Windows 和 Linux。

共付额是一种多重签名由最大的比特币支付服务提供商 BitPay 创建的比特币钱包。多重签名功能提供额外的安全层，因为这意味着比特币地址可以由 2 个或更多人共同控制。这是可用的Windows、Mac 和 Linux。

2) 手机钱包

移动钱包在智能手机或平板电脑上作为应用程序运行，与桌面钱包非常相似，具有二维码扫描仪等附加功能。它们是最常用的钱包类型，这不足为奇，因为现在人们喜欢在旅途中做事，能够检查他们的加密货币余额，随时随地发送和接收硬币。所有主要的加密货币都有适用于 iOS 和 Android 设备的移动钱包，但不太流行的可能只有 Android 版本。

好处：
手机钱包非常实用。您可以在零售店轻松使用它来支付或发送硬币。它们更小、更快，可以随时使用。

缺点：
由于移动设备的空间和容量有限，移动钱包只有基本功能。更重要的是，绝大多数加密钱包都容易受到网络威胁、病毒和恶意软件的攻击，因为它们始终连接到互联网并且具有较弱的加密安全功能。您还必须格外小心地保护您的设备，因为任何可

以访问带有加密钱包的手机或平板电脑的人都可以拿走您的钱。

移动钱包示例

Coinomi
是一款移动加密货币钱包，支持多种货币，包括比特币、以太坊、以太坊经典、莱特币和达世币。它适用于 iOS 和 Android 设备。

Jaxx是一款适用于 iOS 和 Android
设备的多加密货币钱包，支持数十种加密货币和 ERC20
代币，包括比特币、以太坊、以太坊经典、莱特币、ZCash 等。与 ShapeShift
服务的集成允许交换钱包里的硬币。

3) 在线钱包

在线加密货币钱包存在于云中，可以通过网络浏览器从任何支持互联网的计算机或移动设备访问。它们结合了桌面钱包的功能和移动钱包的可访问性，这使得它们非常有吸引力。

好处：
在线钱包提供更快的交易，因为无需等待应用程序连接到服务器。它们中的许多都与加密货币交易所
集成在一起，或者允许在支持的硬币之间转移金额。如果您将它们视为少量的数字存钱罐，它们会非常方便。

缺点：
安全级别低是他们的弱点。您的私钥存储在云中的某个位置，并由其他人控制，而不是您。这使它们成为黑客和其他加密反派的理想目标。您应该始终牢记，在线交易所和在线钱包比任何其他类型的钱包更容易被黑客入侵。因此，基本建议是不要将所有数字货币都放入在线钱包。

在线钱包示例

MyEtherWallet
只是一个在线解决方案，它允许储藏以太坊和基于以太坊的代币。它不支持比特币和比特币现金，或其他相关货币。MyEtherWallet
不在其服务器上存储私钥，这意味着更高的安全性和对您的硬币的更多控制。

MetaMask

是流行浏览器的扩展，允许您存储、发送和接收基于以太坊协议的数字硬币。它是ERC20 代币的三大在线钱包之一。MetaMask
是用户友好的简单的和清晰的界面。

4) 硬件钱包

硬件钱包与上面讨论的所有其他类型的钱包根本不同。他们将您的私钥存储在单独的离线设备上，例如 USB。如果您需要汇款，只需将设备插入具有 Internet
连接的计算机，进行交易并断开钱包。有些型号有 LED 屏幕，这意味着您可以在没有电脑的情况下获得一个。流行的硬件钱包允许您存储超过 22
种加密货币和数百个 ERC-20 代币。它们是保存大量加密货币的最佳选择，您将这些加密货币作为长期投资保留，并且不打算经常移动。

好处：
硬件钱包专注于安全性。它们提供针对网络威胁的最高级别保护，因为它们只进行在线交易，但密钥离线存储。只要确保不会丢失设备本身，您就不会损失金钱。

缺点：
硬件钱包对用户不太友好它们通常与多个网络界面兼容，但与软件钱包相比，它们的功能相形见绌。硬件设备的价格约为 70 至 150
美元，而且通常会在瞬间售罄，因此如果您可能发现自己很难买到一台。

硬件钱包示例

Leger
是最受欢迎的硬件加密货币钱包之一。它支持比特币、莱特币、以太坊、Zcash、ERC20 代币、Ripple 和 Dash 等。Ledger
被认为是最通用的加密货币硬件钱包。费用：95美元。

Trezor
是另一种流行的硬件解决方案，可确保您的硬币安全无虞。它支持比特币、莱特币、以太坊、Zcash、狗狗币、达世币、ERC20 代币等。费用：99 美元

KeepKey
它是最简单的加密货币硬件钱包。它保护比特币、比特币现金、比特币黄金、以太坊、莱特币、狗狗币、达世币和多个 ERC20 代币。费用：129 美元

5) 纸钱包

纸钱包是硬件钱包的早期原型。您通过专用服务创建它，在一张纸上打印您的私钥和公共地址 - 可以是一串字母和数字，也可以是二维码 - 然后开始将硬币从您的软件钱包转移到这个钱包。如果您需要花费一些硬币，您需要将资金从您的纸质钱包转移到您的软件钱包。这个过程通常称为“清扫”。

好处：
它既便宜又安全。看起来很奇怪，它们被认为是最防黑客的钱包类型之一，因为它们不存储在计算机或任何其他连接互联网的设备上。

缺点：
纸钱包不适合新手。您需要一些技术知识、耐心和高度的谨慎来创建和使用它之后.纸不是很耐用的材料，所以你必须格外小心，让你的钱包远离火、水和碎纸机。

纸钱包的例子

ethaddressWallet
是一款免费软件，允许生成纸质钱包并存储具有离线存储安全优势的以太坊。

WalletGenerator 是一种用于生成防黑客比特币纸钱包的在线服务。

加密货币钱包安全量表

总而言之，以下是从非常
安全到非常不安全的钱包类型：硬件钱包、纸钱包、桌面钱包、移动钱包 和
在线钱包

如何保护你的钱包

虽然某些钱包本质上比其他钱包更安全，但用户在使用钱包时应始终采取预防措施并小心。自满和疏忽可能会让您付出高昂的代价。

多样化。
将少量的日常开支存放在热钱包、在线或移动设备中，并将您持有的大部分加密货币存放在一个安全的地方，尽可能远离互联网。硬件或纸质钱包将保护您的资金免受黑客、恶意软件和病毒的侵害，并允许您在计算机或移动设备死机时恢复数据。

保留备份。
备份您的钱包是一个很好的做法，如果您的计算机出现问题，这将帮助您重新获得访问权限。最好在离线设备上完成，例如 USB 驱动器，因为在线存储可能会被黑

客入侵或破坏。还要保留您的助记词、密码、用户名和其他访问数据的硬拷贝，以防万一。

跟上更新。
确保您的钱包软件是最新的，因为开发人员经常发布安全增强功能以保护您的钱包免受新威胁。

使用最佳安全实践。
您的资金安全完全由您负责，因此请尝试为您的加密钱包添加额外的安全层。在您安装了钱包软件的所有设备上使用强密码开始。选择具有强大安全策略的钱包服务提供商，例如每次打开钱包应用程序时都需要双重身份验证和密码请求。

警告！伪装的恶意软件！

有些钱包并不是那么无辜，因为它们的唯一目的是窃取你的钱。他们有时会模仿流行的钱包来误导用户。请按照以下简单步骤保护自己免受诈骗者的侵害：

- 除非您 100% 确定它是有效的软件，否则不要使用未知钱包。做你的研究，检查评论并尝试找到使用这个钱包的人。

- 由于 App Store 和 Google Play 都存在假钱包问题，请从钱包官网获取下载链接。
- 下载前检查Bitcoiorg上的钱包。
- 总是更喜欢非第三方钱包，让你完全控制你的私钥。

移动和桌面钱包的安全清单。确保您已清除列表中的所有项目。

- 仅使用信誉良好的可信钱包；
- 远离鲜为人知的无名公司，仅从受信任的来源安装软件；
- 使用强密码和用户名；
- 获得安全的防火墙；
- 安装并保持更新的防病毒和反恶意软件；
- 始终仔细检查您汇款的地址；
- 始终检查在线钱包的网址；
- 永远不要从公共 Wi-Fi 访问钱包

快速总结关键要点。关于加密货币钱包你应该知道的事

- 加密钱包是一种软件程序，用于安全访问和管理加密资产。您的钱包存储

一对密钥：与全世界共享您的公钥，人们将使用它向您发送硬币，但保密您的私钥，因为它可以解锁您的资金。

- 加密货币钱包可冷可热。取决于他们是否连接到互联网。使用热钱包存储数字零用现金，因为它们速度快但不安全；使用冷钱包来存储您不打算在最近的将来花费的大量加密货币。
- 有五种主要类型的加密货币钱包：桌面、移动、在线、硬件和纸质钱包，各有优缺点。选择适合您需求的那一款。
- 您对您的数字资产的安全负责，因此请确保您已采取措施保护您的钱包免受恶意软件和未经授权的访问。请记住，自满和疏忽可能会让您付出代价。