

在数字货币世界中，安全性是至关重要的。由于加密资产是数字的，保护资产的方法也必须是数字的。就像物理钱包是为存储纸币一样，数字钱包的设计也是为了存储数字货币。与物理钱包不同是物理钱包可以容纳任何纸质货币，数字货币钱包就不能存储所有的数字货币。每个加密钱包都有自己独特的兼容数字货币范围。这意味着，如果数字货币被发送到错误的钱包，发送的金额将永远丢失。



冷钱包特点

- 1.冷钱包的币采取分散存储方式，每个地址存确定数量的比特币。
2. 所有私钥在完全离线电脑上存储。

3. 确保私钥永远没有接触过网络或U盘。
4. 私钥加密文档需在异地有备份，并且由在异地的不同人控制。
5. 私钥的AES密码也须由异地的两个不同人控制，且不得与掌握私钥的人相同。
6. 掌握私钥密文文档或私钥密码的两组人必须在分别在异地，最好是异国。
7. 某个私钥一旦汇币到线上以后，即作废，永不再使用

冷钱包的发展史

冷钱包第一种：因为区块链的爆炸式发展，人们发现我们的电脑和手机里存储的数字资产及重要数据已经远远不能满足我们的要求了。于是就找来了普通的U盘，硬盘，甚至用带了密码保护功能的硬盘来单独存储，这样的好处是，终于可以单独存放了。但又面临新的问题，就是普通的优盘、硬盘很容易损坏，比如不小心摔一下或者进水甚至本身莫名其妙的损坏等，而且因为没有密码保护不安全，（即便是设置了密码也很可能因为时间过长而忘记密码）于是就有了第二种钱包.....

冷钱包第二种：第二代冷钱包主要是在保存数字资产的方式上做了很多调整，主要有如下两种：一，通过加密的方法把数据放在远程网络上。这种方法的优点是数据在远程网络上保存，需要使用的时候输入特定的密码或者助记符来提取数字资产，具有提取和使用方便等优点。但这样同样面临一个巨大的问题，就是本质上我的数字资产依然放在了别人家，因为时时在网络上，万一被黑客盗取了或者存储你个人数字资产的公司带着你的数字资产跑路了你怎么办？二，通过加密的方法把数字资产放在客户本身的离线客户端，这种方法类似第一代的存储方式，现在有一些公司为了追求高大上的外观使用了触摸屏以及安卓系统等改装机，这样虽然看似炫酷，但却大大增加了设备本身的故障率！即便不考虑设备本身故障率的情况下，万一不小心摔一下或者不小心进水等意外情况发生，便让设备的安全性大打折扣。

第三种冷钱包：因为上面的种种不完善，于是出现第三种解决方案。先来看一下我们的数字资产的大概数据结构，无论它千变万化，最终都会变成标识地址的ID字串+所对应的权益字串+相关的辅助信息。通俗的讲就是钱包地址和钱包里有多少钱，外加一些注释信息。在来看看，第一种方案主要缺点在哪里？

- 1，普通的移动硬盘优盘怕摔，怕水

2，普通的移动硬盘或者优盘万一损坏数据很可能就没有了。

3，普通的移动硬盘或者优盘没有密码保护功能，即便是有，也可能因为时间过长而忘记密码。微嘟科技的一款加密存储阵列解决了上面的问题，比如它不需要记忆密码，使用的时候只需要用加密手环或者加密标签贴(可贴手机上随身带着)轻扫主机的表面就可以了。另外内置了多颗在物理上完全独立隔离的存储颗粒，这样的作用是，即便内部部分颗粒因为意外原因损坏了，还有另外一个存储数据。最后，每台设备还经过科学的防摔防水处理。

小编个人倾向于第三种方案来存储个人数字资产和隐私，因为这种方案最主要的特点是自己的钱放在自己这里了，而且还不需要记忆密码，用的时候甚至用手机轻轻一扫就可以了。又不用担心联网被盗，而且还防水防摔。