隐私交易穿透监管平台
产品使用手册

北京众享比特科技有限公司

1. 产品简介

1.1 隐私交易穿透监管平台

隐私交易穿透监管平台利用零知识证明技术，在交易的关键信息为加密的情况下，提供对匿名交易可审计、可监管的解决方案。零知识证明是用户不向审计员和审计平台提供任何匿名信息的情况下，离线生成证明文件，审计员实现对匿名交易的审计和监管。隐私交易穿透监管平台在保障数据隐私前提下，对链上交易进行实时高效的穿透式合规审计，支持对交易金额的“零知识”审计，支持对恶意匿名用户的的去中心化身份追踪及撤销。

1.2 产品优势

传统区块链交易中，用公钥地址来表示交易方，对交易信息进行加密，但交易方的公钥地址等公开信息，有泄露交易隐私的风险，丧失交易的匿名性。

完全匿名性：隐私交穿透监管平台将交易方的关键信息进行加密处理，比如公钥地址、交易金额，除了交易方外任何人无法解密，实现交易的完全匿名化。

可审计：隐私交易监管平台不泄漏用户隐私数据对前提下，对交易进行零知识审计，保证了交易的匿名性和用户的隐私。

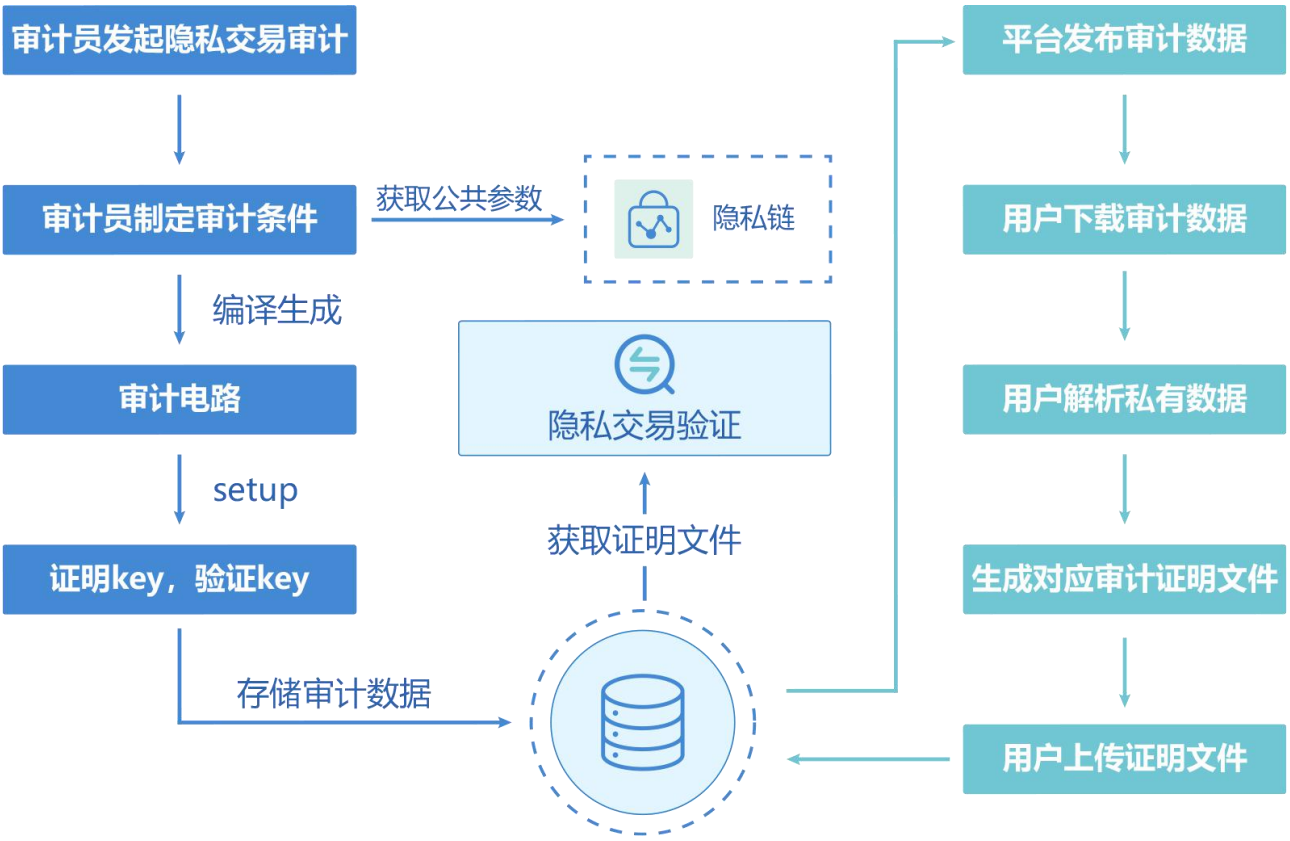
可监管：第三方监管平台可以实现对匿名交易的监管。

1.3 应用场景

隐私交易穿透监管平台在不泄露用户隐私数据的前提下，利用零知识证明技术，验证隐私交易是否符合审计条件，实现了对隐私交易的审计和监管，满足了第三方监管机构的监管需求。

2. 产品说明

2.1 系统架构



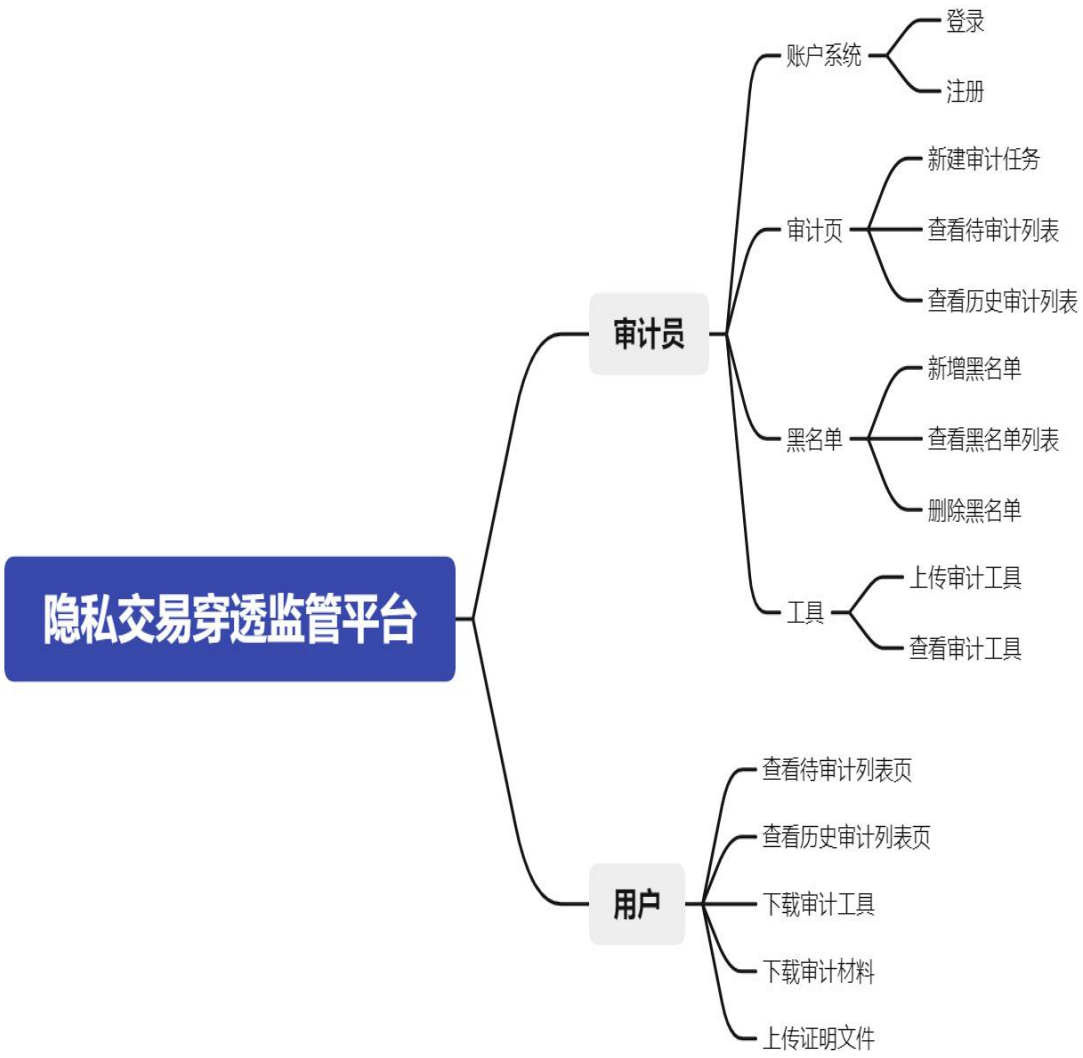
2.2 用户角色

审计员：审计员作为第三方监管机构，获取相关匿名交易的公开数据，在审计平台上，发起审计任务。

用户：作为交易方，用户在不透露交易匿名隐私数据的前提下，离线生成证明文件，上传证明文件到审计平台。

审计平台：平台方没有解密匿名交易的密钥， 无法得知匿名交易的隐私信息，但是通过零知识证明技术，可以验证交易是否符合审计条件。

2.3 功能概览

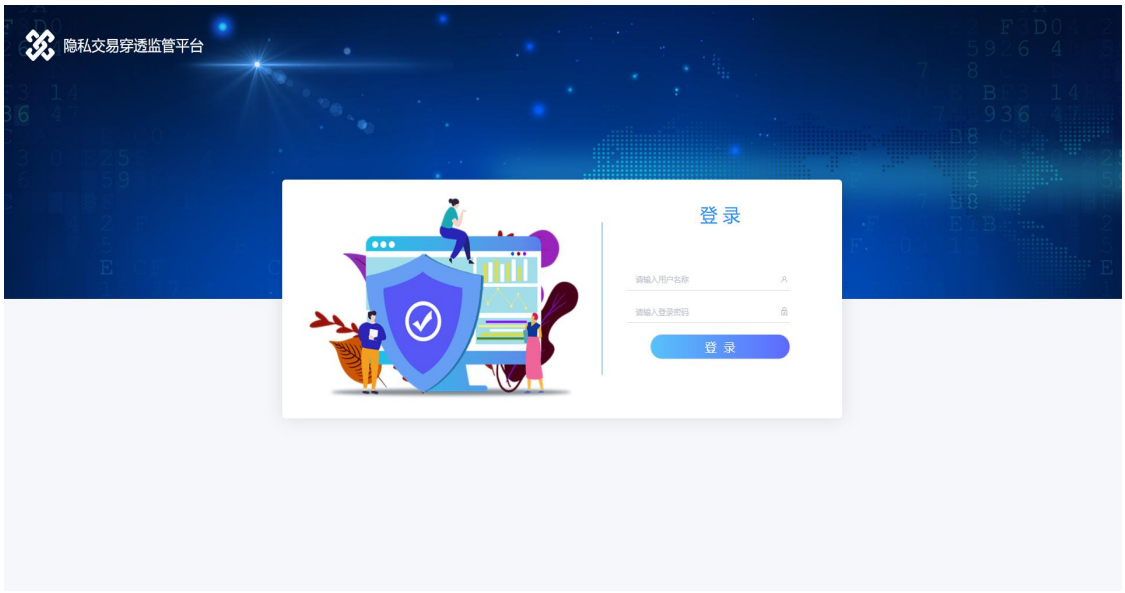

隐私交易穿透监管平台
审计员
账户系统
登录
注册
审计页
新建审计任务
查看待审计列表
查看历史审计列表
黑名单
新增黑名单
查看黑名单列表
删除黑名单
工具
上传审计工具
查看审计工具
用户
查看待审计列表页
查看历史审计列表页
下载审计工具
下载审计材料
上传证明文件

3. 操作指南

3.1 审计员端

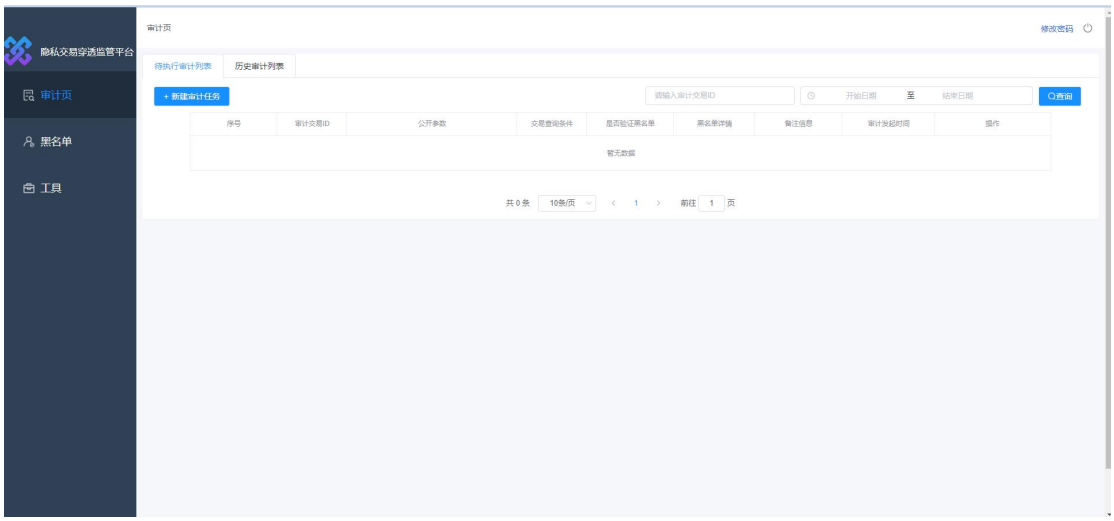
3.1.1 登录

审计员在浏览器地址栏中输入地址，打开登陆界面：

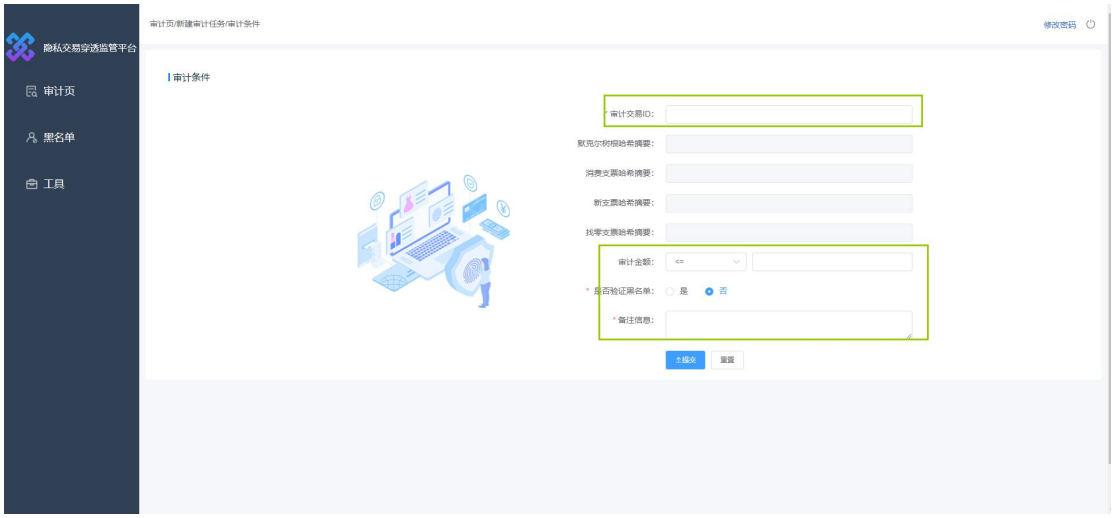


输入管理员用户名、密码，点击“登录”按钮登录系统。

3.1.2 新建审计任务



审计员在审计页点击新建审计任务，进入新建任务页面。



审计员在新建审计页，输入审计交易 ID。审计员获取审计交易 ID 的方式如下：

1. 审计员在在桌面新建一个文件夹，将生成交易的软件 zkchain 和配置文件拖到文件夹里；

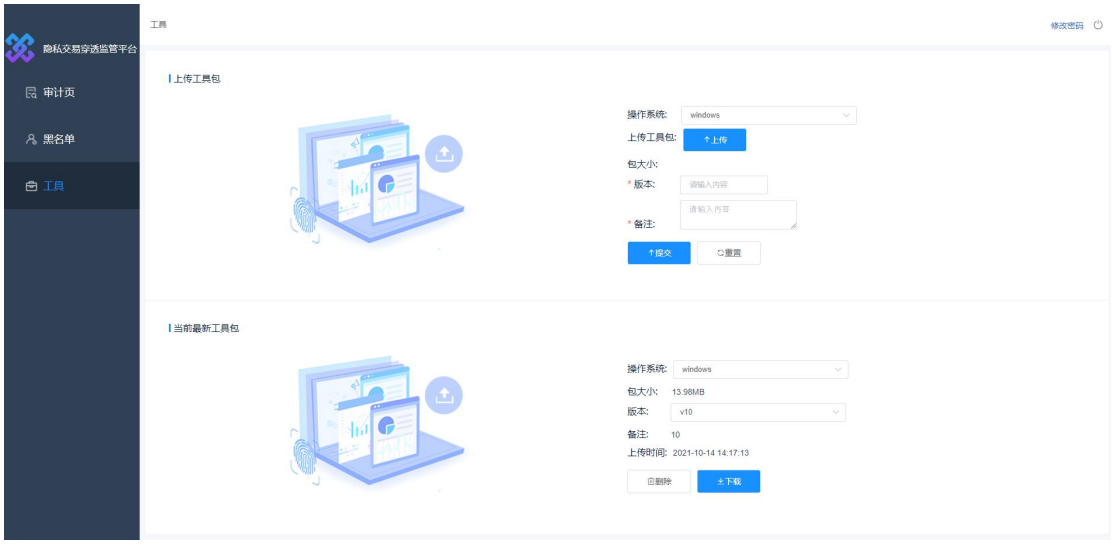
2. 在第一步新建的文件夹目录下运行命令 ./zkchain -func getlist 查看交易 ID 列表，得到待审计交易 ID；

```
PS C:\Users\peersafe\Desktop\audit> .\zkchain.exe
zkchain.go:34 15:18:12.497 [zkchain] DEBU : Usage : ./zkchain -configPath=configFilePath
user.go:102 15:18:12.589 [zkchain] DEBU : default user already exist
zkchain.go:59 15:18:12.591 [zkchain] DEBU : ---zkchain cmd --------------
zkchain.go:60 15:18:12.594 [zkchain] DEBU :     eg:   ./zkchain -func help
zkchain.go:61 15:18:12.596 [zkchain] DEBU :     eg:   ./zkchain -func maketx -value 1
zkchain.go:62 15:18:12.596 [zkchain] DEBU :     eg:   ./zkchain -func getlist
zkchain.go:63 15:18:12.596 [zkchain] DEBU :     eg:   ./zkchain -func getdata -txid xxxx
PS C:\Users\peersafe\Desktop\audit> ./zkchain -func getlist
zkchain.go:34 15:18:23.765 [zkchain] DEBU : Usage : ./zkchain -configPath=configFilePath
user.go:102 15:18:23.868 [zkchain] DEBU : default user already exist
-----THE TX ID LIST-----
00000000000000000000000000000000
uhujza4jlh5x1gm7bppvy7so79aj71o2
sn6m3kfp9r0qu6o13j7ud7va0avp6f9n
98330m442byj6nv1uymclu0jbn7p4tjt
m02rnommfd7pw3cepa5uad8o26sshb11
yzubttw91da1bk2kfesqu5he2pxjhc28
6wzyukt2x7wxo1tkkrkmdjyyx6wp088m
sdmzpr9vu49mddxgwrnjf7b47r69s2mx
jfqxudyij61akru95p3w16fdbely01y4
54x7jnmcegmnn8jtkjowo9pvga0v2915
cmg9v3fucqfu7tdsr5swi651a9n4jzzx
8ey8cm1wziaguh0o2c03gengkbybaox9
------------------------
PS C:\Users\peersafe\Desktop\audit>
```

3. 将待审计交易 ID 复制，粘贴到如上图所示的审计交易 ID 中（交易 ID 下面的摘要信息会根据当前交易 ID 查询自动填充，不可修改），输入想要验证的交易查询条件并选择是否验证黑名单，填写备注信息后点击提交。

4. 当审计员生成新的审计任务后，平台会将该审计任务的相关信息打包压缩成审计材料包，发布到平台上的待审计任务列表中。

3.1.3 上传工具



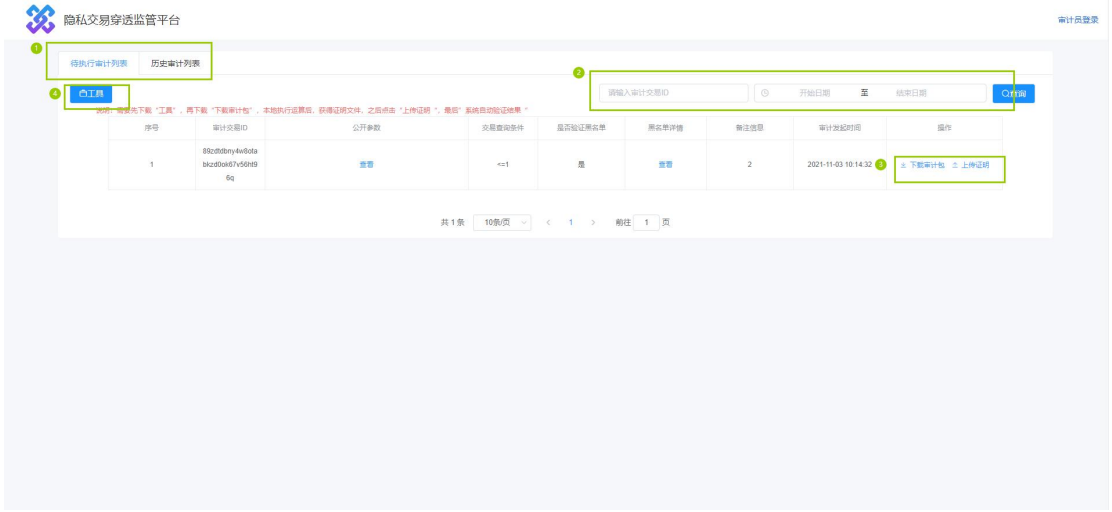
审计员上传工具包：

1. 选择要上传的工具包平台；
2. 填写版本号和备注信息；
3. 点击提交。

3.2 用户端

3.2.1 下载工具

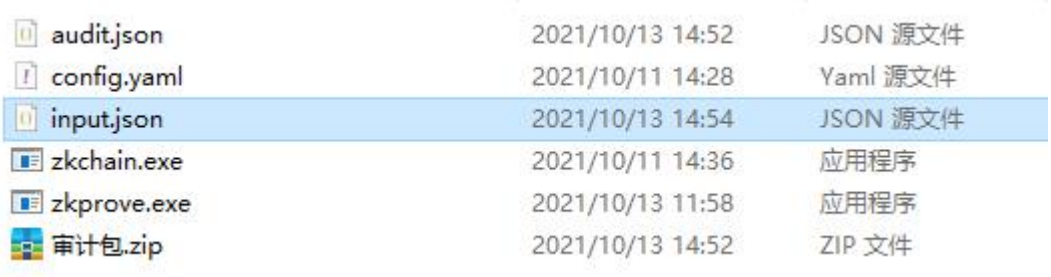
用户输入隐私交易穿透监管平台网址，进入隐私交易穿透监管平台用户端，如图：



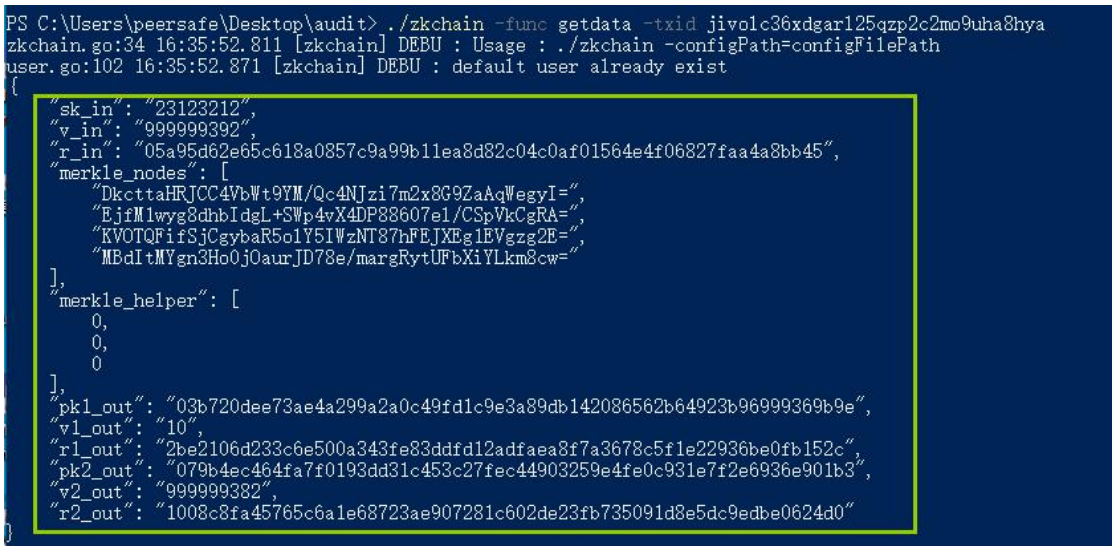
1. 用户查看待审计列表，看到跟自己相关的交易 ID 时，下载要审计的审计包；
2. 点击工具，选择相应的操作系统和版本，点击下载；

3.2.2 生成证明文件

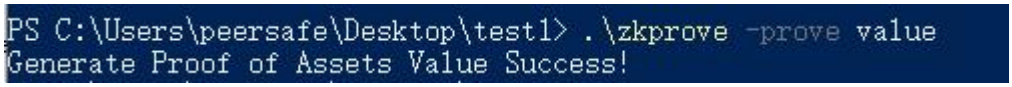
1. 将下载的工具 zkprove，生成交易用的工具 zkchain 和下载的审计包放入一个文件夹中，并将审计包解压到当前文件夹。

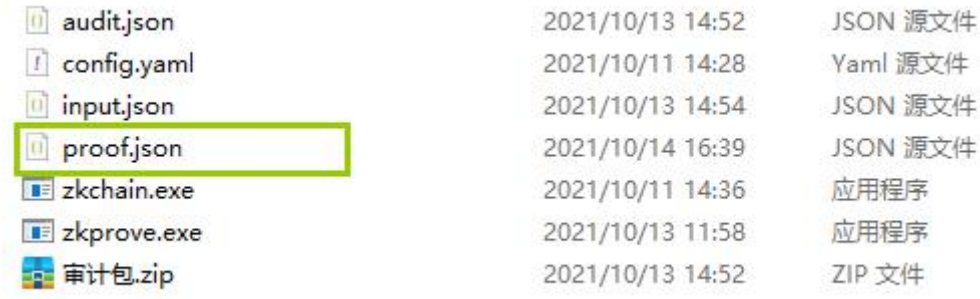


2. 在当前目录执行命令./zkchain -func getdata -txid xxxx（xxxx 替换为下载的审计包的 ID），将生成的结果拷贝到解压得到的 input.json 中；

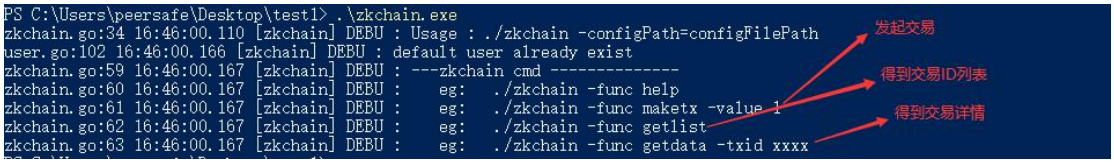


3. 继续执行命令.\zkprove -prove xxx（xxx 为校验不同情况时对应的参数），生成一个证明文件 proof.json；





注：运行对应的工具包即可出现相应的命令提示。



3.2.3 上传证明文件

用户点击隐私交易监管平台中待审计任务上传证明，将生成的 proof.json 上传，系统即可自动验证结果。

4. 常见问题

无