今天给各位分享什么是以太坊私钥储存(Keystore)文件的知识，其中也会对进行解释，如果能碰巧解决你现在面临的问题，别忘了关注本站，如果有不同的见解与看法，请积极在评论区留言，现在开始进入正题！

私钥=银行卡+银行卡密码。

私钥是一个长度为64位的字符串，一个钱包只能拥有一个私钥并且不能修改。为什么说私钥=银行卡+银行卡密码呢？因为在imToken中直接导入私钥可以生成新的密码，将所有的区块链资产全部转移走。私钥作为最高保密级别，应该妥善保管在物理设备上，例如抄在纸上，备份多份并且存放在安全的地方，万万不可将私钥在联网设备上进行传输，避免被黑客截取。

助记词=私钥。

助记词又是什么东西呢？助记词既然等于私钥，那么其应该是私钥的另外一种表现形式，并且具有私钥同等的功能。在imToken中创建钱包，会出来一个助记词，助记词的个数一般为12、15、18、21个单词构成。这些词都取自一个固定词库，其生成顺序也是按照一定的算法得到，且助记词不能修改。助记词的主要作用是帮助用户记忆繁琐的私钥。同样助记词也要妥善保管好，切勿在联网设备中传输，任何人得到了你的助记词都可以轻松的转移你的区块链资产。

keystore+密码=私钥。

keyStore文件是以太坊钱包存储私钥的一种文件格式（JSON格式）。它使用用户自定义密码对私钥进行加密，在一定程度上keystore=加密后的私钥，拿到keystore和密码后照样可以转移走所有的区块链资产。keystore密码是唯一不可修改的，那么钱包密码修改之后，keystore也会相应修改。一定要记住加密keystore的密码，一旦忘记密码，就相当于遗失了该钱包所有的区块链资产。

————————————————————

原文链接：

#看得懂的#区块链知识请跟踪加入牧笛（mudi977612）的私人群

———我们一起知识兑现。

备份钱包，就是备份私钥，但是私钥经常有三种形态:

1. 私钥

2. Keystore

3. 助记词

私钥就是一份随机生成的 256
位二进制数字，你甚至可以用硬币、铅笔和纸来随机生成你的私钥：掷硬币 256
次，用纸和笔记录正反面并转换为 0 和 1，随机得到的 256
位二进制数字可作为私钥。这 256 位二进制数字，就是私钥原始的状态。

在钱包中，私钥与公钥将会以加密的方式保存为一份文件叫 keystore,中文可以叫签名证书,由于是私钥公钥放在一起,相当于钥匙和锁放在一起保存在一个保险箱,必然是需要另外一把钥匙也就是密码上锁的。 所以生成keystore的时候的密码非常重要,忘记了密码意味着这个证书打不开无法使用. 所以备份 keystore
同时需要备份对应的密码。密码忘记了是无法恢复钱包的.

将秘钥(256个0和1)和12~24个词语之间建立映射关系,助记词就成了秘钥的可读懂的形式,钱包很容易将助记词的顺序和内容反向成原始秘,钥,所以当你记住 12 ~ 24
个助记码后，就相当于记住私钥。助记码要比私钥更方便记忆和保管。

助记词是未加密的秘钥, keystore 是加密的私钥,并且还带密码保护.所以安全性上:

私钥=助记词 Keystore

常见的保管秘钥以下做法是不不行的:

不保存秘钥,后果是手机丢了币就丢了

将秘钥截屏,很多手机都可以自定义截屏软件,甚至系统自带截屏软件本身就自带监控.羊入虎口.

将秘钥放在桌面,硬盘,后果是完全暴露在杀毒软件和电脑病毒的控制范围里了.

将秘钥放在云盘,邮箱,在某些国家(你懂的),你这属于裸奔.

本文主要讲解通过助记词、keystore、私钥 3种方式来导入钱包。导入钱包就是说根据输入的这3者中的一个去重新生成一个新的钱包。导入钱包的过程和创建的过程其实是差不多的。

根据助记词导入钱包不需要原始密码，密码可以重新设置。根据用户输入的助记词，先验证助记词的合规性（格式、个数等）,验证正确后，配合用户输入的密码重新生成一个新的钱包。

验证助记词的合规性（格式、个数等）

助记词导入钱包

通过私钥导入钱包其实和创建钱包的过程基本一致。因为私钥在导出的时候转换成了16进制，所以在导入私钥的时候，要把16进制转换为byte数组。

keystore就是钱包文件，实际上就是钱包信息的json字符串。导入keystore是需要输入密码的，这个密码是你最后导出keystore时的密码。将keystore字符串变成walletFile实例再通过 Wallet.decrypt(password, walletFile);
解密，成功则可以导入，否则不能导入。

这是Web3j的API，程序走到这里经常OOM!

具体原因的话，我就不多说了，细节大家可以看这里

解决办法

根据源码修改 decrypt 方法，这里我用一个已经修改好的第三方库

修改后的解密方法

导入Kestore

1、导入助记词和私钥是不需要以前的密码的，而是重新输入新的密码；导入Keystore则需要以前的密码，如果密码不正确，会提示地址和私钥不匹配。

2、关于备份助记词

用过imtoken的同学可以看到imtoken是可以导出（备份）助记词的。这个一开始我也很困惑，后来了解到其实它实在创建钱包的时候，在app本地保存了助记词

，导出只是讲数据读取出来而已。还有一点，imtoken一旦备份了助记词之后，之后就没有备份那个功能了，也就是说助记词在本地存储中删除了；而且导入钱包的时候也是没有备份助记词这个功能的。

公钥、私钥、密码、助记词、Keystore是在使用数字货币钱包时，必须要弄清的概念：如果不搞清楚,很可能会造成数字资产的严重损失。

1.公钥：

相当于所属钱包的地址，可理解成银行账户。

公钥的地址可理解成银行卡号，是由公钥通过计算得来，就像银行先给你开户，后给你银行卡卡号。

钱包地址的主要用途是收款，也可以作为转账的凭证，就像别人汇款给你时你需要告诉他银行卡卡号一样。

常见的钱包地址样式:

比特币:普通地址:1开头、隔离见证地址：3开头

以太坊地址：0x开头：（包括基于以太坊平台代币）瑞波币地址：r开头。

莱特币地址：L开头。

2.私钥：

非常重要，相当于银行卡号+银行卡密码。

创建钱包后，输入密码即可导出私钥。私钥是由字母数字组成的字符串，一个钱包地址只有一个私钥且不能修改。私钥要离线保存,不要进行网络传输，可用纸张记录并保存。

主要用途，导入钱包。有了私钥就可以在同系列的任何一款钱包上，输入私钥并设置一个新的密码就可以把之前的A钱包的资产导入B钱包。比如手机丢了，只要你有私钥就可以恢复。

3.密码 ：

相当于银行卡密码。

在创建数字货币钱包时，需要设置一个密码，一般要求不少于8个字符。

主要用途：①转账时需要输入密码，可理解成你用银行卡给别人转账需要输入密码；②用Keystore导入钱包时，必须输入这个密码。

密码可以进行修改或重置。输入原密码后，就可以直接修改新的密码了；但如果原密码忘记，可以用私钥或是助记词导入钱包，同时设置新的密码。数字货币钱包中，一个钱包在不同手机上可以用不同的密码，彼此相互独立，互不影响。

4.助记词

等于私钥=银行卡号+银行卡密码

由于私钥由64位字符串组成，不便于记录，非常容易抄错，于是就出现了助记词,方便用户记忆和记录。由12个单词组成，每个单词之间有一个空格，助记词和私钥具有同样的功能：只要输入助记词并设置一个新的密码，就可以导入钱包。

一个钱包只有一套助记词且不能修改。助记词只能备份一次，备份后，在钱包中便不会再显示。因此，在备份时一定要抄写下来，防止抄写错误，尽量多次检验。

5.Keystore：

Keystore+密码=私钥=银行卡号+银行卡密码、Keystore ≠?银行卡号

Keystore相当于加密过后的私钥,在导入钱包时，只要输入Keystore 和密码，就能进入钱包了。这一点和用私钥或助记词导入钱包不一样，后两者不需要知道原密码，而是直接重置密码。

keystore进行交易转账等钱包操作,必须知道该keystore的密码。keystore的密码是无法更改的,一个keystore对应一个密码。但是可以通过该钱包的助记词,重新生成一个keystore。这个keystore可以用新的密码生成,重新生成新的keystore之后,最好将旧的keystore删除。

总结：

一个数字货币钱包创建完成后，公钥和私钥是成对出现的。公钥，私钥都是由字母，数字组成的较长的字符串。

keystore和助记词可以理解为私钥的另一种表现形式。助记词作为钱包私钥的友好格式，非常方便备份和导入。

地址可以通过私钥、助记词、keystore+密码，导入钱包找回。密码可以通过私钥、助记词，导入钱包重置密码。如果私钥、助记词、Keystore+密码，有一个信息泄漏，别人就可以拥有你钱包的控制权，钱包内的币就会被别人转移走。

私钥通过加密生成公钥，公钥转换一下格式生成地址。私钥可以推导出公钥，公钥可以推导出地址，但无法通过输出地址、公钥推导出私钥。

在生活中，银行开户是“开设银行账户—银行卡号—设置银行卡密码—开户成功

在币圈里，是先设置“密码”（私钥），再得到“银行账户”（公钥），最后给地址。对于钱包安全管理,主要注意防盗和防丢。防止私钥泄露及丢失。

注意事项：

1.关于各种骗局诱导交出私钥、助记词的行为，都要谨慎操作；

2.重视私钥、助记词、Keystore+密码的备份和保存！多重备份,多次备份,多重验证，防止抄写错误。

3.私钥不好备份的情况下，可选用备份助记词，具体根据钱包的备份要求。

4.不要进行联网备份，或通过微信、qq、邮箱等任何第三方工具进行传输发送你的私钥、助记词、keystore。不要截图。

5.备份内容放到安全、妥善的地方，并告诉家人（以防突发事故发生）

数字货币钱包的作用是安全存储资产，这是最重要的！从投资纪律来讲，本金安全是一切的基础。对于理财类的钱包，声称赚取收益高回报等，应该叫“数字资产理财”更恰当。你的资产他们可以随意动用拿去投资。你对资产没有完全的掌控权，如果投资顺利，本息安全，如果投资失败，血本无归。所以，请慎重使用这类钱包，应该注重的是资产的安全和私密性。

使用了很久的钱包，用得有点诚惶诚恐，钱包除了用于转账外，都不怎么敢动它，怕误操作搞不好就空了，所以大部分都在交易所，不敢提。这也间接印证了李笑来老师的一句话：

在申请钱包时，当然看过不少资料，老老实实地记下了私钥、助记词，备份了keystore，还放在两个U盘里备份。但对私钥、助记词和keystore是一知半解的，也不知道他们到底什么关系。如果不是要了解EOS映射，我可能一直不会动钱包，也不会去了解它们。

下面就一个个来好好学习一下这些概念。

私钥是由64位十六进制的字符组成，每个私钥是随机生成的，随机生成这样的字符串有2的256次方种可能，这个数字已经超过了宇宙中原子的个数，用“暴力破解”的方式逐一遍历可能的私钥，幻想能碰到一个有效的且有币的私钥，可以说是不可能，就算是量子计算机也没用。

一个钱包只有一个私钥且不能修改。

在导入钱包中，输入私钥并设置一个密码（不用输入原密码），就能进入钱包并拥有这个钱包的掌控权，就可以把钱包中的代币转移走。

由于私钥64位，长得太难看，没有可读性，而私钥的备份在电脑上复制起来容易，手抄下来就比较麻烦，但私钥保存在联网的电脑上不安全，有被其他人看到的风险，于是有了助记词工具。

助记词是明文私钥的另一种表现形式，最早是由BIP39提案提出，其目的是为了帮助用户记忆复杂的私钥 (64位的哈希值)。助记词一般由12、15、18、21个单词构成，这些单词都取自一个固定词库, 其生成顺序也是按照一定算法而来，所以用户没必要担心随便输入12个单词就会生成一个地址。助记词是未经加密的私钥, 没有任何安全性可言，任何人得到了你的助记词，可以不费吹灰之力的夺走你的资产。所以在用户在备份助记词之后，一定要注意三点：

助记词一般会在你创建新钱包的时候出现一次，后面就再也不会出现了，所以创建新钱包时一定要把助记词抄下来，想办法备份。最好不要用屏幕截图或保存在电脑里，因为只要泄露，获取了你的助记词就等于获取了私钥，你的钱包就成了别人的钱包。

简而言之：助记词等于私钥，绝对不能泄露。

keystore常见于以太坊钱包，是你独有的、用于签署交易的以太坊私钥的加密文件。keystore是一串Json格式的字符串，可以用任何以太坊钱包打开它。keystore必须配合你的钱包密码来使用，备份了keystore同时别忘了备份钱包的密码。

用户可以使用备份的助记词，重新导入imToken之类的钱包工具，用新的密码生成一个新的Keystore，可以用这种方法来修改钱包密码。

助记词=密钥=keystore+密码 ！保管好私钥或者助记词不被泄露，或是保存好keystore+记住密码，你才真正拥有了虚拟资产。

再来一个比较形象的比喻。

概念清楚之后，瞬间感觉轻松多了。再也不用担心因为不明白而担心操作失误的问题。最重要的是将私钥、助记词和keystore备份好，尽量离线备份多份，这样才能保证账号的安全。

1、 科普 | 什么是以太坊私钥储存（Keystore）文件？

2、 如何妥善备份你的以太坊钱包？

3、 币圈名词：地址、密码、私钥、助记词，你真的分清楚了吗

4、 「地址、密码、私钥、助记词、Keystore 」那些事

下面开始介绍myetherwallet

记住，这个钱包只支持如下几种

ETH、ETC、和符合ERC20协议的token，

其他 不支持的币不要转进来（转进来会丢失）

浏览器打开网站：

在页面右上角选择你喜欢的语言，如下图所示

第一步 创建钱包

输入密码（至少9位）

下载keystore文件（这里保存你的公钥和私钥）

保存你的私钥

初次解锁钱包（建议一定要多试下第二步，不要立马就转币进去，否则有可能你没记住密码或者keystore没放好，多试几次可以让你更加熟悉）

一般初次点击解锁之后，页面可能不刷新，直接鼠标往下滚下来就看到你的钱包信息了

第二步 查看钱包信息

当你完成了第一步，钱包就已经建好了。

这一步只是教你平时怎么打开钱包看看里面的余额之类的

你的ETH的余额和交易历史

你的所有代币token的余额和交易历史

第三步 接收和发送ETH及其他token代币

接收ETH和其他的代币token（这个钱包所支持的，点击show all tokens看所有支持的代币）

都用同一个地址即可，不需要任何额外的标记或操作

点击左上角 发送以太币/发送代币，选择keystoreFile,

上传keystore文件，填写密码，解锁账号

3.发送给别人ETH或代币的时候，你就要输入对方对应的ETH地址或代币地址，不要填错，

比如你要发送到你的交易平台，如果发送EOS,这里就要放你交易平台的EOS的充值地址，

而不是放ETH充值地址，当然你还需要在下面这个下拉菜单这里选择一下相应的代币类型，

比如EOS

关于什么是以太坊私钥储存(Keystore)文件和的介绍到此就结束了，不知道你从中

找到你需要的信息了吗 ？如果你还想了解更多这方面的信息，记得收藏关注本站。