区块链钱包简介

一、什么是区块链钱包

钱包是进入区块链世界的基础设施和重要入口。

“钱包”一词在区块链中有多重含义。

广义上讲，钱包是一个应用程序，为用户提供交互界面。钱包控制用户访问权限，管理私钥和地址，跟踪余额以及创建和签名交易。

狭义上讲，“钱包”是指用于存储和管理用户私钥的工具。

一个误区：钱包里存有资产。

实际上，资产不是存储在钱包里，而是存储在区块链上。钱包只包含密钥。使用密钥（私钥）来签名交易，来控制区块链上的资产，从而证明拥有该资产。

先理解几个概念：私钥、公钥、地址、助记词、keystore

私钥

私钥(Private Key)是一串由随机算法生成的数据。

一般使用 256 位的随机整数作为私钥（256 位的二进制数以 64 位十六进制数显示）：
0x2a871d0798f97d79848a013d4936a73bf4cc922c825d33c1cf7073dff6d409c6

公钥

公钥(Public Key)是和私钥成对出现的，和私钥一起组成一个密钥对。
eg: 0x023255458e24278e31d5940f304b16300fdff3f6efd3e2a030b5818310ac67af45

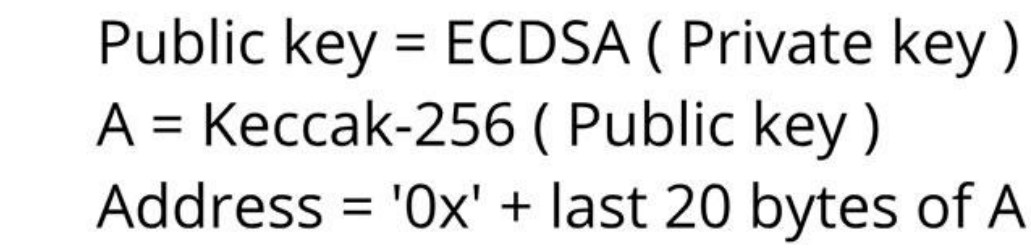
公钥由私钥生成，但是无法通过公钥倒推得到私钥。

公钥和私钥之间存在数学关系，允许私钥用于在消息上生成签名。该签名可以在不公开私钥的情况下使用公钥进行验证。

比特币和以太坊都使用了椭圆曲线算法生成公钥和私钥。

地址

公钥能够通过一系列算法运算得到钱包的地址。
地址是公钥哈希的编码，并不是公钥本身。通过公钥可推导出地址。通过地址不可推导出公钥。
以太坊地址，eg：0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266



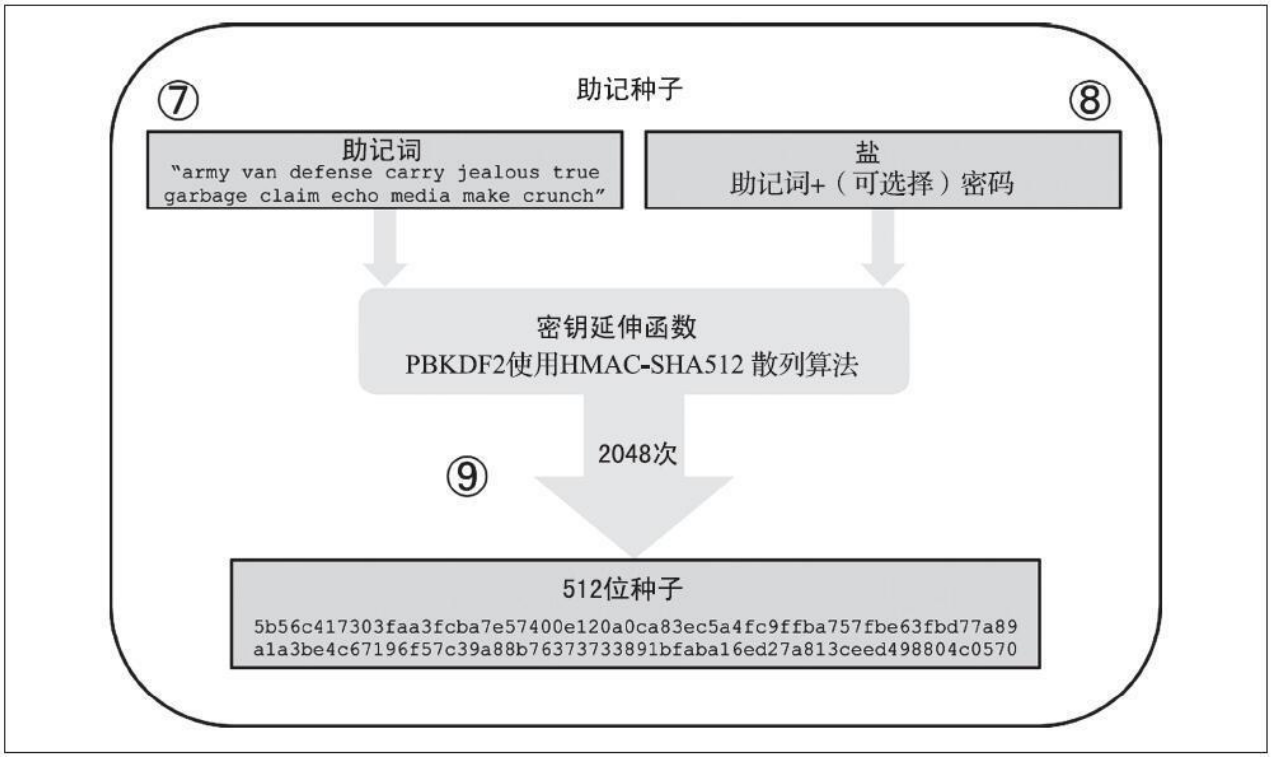
助记词

由于私钥是一长串毫无意义的字符，比较难以记忆，因此出现了助记词(Mnemonic)。

助记词是明文私钥的另一种表现形式。助记词即私钥！

助记词一般由 12、15、18、21、24 个单词构成，常用的是 12 个单词。这些单词都取自一个固定词库。wordlists

比如：test test test test test test test test test test test junk



Keystore

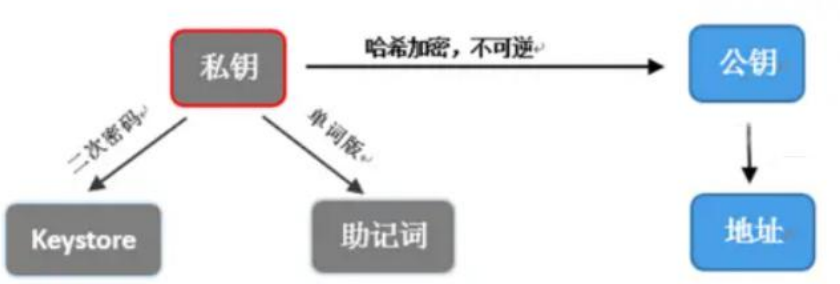
Keystore 是加了”锁”的钱包

Keystore 文件是钱包存储私钥的一种文件格式 (JSON)。它使用用户自定义密码加密，以起到一定程度上的保护作用，而保护的程度取决于用户加密该钱包的密码强度

Keystore 主要在以太坊钱包 App 中比较常见。需要配合钱包密码来使用，才能导入钱包

Keystore 的样式

```
{
  "version": 3,
  "id": "b7467fcb-3c8b-41be-bccf-73d43a08c1b7",
  "address": "540f18196da5a533fa36577a81de55f0a2f4e751",
  "Crypto": {
    "ciphertext": "78ed11b8b6bf29b00f52b42b8542df0e4a6ac078e626af7edcf885c3b68154a4",
    "cipherparams": {
      "iv": "4516579601d96695fe30ace985a9066f"
    },
    "cipher": "aes-128-ctr",
    "kdf": "scrypt",
    "kdfparams": {
      "dklen": 32,
      "salt": "6276cfda7d40872352c801db5871e5a3368a8d0994cea39ed936760db78d1cdc",
      "n": 1024,
      "r": 8,
      "p": 1
    },
    "mac": "d889a5dc609c3f312a41394cc47640676d2612501a6f8c837ed55598158336db"
  }
}
```

二、钱包分类

按私钥是否接触网络，可分为冷钱包和热钱包

- 冷钱包

常见的冷钱包：纸钱包、脑钱包、硬件钱包、离线手机钱包等。只要没有联网的数字钱包都可以统称为冷钱包。

- 热钱包

冷钱包不触网不同的是，热钱包是联网了的。我们平时比较常用的手机钱包、浏览器插件钱包等，都属于热钱包。

按私钥签名方式，可分为单签名钱包、多重签名钱包

- 单签名钱包

仅需一人使用私钥签名即可使用的区块链钱包。

- 多重签名钱包

需要 2 个或 2 个以上不同的私钥签名才可以使用的区块链钱包。通常用在需要共同管理账户的场景中，例如数字资产组织合作、区块链企业管理等等。

按照去中心化程度，可分为全节点钱包、轻钱包，以及中心化钱包

- 全节点钱包

除了保存私钥外，还存储了整个区块链数据，这样就可以在本地直接验证交易数据的有效性。占用为较大的存储空间与网络流量。

- SPV 钱包（simplified payment verification wallet，简单支付验证钱包，又名轻钱包）

与前者比，此种钱包仅存储私钥，依赖于其它全节点，只同步和自己相关的数据，不存储整个区块链数据。占用资源很少，较适用于移动设备。

- 中心化钱包

交易所钱包，不会提供私钥给用户，但会提供对应钱包的地址，方便资产转移。

三、常用的钱包介绍

MetaMask

MetaMask（小狐狸），是用于与以太坊区块链以及兼容 EVM 的链进行交互的钱包。它可以通过浏览器扩展程序或移动应用程序让用户访问其以太坊钱包，与 DAPP 进行交互。
下载地址：https://metamask.io/download/

imToken

- imToken 支持 Ethereum、Bitcoin 和 TRON 等 12 条主流公链
- 查看最新行情，集成去中心化交易所 Tokenlon 实现资产兑换
- 内置开放的 DApp 浏览器功能，输入任意 DApp 网址，即可访问和使用 DApp

官网：https://token.im/

Gnosis Safe 多签钱包

Gnosis Safe 是一个运行在 EVM 上的智能合约钱包，需要最少数量的人在交易发生之前批准，交易才会发生。

官网：https://gnosis-safe.io/app/

四、安全建议

- 备份你的钱包，对私钥、助记词、Keystore 一定要进行多重、多次备份。
- 不要使用云备份存储私钥
- 不要截屏或拍照保存私钥
- 不要使用微信、QQ 等 IM 工具传输私钥
- 不要使用第三方提供的未知来源钱包应用

记住：Not your keys, not your coins.

不要泄露私钥！
不要泄露私钥！
不要泄露私钥！