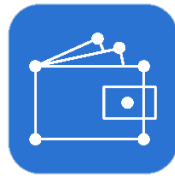


Keycrux 使用说明



Keycrux 魂器钱包

目录

Keycrux 使用说明.....	1
Keycrux 魂器钱包.....	1
1. 安装需求.....	3
1.1. 操作系统.....	3
1.2. 权限.....	3
2. 使用说明.....	3
2.1. 分存密钥.....	4
2.2. 找回密钥.....	8

1. 安装需求

1.1. 操作系统

应用需要 **android 7.0** 以上系统，推荐使用 **android 10.0**。

1.2. 权限

安装后应用需要申请以下权限，请在弹窗时放行：

权限	说明
手机相册访问	用于在相册中写入和读取分存图
外部存储写入	用于在手机存储中额外存储一份分存图
摄像头调用	用于扫码识别分存图

2. 使用说明

应用需要由用户**手动输入**账户的**密钥与地址**，使用我们开发的算法，在服务器上计算出分存图之后，将图片保存在用户的手机上。随后用户可以自行将图片分存到合适的载体或介质上（电子设备或纸张等）。

当用户需要找回自己的密钥时，可以收集之前分开保存的分存图片，扫码采集信息，当获取到足够的数量时，即可还原出原本的密钥

启动应用后，在短暂的预加载界面结束后，您将看到以下界面：

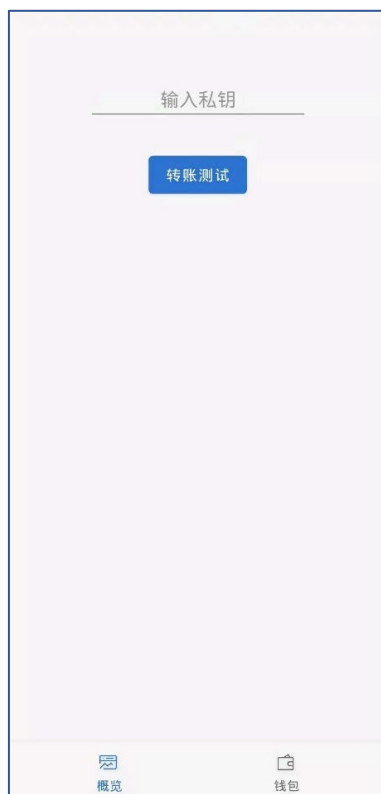


图 1 首页

2.1. 分存密钥



在图 1 所示的首页点击右下角  钱包按钮，进入 **账户管理** 页面，如图 2。如果您之前没有安装过本应用，这里将会显示空白的账户列表，您可以点击下部的  加号按钮新建一个账户。点击后您将会跳转到 **新建账户** 页面。



图 2 账户管理页

在 **新建账户** 页面（图 3），您可以输入自己的私钥与地址，并用合适的账户名称来标记这个账户。请放心，您的私钥不会被任何设备存储，它是绝对安全的。

注意：私钥的填写有格式要求，必须为 **64 个 16 进制字符**，可以带有 0x 前缀，如 **345890abef67812341234567890abcdef567890ab1567890abcfcd90abcdef**。账户类型应当为 BTC，ETH，XRP，USDT 等常见数字货币的**大写缩写**。



图 3 新建账户页面

在填入密钥和账户信息之后，您可以在下方的门限数和分存数中选取适合您的组合。

- **分存数 K** 表示您的密钥将被分割到多少份，可以在 3 到 5 之间任意选择。
- **门限数 N** 表示您的密钥至少需要多少份才能还原。门限数可以在 2 到 5 之间选择，但是必须小于分存数。当分存数为 5 时，门限数只能为 2 或 3。

这里的表格列出了可选的组合。

门限数 分存数	2	3	4	5
2	否	否	否	否
3	是	是	否	否
4	是	是	是	否
5	是	是	否	否

表 1 可用的 K-N 组合

在输入合适的 (K, N) 之后，点击下方的箭头按钮，等待 3 到 8 秒之后（请不要离开当前页面），应用将会自动从当前的 **新建账户** 页面返回 **账户列表** 界面，此时，您的手机相册中将会出现一个名叫 VisualWallet 的相册，它存储了您的分存图。此外，手机的 /DCIM/VisualWallet 文件夹下也备份了对应的分存图片。

TIPS:

- 如果您的账户页面仍然看不到账户，请点击一次左下角的概览页面再点回钱包页面以刷新列表。
- 部分安卓系统的最近图片功能会显示重复的两份图片，建议您前往 **手机相册 -- 其他相册 -- VisualWallet** 以访问刚刚存储的分存图。

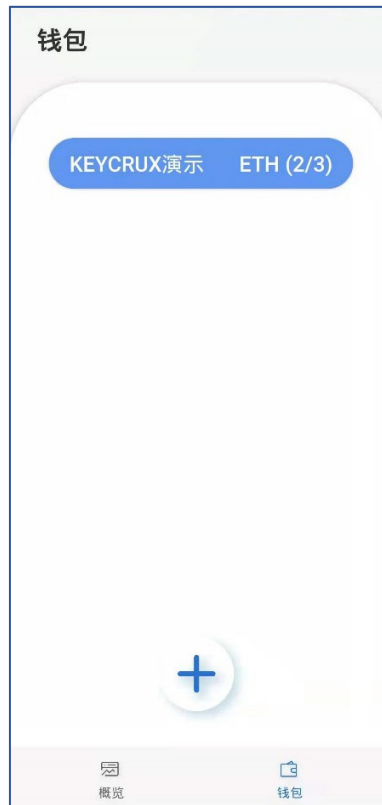


图 4 添加账户后的账户列表

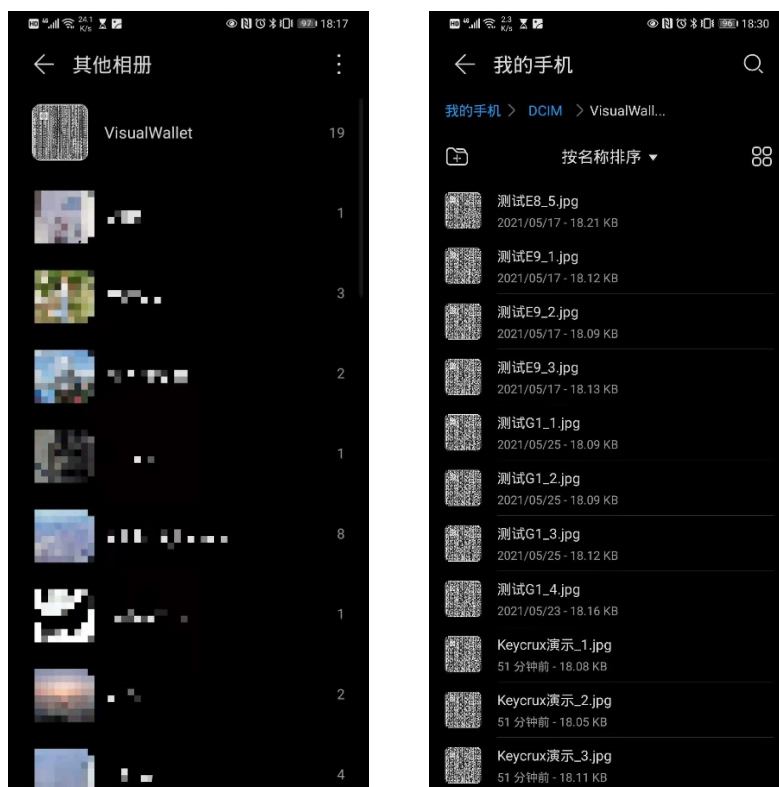


图 5 Keycrux 分存图所在的相册 和 额外备份的文件

账户密钥分存流程到此结束，您可以把刚刚的图片通过相册分享等方式分存到其他设备或者打印出来。随后的流程将会演示如何还原您原有的密钥。

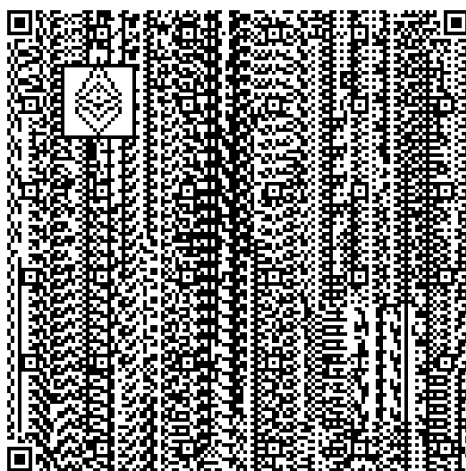


图 6 分存图示例

2.2. 找回密钥

当您已经在自己手机的 keycrux app 上创建了账户，并且获取了足够的分存图（大于等于门限值）。您可以从图 2 所示的 **账户列表** 中，点击对应的账户，进入到图 7 所示的 **账户详情** 页面。

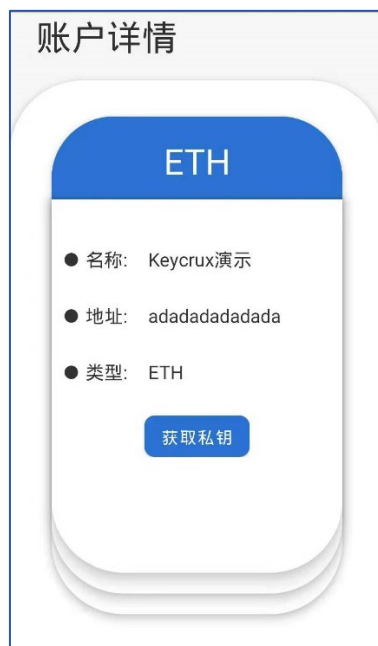


图 7 账户详情页面

点击获取私钥按钮进入 **密钥收集** 界面，如图 8。

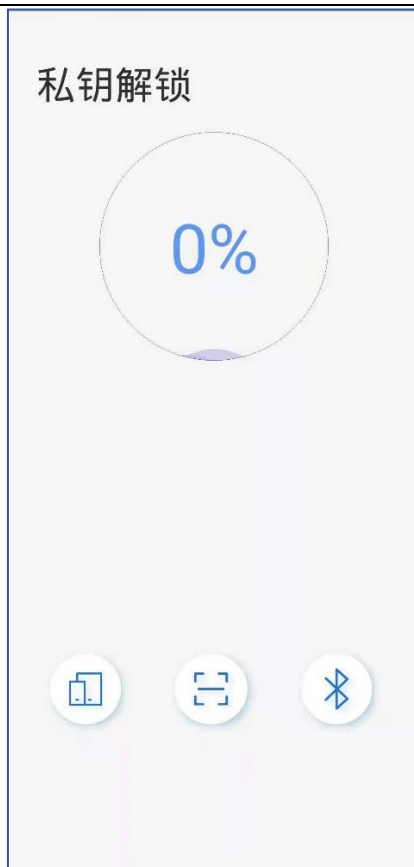





图 8 密钥收集

在密钥收集界面，点击下方的  本地选取按钮，可以从手机相册选取图片。点击下方的  扫码按钮可以扫描打印出来的分存码。点击右下角的  蓝牙按钮可以从蓝牙设备获取图片，**但是目前未实现，目前该按钮是无效的。**

每次扫描到正确的分存码时，进度球将会显示目前的收集进度，如图 9，如果扫描到错误的二维码或者扫码重复，会显示对应的错误信息。



图 9 密钥收集中

当收集到足够的分存图时，点击右图下部的放大镜图标，可以将结果进行处理，获取原本的密钥。



图 10 私钥找回成功

应用有一套离线的分存图校验机制。如果您中途扫描到了重复的分存图，应用将会检测出来并弹窗。如果您扫描到了被篡改或不是分存图的二维码，应用将亮警示标记，您可以继续扫码直到获得足够的分存图。



图 11 分存图校验