readme

倪浚桐、曹玉娟

202022161224、202000130060

Lab8-option3 hs-airdrop

macOS Monterey 12.0.1

Pycharm 11.0.12 x86-64

Python 3.9.9

Node.js v17.0.1.

1.获得Handshake Airdrop前提

1.拥有 github 账号

2.在2019 年 2 月份的时候拥有至少 16 个 followers

3.当时的私钥还保存着

2.领取步骤

1.下载项目

git clone https://github.com/handshake-org/hs-airdrop.git

2.安装依赖

cd hs-airdrop && npm install

3.验证私钥并获取领取 key

/bin/hs-airdrop <SSH私钥路径> < HNS 钱包地址> <给矿工的费用>

HNS钱包地址的获取可以去官方教程中Step4中点击Click to show your Handshake wallet address来获得

4.将生成的一串 base64 字符串粘贴到网页上提交，硬币就会出现在钱包里

3.为什么需要私钥

从密码学角度，之所以能领到这些 HNS 币，是因为 Handshake 团队抓取了 GitHub 上 Top 250,000 的开发者的公钥信息，并且把这些公钥经过某种算法处理放到了 HNS 的区块链上。通过私钥可以证明这个公钥是你的，证明你可以拿这些 HNS 币。用私钥生成一个密码学上的证明，放到 HNS 区块链上，这样网络就会承认你拥有H这些 HNS 币了

4.hs-airdrop的使用

根据 Wikipedia，数字货币领域的空投(Airdrop)是这样定义的：

> 区块链领域的空投是一种将数字货币通过区块链技术大规模分发到一些已有的数字货币，比如以太币、比特币、EOS.IO 钱包地址上的技术。空投在区块链领域亦视作一种提升一个产品概念影响力的市场策略。在 Facebook 等社交媒体拒绝刊登数字货币广告后，空投在区块链的营销中已变得越发重要。

Program已经提供了一个SSH密钥对，Namebase已经提前通过爬虫获取了**部分符合条件的用户**的SSH公钥，现在这些符合条件的用户可以通过用自己的SSH私钥去验证自己是否属于这一部分符合条件的用户。那么，hs-airdrop就是用来让我们在本地对SSH私钥进行验证的一个工具。如果验证成功，则hs-airdrop会返回一个base64编码的bytes，我们把这个复制到网站上进行验证即可兑换Namebase发放的**4,246.994314 HNS**币。

Handshake 空投是一棵**默克尔树**，其根被添加到 Handshake 协议的共识规则中。 这允许合格私钥的所有者在链上发布签名的默克尔证明以兑换他们的空投。 如果此工具在默克尔树中未找到您的私钥，则我们没有资格领取 HNS 币。 关于隐私，hs-airdrop为每个接收者生成了一个随机数，用这个随机数为存储在默克尔树的公钥加密。

那我们可以尝试着兑换（显然我们不满足条件）

（1）用homebrew下载node.js。因为hs-airdrop基于node.js编写，版本要求Node.js >= 8.0.0

```
% brew install node
```

（2）用nmp下载hs-airdrop的环境依赖。nmp是随同Node.js一起安装的包管理工具，可以下载并安装别人编写的第三方包到本地使用。

```
% npm install
```

```
#命令行给出npm干的事，新添加了8个包
added 8 packages, and audited 9 packages in 1m

found 0 vulnerabilities
npm notice
npm notice New patch version of npm available! 8.1.0 -> 8.1.4
npm notice Changelog: https://github.com/npm/cli/releases/tag/v8.1.4
npm notice Run npm install -g npm@8.1.4 to update!
npm notice
```

（3）找到我们需要的SSH私钥。这个就存放在`hs-airdrop-ssh-key`文件夹的`id_rsa`文件中。

（4）将SSH私钥提交给hs-airdrop进行验证。在这个过程中，SSH私钥不会离开我们的电脑，这保证了私钥的安全性；在`<address>`位置我任意输了一个地址，因为我自己尝试生成Handshake钱包地址时浏览器会报错，需要钱包进行实名验证。

```
hs-airdrop % ./bin/hs-airdrop --bare ./hs-airdrop-ssh-key/id_rsa
d99a97646054ad623b1243755f0a543fbaacf304 0.1
```

（5）报错。应该是钱包地址不对。

```
Error: Encoding failed.
    at Object.decode (/Users/lingfeng/hs-airdrop/node_modules/bcrypto/lib/native/bech32.js:52:18)
    at parseAddress (/Users/lingfeng/hs-airdrop/bin/hs-airdrop:800:39)
    at parseArgs (/Users/lingfeng/hs-airdrop/bin/hs-airdrop:749:37)
    at processTicksAndRejections (node:internal/process/task_queues:96:5)
    at async main (/Users/lingfeng/hs-airdrop/bin/hs-airdrop:755:19)
```

5.结语

通过本次实验，我们了解了空投的概念，如何薅资本主义的羊毛