当你打开数字货币新世界的大门时，你需要学习一门在这个世界生存的技能，如何正确备份你的钱包。

在过去的世界里，当你丢失密码时，你只需要向服务提供商提交一份忘记密码的申请，过一段时间。，您将收到一封电子邮件，拿起键盘并输入您的新密码。这个过程就像魔术一样，你重新控制了账户。

如此自然的功能，你在新世界里再也看不到了。

这是你在数字货币中看到的诸多不便之一，也是让你着迷的另一面。因为这是人类历史上第一次&quot私有财产神圣不可侵犯&quot是完全纯粹通过技术保证的。而这一切都是基于你保管好自己的私钥。

私钥，也就是财富。

在数字货币的世界里，你的钱包由一个私钥和一个公钥组成。在学会保管钱包之前，你需要了解私钥和公钥的生成机制：非对称加密算法。

1976年以前所有的加密方式都是一样的模式：

1。甲方选择加密规则对信息进行加密；

2。乙方使用相同的规则解决信息；

因为加密和解密是同一个规则。，被称为&quot对称加密算法&quot。这种加密算法最大的弱点是需要双方都知道解密规则，解密规则的保存和传输过程存在极高的安全风险。直到1977年罗恩里维斯特、阿迪萨莫尔和伦纳德阿德曼设计了一种非对称加密算法，并以他们的名字命名，称为RSA算法。

上述图为例解释非对称加密模式的过程：

1。Bob和Alice通过非对称算法生成他们的私钥和公钥(公钥可以从私钥导出)；

2。鲍勃想给爱丽丝发送一条加密的消息；

3。Bob用Alice加密信息&#039；的公钥；

4。加密的信息只能由爱丽丝解密&#039；的私钥；

目前数字货币(比特币、以太坊等。)采用了&quot椭圆曲线算法&quot。椭圆曲线算法也是一种不对称算法。与RSA算法相比，它具有安全性高、计算量小、存储空间小、带宽要求低等优点。

每个钱包帐户都包含一个密钥对，即私钥和公钥。。私钥(k)是一个数字，通常是随机选择的。有了私钥，我们可以使用椭圆曲线乘法的单向加密函数来生成公钥(K)。有了公钥(K)，我们可以使用单向加密哈希函数来生成帐户地址(A)。

当您进行交易时，每笔交易都需要一个有效的签名存储在区块链中。只有有效的私钥才能生成有效的数字签名，因此拥有钱包帐户的私钥有权控制该帐户。

了解了钱包的生成机制后，我们很快意识到，当我们备份钱包时，我们只是备份了我们的私钥，但由于保管方式的不同，我们的形式也不同。

目前常见的私钥形式：

1。私钥

2。Keystorepassword

3.Mnemonicseed

privatekey

私钥是随机生成的256位二进制数。你甚至可以用硬币、铅笔和纸随机生成你的私钥：将一枚硬币翻转256次，用纸和笔记录正反面并转换成0和1。随机获得的256位二进制数可以用作私钥。这个256位二进制数是私钥的原始状态。

keystorepassword

在以太坊官方钱包里。，私钥和公钥会用(创建钱包时设置的密码，请记住！)作为JSON文件存储在/users/yourname/library/ethereum/keystore中。。这个JSON文件就是密钥库，因此您需要备份密钥库和相应的密码。

助记码

助记码由BIP39提出，旨在随机生成12~24个容易记忆的单词，通过PBKDF2和HMAC-SHA512函数对单词序列创建随机种子。种子通过BIP-0032的提议生成确定性钱包。

BIP39定义创建助记符的过程如下：

1。创建一个128到256位的随机序列(熵)。

2。提出SHA256hash的前几个数字，就可以创建一个随机序列的校验和。

3。在随机顺序后添加校验和。

4。将订单分解为不同的11位组。并使用这些集合来对应2048个单词的预定义词典。

5。生成一个12到24个单词的助记码。

所以当你记住了12到24个助记符，就相当于记住了私钥。。助记符比私钥更便于记忆和保存。目前支持助记符的钱包有imToken和jaxx。

因为钱包有各种形式(本质是一样的)，也有很多备份方式，但最终目的都是防盗、防丢失、分散风险。

防盗：单独备份，如果密钥库或密码被盗，但对应的密码和密钥库仍然安全；

防丢失：多个备份降低丢失所有相应密钥库密码、助记符、私钥等的风险。

分散风险：适当分散资金以降低损失程度，同时采取多签名提取超过限额，需要更多私钥授权；

下面是一些常用的备份方法：

1。多个单独的备份密钥库密码

2。纸质钱包

3。大脑钱包

。

多个且分隔的备份密钥库密码

打开以太坊官方钱包，在菜单栏中选择账户-

备份-

。

ACCOUNTS，您将看到一个keystore文件夹，您将在其中保存您创建的wallet帐户，以及以UTC2016-08-16命名的JSON文件..这是您的密钥库文件。

把keystore文件放在几个安全的地方，比如你信任的离线USB和云存储服务提供商。

对于keystone对应的密码，应该使用强密码。，备份数量相同，并与密钥库分开。

纸质钱包备份

纸质钱包的本质是将密钥库或私钥以纸质的形式保存，通常是二维码的形式。

您可以使用命令行。

YoucanalsosubmityourkeystoreorprivatekeyofflinetoMyEtherWallet:opensourceJavaScriptclientEtherWallet.，可以直接打印对应的二维码纸质钱包。

大脑钱包我们说的大脑钱包，不是由用户产生的&#039；自己输入的自定义单词(因为不安全)，而是通过BIP39提案的方式随机生成的。可以记忆的助记码。这是一个计划，但不是一个很好的计划，因为人脑并不总是可靠的。

多重签名

多重签名是个不错的选择。它的好处是，当你需要提取超过限额。需要同时授权更多的私钥，同时提高防盗防丢的安全性。

在以太坊官方钱包中，您可以选择钱包合同下的添加钱包合同。，前提是你用来创建钱包合约的账户有不少于0.02ETH，足够支付交易所需的费用。

当您选择多重签名钱包合同时，您将看到以下提示：

"ThisisajointaccountcontrolledbyXowners.YoucansendYEtheratmosteverday.Anytransactionthatexceedsthedailylimitneedstheconfirmationof Zowner."

X代表有多少个账户受此钱包合约控制

Y代表单个账户授权下的每日提现上限

Z代表超过提现限额需要多少个账户授权

默认情况下我们采用X=3。Z=2，钱包合约由三个账户管理，需要两个账户同时授权才能突破提现限额。

采用多重签名机制后，您可以将您的密钥库和密码分放在多个地方，以单独的方式保存，从而增强了防盗性。，防丢安全。

关于多重签名的更多细节，请参考官方文档：账户管理-EtherealHomestead0.1文档

。

无论如何备份钱包，都能达到防盗、防丢失、分散风险的目的。

以上是区块链科普：如何正确备份你的以太坊钱包？详情更多如何正确备份以太坊钱包的信息，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！

本站提醒投资有风险，入市需谨慎。此内容不作为投资理财建议。