通过前面几篇的介绍，想玩加密世界的老铁，初步应该能过一个小门槛。

对于资产管理，大多数接触加密世界的用户首先使用的是交易所。关于管理你自己的资产前几年很少有人做。毕竟钱包里能做的事情不多。再加上担心资产流失，大部分用户选择将资产放在交易所。

从去年DeFi的火爆到今年NFT、道等WEB3应用的爆发。把资产放进你的钱包是一个非常大的需求。在交易所里，你能做的大多是简单的交易。放进你的钱包，你可以做更多。

以下文章将介绍加密钱包的类型如何管理钱包，在不同的钱包和交易所之间转移代币。

在真正掌握钱包并使用之前，建议用户详细了解钱包的基本原理和安全风险，避免个人资产的损失。钱包归个人使用，意味着资产完全掌握在自己手里。一些操作不当或隐藏的风险可能会导致资产的损失。案例数不胜数。

托管钱包：

用户不知道助记符或私钥。

可以认为交易所是一个托管的钱包，用户资产都在交易所里。

也有一些app是托管的，比如argent。

非托管钱包：

由用户自己持有助记符或私钥的钱包。

钱包里的助记符大多是通用的，可以互相导入。

私钥是完全通用的。

Metamaskwallet是最常用的非托管wallet。

冷钱包：

助记符或私钥存储在离线设备中，不接触网络。

交易通过扫码签名进行。

冷存储也被认为是保存加密资产相对最安全的方式。

冷钱包可以是硬件钱包、APP应用或纸张。

热门钱包：

助记符或私钥会触网，存储的设备如果被黑，有资产被盗的风险。

大部分手机应用钱包和浏览器插件钱包都是热门钱包。

硬件钱包：

将助记符和私钥存储在专用硬件中进行加密。在硬件中确认交易签名。

可以保证助记符和私钥不被直接窃取。

但是也存在交易过程被攻击的风险。

Metamask浏览器插件硬件钱包(Ledger、Trezor、Onekey等。)，Metamask创建一个帐号，但是不直接使用这个帐号。

链接硬件钱包，使助记符和私钥在硬件中。，相对安全。

移动钱包应用程序。

argent等具有社交恢复功能的手机钱包和TokenPocket等手机钱包虽然方便存储加密资产，但对DeFi的支持明显滞后。

我们经常谈论加密钱包。其实一个加密的钱包是由很多部分组成的，通常包括：钱包账号、公钥地址(账户)、区块链网络、基本令牌、合约令牌、发送/接收、交易、应用等等。

钱包账号是钱包应用的身份认证主体。账号丢失意味着资产的丢失

对于一个托管的钱包来说，一般由邮箱/手机号/用户名密码组成，和一般的应用没有太大区别。

对于非托管钱包，钱包账号是一个助记词，一般由12/24个英文单词组成。在大多数情况下，助记符在不同的钱包中是通用的。也就是说，钱包A中生成的助记符导入到钱包B中后仍然可以使用，可以在钱包B中控制自己的资产。。

一个钱包账户可以生成许多不同的账户(公钥地址)，这些账户可以位于不同的网络中。在交换中，会有不同网络的资产。显示在非托管钱包中，在不同网络之间切换后是资产。

账户(公钥地址)是个人链中资产存储的主体。所有的代币最终都会关联到一个特定的账户地址，所有交易的主体也是账户地址。一个钱包账号可以在不同的网络上生成无数个账号地址。比如以太坊网络的账号地址是0x开头的，terra网络的账号地址是Terra开头的，所以不同网络的地址之间不能直接转账。

对于托管钱包，不控制个人账户地址，一般只作为取钱的地址，不能用于其他用途。一旦应用，它可能会导致记入其中的令牌不可恢复。

对于非托管钱包，帐户(公钥地址)对应于私钥。一个私钥地址对应一个公钥地址，是通过非常安全的加密算法计算出来的，目前的技术无法破解。掌握私钥，您已经掌握了相应公钥地址中资产的操作权限。

私钥是账户的密钥(公钥地址)，助记符是账户的密钥(钱包应用)。这两个键不能在网站上输入。。不是你的钥匙，不是你的硬币。[XY002][XY001]对应于银行应用程序。当用户注册时，他将拥有一个用于登录银行应用程序的帐号和密码。登录后会有不同的账号。，比如储蓄账户、信用卡账户、理财账户等等。这里登录银行应用的账号是加密钱包的钱包账号(助记符)，储蓄账户对应账户(公钥地址)。

使用元掩码&#039；s浏览器插件钱包为例。当我们创建一个新的Metamask钱包时，我们会记录一组助记符，成功创建后就是一个钱包账户。当我们点击&quot创建帐户&quot函数，将添加一个新的帐户AcountX，它是Metamask帐户的帐户地址。，可以无线增加。

同时，我们还可以添加外部账号。我们可以通过单击&quot导入帐户&quot。可以发现这里不能导入助记符，因为助记符是顶层账户的载体，不能相互嵌套。。我们还可以链接硬件钱包，此时，位于硬件钱包中的账户也会被加载，也可以通过选择将其添加到元掩码中使用。我们经常听到的，如比特币(比特币网络)、以太坊(以太坊网络)、BSC(硬币安全智能链)、Solana等。都是不同的区块链网络。所有加密资产都在这些区块链网络上运行。不同的网络有不同的基本令牌。

比特币&#039；以太坊的基本令牌是&#039s基本令牌是ETH，BSC是BNB，Sola

na是sol。这些基本令牌作为网络最基本的资产运行，它们被不同的网络用来支付网络费用。

几乎每个独立的区块链网络都会对应一个基本令牌，比如AVAX、Terra、Loopring等。我们经常听说、戴和UNI是ERC20合约的代币。它们由以太坊契约控制，以太坊契约与基本代币的不同之处在于它们是可编程的。

契约令牌其实很复杂，分类不同，背后有不同的资产或规则。后面会单独写教程介绍这部分。

基本令牌只有在本网络运行时才是最安全的，其他网络上的基本令牌通常都是打包令牌。比如以太坊里BTC的包装wBTC，通过比特币网络，通过第三方锁定相等数量的BTC。，然后是以太坊发行的契约令牌。如果第三方资产管理出现问题，wBTC的价值就会偏离BTC。

令牌不能在不同网络之间直接发送，必须通过跨链桥和交换机等第三方设施传输。

相同的帐户地址可用于相同类型的网络管理资产。例如，EVM兼容链(以太坊，BSC，多边形，L2等。)都可以使用以0x开头的地址进行资产管理。但是位于不同网络中的资产是相互独立的。。他们的关系是&quot网络帐户令牌&quot，只有这三者对应，才能确定一项资产的归属。

了解了以上概念，我们就可以清楚的理解为什么每次在交易所取钱，都会让人选择不同的网络。

以太坊网络需要ETH，BSC网络需要BNB，多边形网络需要MATIC，Terra网络需要UST，比特币网络需要BTC。用户经常发现他们可以&#039；t提现后交易。因为我忘记在我的账户里存基本代币了。

以太坊网络中的令牌无法转移到BSC，不同网络之间的令牌转移需要跨链桥接或交换转移。

一些不常见的令牌无法在钱包应用程序中自动显示。。我们只需要找到令牌的合约地址，在我们的钱包中添加一个自定义令牌，然后就可以查看相关的资产了。

发生在分散式区块链网络(公共链)上的事务基本上是不可逆的。所以在交易之前，，以确定这是否是他们的真实意图，并确定交易地址。避免操作失误造成的资产损失。

很多人都爱西欧17年遗留下来的操作习惯，习惯直接把钱转到合同地址。这种操作多数情况下会导致资产流失。

常用的转账地址都存在通讯录里，避免每次都复制粘贴。在确认交易之前，请仔细检查地址，以避免转移错误的地址。

一开始我也是把资产放在交易所，后来因为担心交易所倒闭，就把钱提到了个人钱包里。在这个过程中也担心各种问题导致资金流失。

一般来说，个人在掌握资产方面有一个心理建构过程。根据个人经验，我给出一个大概的流程建议：

在0资产的情况下，熟悉各种钱包应用。、metamask、手机钱包、硬件钱包等。

您可以在一个应用程序中设置帐户，然后在另一个应用程序中恢复它，这取决于地址是否相同。

这是一个多通道备份。

在转小资金之前，一定要熟悉各种操作。

然后做一些转移练习。

关键是养成良好的安全习惯。

慢慢增加量，做好各类密码的备份。

进行一些恢复演练，确保方案的可靠性。

随着手术时间的增加，，慢慢就会建立起良好的信心。

同时要时刻保持安全习惯的执行，不能马虎。

原计划写完本文的基本概念后继续讲个人钱包的基本操作。但是感觉有点太长了。那&#039；这就是本文的全部内容。这些概念很多都需要在实践中去理解。

下篇文章将介绍各种钱包的基本操作，可以实现自由接入不同网络，处理一些特殊情况。

最后，再次强调安全习惯对于个人钱包应用的重要性。。说个最真实的案例，有些用户在练习的时候建了钱包，但是没有&#039；之前没有资金，助记符也可能是潦草的。后来因为一些情绪，他把资金存进了这个钱包。后来可能是电脑或者手机坏了，钱包打不开了。直到那时我才发现。我可以&#039；找不到原始的助记符！

所以，当我们真正使用个人加密钱包时，一定要做到安全习惯闭环，即从构建到恢复，一定要保证有可用的路径！

以上是科普基本概念的细节：加密钱包的高级用法。更多关于加密钱包的信息，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！