不管你是币圈新手还是币圈的达人，我们在进行数字货币的买卖时，除了数字货币交易所之外，我们还会频繁接触到的一个工具就是数字资产钱包了，其实这个钱包就是用来存放数字资产的。对于一部分的投资新手来说，他们的买入量并不是很大，所以他们习惯以将自己的币直接放在交易所中，投资的稍微多一些的投资者都会选择创建一个独立的钱包来存放自己的资产，毕竟资产的安全是非常重要的。很投资者担心数字资产钱包靠谱吗？那么究竟数字资产钱包安全吗？下面就让小编说一说。

数字资产钱包靠谱吗？数字资产钱包靠谱。数字钱包是存储和管理、使用数字货币的工具，在区块链领域有举足轻重的地位。它是一个存储加密货币的软件程序或者硬件设备，从形式上，类似于网络银行的账户，也有客户标识、账号、密码。数字钱包的密码就是“私人秘钥”，只有通过它，才能打开和操作钱包。数字钱包具备“收款“和“转账”功能，就像用银行卡存取钱一样，要有卡号和密码，才能正常进行存款和安全支取。数字钱包存的可不是钱，而是你的比特币、以太币等数字货币或数字资产的信息。数字资产钱包安全吗？数字资产钱包安全，但是也面临着许多的风险，安全可靠的数字钱包应该至少从5个维度来进行设计：1、运行环境的安全风险加密数字货币钱包最核心的文件—私钥/助记词是存储在终端设备上的，无论是PC端还是移动端，终端设备如果出现不安全的现象，对于私钥/助记词来说是有非常高的安全风险的。一个安全的数字钱包，在设计之初就避免因为运行环境而导致的私钥/助记词存在被盗可能。终端上运行环境的安全问题主要包括病毒软件、操作系统漏洞和硬件漏洞。2、网络传输的安全风险网络传输的安全性更多地体现在是否有良好的对抗中间人攻击的能力上。中间人攻击是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。虽然大部分数字钱包应用都会使用HTTPS协议和服务端进行通讯，但是中间人攻击方法上是可以通过在用户终端中安装一个数字证书的方式拿到HTTPS协议里面的内容。安全的数字钱包需要能够对终端里面全部的数字证书的合法性进行扫描、对网络传输过程中的代理设置进行检查并能够保障基础的网络通讯环境的安全性。在数字钱包的开发中，在网络传输层面是否使用双向校验的方式进行通讯验证也是衡量一个数字钱包应用安全性的重要评判标准。3、文件存储方式的安全风险对于数字钱包的私钥/助记词，终端设备的存储方式也是需要在安全性设计上加以注意的。私钥/助记词文件存放目录的访问权限、私钥/助记词存储的形式和加密算法设计都需要通过严密设计。在对多款主流数字钱包进行安全性分析时，我们发现即使是知名的数字钱包，在私钥/助记词的存储上也是比较随意的。既有明文存储的，也有虽然是加密存储但是解密的密钥却是在代码里面固定写死的，起不到任何的安全防御作用。4、应用自身的安全风险应用自身的安全风险主要集中在应用安装包自身的安全防御上。应用安装包是否具备抗篡改能力是非常核心的技术能力。另外，应用运行过程中的内存安全、反调试能力、私钥/助记词使用的生命周期管理、调试日志的安全性、开发流程的安全等方面也是需要去设计增强的。5、数据备份的安全风险如果移动应用

能够被备份出来，就可以使用计算性能更加强大的机器对私钥/助记词进行暴力破解。举例来说，如果android：allowBackup属性设置为允许备份，那么就可以利用系统的备份机制对应用的数据文件进行备份，而加密数字货币的私钥/助记词也就被备份到外部介质了，这就从另外一个方向打破了操作系统的安全边界设计。以上的所有内容就是小编对于数字资产钱包靠谱吗以及数字资产钱包安全吗这两个问题的具体阐述。为了更好的保障数字钱包的安全，大家在使用数字钱包的过程中一定要保护好区块链的私钥，千万不要把自己的私钥弄丢了，也不要轻易将自己的私钥告诉别人，要知道私钥可是代表着钱包的所有权。私钥与银行卡的密码是不同的，银行卡的密码忘记了还可以先冻结凭身份证去重置，但是在区块链的世界里，我们如果弄丢了私钥，那钱包就永远不属于我们了，这个钱包是去中心化的，所以是没有中心机构可以追溯的。