有关钱包的基本科普

钱包是什么？为什么要钱包？有关钱包的基本科普

因为国内很多老铁都是因为亲戚朋友等关系进场数字货币的，大部分对数字资产连最基础的认知都没有。（这很危险）

在数字货币的世界里，钱包的作用就是密钥管理。

而密钥包含私钥和公钥。

私钥用来进行签名交易，证明你对该交易的输出权。

公钥由私钥通过非对称加密算法生成，用来生成区块链地址，储存交易信息。

钱包地址是一个以双字母开头（代表币种）的42位16进制哈希值字符串，相信大家都在平台上见过。

（大家可以这么理解，钱包是银行卡，钱包地址就是银行卡号）

那么有老铁就要问了：我知道钱包是什么了，但是一般交易平台不都有钱包么？为什么还要一个自己独立的钱包呢？

这里老白就要特别说明一下：
因为考虑到网站使用的便利性以及账户的安全性，一般平台的交易只会涉及账号和密码。

发现了么？你虽然知道钱包地址，但你并不知道这个钱包的私钥，也就是说你并不真正持用交易的输出权，一切靠的都是你对平台的信任。

那为什么还说是为了安全呢？那是因为区块链的不可逆性导致一般小白如果被人盗取了密钥将是一件非常恐怖的事情，所以不如不知，而且区块链交易是全透明所以平台不敢随便乱动你的钱包。

那么又有老铁要问了：但是把货币从国内平台移到个人钱包到手续费，在从个人钱包移到国外平台又要手续费，这层层

再来说说，为什么密钥这么重要。


保存
钱包名
密码提示
导出私钥
修改密码
备份助记词
备份 Keystore
删除钱包

什么是助记词？

助记词由BIP31提案提出, 主要目的就是让用户更好的记住自己的私钥。

目前助记词有多语言版本, 包括中文、英文、日文、法文等。

——白话八比特 baihuabtc——

注：不同的钱包可能使用不同词库，所以导入钱包时可能出现助记词不兼容的情况，但私钥和Keystore是一致的,所以无需担心。

重要：助记词是未加密的私钥, 安全性低, 所以一定要备份好助记词。

重要+1：一旦忘记Keystore密码, 或者要更改Keystore密码,都需要使用助记词找回钱包，更换设备导入钱包同样需要助记词。

重要+2：千万不要用拍照或截屏的方式备份助记词，更不要使用邮件或其他即时通讯方式传输助记词。（沾网络就有被黑的风险）请务必手抄到纸上（清晰可读）！并放在安全的地方,谁都不能给！

接下来说说Keystore

不同于助记词，Keystore是加密过后的私钥，而Keystore的安全程度取决于加密该Keystore的密码强度。

重要：一定要将Keystore和密码分开存储，且Keystore密码不可更改。

将以上两者备份后，我们就可以安心使用钱包,
不用怕因为误删应用或设备损坏而丢失钱包了！

（当然最重要的还是钱包的密钥，千万千万不可被其他人看到）

最后提下矿工费这个东西。

操作过钱包的人应该都知道将钱包的币提出去需要付矿工费的，这里老白不想给大家细谈为什么要交矿工费，以及矿工费是如何产生的。

我们就说说是不是直接把滑竿拉到最大转账就会最快。

一笔交易的矿工费由交易所消耗的【gas】和每个gas的价钱【gas price】组成。

公式为：矿工费=gas数*gas price

但是有个问题，一个交易区块体积有限（即总gas数有限），所以对矿工来说，高额的矿工费最好是由适量的gas数和高额的gas price组成，这两者可以在imToken转账页面的【高级选择】里进行设置。

平台版本不同，支持的币种会有些许不同，建议选用Windows版本。

支持币种：BTC / ETH / DASH / ETC / REP / LTC / ZEC / RSK / DGE / ICN / GNT / GNO / DGD / BCAP / CVC / STX / POE / MCI / QTUM / CFI / ART / PAY / BAT / RLC / EDG / WINGS / SAN 等

imToken：国内一款支持Android和iOS的钱包，主要支持ETH系的币种。