

怎样使用数字货币钱包更安全？数字货币钱包安全解读，说起炒币来，这可不是一件简单的事，不是跟风倒买倒卖就赚钱的。除了要懂经济、跟政策、了解国际形势，做好必要的投资分析以外，还要给自己选择一款适合自己的数字货币钱包，必要时做好USDT避险准备。很多人说，数字货币钱包就是用了装数字货币的，通俗来说这样理解没有问题，但实际上，数字货币钱包装的并不是数字货币，而是装密钥(私钥和公钥)的工具，有了密钥就可以拥有相应地址上的数字货币的支配权，利用钱包中生成的数字货币收款地址，可以接受他人给你转账的数字货币，也可以把你所拥有的数字货币转账给其他人，所以钱包的安全至关重要。

数字货币钱包分为4种，分别是硬件钱包、在线客户端钱包、app钱包(IOS/安卓)、PC电脑版钱包，要想让数字货币钱包更安全，要不使用无背钱包;不使用邮件传输或存储私钥;不使用微信集合或云备份来存储私钥;不要截取截图或照片来保存私钥;不要使用微信和QQ传输私钥;不要告诉身边人私钥;不要将私钥发送给该组;要使用第三方提供的未知来源钱包应用程序;不要使用他人提供的App ID;不要将私钥导入未知的第三方网站。

这里有一些安全存储和管理数字资产的具体方法：

1.从官方渠道下载数字钱包应用程序

如Google Store , Apple Store。如果系统是Dapp属性会更好。毕竟区块链是权力下放的产物。

2.做好私钥备份

应记录帐户，登录密码，支付密码和助记符，好记性不如烂笔头，记录在纸上，别放在电脑或者手机的备忘录，那也是不安全的。

3.及时更新版本，注意最新信息

从上面的一些数字钱包被盗的例子我们可以发现，其实区块链数字钱包并不安全，只要通过网上传输的信息，就没有百分百的安全可言。区块链钱包还需要不断的发展，让用户的隐私安全有保障。让数字钱包成为区块链行业的有利障碍和护城河，并使数字钱包能够让我们真正体验区块链钱包技术带来的生命价值。

提醒：每年都有大量的交易所被黑客攻击，导致数字资产大量丢失。由于加密数字货币的不可追溯、不可挂失、匿名的特性，一旦数字资产丢失，就再也不可能找回

。另外账户名和密码的安全隐患，大多数用户习惯性的使用同一个账户名和密码在不同的网站里面进行注册，如果这其中有任何一个网站被黑客攻击成功，那么这个网站的全部用户名和密码都可能被用于对交易所账户系统的登录攻击，谁都不想自己攒下来的数字货币被轻易的盗走或者是骗取，因此一个安全性高的数字货币钱包是币圈炒币玩家至关重要的利器。