区块链钱包概念

钱包用来存钱的，在区块链中，我们的数字资产都会对应到一个账户地址上，只有拥有账户的钥匙（私钥）才可以对资产进行消费（用私钥对消费交易签名）。数字钱包实际是一个管理私钥（生成、存储、签名）的工具，注意钱包并不保存资产，资产是在链上的。

冷钱包 Cold Wallet

冷钱包(Cold Wallet)是一种脱离网络连接的离线钱包，将数字货币进行离线储存的钱包。使用者在一台离线的钱包上面生成数字货币地址和私钥，再将其保存起来。冷钱包是在不需要任何网络的情况下进行数字货币的储存，因此黑客是很难进入钱包获得私钥的，但它也不是绝对安全的，随机数不安全也会导致这个冷钱包不安全，此外硬件损坏、丢失也有可能造成数字货币的损失，因此需要做好密钥的备份。

热钱包 Hot Wallet

热钱包(Hot Wallet)是一种需要网络连接的在线钱包，在使用上更加方便。但由于热钱包一般需要在线使用，个人的电子设备有可能因误点钓鱼网站被黑客盗取钱包文件、捕获钱包密码或是破解加密私钥，而部分中心化管理钱包也并非绝对安全。因此在使用中心化交易所或钱包时，最好在不同平台设置不同密码，且开启二次认证，以确保自己的资产安全。

密码

密码不是私钥，它是在创建账户时候的密码（可以修改）

密码在以下情况下会使用到：

1. 作为转账的支付密码
2. 用keystore导入钱包的时候需要输入的密码，用来解锁keystore的

私钥 Private Key

私钥由64位长度的十六进制的字符组成，比如：0xA4356E49C88C8B7AB370AF7D5C0C54F0261AAA006F6BDE09CD4745CF54E0115A，一个账户只有一个私钥且不能修改。

通常一个钱包中私钥和公钥是成对出现的，有了私钥，我们就可以通过一定的算法生成公钥，再通过公钥经过一定的算法生成地址，这一过程都是不可逆的。私钥一定要妥善保管，若被泄漏别人可以通过私钥解锁账号转出你的该账号的数字货币。

公钥 Public Key

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，保存在钱包中。公钥由私钥生成，但是无法通过公钥倒推得到私钥。公钥能够通过一系列算法运算得到钱包的地址，因此可以作为拥有这个钱包地址的凭证。

Keystore

Keystore常见于以太坊钱包，它是将私钥以加密的方式保存为一份 JSON 文件，这份 JSON 文件就是 keystore，所以它就是加密后的私钥。Keystore必须配合钱包密码才能导入并使用该账号。当黑客盗取 Keystore 后，在没有密码情况下, 有可能通过暴力破解 Keystore 密码解开 Keystore，所以建议使用者在设置密码时稍微复杂些，比如带上特殊字符，至少 8 位以上，并安全存储。

助记词 Mnemonic

私钥是64位长度的十六进制的字符，不利于记录且容易记错，所以用算法将一串随机数转化为了一串12 ~ 24个容易记住的单词，方便保存记录。注意：

1. 助记词是私钥的另一种表现形式
2. 助记词可以获取相关联的多个私钥，反过来私钥没法获取助记词。

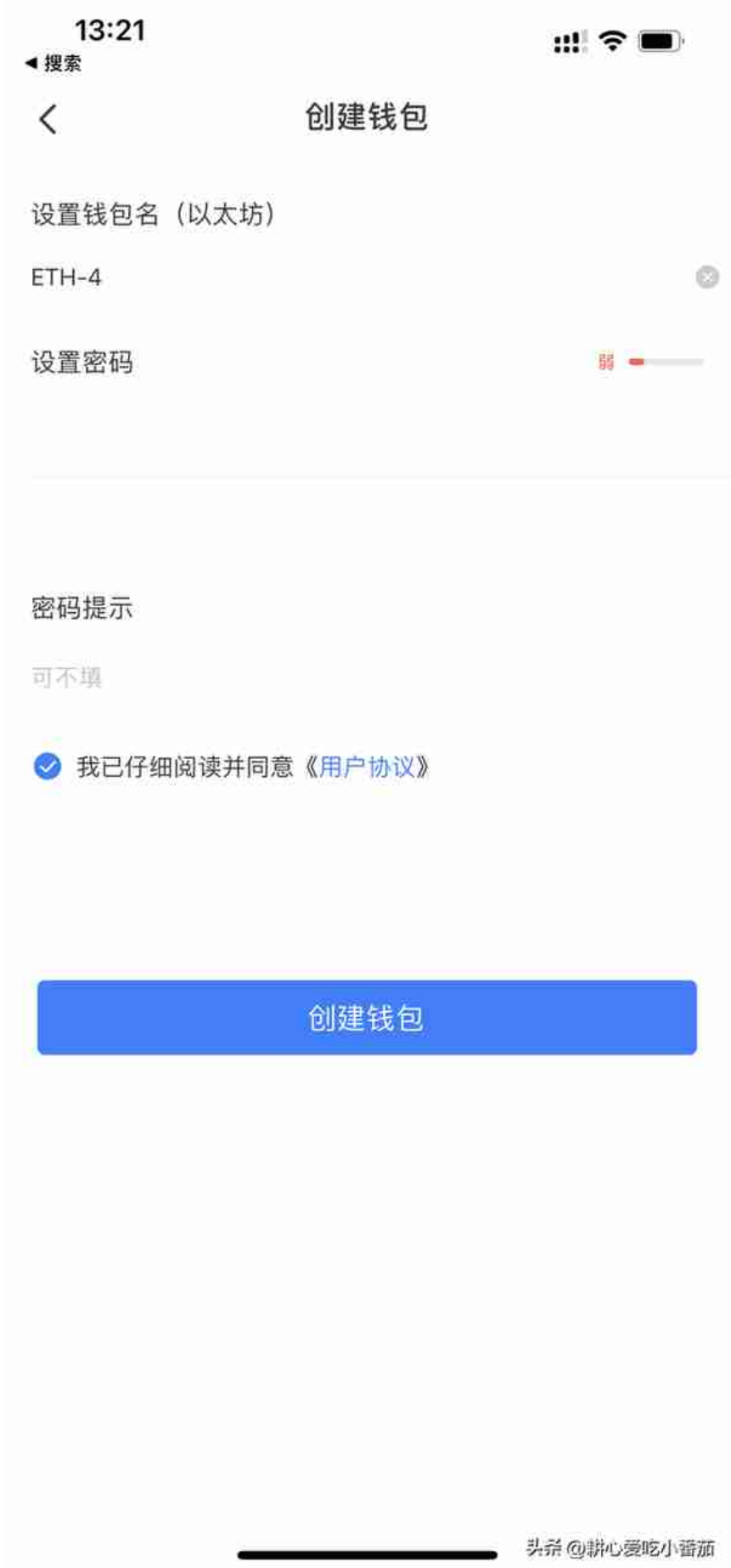
如何解锁账户

解锁账户有如下几种方式：

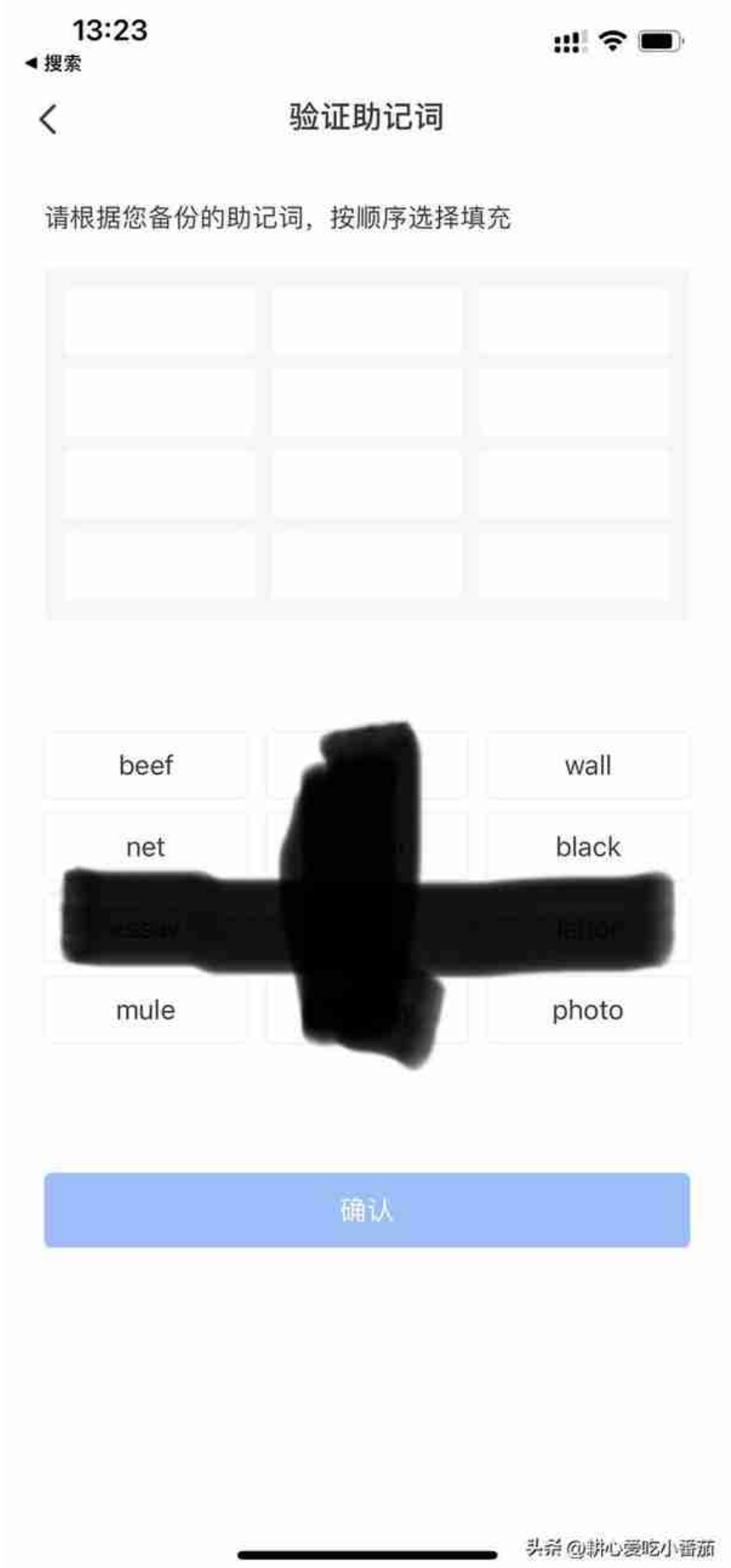
- 私钥（Private Key）
- Keystore+密码（Keystore+Password）
- 助记词（Mnemonic code）

TokenPocket


13:20
搜索
选择网络
身份钱包 (HD)
KeyPal硬件钱包
比特币
以太坊
币安智能链
波场
火币生态链
Solana
Polygon (Matic)
ETC
OKXChain
EOS
Avalanche C-Chain
KCC Mainnet
BTTC
GT
以太坊 钱包
创建
导入
取消
头条 @耕心爱吃小番茄


13:21
搜索
创建钱包
设置钱包名（以太坊）
ETH-4
设置密码
弱
密码提示
可不填
我已仔细阅读并同意《用户协议》
创建钱包
头条 @耕心爱吃小番茄


13:21
搜索
备份助记词
在下一步里，您将看到可以恢复钱包的助记词 (12 个单词)，请谨记以下安全点！
如果我弄丢了助记词，我的资产将永远丢失！
如果我向任何人透露或分享我的助记词，我的资产可能会被盗！
助记词只存在我的手机里，保护好助记词的安全的责任全在于我！
我知道了
头条 @耕心爱吃小番茄


13:23
搜索
验证助记词
请根据您备份的助记词，按顺序选择填充
beef
wall
net
black
mule
photo
确认
头条 @耕心爱吃小番茄

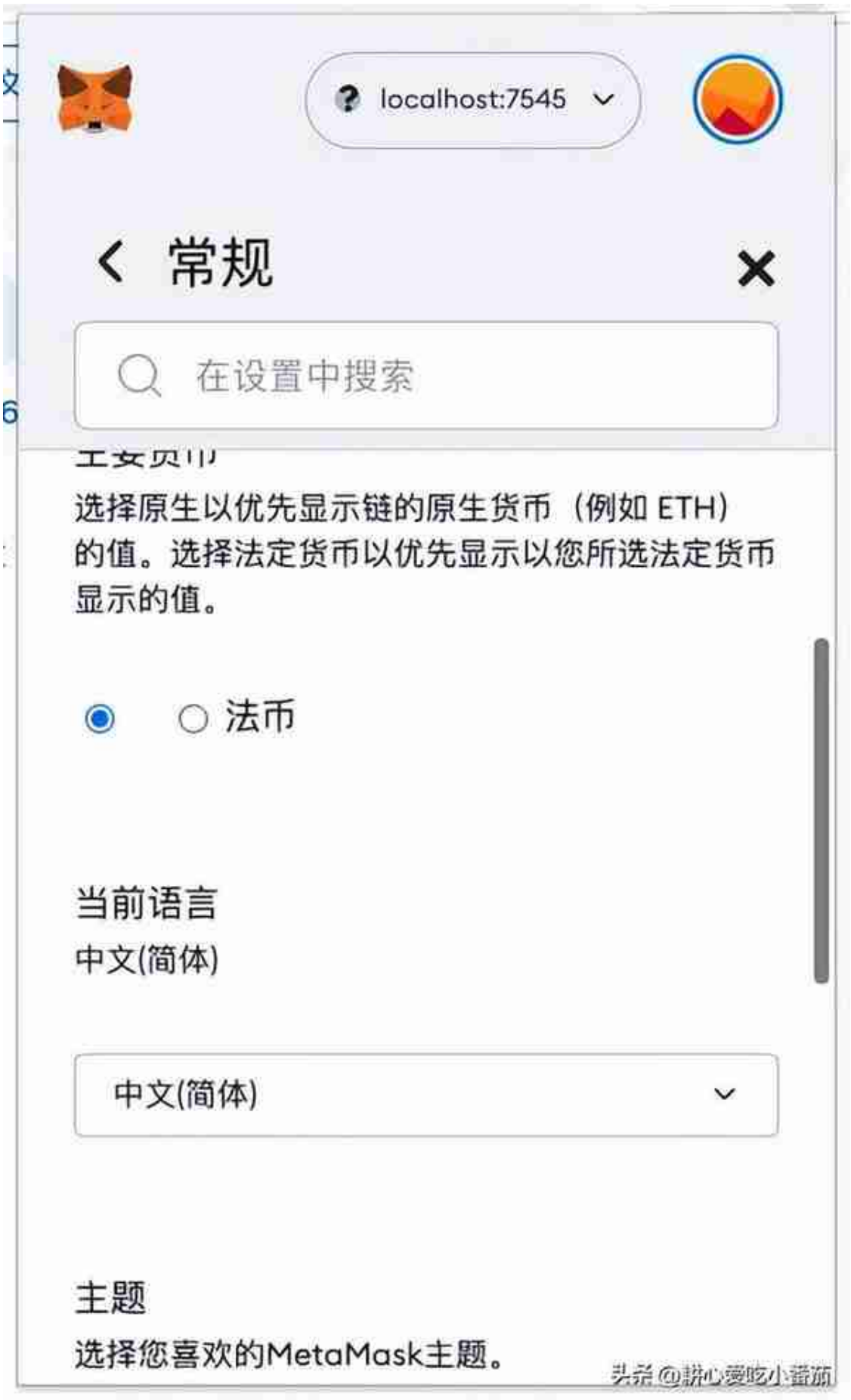
MetaMask

官网：https://metamask.io/

创建账户

点击“创建钱包”。在下一页中，系统将询问是否提交匿名数据，以帮助开发人员改进App。该项无强制要求，可随意选择。现在需创建密码。如需详细阅读软件用户协议，点击使用条款即可查看。或直接跳过，然后设法设置高强度密码，勾选复选框，点击“创建”。


localhost:7545
我的账户
注销
搜索账户
0 ETH
账户 5
0 ETH
BNB正式地址
已导入
0 ETH
Account 4
已导入
999.76216318 ETH
创建账户
导入账户
连接硬件钱包
获取帮助
设置
头条 @耕心爱吃小番茄


localhost:7545
常规
在设置中搜索
选择原生以优先显示链的原生货币（例如 ETH）的值。选择法定货币以优先显示以您所选法定货币显示的值。
法币
当前语言
中文(简体)
中文(简体)
主题
选择您喜欢的MetaMask主题。
头条@耕心爱吃小番茄