

当投资者使用数字货币钱包的时候应该都需要输入一个助记词，可能许多投资者对助记词的概念还不是很了解，首先大家都知道，数字货币并不是真实存在的，因此保存方式也比较特殊，只能用特定钱包存储，其次，在使用钱包的时候需要输入的东西比较多，不光有助记词，还要有私钥、公钥等信息，其中助记词与私钥之间有着密切的联系。说到这大家可能更加疑惑了，那么数字钱包助记词是什么意思？下面C18快讯小编就给大家详细介绍一下。

说助记词之前，先说一下私钥。私钥是管理和使用数字货币中最关键的东西，对所有数字货币用户而言，私钥决定了所有权，拥有私钥才能支配相应的数字资产。简而言之，如果私钥丢失，你的数字资产就有可能成为别人的资产，或者永远无法找回。

但是，私钥一般由64位十六进制的字符组成，是一个随机数，很难理解和记忆，甚至在抄录的时候一不小心就会弄错。而助记词则是通过某个算法把这64个字符转换成一系列的单词(可以是英文、法文、中文甚至是你会的方言)，其目的就是为了帮助用户记忆复杂的私钥。

值得注意的是，助记词一般由12、15、18、24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。

### 1.降低出错概率

通常来说，我们存在银行的钱都会有很多账户，有的账户用来日常消费，有的是用来长期存款，有的是攒彩礼。这些账户的办理只需要一个身份证即可，一个身份证可以在网银上登录所有的账户，万一银行卡不慎丢失了，也可以通过身份证进行补办。

而到了数字货币的世界，助记词就相当于我们的身份证，私钥就相当于卡号和密码。但是通常来说私钥是由64位的长的字符串组成，如果我们想要创建100个账户，那就要记100个私钥6400位字符，并且一一对应不能出错。这对任何一个人来说都不是一件简单的事情。为了方便交易我们通常都要多个账户，满足不同场景的需求。如果说每次创建账户都在公链上生成一个私钥，那就像每次办理银行卡都要记忆一长串的银行卡号一样的麻烦。而有了助记词只需要我们记住这12个单词就能让此钱包的所有账户都有了保障。

### 2.保护隐私

由于区块链公有链的公开的特性，链上的所有转账记录任何人都可以查到，如果同一个账户关联的收入支出太多了，最终是可以摸出一些线索，把你和一些交易给匹配起来的，所以为了隐私考虑，我们的很多隐私业务通常会创建出新的账户来进行交易。

以上内容为大家解答了数字钱包助记词是什么意思？这个问题，现在各位投资者已经知道了助记词和钱包直接的关系了，对于投资者来讲，私钥是很重要的，但助记词同样重要，如果助记词不慎丢失，那么用户存放在钱包中的数字资产也就面临巨大的风险，所以C18快讯小编希望大家在记录私钥的同时也要将助记词备份保存，如果条件允许的话可以将这两样信息写在纸上，放置在只有自己知道的安全位置，后期需要的时候再拿出来使用。