Market Talks
教育中心

区块链 · 初级 · 第9课，共13课

助记词与备份

能够重建整个钱包的12或24个单词，如何妥善保管，以及谁会想方设法得到它们

阅读约6分钟　　6道测验题，附答案

区块链 · 初级 · 第9课，共13课

助记词与备份

一句话概括

助记词是一串由12或24个普通单词组成的列表，可以重新生成你钱包里的每一把私钥。保管好它，设备丢失或损坏后也能恢复。一旦泄露，任何人都能拿走一切，而且无法挽回。

一份备份，管住所有密钥

在第8课中我们看到，钱包会为每笔支付生成一个新地址，而每个地址都来自它自己的私钥。要逐一备份几十把私钥简直是噩梦。现代钱包的解决办法是：所有密钥都从同一个初始数字生成，这个数字叫作**种子**（seed）。

种子只会在你首次设置钱包时显示一次，形式是12或24个单词。这就是你的**助记词**，也叫恢复短语。把同样的单词输入几乎任何一个现代钱包应用，它都会按同样的顺序重新生成完全相同的密钥，并找到同样的币。手机或硬件设备可能丢失、被盗或损坏，但只要你还有这些单词，你的比特币就没有丢。

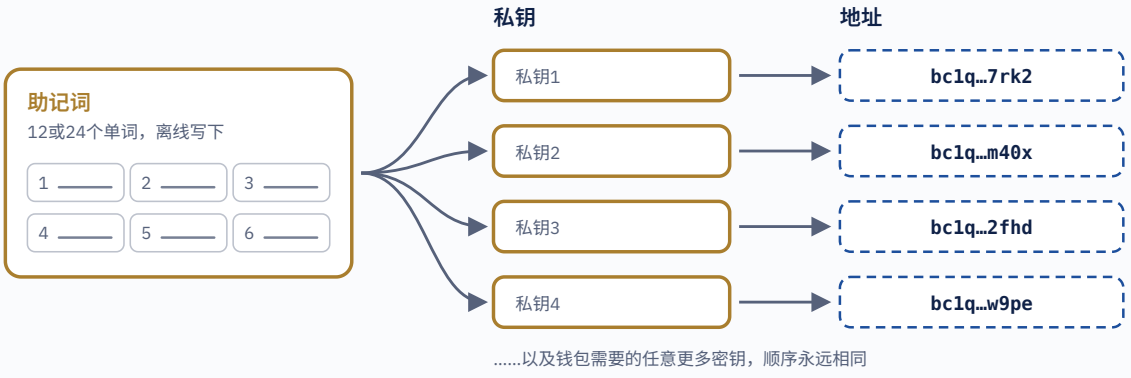


图1. 一组助记词生成钱包里的每一把私钥，每把私钥又对应一个地址。在任何兼容的钱包里恢复助记词，同样的密钥和币就会回来。

类比：照片底片

在胶片相机的年代，底片比任何一张照片都重要。照片丢了，可以拿底片在任何一家冲印店再洗一张，想洗多少张都行。助记词就是你钱包的底片，手机里的应用只是其中一张照片。但任何拿到底片的人，也都能洗出自己的照片。

为什么用单词，又为什么是这些单词

本质上，种子只是一个非常大的随机数。把它写成64个数字和字母很容易出错，所以一个被广泛采用的标准把它转换成单词，这些单词取自一份固定的、包含2,048个简单英文单词的列表。每个单词代表这个数字的一部分。

这份列表经过精心设计。在英文版本中，没有任何两个单词的前四个字母相同，所以即使单词末尾被弄脏，也仍能辨认。最后一个单词还起到内置校验的作用：如果你抄错了一个单词，钱包通常会提示助记词无效，而不是悄悄打开一个空钱包。

单词由钱包随机选择，而不是由你来选。这正是关键所在。一组12个单词的助记词可能是大约3.4乘以10的38次方种组合中的任意一种，这是一个39位数。你自己编的句子或歌词，会被专门尝试数百万常见短语的程序很快猜中。

有些钱包还允许你额外添加一个可选的密码，通常称为passphrase。设置之后，仅凭12或24个单词就无法打开钱包。这增加了保护，但如果你忘了这个密码，单词也帮不了你。

保管：离线、耐用、找得到

好的备份必须扛得住三种威胁：小偷、火灾或水浸等意外，以及多年以后你自己的记忆。常见方式对比如下：

存放方式	能防范	怕什么
写在纸上，放在家里	黑客，因为从不接触网络	火、水，以及任何发现它的人
刻在金属板上	黑客、火和水	任何发现它的人，除非藏得很好
在另一处放第二份，比如银行保险箱	一次灾难就丢掉唯一的备份	备份越多，可能泄露的地方也越多
照片、截图、备忘录、邮件或云盘	没有什么是纸张做不到更好的	账户被盗、同步备份，以及会扫描图片的恶意软件

无论选择哪种方式，都要按顺序写下单词、给它们编号，并逐个与屏幕核对。然后做一次恢复演练：在钱包里只放少量资金时，清除钱包或换一台设备，重新输入单词，确认出现的是同样的地址。现在发现错误代价很小，等到紧急情况再发现就不是了。

正当的人永远不会向你要它

由于助记词能打开一切，它是加密货币诈骗的头号目标。手法各不相同，但要求永远只有一个：把你的单词输入到某个地方。它可能以私信里的“客服”出现，也可能是弹窗说你的钱包需要“同步”或“验

证”，可能是应用商店里的假钱包应用，也可能是承诺免费空投的网站。

规则很简单，没有任何例外。助记词只在你自己恢复钱包时，输入到你自己的钱包里。任何钱包公司、交易所、开发者或频道管理员，永远都不需要它。

真实案例：假冒的“替换”钱包

2020年，硬件钱包制造商Ledger的一个数据库遭到入侵，同年12月，约272,000名客户的姓名、家庭住址和电话号码被公开到网上。几个月后，一些客户收到一个包裹，包装看起来和Ledger正品一模一样，里面附有一封信，说他们的设备不安全，并附上了一台“替换”设备。说明书要求他们输入恢复短语。设备已被篡改，这些单词直接落入了窃贼手中。

这对交易者为何重要

- **交易群是骗子的猎场。**骗子会加入活跃的加密货币群，冒用管理员的名字和头像，私信用户提供帮助或“钱包检查”。MARKET TALKS永远不会向你索要助记词、私钥或密码，任何真正的团队都不会。
- **你的交易所账户也有类似助记词的秘密。**交易所账户不使用助记词，但双重验证的备用代码起着类似的作用。如果有人拿到它们以及你的密码，就能接管你的账户。请像保管助记词一样离线保存它们。
- **为身后的人做好安排。**研究人员估计，已有数百万枚比特币永久丢失，其中很多是因为唯一知道密钥的人去世了或忘记了。如果你持有可观的数量，想一想将来如何让一位可信的人能够恢复它们，同时今天不给任何人访问权限。

关键术语

种子	钱包用来生成全部私钥的那个唯一的大随机数。
助记词	以12或24个单词形式写出的种子，可以重新生成钱包里的每一把密钥，也叫恢复短语。
单词表	助记词所取自的固定的2,048个单词列表，以便任何兼容的钱包都能读取。
校验和	包含在最后一个单词中的内置校验，帮助钱包发现助记词被抄错。
Passphrase	附加在助记词上的可选额外密码。没有它，仅凭单词无法打开钱包。
恢复演练	在往钱包里存入大额资金之前，先用写下的助记词练习一次恢复。

要点总结

1. 现代钱包从一个种子生成所有密钥，种子以12或24个单词的助记词形式展示给你。
2. 有了助记词，即使旧设备丢失或损坏，也能在新设备上重建钱包。
3. 单词来自一份固定的2,048词列表，由钱包随机选择，最后一个单词用于检查错误。
4. 请离线并以耐用的方式保存助记词，绝不放在照片、备忘录、邮件或云盘中，并用少量余额测试恢复。
5. 任何向你索要助记词的人都是想偷你的钱。它只应输入到你自己的钱包里。

自我测验

请为每道题圈出一个答案。答案及解释在下一页。您也可以在 markettalks.info 在线完成此测验，并立即查看得分。

1. 助记词能做什么？

A 重置交易所密码
B 重新生成你钱包里的每一把私钥
C 加快你的交易速度
D 取消已发出的付款

2. 装有钱包应用的手机被偷了，而你写下了助记词。该怎么办？

A 在另一台设备上用助记词恢复钱包
B 联系比特币客服
C 接受币已经丢失
D 请交易所撤销这次盗窃

3. 为什么不应该用你最喜欢的名言自己编一组助记词？

A 钱包读不懂句子
B 会让交易变慢
C 人们自己编的短语很容易被程序猜中
D 名言受版权保护

4. 保存助记词最安全的方式是哪一种?

A 存在相册里的截图
B 邮件草稿里的一条笔记
C 云盘里的一个文件
D 离线写下或刻下，放在防火防盗的地方

5. 助记词的最后一个单词有什么用?

A 设置钱包密码
B 充当校验，能发现大多数抄写错误
C 决定钱包存放哪种币
D 显示钱包余额

6. 交易群里有人私信你，说只要你提供助记词就能帮你修好钱包。这是怎么回事?

A 这是正常的客服流程
B 他需要它来查看你的余额
C 这是骗局，因为任何正当的帮助者都不需要你的助记词
D 他在验证你的身份

答案与解释

1 B

重新生成你钱包里的每一把私钥

助记词是生成你所有密钥的种子的书面形式。任何兼容的钱包都可以用它重建同样的密钥，并找到同样的币。

2 A

在另一台设备上用助记词恢复钱包

币在区块链上，不在手机里。用助记词恢复能让你重新掌控，立刻把资金转到新钱包则能保护它们。

3 C

人们自己编的短语很容易被程序猜中

安全性来自于单词是从海量组合中随机挑选的。人选出来的短语要容易预测得多。

4 D

离线写下或刻下，放在防火防盗的地方

任何存放在联网账户或设备上的东西，黑客或恶意软件都可能拿到。离线且耐用的备份可以避免这种风险。

5 B

充当校验，能发现大多数抄写错误

最后一个单词的一部分是由其他单词计算出来的，所以如果抄错了一个单词，钱包通常会提示助记词无效。

6 C

这是骗局，因为任何正当的帮助者都不需要你的助记词

拿到你的助记词就能拿走钱包里的一切。真正的客服团队从不索要它，所以这个要求本身就证明了是骗局。

资料来源

- 比特币改进提案39，用于生成密钥的助记码（GitHub）: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer，犯罪分子邮寄篡改过的Ledger设备窃取加密货币: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph，多达四百万枚比特币可能已永久丢失（Chainalysis估计）: https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

继续学习

下一课：第10课
托管：交易所账户还是自己的钱包

本课属于 MARKET TALKS 教育中心免费的区块链课程，涵盖初级、中级和高级课程，每课都配有测验和可下载的PDF。

教育中心
从基本原理到高级主题的课程

市场分析
主要市场的技术面与基本面分析

报告
比特币、黄金、白银、SPX等

markettalks.info

Telegram @MARKET_TALKS

仅供教育用途。本文件的任何内容均不构成投资建议。© 2026 MARKET TALKS。欢迎在不作修改的前提下分享本PDF。