

# 跳出如来佛的五指山

## ——自制真随机助记词V2

看到别人用冷钱包，你是不是也很羡慕？许多人可能还在使用热钱包，而墙内的冷钱包又不一定好买。在没有冷钱包的情况下，选择一款不会采集数据，并且对本地助记词和密钥进行加密保护的热钱包，依然可以做到相对安全。

接下来我将教你如何制作真正的随机数助记词，彻底抛弃所有热钱包的伪随机数生成器

即便是冷钱包用户，如果不放心，也可以使用这个方法。不要以为使用冷钱包就绝对安全，在助记词生成上加入后门是完全不需要联网的。

之前的版本是分三个步骤完全自制，比较复杂。我最近发现一个更好的方案，通过一款叫Airgap vault的手机APP也能实现相同的功能。

## 准备工作

首先要有一闲置手机iPhone或者Android都可以。手机要能完全离线，最好事先已经恢复过出厂设置，并清空了所有的存储空间。

另外还要准备几枚硬币🌐，最好是8枚硬币或者多颗骰子🎲也是可以的

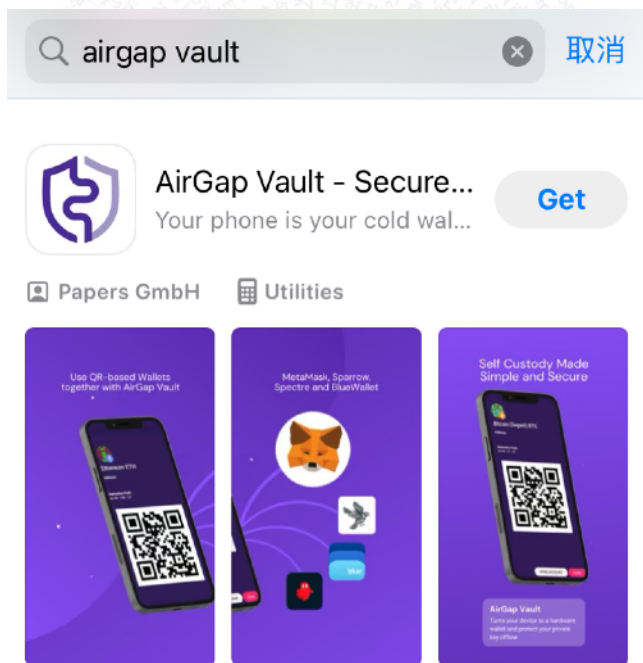
(⚠️必须是真实物品，不能是电子产品)

# 安装airgap-vault

## iPhone下载安装

(尽量使用非中国区Apple ID)

打开AppStore，搜索”airgap vault”



点击”Get”进行下载安装

# Android下载

从github上下载APK，地址如下

<https://github.com/airgap-it/airgap-vault/releases>

点击Assets里的apk进行下载

(这是一款开源软件)

Jan 28

IsaccoSor do

v3.32.6  
2cee865

Compare

**v3.32.6** Latest

- Resolved an issue that prevented users from transferring tokens on Moonriver and Moonbeam.
- Updated LifeHash icons.

**SHA-256 Hash**

airgap-wallet-65919.apk:  
72c7b4b88dc1d0147b4993df406087444171b6cae5c2754c347c86ad0507ae74

**Assets** 3

airgap-vault-65919.apk	76.7 MB	Jan 28
Source code (zip)		Jan 28
Source code (tar.gz)		Jan 28

点击下载 最新版本  
(当前是3.32.6)

# 让设备完全离线

在开始操作前，我们要让设备完全离线，避免数据泄漏，需要做到以下几点（加强部分可选）

- 有sim卡拔掉sim卡、开启飞行模式
- 关闭移动网络、关闭Wi-Fi
- 关闭蓝牙
- [加强] 找一个无手机信号的地方操作
- [加强] 用金属网包住手机大部分区域，削弱信号

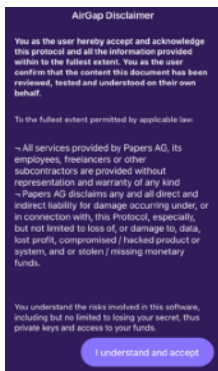
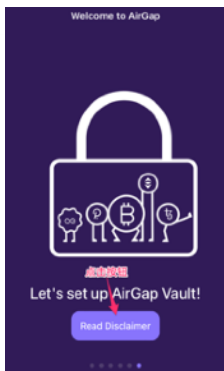
⚠ 这步很重要，我们接下来的所有步骤都必须在完全离线的环境下完成

## 打开应用

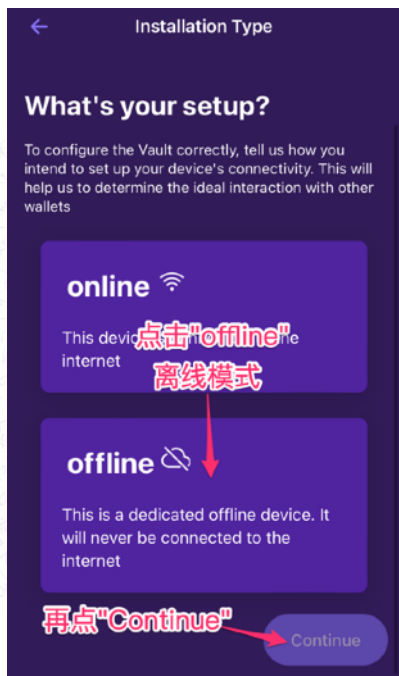
Android需要先安装应用

(iPhone按照上面步骤已经安装完毕)

打开APP，划过所有欢迎页，点击”Read Disclaimer”按钮，会跳出AirGap的声明  
声明页点底部的”I understand and accpet”



进入Installation Type页面，选择“offline” -> 点“Continue”



如果之后跳出“Install AirGap Wallet”则点“Skip”即可

最后来到”Secret Setup”界面，拉到底部会有一个”Advanced Entropy Generation”的选项，把其右侧的开关打开



点击后会出来两个选项

Generate with Dice Rolls表示掷骰子来产生助记词

Generate with Coin Flips表示掷硬币来产生助记词



下面我们以硬币为例，点击掷硬币做助记词（骰子也是类似的）

每投掷一次，根据结果点击下方的”Head”或者”Tail”  
上面的数字1,2,3,4...代表每次投掷，点击”Head”  
或”Tail”后，投掷结果会显示到对应的数字下面  
我们一共要投掷256次，如果你有8枚硬币就做32组  
即可。





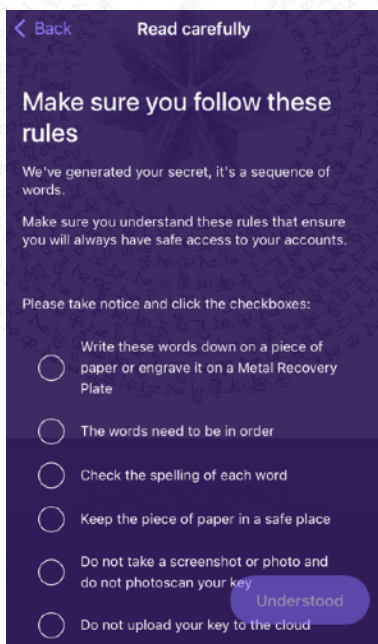
如果填写错误，可以点击垃圾桶删除最后一次投掷结果。当完成256次投掷后，点击右下角按钮表示完成。

注意整个过程必须用真实的硬币来投掷，自己随便填很容易出现非随机的情况



进入”Read carefully”页面，这个页面主要提醒你助记词的存放注意事项

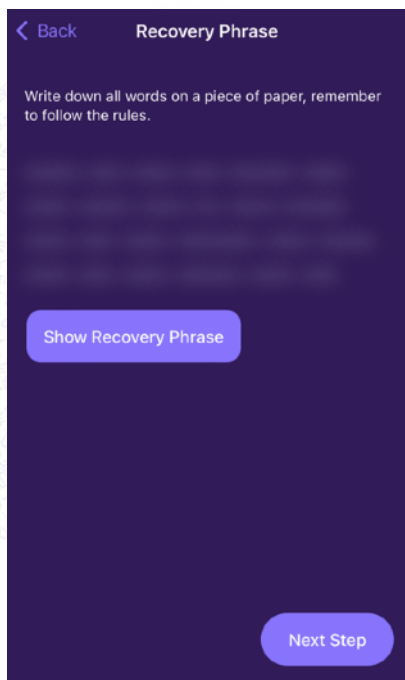
- 把助记词写在一张纸上，或者刻在金属板上
- 助记词是有顺序的不能打乱
- 检查每一个单词的拼写
- 把记录助记词的纸张放到安全的地方
- 不要截屏或者拍照，也不要用手机扫描这些助记词
- 不要把助记词存到云端



将以上内容全部打勾，点击”Understood”按钮

（助记词的存储请参考 不会被偷不会丢的助记词存储法）

点击后进入”Recovery Phrase”页面，点击”Show Recovery Phrase”就可以看自己刚刚用硬币投掷256次，造出的助记词了。将它抄写到一个本子上。



如果你身边有几颗骰子，也可以用掷骰子的选项，整个过程基本一样。


接下来还有最后一步也是至关重要的，那就清理使用痕迹。

# 清理使用痕迹

接下来我们将刚才使用app的痕迹完全抹除，抹除后这个闲置手机又可以留作他用了。

步骤如下：

- 1、（可选）再次重新再生成一次助记词，只不过这次点Head和Tail就不用掷硬币，快速点到256个即可。
- 2、卸载airgap-vault app
- 3、手机恢复出厂设置，清空存储。

 整个过程一定要完全离线

接下来你就可以用抄写在本子上的助记词了。

无论你是用Phantom、Solflare热钱包，还是Ledger、Trezor、Keystone等等，都可以把上面的助记词导入，恢复出自己新做的24位助记词的钱包了🙏

想要了解更多数字钱包安全内容，请看《防火、防盗、防中共 —— 数字钱包安全三重岛链》