

没有冷钱包的冷钱包方案

这是一个冷钱包方案，适合所有没有冷钱包的兄弟姐妹🙏。此方案适合存入后长期不取的人，只要不取一直都是“冷钱包”。

此方案的安全等级绝不亚于市面上所有冷钱包，虽然没有冷钱包的Passphrase加持，但backpack wallet带来的非常强大的自定义派生路径，这是市面上所有冷钱包都不具备的。有了她即使你的助记词不小心泄漏，只要派生路径定义的足够好，也不一定能发现你钱包里的数字资产！！

简单说一下流程：首先生成24组真随机助记词；然后安装一个支持完全离线的Solana热钱包；在完全离线的环境下，将24组助记词导入；再用自定义派生路径生成钱包地址；将钱包地址Copy到记事本中；删除热钱包APP并恢复出厂设置。

这里要特别感谢 流光飞舞#1391 提供的点子和 @brezel8899 战友的分享。当看到这个点子时激动不已，只要将它做适当完善那就是一个绝不亚于冷钱包的安全方案。接着立马找到了支持此方案的热钱包backpack wallet，真是天意🙏

目录

准备工作

整个过程介绍

自制真随机助记词V2

让设备完全离线

清理使用痕迹

自制只存冷钱包

查看只存冷钱包资产

提取只存冷钱包资产

不会被偷不会丢的助记词保存法

助记词中英文转化

如何记住\$TDCCP合约地址

准备工作

在进行所有操作之前，先要准备以下几样东西。

- 一个闲置的iPhone手机，这个手机可以恢复出厂设置同时清空所有存储内容，iOS版本要13.4以上；或者一个闲置的Android手机，同样可以恢复出厂设置并清空所有内容，Android版本可能需要7.0以上。
- 准备多个硬币🌐或者多颗骰子🎲，用于制造真随机数。还要准备一个本子或者一张纸，和一只笔，用于记录自己制作的24组真随机数。

整个过程介绍

整个过程分为三个步骤

- 1、生成24组真随机助记词（如果你之前也生成过但已经导入了联网的热钱包，需要重新生成，之前的助记词只能作为热钱包使用）。
- 2、自制只存冷钱包（使用backpack wallet），生成自己独有的钱包地址。
- 3、将数字资产转移到新的钱包地址中。
- 4、保存好助记词（参考不会被偷不会丢的助记词保存法）。

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。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。手机脱敏工作也要做，特别是针对iCloud部分

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

让设备完全离线

在开始操作前，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

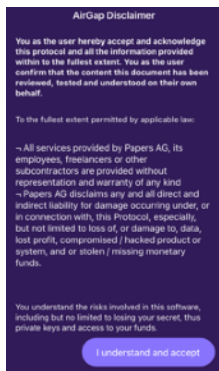
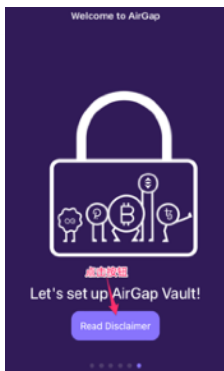
⚠ 这步很重要，接下来的所有步骤都必须在完全离线的情况下完成

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 accept”



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
一共要投掷256次，如果你有8枚硬币就做32组即可。



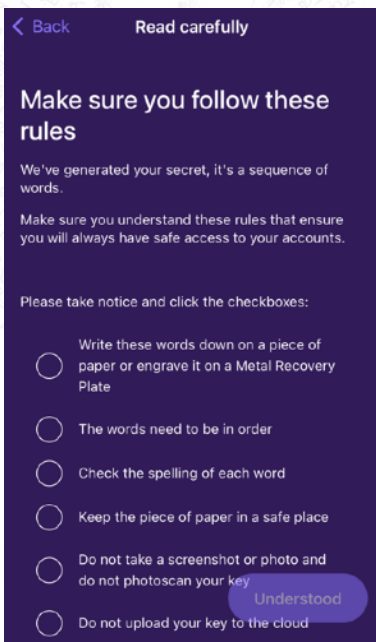
如果填写错误，可以点击垃圾桶删除最后一次投掷结果。当完成256次投掷后，点击右下角按钮表示完成。

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



< Back Read carefully

Make sure you follow these rules

We've generated your secret, it's a sequence of words.

Make sure you understand these rules that ensure you will always have safe access to your accounts.

Please take notice and click the checkboxes:

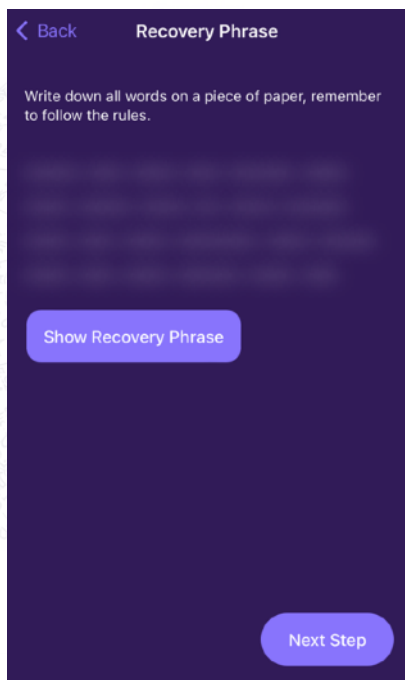
- ☐ Write these words down on a piece of paper or engrave it on a Metal Recovery Plate
- ☐ The words need to be in order
- ☐ Check the spelling of each word
- ☐ Keep the piece of paper in a safe place
- ☐ Do not take a screenshot or photo and do not photostan your key
- ☐ Do not upload your key to the cloud

Understood

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

接下来要将刚才使用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、Backpack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🙏

自制只存冷钱包

准备工作

- 24组的真随机助记词
- 一个闲置的手机（iPhone或者Android，iPhone优于Android）可以恢复出厂设置，并清空存储

清理和脱敏工作

首先清理设备，并做一些脱敏操作

iPhone脱敏

首先恢复出厂设置，并抹除所有内容

1、打开设置->隐私与安全性

- 定位服务 -> 将其关闭
- 跟踪 -> 关闭允许App请求跟踪
- 分析与改进 -> 里面所有项都关闭
- Apple广告 -> 关闭个性广告
- 蓝牙、本地网络、麦克风等能关都关闭

2、打开设置-> 点击Apple ID账户，登录非中国区

Apple ID -> 点iCloud -> 关闭iCloud云备份

（特别是“密码和钥匙串”要关闭）

Android脱敏

恢复出厂设置，确保同时清空设备存储。

在系统恢复模式中完成清空各种存储，不是仅仅是恢复出厂设置。

具体步骤

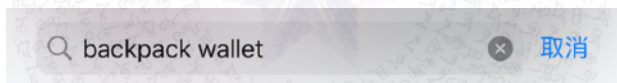
1、下载安装APP

如果对匿名要求极高，此处可开启VPN（普通人并不用）

iPhone安装

iPhone必须是非中国区Apple ID，搜索backpack wallet。下载安装，打开APP

提示 允许“Backpack使用无线数据？选择无线局域网和蜂窝网络。



Backpack: Buy & Trade Crypto

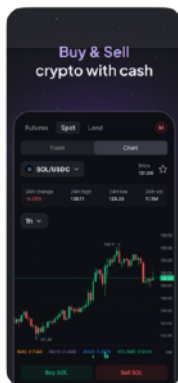
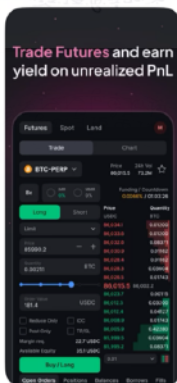
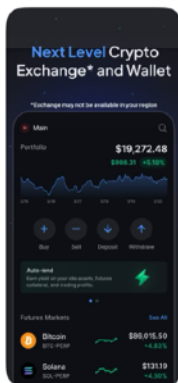
Crypto Spot & Futures Exchange

Get

★★★★★ 3

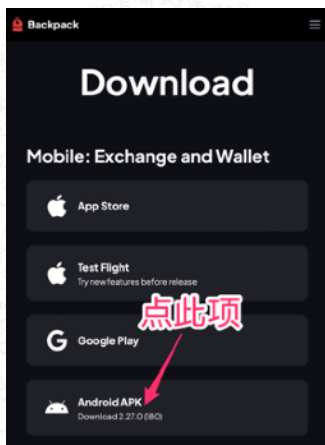
200ms.io Labs Ltd.

Finance

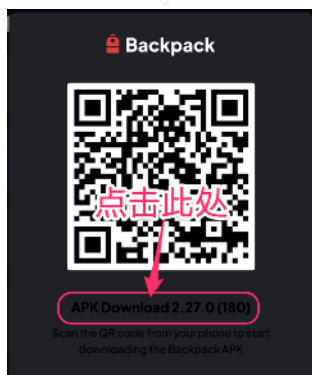


Android安装

Android通过官方网址 <https://backpack.app/download> 点击“Android APK”，出现二维码后



点击二维码下方的“APK Download ...”，Android下载安装，打开APP



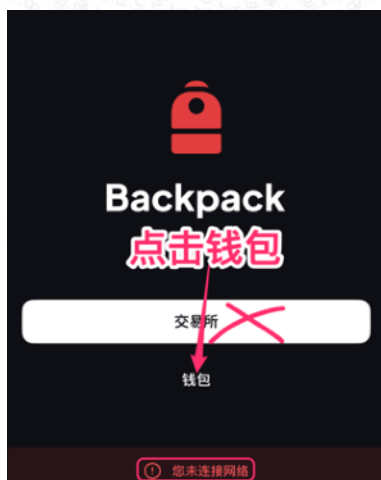
2、出现“交易所”和“钱包”两个按钮的界面




3、让设备完全离线

参考，生成真随机数中的“让设备完全离线”

4、点击“钱包”按钮，不要点“交易所”

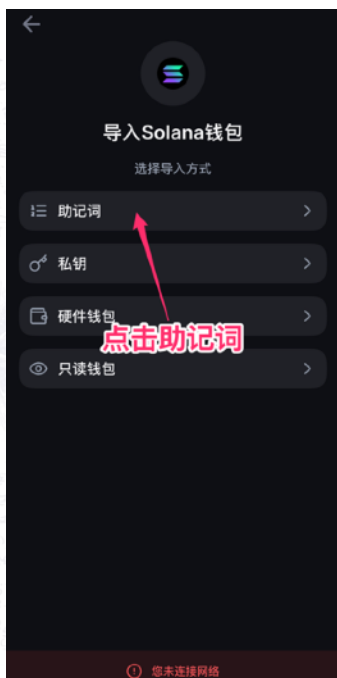
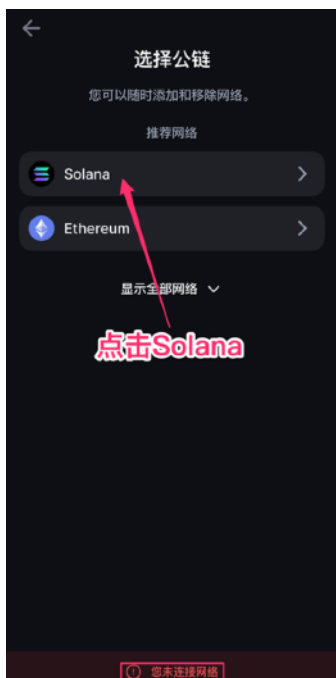


5、在 建立你的钱包 页面，同意服务条款，点已有钱包。（不要使用“创建一个新钱包”这样创建的钱包安全性有待考量）

注意，看底部显示“您未连接网络”，必须要有此标记，接下来所有步骤有“您未连接网络”的标记。没有请完成步骤3让设备完全离线。



6、在 选择公链 页面，选Solana -> 导入Solana钱包 页面，点击“助记词”。



7、进入 密钥恢复短语 页面，默认是12个助记词，
点击“使用24个助记词” -> 依次输入24个真随机数助
记词 -> 完毕后，点击“导入”

注意：输入到后面几个可能会被键盘挡住，没关系
一直输入，直到输入完毕，点键盘右下角的按钮或
者轻触屏幕空白区域可将键盘收起，并检查输入的
助记词是否一致



8、来到 导入有余额的账户 页面，点击“高级” -> 进入 导入钱包 页面，这一步就是选择自己的冷钱包地址。默认情况下Backpack的solana钱包地址的派生路径就是m/44'/501'/x'/0'

其中x会从0一直自增，默认第一个0

其他钱包还会有不同的派生路径



9、设置独有地址派生路径，导入钱包地址

此法并不符合区块链钱包标准，定义非常特殊的派生路径会导致同样的助记词导入其他钱包，无法发现自己的资产，而这恰恰就是一个高安全级别钱包应具有的特征。

做以下调整：

- 把44改成其他数字，比如202064
- 把501改成，比如419
- 把最后的0改成，比如20230315

于是派生地址变成了

m/202064'/419'/x'/20230315'



然后选择其中一个钱包地址，点击导入
可以把上面的数字换成自己想要的任何数字
这个派生地址用的数字你最好要记住

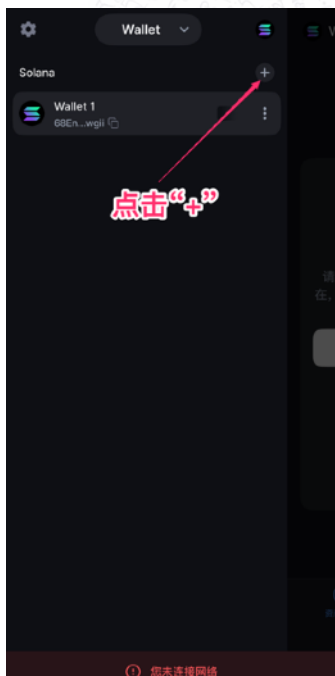
注：如果忘了派生路径的数字只要助记词对，你知道所用的格式，还是有办法遍历出所有隐藏资产的地址的，只是需要程序来完成，会比较复杂



10、很多时候一个钱包地址不够用

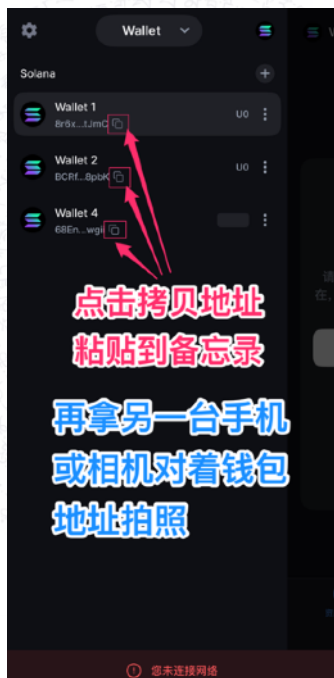
币圈正确的做法是新建多个钱包地址，用来接受不同的资产。避免接收款项时其他钱包地址的转账历史被对方知晓。

点击主界面左上角钱包名称 -> 点“+” -> 选择“查找



钱包”，再按照第9步的做法，导入钱包地址。

11、点击主界面的钱包名称，会出现钱包地址列表，选择复制钱包，把它粘贴到备忘录里面。然后用一个相机或者手机对这些钱包地址进行拍照，以防手抄出错。



12、这样就有了自己的冷钱包地址了，可以用来收款存数字资产了。

最后一步就是清理痕迹，这部很重要**!!**

先删除backpack wallet这个应用，同时手机恢复出厂设置并抹除所有内容。（从输入钱包助记词到最后清理痕迹，必须都是完全离线，这样就能完全避免backpack wallet往外界传递任何助记词和地址相关的信息）

注：清理和脱敏工作，在一开始就需要完成

查看只存冷钱包资产

在自己常用的联网手机中

安装一个backpack wallet APP -> 点击创建一个新钱包 -> 选Solana 设置钱包

再点击主界面左上角的钱包名称 -> 点“+” -> 选择“只读钱包” -> Public key中粘贴冷钱包地址 -> 点击“导入”即可。



提取只存冷钱包资产

在自己常用的联网手机中

把助记词导入backpack wallet中，再按照第9步恢复出对应的冷钱包地址，然后你就可以转账。一旦做了这步，你的助记词将不再拥有冷钱包的安全级别，就是一个妥妥的热钱包。

如果还需要相同安全级别的钱包，必须重新生成新的24个助记词，再按照自制只存冷钱包的流程来实现。

不会被偷不会丢的助记词保存法

你是否曾担心你的助记词即使抄在本子上，仍然有可能遗失或被盗？如果本子被人拿走，或者因不可抗力（如火灾、浸水）损坏，那对你来说是不是也难以接受？

今天介绍一种方法，让你的助记词既不会丢，也不会被盗，即使有人拿到你的“助记词”，也无法轻易破解。

假设助记词只有四个，以下四个为例：

nature sort toilet rigid

步骤一：将助记词转换为密码

找一本英文词典（或任何包含上述单词的英文书都可以），找出每个单词在书中的页码和它在该页内排第几个单词。

以英文词典为例：

nature 在第 520 页，第 10 个词条

sort 在第 748 页，第 2 个词条

toilet 在第 838 页，第 18 个词条

rigid 在第 678 页，第 19 个词条

依次找到所有助记词所在页码和词条序号，形成一组数据：520, 10; 748, 2; 838, 18; 678, 19

为了便于之后拆分助记词，以6个数字表示一个助记词，不足的前面补0

520, 010, 748, 002, 838, 018, 678, 019

助记词中英文转化

有人说英文词典少见，可以尝试换成汉字

打开助记词BIP39的标准列表

<https://github.com/bitcoin/bips/tree/master/bip-0039>

你在这个网页english.txt找到每个英文的单词的助记词对应的行号，分别记下后

再到chinese_simplified.txt里找到相同行号对应的中文汉字

最后转成12-24个汉字就是你的中文助记词，再尝试在书本里找出这些助记词页码和位置

步骤二：加入混淆机制

为了防止别人即使拿到这串数字，也无法直接还原助记词，这是另一串密码。

湖南卫视有段黄磊拷问李荣浩的问答：

为什么数鸭子是24678？

“门前大桥下，游过一群鸭，快来快来数一数，2、4、6、7、8。”

下面用 24678 这串数字来干扰原始编码：

第一个数字+2，第二个+4，第三个+6，第四个+7，第五个+8，然后再从头开始

520+2, 010+4, 748+6, 002+7, 838+8, 018+2,
678+4, 019+6

经过加密，新的密码变成：

522014754009846020682025

这串数字看似随机，即使别人拿到了，也无法直接解密（必须配合你的词典+混淆机制才可以）

步骤三：公开存放密码

可以放在email、网盘，以及各种可以公开存放的地方，哪怕是你的gettr账号备注，或者你发的一个帖子里，某一个你制作的视频里或者图片里的一串水印

甚至用HPay给人转账的时候备注上这串码

✗不要告诉别人用的书本

✗不要告诉别人你自己的混淆规则

书本尽量找发行广泛的版本（万一书丢了，你得能找到一样的）

题外话：如果你理解上面整个流程，动手能力强。将公开存放的密码替换成自己记得住的简单数字串，再配合词典、混淆规则，将整个过程逆转来生成助记词，就可以设计出完全不需要公开且不会丢失的助记词（这种情况生成的助记词要做随机性评估，0和1分布、转换频率、连续相同位长度、香农熵这些指标，保证其在合理范围）

步骤四：还原助记词

尝试把助记词再次还原出来，看看和记录在纸上的是否一致。

区块链丢了助记词就谁也无法打开，包括你的亲人孩子也无法获得，你要考虑到各种意外情况🙏

一切完毕后，把记录助记词的纸张销毁。等未来需要重新恢复时，再通过助记词保存方式反过来还原即可。



如何记住\$TDCCP合约地址

签名时一定要看合约地址是否熟知，避免遇到恶意合约将资产盗走。判断一个代币真假的唯一标准也是合约地址。\$TDCCP是一款在Solana区块链上的代币，其合约地址是：

**Hg8bKz4mvs8KNj9zew1cEF9t
Dw1x2GViB4RFZjVEmfrD**

没有非常特殊意外，这个地址会永久使用下去。

这是一串随机生成的地址，方便大家记忆，以每首字母拼音做一口诀：

**喜国八宝 馗战四魔
威慑八寇 牛劲九州
俄乌一挫 恶匪九瘫
末法人道**

【注释】

喜国八宝：喜国（新中国联邦）灭共有八宝

馗战四魔：钟馗（郭文贵先生）大战四方之魔

威慑八寇：震慑八路军（中共党卫军）

牛劲九州：\$TDCCP会牛遍九州大陆

俄乌一挫：俄乌战争没有按照CCP预想的进行

恶匪九瘫：中共几近瘫痪

末法人道：尾句表示这是一个新旧更替的时代，文明的转折点，要走出人类新的文明，她不是共产主义也不是资本主义，而是符合人道的正道主义🙏

俄乌 由 @JulianaProkhor9 文晨 所创
末法人道 由 @MarkLi49 Mark Li 所创

Hg8bKz4mvs8KNj9zew1cEF9tDw1x2GVib4RFZjVEmfrD

天 龍 機 房



喜国八宝
馗战四魔
威慑八寇
牛劲九州
俄乌一挫
恶匪九瘫

末法人道