硬件钱包是一种物理保险库，目的是为用户的加密货币私钥提供安全存储，这些专门设计的硬盘通常通过USB连接到您的计算机或智能手机。因为它们保持脱机状态，所以它们可以为货币令牌提供冷储藏。目前市场上已经有的传统硬件钱包有USB连接类型、蓝牙连接类型、NFC连接，这些都需要一定的技术基础和复杂的安装流程才能正确使用。

硬件钱包，如GoldLar(库神)、Cobo、Ledger等已成为区块链服务中的重要产品，这几款也是相对比较好用的，由于比特币每天都在吸引着越来越多的买家，因此人们存储加密货币资产的方式变得越来越多样化。一些人满足于将加密货币放在软件或桌面钱包中，而另一些人则喜欢更安全的替代品。如果你打算长期投资，寻找安全的数字货币钱包是非常有必要的。对于长期持有加密货币的投资者，建议您使用纸质钱包或硬件钱包。

硬件钱包是一种物理电子设备，其唯一目的是存储加密货币。硬件钱包比软件钱包具有更好的安全性，将私人密钥与互联网连接设备分开。你的资产不会受诈骗和黑客攻击等威胁的影响，即使你的硬件钱包被盗或有人黑了你的电脑，你总是可以将加密货币恢复到一个新的钱包中。这是因为没有人可以在不知道你的密码的情况下转移比特币或altcoins。到目前为止，还没有人报告硬件钱包被盗或丢失。我们将列出市场上一些最好的硬件钱包。

当你想买一个硬件钱包时，你必须考虑以下几个特点:

安全特性——钱包最重要的方面是它的安全实现。

易用性——您应该能够轻松地导航设备及其功能。

支持的货币——验证钱包是否支持所有您感兴趣的加密货币存储。

操作系统兼容性——检查设备是否与您的计算机或智能手机上的操作系统兼容。

备份和恢复功能——钱包应该有一个备份功能，以防你的设备被盗、丢失或损坏。

价格——把钱包放在你能承受的范围内。

顾客意见——在网上搜索真实用户对产品的评价，如果他们不满意，继续搜索。

库神钱包简介：

库神是一家提供区块链数字资产安全存储方案的专业公司。库神冷钱包可以存储多种数字资产(比特币，莱特币，以太坊等)，冷钱包采用二维码及 NFC 的通信方式让私钥永不触网，彻底根绝了私钥被黑客窃取的风险。库神钱包由两部分组成：硬件冷钱包及库神
App(联网端)。硬件冷钱包主要负责构造交易并对交易进行数字签名，库神 App 负责查询地址余额及广播发送交易。库神 App
涉及的都是公开透明的信息，无安全风险。

库神冷钱包专业版(P3)可以存储比特币、以太坊、EOS
等多种区块链资产。钱包由两部分组成：硬件冷钱包(冷端)和库神 App(热端)。冷端管理私钥，主要负责生成私钥、构建交易及数字签名;热端链接区块链网络，主要负责查询余额、广播交易及监控资产动态。冷热端通过二维码或 NFC
传递信息，确保私钥永不触网，彻底根绝私钥被网络黑客窃取的风险。

Cobo钱包简介：

「Cobo金库」软硬结合，包含了软件钱包+硬件钱包，Cobo钱包是一款手机APP，除了为大家提供存取和转账功能，同时还辅以各种“增值服务”，比如币币兑换、数字货币理财、各种Dapp等等，而「Cobo金库」是一个实体设备，它存在的目的有且只有一个：让用户安全地保管自己的私钥，也就是数字资产。Cobo 金库除软件防护机制外，还支持IP68防水，IK10抗震，达到了美军军标级三防标准(MIL-STD-810G)，并设计有可分离式电池，防止长期存放过程中电池异常损坏主机。

Cobo钱包通过采用HSM加密机和多重签名冷钱包来实现高性能的安全存储。HSM加密机多应用于商业银行，比如信用卡系统、银证转账系统、网上证券交易等，Cobo钱包全部使用加密机确保密钥安全;同时多重签名冷钱包可以做到当用户资产托管到Cobo钱包后，资产将导入多个冷端钱包，在物理上直接隔离各种突发网络风险，保障用户资产安全。

Ledger Nano S钱包简介：

Ledger 是法国硬件加密货币钱包制造商，在冷钱包领域技术实力较领先，是最受欢迎的冷钱包之一。Ledger Nano S是其主打产品，一款支持多种数字货币的硬件钱包，可以理解为日常使用的银行“U盾”，都是为了保护你的资产。但二者工作原理不一样，Ledger Nano
S基于强大的安全功能来储存你的数字资产以及保护资产交易。

Ledger钱包接入EtherFlyer后，基于以飞去中心化交易的特性，您可以直接交易资产，无需导入私钥。买卖完成后，资产进入冷钱包，可直接将其取走，EtherFlyer

“去中心化交易”和冷钱包“资产隔离”将为您的交易上一个双保险。

Ledger Nano S支持多种数字货币的同时存储，包括比特币、比特币现金、比特币黄金、以太坊、以太经典、达世币、狗狗币等以及上百种以太坊代币(ERC20)，包括但不限于1ST，EOS，QTUM，BTM等。并且还在不断更新增加中。

CoolWallet S钱包简介：

CoolWallet S是一款由CoolBitX在2018年推出的，外观和信用卡类似的加密货币硬件钱包。CoolBitX是一家台湾金融科技公司，专业制造数字资产硬件，投资机构有SBI Holdings，Midana Capital，OwlTing，Kyber Capital和Bitmain等。CoolBitX于2015年开展了Indiegogo活动，其中包括CoolWallet，第一代信用卡形状的硬件钱包。有了第一代钱包的技术积累，当前第二代产品CoolWallet S的稳定性和安全性应有所提升。虽然在硬件钱包领域，Trezor和Ledger技术积淀更多、名声更大，但是在易用和便携上不够完美。而CoolWallet
S像信用卡一般轻薄和柔韧，搭配蓝牙连接，易用性更佳。

Trezor钱包简介：

TREZOR钱包它具有高安全性，同时又不会以牺牲方便性为代价。Trezor可以通过USB连接电脑并签署比特币交易，不需要允许计算机访问私人信息。与冷储存(cold storage)不同，TREZOR在连接到一个在线设备时是可以实现交易的。这意味着即便是在使用不安全的电脑的时候，使用比特币都是十分安全的。Trezor的优点：

快速设置：用户可以在几分钟内完成个性化的设置，无需注册，即可让Trezor准备就绪。

轻松使用：使用Trezor很容易。只需按照显示屏上的说明进行操作，然后单击按钮确认重要操作。

恢复备份：如果你的Trezor丢失了怎么办?不用担心，你可以使用你的密语来快速重新获得所有的钥匙、比特币资金、历史记录、账户和电子邮件。

保护多种数字资产：现在，Trezor不仅仅是能够保护你的比特币，其他的数字货币也在保护范围内。例如ETH、莱特币、达世币和Zcash。

KeepKey钱包简介：

KeepKey是一个硬件钱包，保护你的比特币，以太坊等数字资产，免受黑客和小偷

的侵害。您的私钥被安全的存储在KeepKey上，永远不会离开设备，您的KeepKey是PIN码保护的，即使落入不法分子受众，也无法使用。

KeepKey的屏幕显示了每笔离开设备的数字资产，每笔交易必须使用KeepKey的确认按钮进行手动批准。

如果您的KeepKey丢失或被盗，您可以安全的恢复您的设备，而不会影响到私钥。
其他特点

支持比特币，以太坊，莱特币，狗币等数字资产。

使用shapeshift在设备上直接交换数字资产。

有效防止病毒和恶意软件。

Casa钱包简介：

为富人提供加密货币钱包服务的初创公司 Casa 推出的数字钱包，帮助用户安全地存储加密货币，要求用户通过电子方式签署三种不同的设备移动数字资产。其服务包含一些额外的步骤，旨在阻止包括物理威胁在内的攻击。将与 Coinbase 托管的同类产品竞争。

比特币团队中最知名的人物之一、BitGo 工程师 Jameson Lopp，他与 Bitgo 首席执行官 Mike Belshe 因为 Segwit 2x 分叉的意见不一致，而加入了 Casa 团队。

imKey钱包简介：

由 孵化，安全、好用的硬件钱包，支持 imToken，也兼容 Metamask、Scatter 等。

私钥离线存储，永不联网。CC EAL 6+ 安全芯片，助记词备份随时恢复钱包。物理按键控制确认，交易多重安全验证。支持 imToken，管理丰富的代币和 DApp。2.3mm 超轻薄，蓝牙无线设计，让使用再无限制。无需更换硬件，即可享受定期的软件更新服务。

币派钱包简介：

BEPAL 是一家专注于区块链资产安全的公司，核心成员来自阿里、腾讯、酷派等国

内顶级科技企 业，目前全职员工超过 50 人。

BEPAL 以区块链资产安全管理为核心业务，拥有行业领先的芯片级安全硬件研发生产能力及区块链资产安全管理技术。

针对各类数字资产管理场景，BEPAL 研发了 BEPAL Pro、BEPAL Q 等多款硬件钱包，并推出 BEPAL Card、BEPAL Wallet、BEPAL Enterprise、BEPAL TangkaPro、BEPAL 星球等产品，形成了专业的区块链资产安全管理产品矩阵。

碧盾钱包简介：

碧盾 BTXON 是简单的加密数字硬件钱包，将密钥放入了安全芯片，如果带电破解会触发芯片数据自毁。同时，该芯片能够抵御一定的电子探测攻击。针对国内用户，操作界面简洁，由于没有设计按键，在输入密码方面降低了操作的繁琐性;没有电池以及按键的设置，延长了产品使用寿命。碧盾 BTXON 内建封闭完全的智能卡安全操作系统 BtxOS，为秘钥存储和数据签名提供可信执行环境。硬件防破拆攻击，防止黑客采用电子探测攻击，电磁辐射攻击和物理攻击手段探测用户账户信息。

我们判断一款硬件钱包是否安全的最重要的一点便是看它是否使用了加密芯片，硬件钱包最怕的便是丢失落入黑客之手，虽然硬件钱包对于私钥都有一定程度的保护，但是这也不能代表私钥就绝对不会泄露的,所以在使用时一定要注意安全！