1 钱包基础

主题：理解私钥、助记词等核心概念，完成钱包创建与安全备份

一、导引

1. 区块链中的“钱包”和现实中的钱包，有什么相同点和不同点？
2. 如果手机/电脑丢了，你的钱包资产会不会跟着消失？
3. 私钥和密码最大的区别是什么？哪个更重要？
4. 为什么助记词可以恢复整个钱包，而不是单个账户？
5. 如果有人知道了你的助记词，会发生什么？

二、核心知识点讲解

1. **钱包（Wallet）**

- 钱包在区块链世界里，不是“装钱的口袋”，而是**管理私钥的工具**。
- 钱包的核心功能：生成、存储和使用私钥，帮助用户和区块链进行交互。
- 分类：
  - **热钱包**（在线钱包，方便操作但相对不安全，如 MetaMask）
  - **冷钱包**（离线钱包，安全性更高，如 Ledger、Trezor）

2. **私钥（Private Key）→ 公钥（Public Key）→ 地址（Address）**

- **私钥**：
  - 本质是一串随机生成的数字字符串。
  - 就像你的“签名笔”，决定了你是否有权花费资产。
- **公钥**：
  - 由私钥经过算法推导出来，相当于“门锁”。
  - 公钥本身不能控制资产，但可以用来生成地址。
- **地址**：
  - 由公钥进一步压缩、编码后得到，相当于“银行卡号”。
  - 别人需要知道你的地址，才能给你转账。

👉 关系链：**私钥 → 推导出公钥 → 生成地址 → 用地址收发资产**。

3. **助记词（Mnemonic Phrase）**
    - 一组 12 或 24 个英文单词，实际上是私钥的**人类友好型表达**。
    - 一个助记词可以恢复整个钱包（包含所有账户和地址），而不是单个私钥。
    - 因此，助记词是**钱包的根钥匙**，比单一私钥更重要。
4. **钱包创建与安全备份**

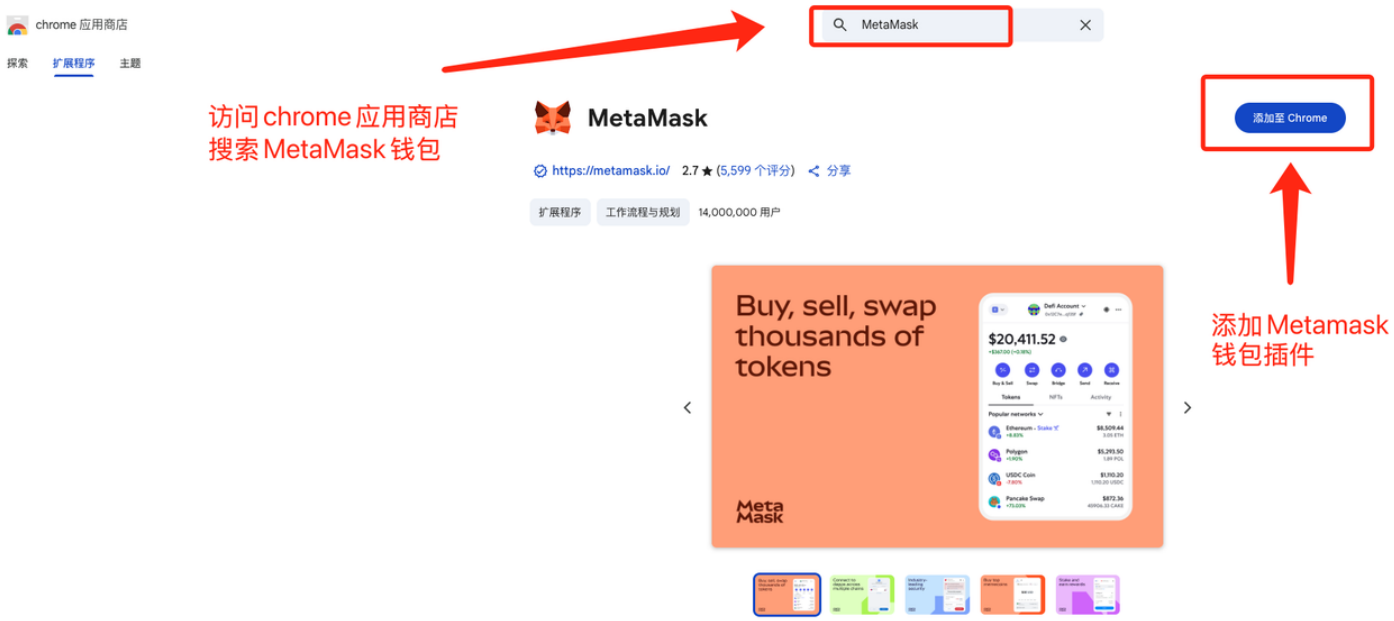
- **创建过程**：
    - 系统生成随机数 → 生成私钥 → 推导出公钥 → 生成地址 → 同时生成助记词。
- **安全备份要点**：
    - 正确方式：手写助记词、使用硬件钱包、存放在安全位置。
    - 错误方式：截图、保存到云盘、通过微信/邮箱传输。
- **核心原则**：资产不在钱包里，而在区块链上；钱包只是你掌握资产的“钥匙”。

三、实操案例

案例1 创建Metamask热钱包并添加区块链网络

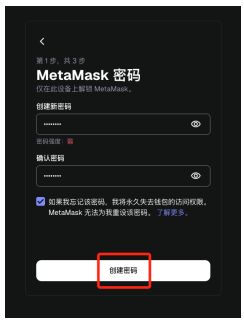
步骤 1：下载安装

- 打开 Chrome 应用商店 → 搜索 “MetaMask” → 添加插件。



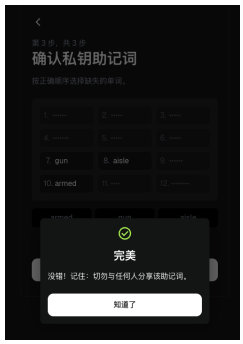
步骤 2：创建新钱包

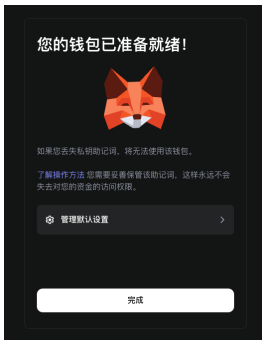
- 点击“开始使用” → “创建新钱包”。
- 设置密码（本地解锁用）。



步骤 3：备份助记词

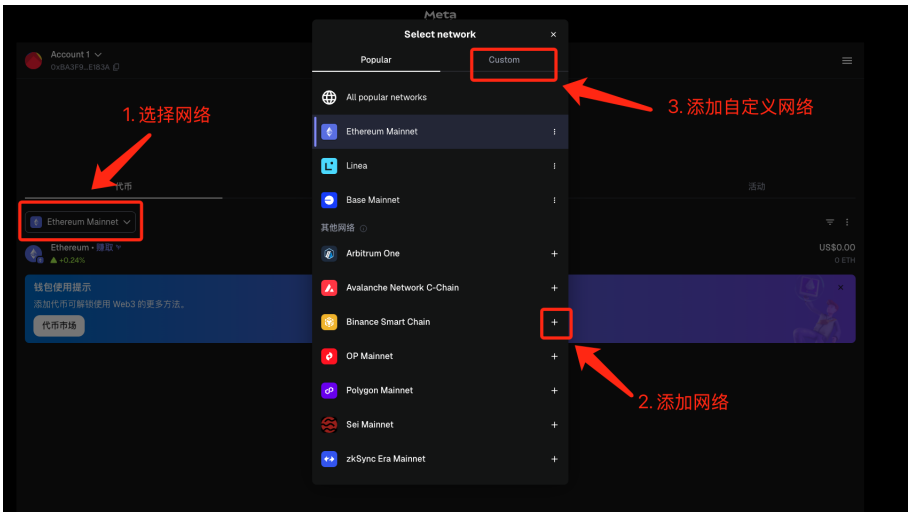
- 系统会生成 **12 个英文单词**，必须抄写保存。

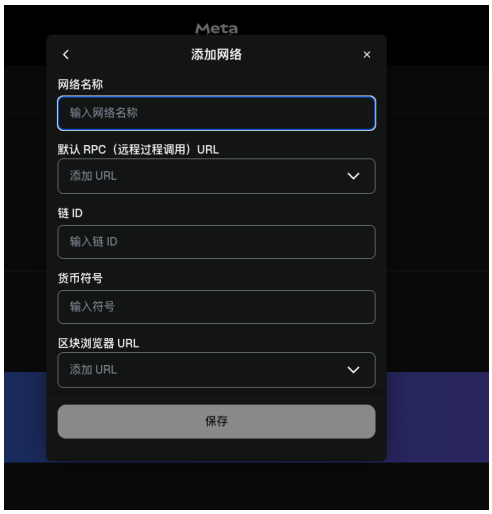




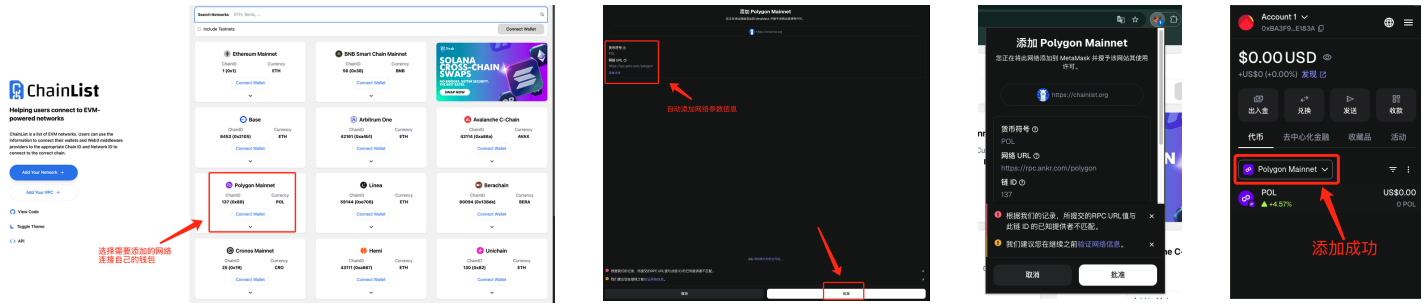
步骤 4：添加网络（以 Polygon 为例）

- 方法1：
  - 点击“设置 → 网络 → 添加网络”。
  - 输入 Polygon 的 RPC 地址 → 保存。



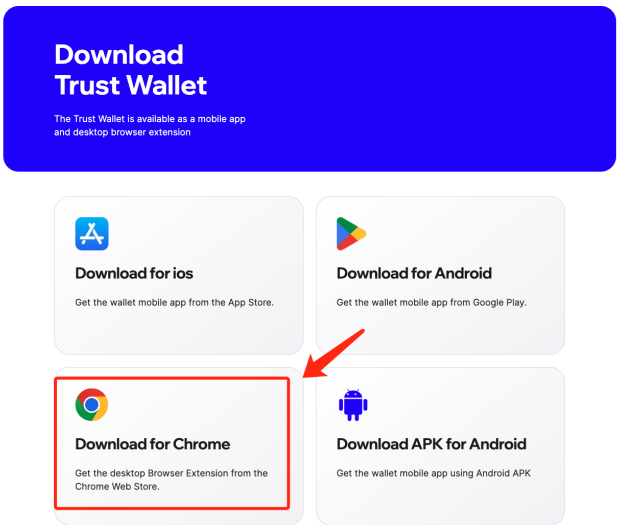


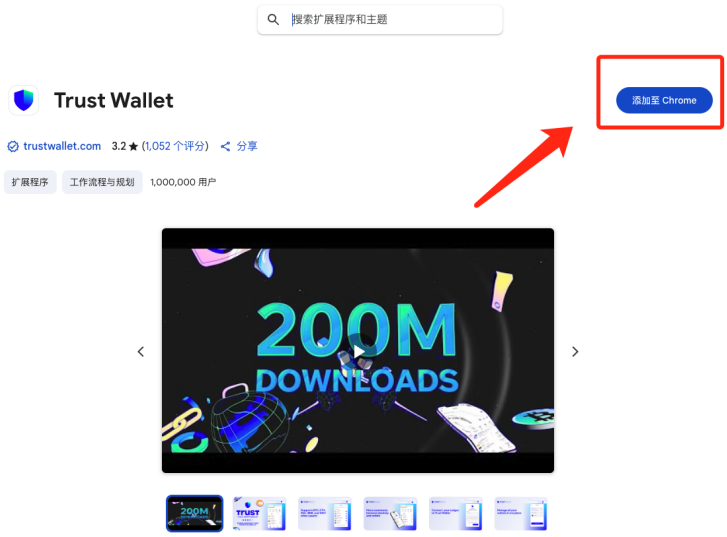
- 方法2
  - 通过chainlist添加快速网络参数 https://chainlist.org/



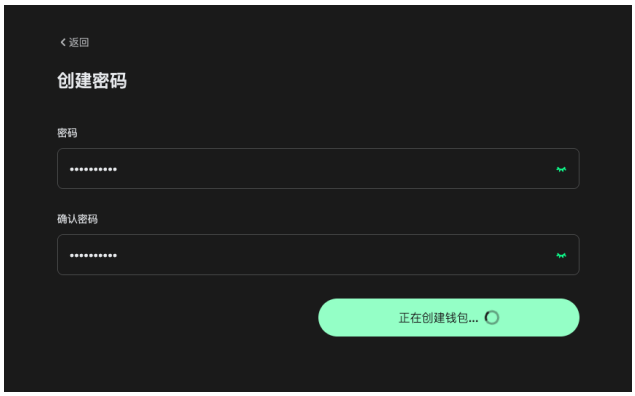
案例2 Trust Wallet 安装与创建钱包

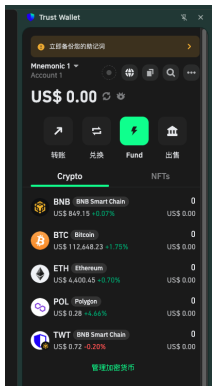
步骤 1：下载安和添加插件





步骤 2：创建新钱包和设置密码





四、总结

1. 区块链钱包 vs 现实钱包

- 相同点：都用来管理资产。
- 不同点：现实钱包装钱，区块链钱包装“私钥”，资产存在区块链上。

1. **设备丢失是否等于资产丢失?**

- 不会。资产存在链上，只要助记词/私钥还在，就能恢复。
- 设备丢失只影响“钱包的入口”，不影响资产本身。

2. **私钥 vs 密码**

- 密码：可以修改、重置。
- 私钥：一旦丢失无法找回，不能修改。
- 私钥是最终控制权，比密码更重要。

3. **为什么助记词能恢复整个钱包?**

- 助记词 = 根私钥的种子，可以推导出所有子私钥、公钥和地址。
- 所以助记词恢复 = 钱包完全恢复。

4. **助记词泄露的后果?**

- 一旦被别人知道，等于把资产拱手送人。
- 区块链是不可逆的，转走后无法追回。

---

2. 核心知识点总结

- **钱包**：管理私钥的工具，不是资产本身。
- **私钥**：控制资产的根本凭证。

- **公钥**：由私钥推导出，用于生成地址。
- **地址**：收发资产的唯一标识。
- **助记词**：钱包的根钥匙，可恢复整个钱包。
- **安全备份**：必须离线保存，避免网络泄露。