经过我们知识星球课程的学习，我们了解到了交易所之间转账及代币的地址，但我们还必须用到钱包。前段时间朋友圈在传一个信息，某人400万资产被骗走。2018年1月25日晚coincheck损失了5.26亿个XEM加密货币，约合5亿美元。盗币事件频发，我们该如何保存我们的资产？安全在区块链投资中的重要性非常高，接下来我们先了解下一些基本术语。

比特币的所有权是通过数字密钥、比特币地址和数字签名来确立的。数字密钥实际上并不是存储在网络中，而是由用户生成并存储在一个文件或简单的数据库中，称为钱包。但资产是存储在网络中的。

密钥的用途：生成签名、证明所有权以及创造比特币靓号地址和纸钱包。

地址: 以太坊以 0x 开头的 42 位的哈希值 (16 进制) 字符串。

0x5a943383f20bdd974a39465cb9fc6e9b03db9cb0fd9b064a66c5495abf5424cc

地址以bc1开头BTC不分大小写，以后看到这样的地址也不要惊讶。
bc1qk4ystzdm0helwtxvpzzazsh99qxtpr3wel4zt3

地址=银行卡号

一个钱包中包含一系列的密钥对，每个密钥对包括一个私钥和一个公钥。

私钥(k)是一个数字，通常是随机选出的。有了私钥，我们就可以使用椭圆曲线乘法这个单向加密函数产生一个公钥(K)。有了公钥(K)，我们就可以使用一个单向加密哈希函数生成比特币地址(A)。

明文私钥: 64 位的 16 进制哈希值字符串, 用一句话阐述明文私钥的重要性
"谁掌握了私钥, 谁就掌握了该钱包的使用权!" 同样, 如果他人得到了你的明文私钥, 不需要任何密码就可以轻而易举的转移你的资产。

私钥=银行卡号+银行卡密码

Keystore: 明文私钥通过加密算法加密过后的 JSON 格式的字符串,
一般以文件形式存储。

Keystore+密码=银行卡号+银行卡密码

助记词: 若干个单词构成, 用户可以通过助记词导入钱包, 但反过来讲,
如果他人得到了你的助记词, 不需要任何密码就可以轻而易举的转移你的资产,
所以要妥善保管自己的助记词。

助记词=银行卡号+银行卡密码

广义的私钥包括：助记词、Keystore
和明文私钥，抄写的其实是助记词，汇总上述概念如下：

地址=银行卡号

密码=银行卡密码

私钥=银行卡号+银行卡密码

助记词=银行卡号+银行卡密码

Keystore+密码=银行卡号+银行卡密码

Keystore ≠ 银行卡号

关于私钥安全，由于新入场的区块链玩家很多，实际上很多人并不明白区块链私钥的意义和价值，会出现这样的情况，认为在交易所，或者钱包的账号和密码是最关键的，保护好了账号密码就万无一失，但糊里糊涂就被人钓鱼，把私钥拱手送出。这里安全性的风险之大，其实是很多玩家所不了解的，如果你只在手机或电脑装了一个钱包，而没有做任何备份处理，你的手机或电脑丢了，或者硬盘损坏了，你的币就没有了。

如果你装的是在线钱包，恭喜你，你可以在网上登陆找回，那么你账号密码被人窥破，你的币就没了。你账号密码都安全，但你不留神把私钥放到哪里被人看到了，或者那串备份单词被人看到了，你的币就没了。你一切都安全，然而在线钱包或交易所失窃了，你的币也没了。

钱包安全知识四个部分,
即钱包备份、防盗策略、防丢策略以及紧急事件处理方法。

创建钱包之后立即备份! 升级应用的时候备份! 删除应用的时候备份! ...
备份备份备份, 要把钱包备份当做一种习惯!

我们要清楚我们被盗的是什么? 是某个资产吗? 是某个确定的代币吗? 其实都不是, 防盗的实质是防止我们的私钥泄露, 或者被黑客盗取。而在防盗策略上, Keystore 和助记词(或者明文私钥) 的侧重点有所不同。

Keystore 防盗策略: 由于 Keystore 是被加密过后的私钥, 并且一般是以 JSON 文件形式存在, 采用"抄写"这种策略明显是不科学的, 所以可以存储在 U 盘里或者密码管理工具里。存储 Keystore 时要和密码分开存储, 这样只要密码强度足够高, 即使被黑客盗取了 Keystore , 也很难破解, 备份 Keystore 时也要多处存储, 比如你只存在 U 盘里, 如果 U 盘丢失, 那么也相当于丢失了钱包。

助记词防盗策略:在存储助记词时, 就需要更加谨慎一些, 因为助记词毫无安全性可言, 一旦被第三方窃取, 那么我们的资产将面临巨大的威胁, 所以建议采用物理介质备份, 抄写在一张纸上, 并且妥善保管, 抄写时要注意准确性, 也要注意长久保存, 不要出现字迹看不清楚等问题。

可以说防丢策略和防盗策略是整个钱包安全知识的重中之重, 钱包丢失一般分为三种情况:

删除钱包时, 没有备份钱包。建议在创建完钱包之后, 立即备份钱包, 采用双重备份和多次备份两种策略。双重备份是指 Keystore 备份和助记词备份, 多次备份是指在备份完 Keystore 和助记词之后, 要验证备份是否正确, 反复验证, 确认无误即可。

忘记了 Keystore 密码。我建议使用强度较高的密码加密 Keystore, 这个密码最好是随机生成, 不常用的密码。这样提高了 Keystore 的安全性, 但是也对保管密码带来了巨大的挑战, 我推荐使用 1password 或者 lastpass 等密码管理工具, 妥善保管好自己的密码, 以防遗忘。

遗失了私钥。这里的私钥包括助记词、Keystore 和明文私钥, 有些小白在备份助记词时, 抄写过后并没有做验证, 或者自己过于潦草, 导致后期很难辨识, 这些都会导致无法再找到自己的钱包。所以我们在备份钱包时要仔细认真, 在后期保管钱包时, 要善于使用一些安全的管理工具, 确保自己可以随时找到私钥。

一旦发现自己钱包出现不是自己操作的转出交易, 或者意识到自己的私钥已经泄露, 那么立即停止使用该钱包 (不要再向该钱包转账), 新建钱包 (当然要做好新钱包的备份) 然后立即将资产转移至新钱包。

很多人希望钱包服务商帮忙查找盗币者或者黑客的信息,

这一点在之前的基础知识部分已经讲的比较清晰了，因为是去中心化钱包，所以很难提供什么有效线索去帮助受害者"破案"。因此，在我们初次使用imToken创建钱包时，imToken给用户一个风险测评，这个测评可以加强我们对钱包的认识。这里附上通关攻略，让你更好的了解自己的钱包：

Case1:某女因为怕自己遗忘备份的助记词，所以将助记词告诉身边的亲朋好友，帮忙记住，结果被其妹夫盗取资产预计 3 万 RMB (后因其妹夫主动承认，才得以查清事实)

Case 2: 某女将自己的 Keystore 通过邮件进行传输，Keystore 密码和邮件密码是一致的，结果邮件被黑客拦截，被盗资产预计 30 万 RMB.

Case 3: 2017 年 10 月 16 日，广东东莞用户发现自己 100 多个 ETH 被盗，该用户最终确认是身边的朋友盗取了他的代币。该用户回忆说，当时在备份钱包时，这个朋友就在他身边，通过什么手段盗取他的私钥不得而知，因为这个朋友在归还了所盗取的代币之后，就与我们失去了联系，并没有说出具体的作案技巧，但是从理论上推测，有可能是在用户备份的时候采用拍照等手段记住助记词。

Case4:2017 年 10 月 23 日，hack@consenlabs.com 收到一封江苏无锡的被盗用户邮件，通过沟通得知，该用户将私钥曾经泄露给一位某知名小密圈的运营人员，后根据盗币地址查询以及转账行为分析，确定是这个人盗取了他的代币。当我询问他为什么要将私钥告诉这个盗币人，他说当时因为出现转币不到账的情况，情急之下将私钥发给这个盗币人，让其帮忙查明为什么转币不到账。

Case5: 类似冒充钱包运营人员2017 年 9 月 23 日，我们收到一封来自广东河源用户的工单，工单告知我们 "你们的客服，把我的币转走了"。收到消息后，我们第一时间与被盗用户建立联系，得知原来是有人冒充 imToken 客服人员，索取他的私钥。经过被盗用户提供的盗币人的邮箱，我们查找到了这个假客服，并协助用户将盗取的代币追回。

Case6:【投资者在imToken钱包被盗价值超250万人民币BTM】2018年1月18日，新浪微博用户“币圈诸葛亮”在微博求助，称其imToken钱包被盗价值超过250万BTM(比原链)。受害者表示其手机和电脑都有存私钥，但不清楚盗币者如何得逞。发现其有过极其危险的备份私钥或传输私钥的操作。

如果你觉得那些案例都很远，那看看发生在我们身边的黑天鹅事件：

在我们007不出局的一位战友，损失ETH 大约2000个，当时价格约价值16，000，000，原因：换手机的时候把旧有的imtoken钱包直接删除了，没有备份私钥。

另一位007战友当时是丢了500万等值的以德币，1260个ETH换的以德的真币，他以为是测试币没备份私钥在换手机的时候直接把imtoken删除了

区块链布道者金马朋友圈一位朋友，账户被盗数字货币价值400万，原因：骗子注册EOS官方Twitter，长期模仿官方内容混淆用户，然后发出令人垂涎的高利润诱惑用户交出钱包私钥，盗走你钱包所有的ERC 20代币。

娜写年华，007的实力女神。imtoken丢失EOS 3819个，按当时价格差不多30多万。具体细节不详细但应是熟人作案，盗走了她的私钥，后来追回来了。

（一）不要将私钥告诉任何人!

（二）私钥你要看的比命都重要!

（三）必须备份私钥(助记词)，且必须手写，放在安全的地方。

（四）不可使用 邮箱、QQ 或微信存储或传输私钥, 黑客也会采用 "放长线钓大鱼" 的方式, 不会立即盗取资产, 而是等到有更多的代币转入,
或者当用户进行了转出操作, 黑客会立即盗取剩余代币。

上述就是一文读懂钱包术语及钱包的安全知识的详细内容，更多关于钱包术语及钱包的安全知识的资料请关注（www.dadaqq.coM）Dadaqq.Com其它相关文章！

本站提醒：投资有风险，入市须谨慎，本内容不作为投资理财建议。

Tag：钱包 术语 安全知识