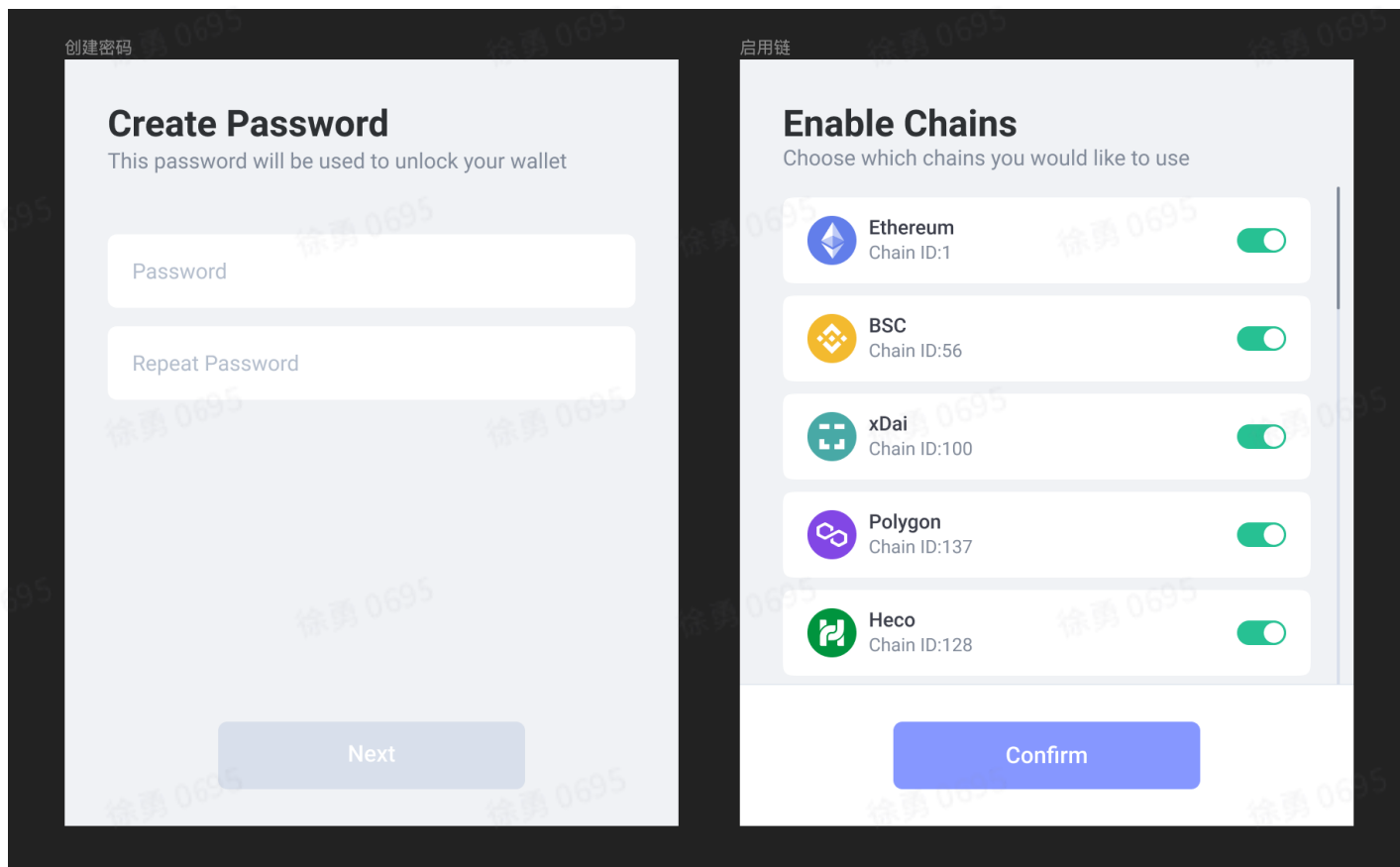


# Rabby 0.1 产品功能文档

Rabby 是一个围绕 DeFi 应用场景设计的多链钱包，帮助用户在多链场景下管理私钥、确认和校验 DApp 发起的交易、并将交易推送到链上。

## 初始化流程



插件完成安装后，需要点击浏览器右上角的插件 icon 进入初始化流程：

### 1. 设置解锁密码

- 浏览器重启或者用户手动在钱包中点击 lock 后，钱包都会进入锁定状态，用户需要输入解锁密码解除锁定状态；
- 用户如果未完成设置解锁密码操作，下次打开钱包时，重新进入设置解锁密码流程；

### 2. 确认启用哪些链

- 一条链如果未在钱包中启用，则 DApp 页面在该链上提交交易时，钱包不会进行处理；
- 所有已支持的链默认都处于启用状态，除非用户手动禁用；

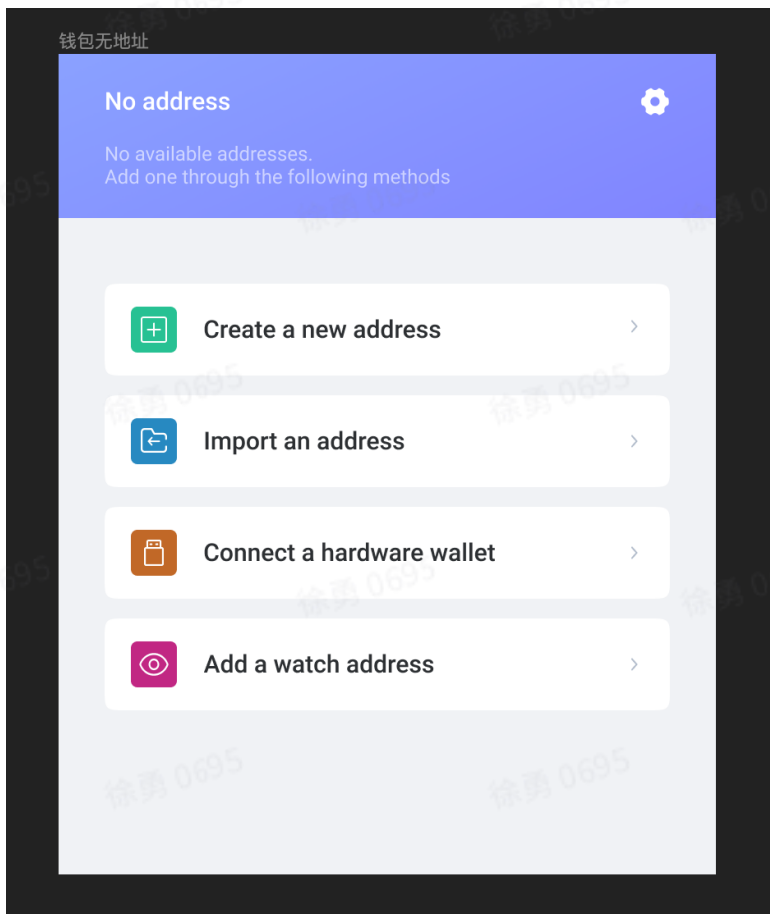
- c. 钱包中必须有至少一条链处于启用状态；
- d. 用户如果在该页面未进行任何操作直接关闭页面，下次打开时不再进入该流程，所有的链维持启用状态。

用户完成上述步骤后，可以开始进行添加地址的操作。

## 添加地址

钱包中的地址分为以下几类：

1. 助记词地址：由钱包中的助记词关联的地址（钱包中有私钥）
  - a. 钱包中允许存在 0 个或者 1 个助记词
2. 私钥地址：通过导入私钥得到的地址（钱包中有私钥）
3. 硬件钱包地址：通过与硬件钱包连接获得的地址（钱包中无私钥）
4. 观察地址：直接输入地址到钱包（钱包中无私钥）



对应的，有以下几种添加地址的方式：

## 创建地址

1. 如果钱包中没有助记词，点击创建地址后，进入创建助记词流程，并在助记词创建完成后，生成该助记词对应的第一个地址，然后将该地址设为钱包的当前地址；
2. 如果钱包中已经存在助记词，点击创建地址后，直接使用该助记词生成下一个地址，并将该地址设为钱包的当前地址。

钱包中会记录当前的助记词已经生成了几个地址，以保证用户再次点击「创建地址」的时候，钱包知道新创建的地址是哪一个。

## 导入地址

1. 如果钱包中没有助记词，可以通过以下三种方式导入地址：
  - a. 导入私钥：将私钥导入钱包，该私钥对应的地址会被设为当前地址；
  - b. 导入助记词：将助记词导入钱包，用户可以在该助记词对应的地址列表中，选择任意数量的地址导入钱包，选中的地址中的第一个会被设为当前地址；
  - c. 导入 json 文件：通过 json 文件批量导入私钥（需要输入 json 文件的密码），导入地址中的第一个会被设为当前地址
2. 如果钱包中已经存在助记词，则只能使用导入私钥和导入 json 文件，不能选择导入助记词

## 连接硬件钱包

当前支持的硬件钱包包括：

1. Ledger
2. Trezor
3. OneKey

硬件钱包的连接过程基本一致：

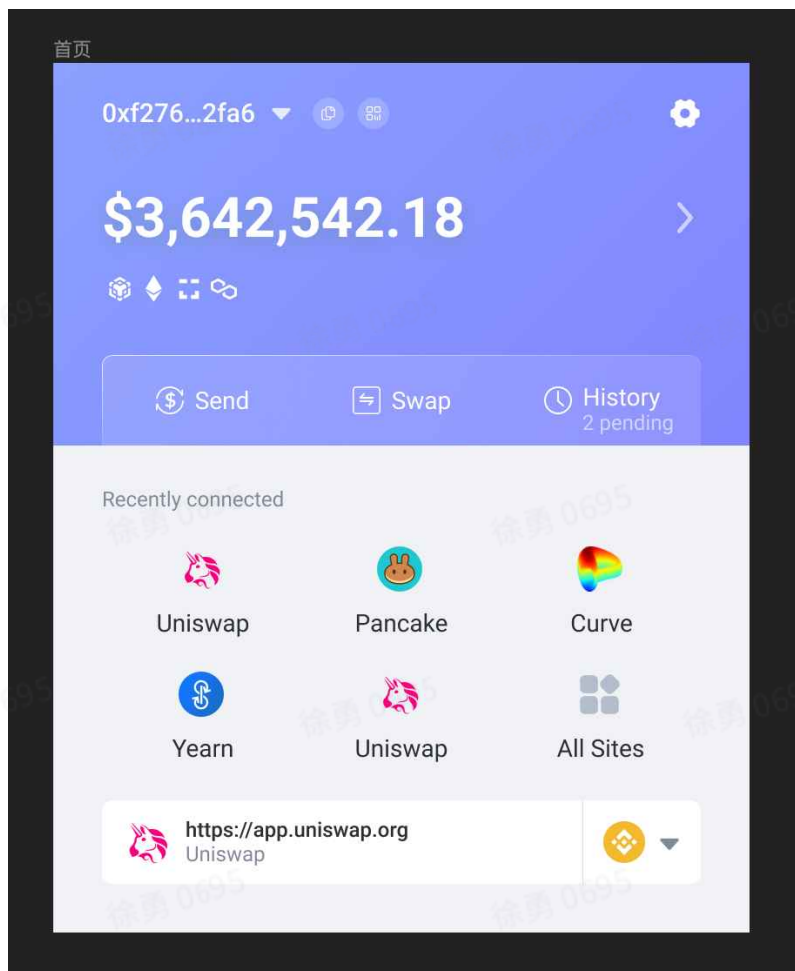
1. 点击连接硬件钱包，在浏览器 tab 页中打开连接页面；
2. 选择需要连接的硬件钱包品牌，调用对应钱包的 sdk 弹出钱包自己的连接界面
3. 用户在硬件钱包的界面中完成相应操作后，Rabby 的连接页面会拿到硬件钱包送过来的地址列表
4. 用户在 Rabby 的连接页面中选择任意数量的地址导入，并将第一个地址设为当前地址

## 添加观察地址

用户可以不导入私钥，直接将任意的地址添加到钱包中，作为当前地址试用和体验几乎所有的产品功能；只用当需要使用私钥进行签名时，用户的操作才会被阻断。

当钱包中存在至少一个任意类型的地址后，钱包的所有功能可以被正常使用。

## 首页



钱包首页可以划分为 菜单栏，资产概览，常用功能，最近使用 DApp，当前连接网站 几个模块

### 菜单栏

首页顶部的菜单栏展示以下内容：

1. 当前地址：用户当前选用的地址
  - a. 点击当前地址可以进行地址切换操作
  - b. 可以点击复制当前地址或者查看地址二维码
2. 设置按钮：点击后进入设置页面

## 资产概览

展示用户在所有链（无论是否处于启用状态）的资产总额，及资产分布在哪些链上（按资产数量从多到少排序）

点击后跳转到用户在 [debank.com](https://debank.com) 的 portfolio 页面。

## 常用功能

包括：

1. 转账：点击后跳转到 [debank.com](https://debank.com) 的转账功能页面（待开发）
2. swap：点击后跳转到 [debank.com](https://debank.com) 的 token swap 页面
3. 交易历史：点击后跳转到 [debank.com](https://debank.com) 的交易历史页面
  - a. 同时展示处于 pending pool 中的交易数量，包括当前账户在所有链上的 pending 中交易

## 最近使用 DApp

按照使用时间从新到旧展示钱包连接过的网站，点击后跳转至对应的网站。

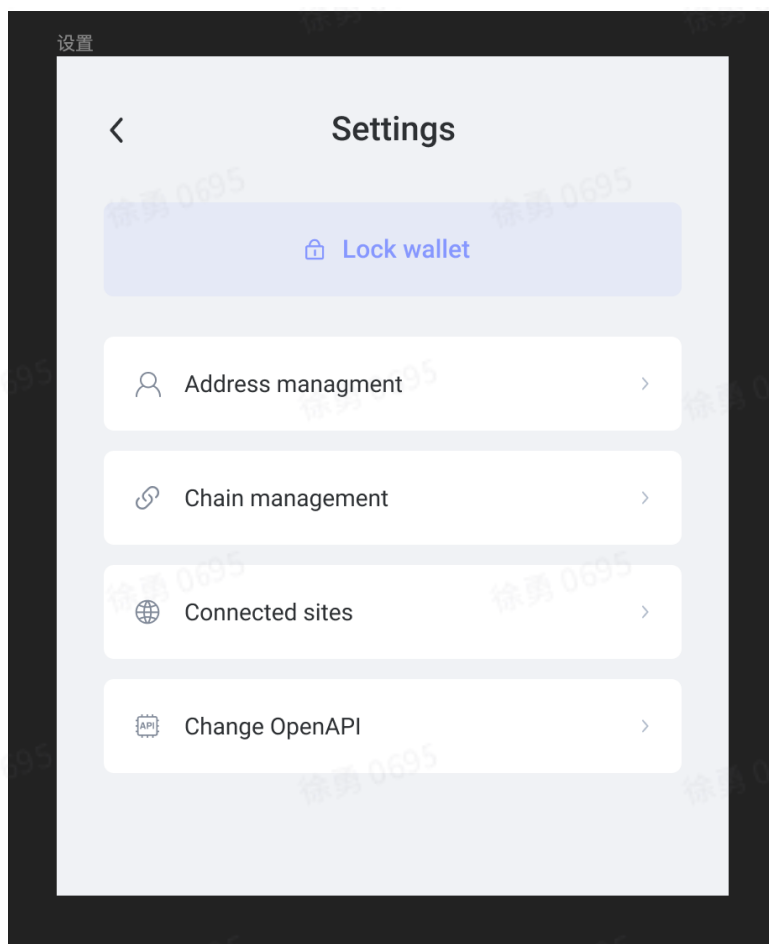
数量超过 6 个时，最后一个位置展示为「查看全部」，点击后跳转到设置页面中的网站管理页面。

## 当前连接网站

钱包当前连接中的网站显示在主页的最下方，展示信息包括网站 logo、名称（信息均取自网站的前端）、以及该网站当前连接在那条链上。可以点击切换网站连接的链。

该网站连接到哪一条链的信息保存在前端，用户再次打开该网站时，默认连接到上次选择的链上。

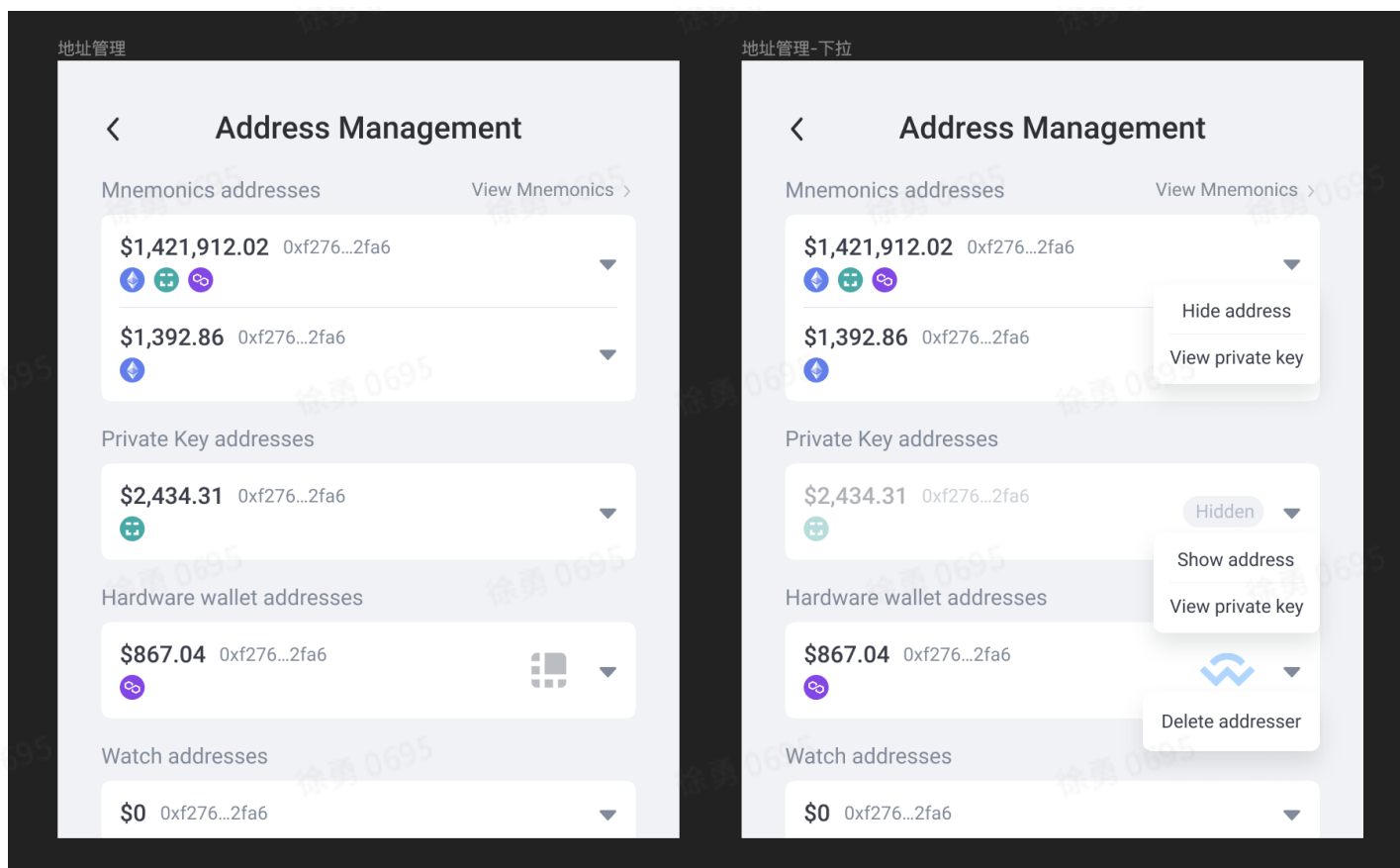
## 设置



设置页面包含以下功能或入口：

1. 锁定钱包：点击后锁定钱包
2. 地址管理入口
3. 链管理入口
4. 已连接网站管理入口
5. 修改 OpenAPI

## 地址管理



钱包中所有的地址按类型分组排列，每个类型的地址对应的管理操作如下：

1. 助记词地址

- a. 输入密码查看助记词
- b. 隐藏地址/显示地址：隐藏中的地址，将不会在首页的地址选择框内出现
- c. 输入密码查看私钥

2. 私钥地址

- a. 隐藏地址/显示地址
- b. 输入密码查看私钥

3. 硬件钱包地址

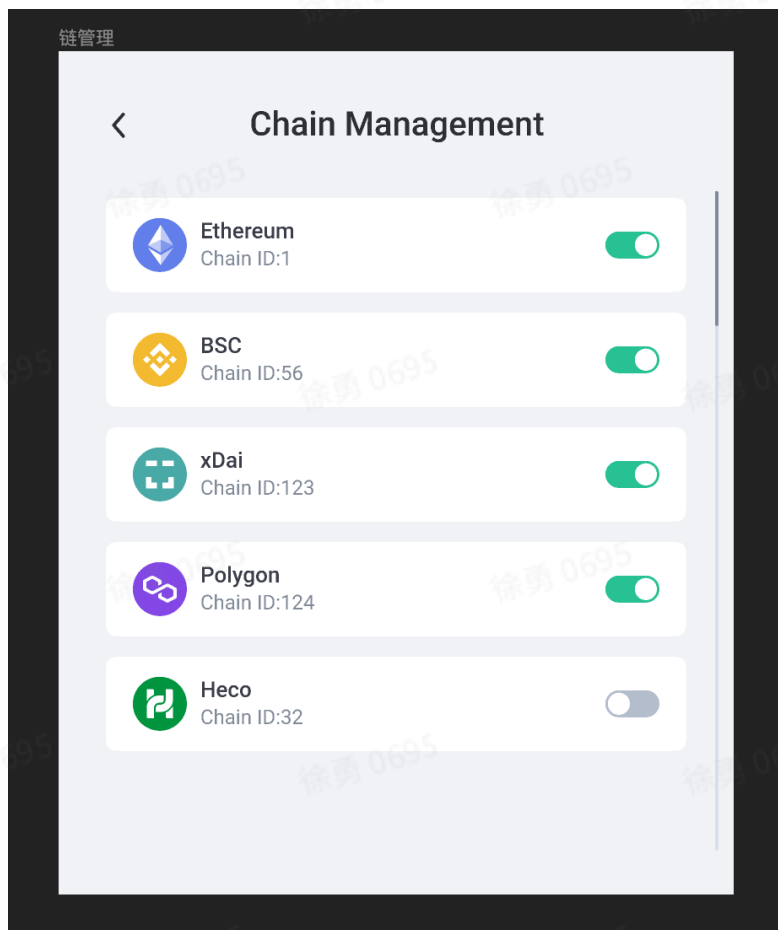
- a. 删除地址

4. 观察地址

- a. 删除地址

在钱包中有私钥的地址都不能被删除，只能隐藏；钱包中没有私钥的地址可以被删除

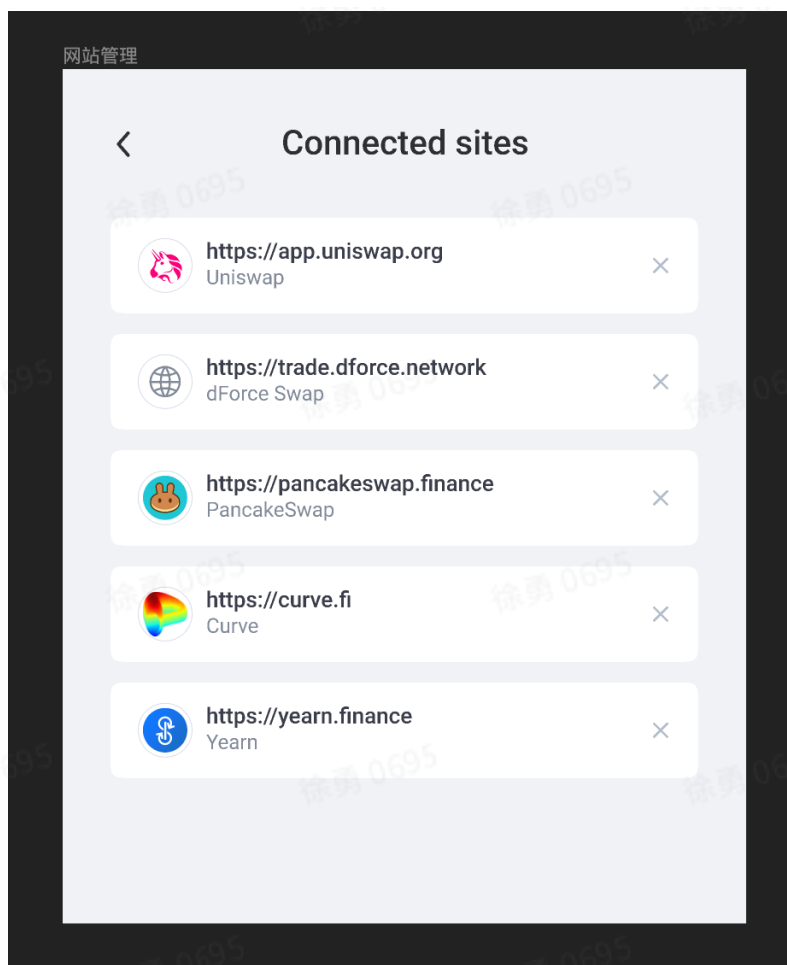
## 链管理



启用或者禁用特定的链，产品逻辑同前述的初始化流程

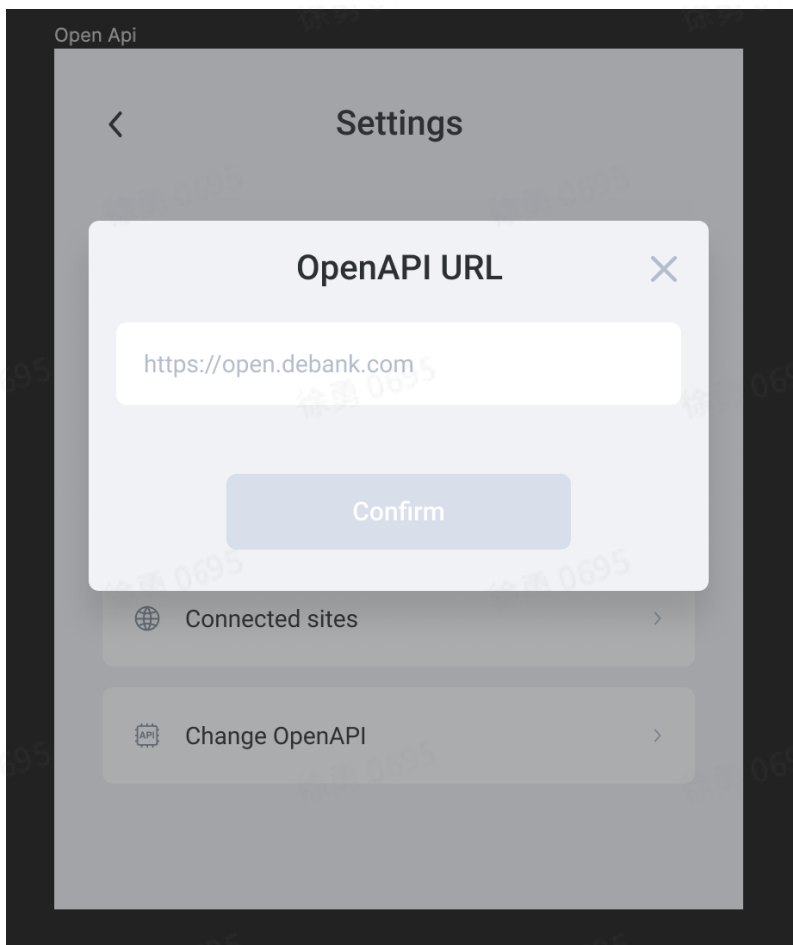
## 已连接网站的管理





该页面按照访问时间从新到旧排列展示所有钱包连接过的网站。可以删除选定的网站，删除后，用户再次访问该网站时需要重新发起连接流程。

## 修改 OpenAPI



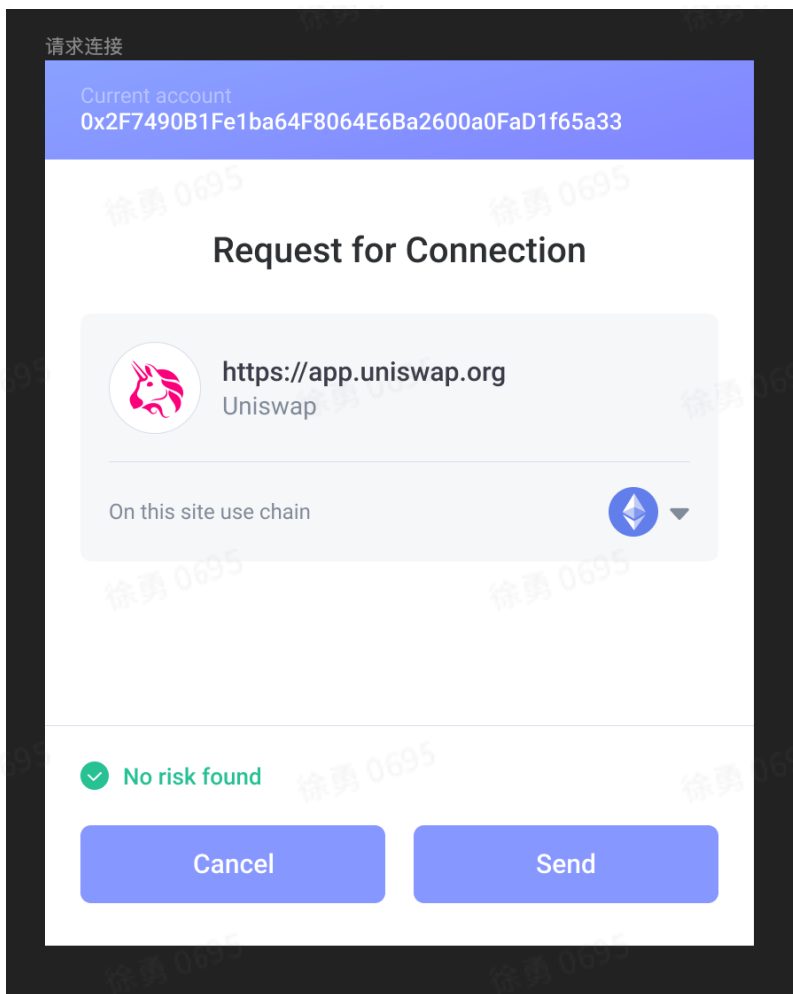
修改 OpenAPI 的 URL，默认为 DeBank 提供的 OpenAPI

## 网站交互

用户在 DApp 页面进行操作时，涉及到的同插件钱包之间的交互，主要包括以下几个：

1. 请求连接
2. 请求签名一段文本
3. 请求签名某条链上的一笔交易
  - a. 代币转账
  - b. 合约授权/取消授权
  - c. 取消交易
  - d. 其他的同合约进行交互的交易
4. 请求变更连接的链

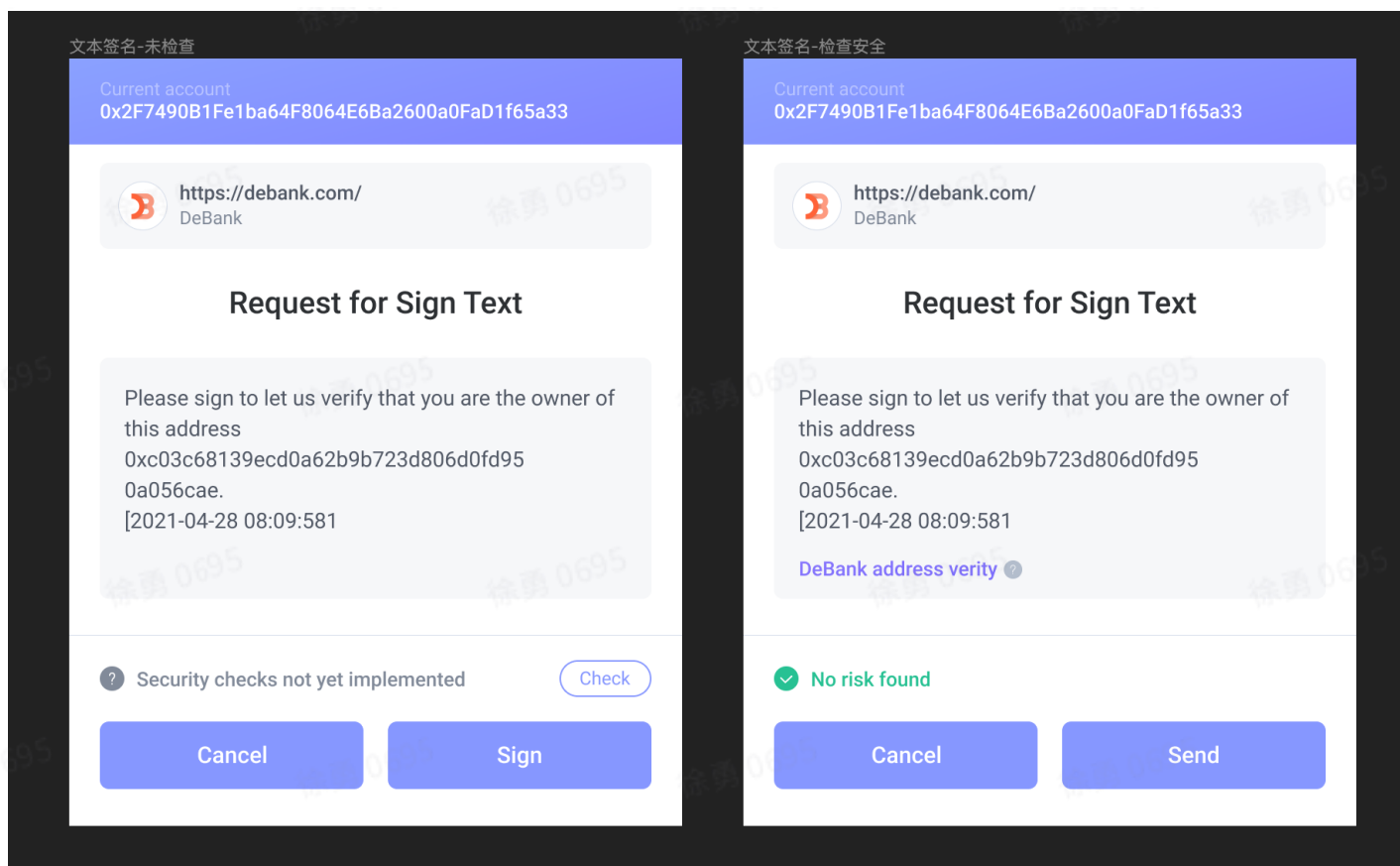
## 请求连接



网页发起连接请求，即要求获得用户当前的地址，用户可以在弹窗中选择是否同意。

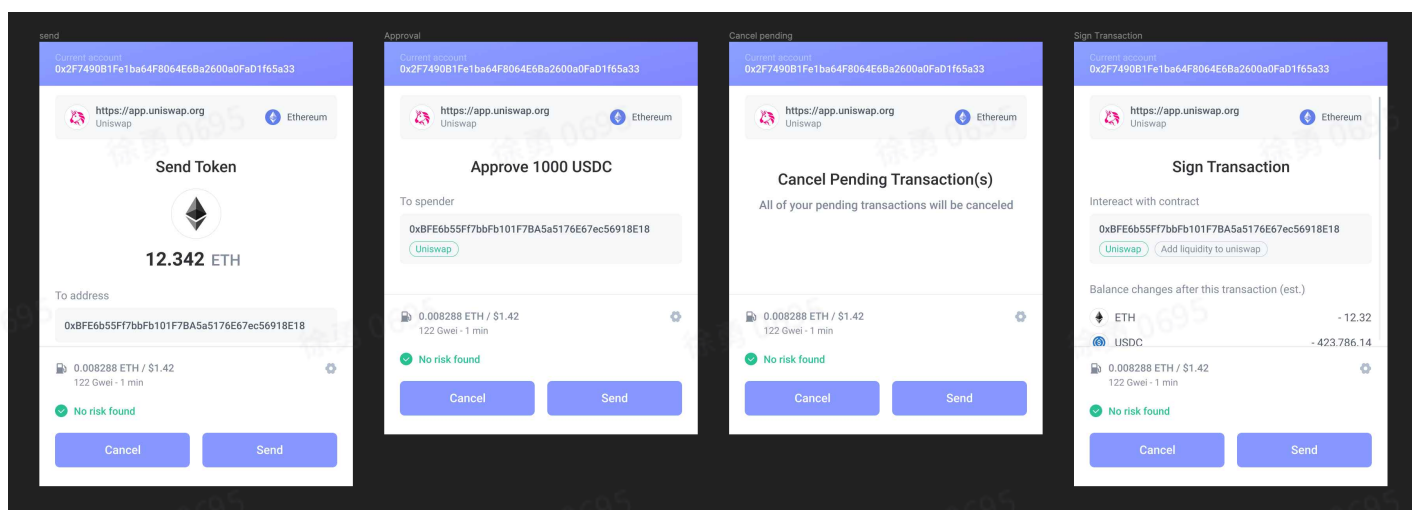
同时，可以设置该网站连接到的链。连接到的链的默认值由后端返回，用户可以自行修改。连接后，网页获得用户的当前地址，该网站连接到哪条链的信息前端保存。

## 请求签名文本



网页发起文本签名请求时，用户可以选择是否将需要签名的文本送到后端进行安全检查。如果用户选择进行安全检查，后端将会返回安全检查的结果、以及对文本的描述性解释。

## 请求签名交易



网页发起交易签名请求时，钱包弹窗又以下几个部分组成：

1. 交易描述信息
2. gas 设置模块

### 3. 安全检查信息

### 4. 签名操作模块

## 交易描述

描述一笔交易的信息包括以下几个部分：

1. 交易需要由哪个账号签名：用户当前在钱包中选择的地址
2. 交易由谁构造发起：发起交易的网站信息
3. 交易的具体内容是什么：根据交易的类型，这一信息的描述方式各有不同
  - a. 代币转账：将多少什么 token 转给哪个地址
  - b. 合约授权：将多少什么 token 授权给哪个地址
  - c. 取消合约授权：针对什么 token 取消对哪个地址的授权
  - d. 合约交互：同哪个合约地址进行交互，进行什么样的交互（调用的函数名），完成交易后，我的资产会发生什么变化

## gas 设置

用户在设置 gas price 时，钱包提供以下信息帮助用户进行决策：

1. 使用某一价格时，预估的交易完成时间
2. pending pool 中高于某一价格的交易数量有多少

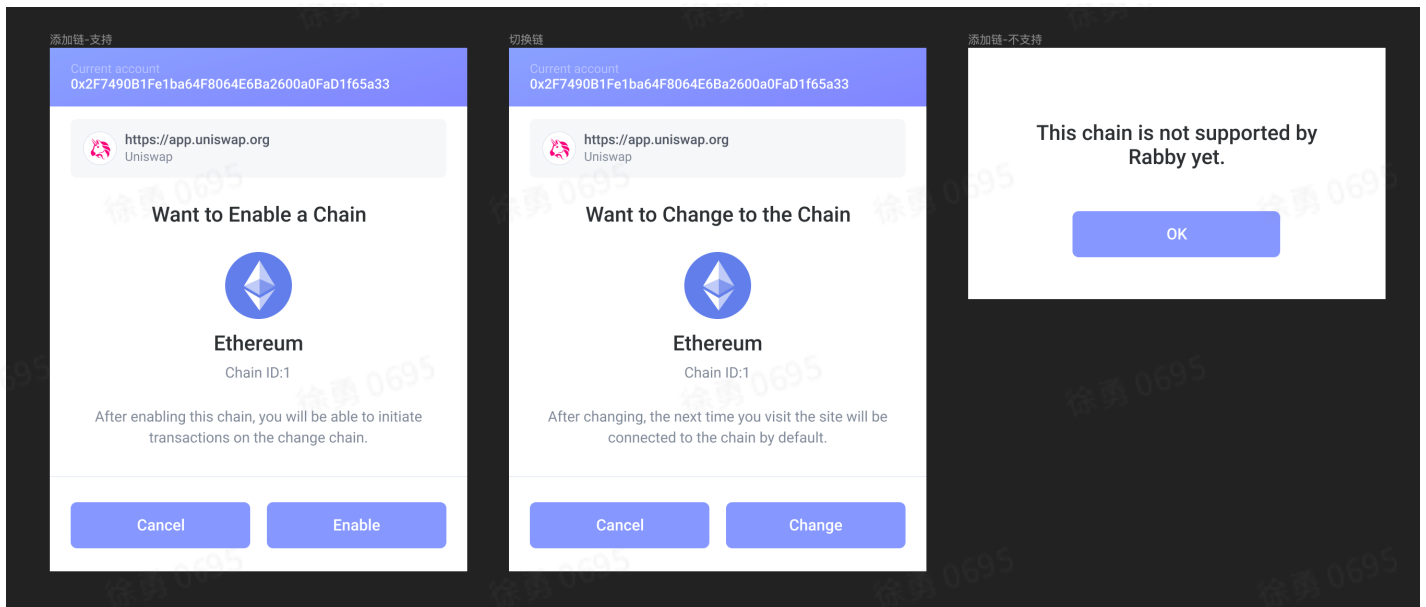
## 安全检查信息

展示安全检查的结果，安全检查的详细逻辑后述。

## 签名操作模块

拒绝签名或者同意签名。具体的交互逻辑同安全检查结果相关，详细逻辑后述。

## 请求变更链



网页可以发起请求，变更当前网页所连接到的链。这类请求可以分为以下几种情况：

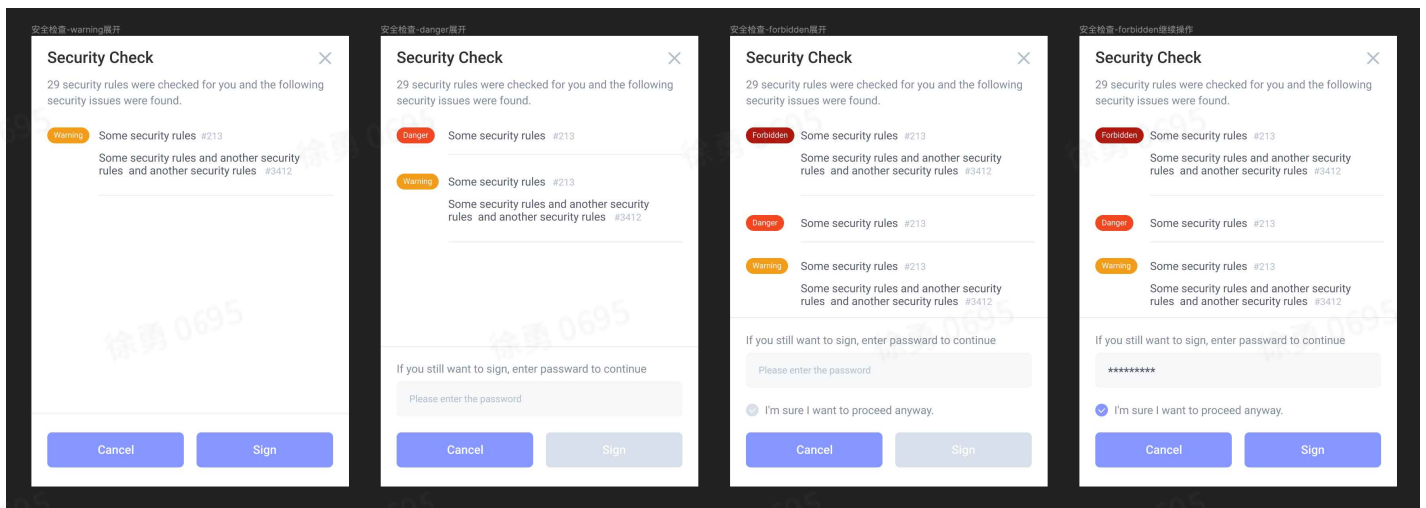
- 1. 请求变更到的链，钱包支持，但用户未启用：用户可以选择是否启用这条链，并切换至这条链
- 2. 请求变更到的链，钱包支持，且用户已启用：用户可以选择是否切换
- 3. 请求变更到的链，钱包不支持：提醒用户，该链尚未支持

## 安全检查

交易签名请求会自动送到后端进行安全检查，文本签名请求由用户自行决定是否送到后端进行安全检查。

送到后端的信息按其类型进入不同的安全规则集进行检查，所有命中的规则（fail 的）返回给插件。

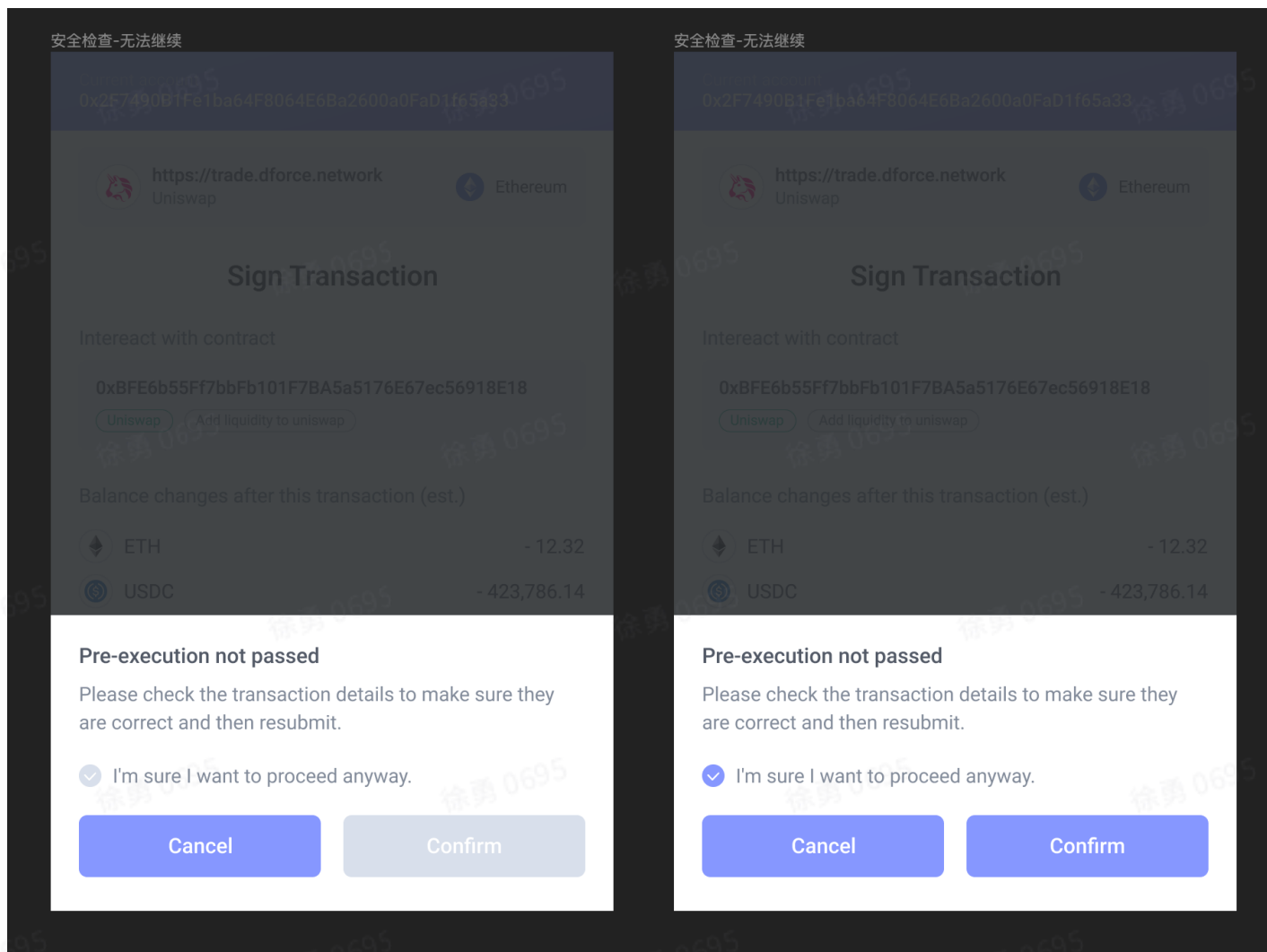
每一条安全规则按其严重程度分为 warning、danger、forbidden 三个级别。针对一次检查，所有命中的规则中安全级别最高的一条会作为该次检查的最终结果。



不同级别的安全检查结果，对应的用户交互逻辑如下：

1. no risk found：未检测的风险，用户可以直接签名
2. warning：用户需要查看所有命中的规则后，再进行签名
3. danger：用户需要查看所有命中的规则，输入钱包的解锁密码，再进行签名
4. forbidden：用户需要查看所有命中的规则，输入钱包的解锁密码，勾选免责声明，再进行签名

另外，如果交易预执行失败，用户需要勾选免责声明，再进行签名



## 推送交易

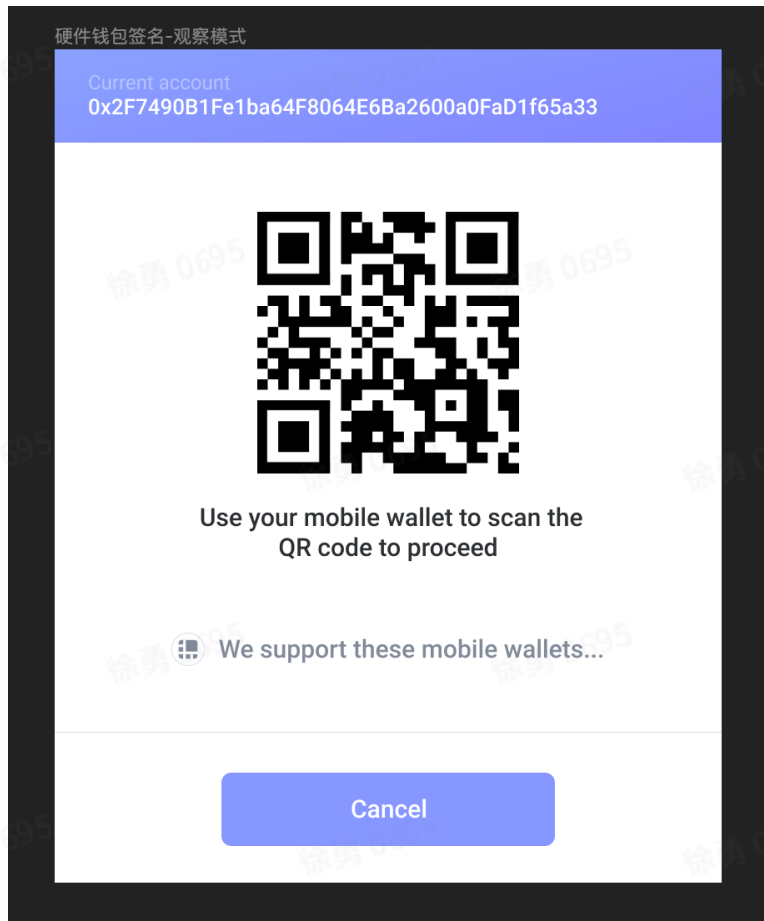
### 助记词地址/私钥地址

如果用户的当前地址是助记词地址或者私钥地址，用户可以在交易签名页面，直接点击签名，钱包将签名后的交易传给后端推送到链上；

## 硬件钱包地址

对于硬件钱包地址，用户在交易签名页面点击签名后，进入硬件钱包的签名流程，插件拿到硬件钱包的签名结果后传给后端推送到链上；

## 观察地址



对于观察地址，用户在交易签名页面点击签名后，插件弹出一个二维码页面，用户可以使用支持该功能的手机钱包扫码，在手机钱包中完成签名，后端拿到手机钱包的签名结果推送到链上，同时将该消息告诉插件钱包，以更新插件钱包中的交易状态。