

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
	1.1 隐私交易穿透监管平台	1
	1.2 产品优势	1
	1.3 应用场景	1
2.	产品说明	2
	2.1 系统架构	2
	2.2 用户角色	. 2
	2.3 功能概览	3
3.	操作指南	4
	3.1 审计员端	.4
	3.1.1 登录	.4
	3.1.2 新建审计任务	.4
	3.1.3 上传工具	.6
	3.2 用户端	6
	3.2.1 下载工具	.6
	3.2.2 生成证明文件	. 7
	3.2.3 上传证明文件	. 8
4.	常见问题	9



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。

1



2. 产品说明



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





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

\$\$	审计页										修改密码 🕚
₩私交易穿透监管平台	待执行审计列目	历史审计列制	5								
民 审计页	+ 新建审计(15				清油	入审计交易印		开始日期 罿	结束日期	〇直询
8 帶名前		序号	审计交易印	公开参数	交易查询条件	是否验证黑名单	黑丝单洋情	論注信息	审计发起时间	很作	
						智无数据					
ē Iļ					共0 条 10 条/页 ∨	< 1 >	前往 1 页				



审计员在审计页点击新建审计任务,进入新建任务页面。

路私衣要突逐步算业人	兩计页物建南计组织南计组件	修改密码 🖑
 (元 申計页 八 申計页 八 用名单 ① 工具 	J 康士条件	

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 15:18:12.598 [zkchain] DEBU : default user already exist zkchain.go:50 15:18:12.594 [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 getlist zkchain.go:63 15:18:2.596 [zkchain] DEBU : eg: ./zkchain -func getlist zkchain.go:34 15:18:23.765 [zkchain] DEBU : eg: ./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
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。

5



3.1.3 上传工具

於 京新 京新 京 京 京 京 京 京 京 京 京 市 京 市 京 市 市 市	IR		修改重码 ()		
民 审计页	「上传工具包				
冬 黒名单		操作系统: windows ✓ 上传工具钮: ◆上传			
€ IĄ	110	名文小: * 版本: 部品入り(部 () () () () () () () () () () () () () (
		* 留注: 1版文 ①重要			
	当前最新工具包				
		操作系统 windows つ 包大火 15.58MB 版本: マイロ			
		1987年 10 上使时间: 2021-10-14 14:17:13 □回時 21FR			

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:

OIR		BTH (THOLE) +MAG	ten statutationa materia i Laborat	· BLASK STORMSHOLTON B	1916	入审计交题10	9	开始日期 至	结束目期 Qrt
	序号	审计交易ID	公开参数	交易查询条件	是否验证黑名单	黑名单详情	音注信息	审计发起时间	操作
	1	892dtdbny4w8ota bkzd0ok67v56ht9 6q	22	<=1	景	27	2	2021-11-03 10:14:32 (3)	≥ 下號审计包 △ 上侍证明



- 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。

audit.json	2021/10/13 14:52	JSON 源文件
[] config.yaml	2021/10/11 14:28	Yaml 源文件
间 input.json	2021/10/13 14:54	JSON 源文件
📧 zkchain.exe	2021/10/11 14:36	应用程序
zkprove.exe	2021/10/13 11:58	应用程序
审计包.zip	2021/10/13 14:52	ZIP 文件

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;

PS C:\Users\peersafe\Desktop\test1> .\zkprove -prove value Generate Proof of Assets Value Success!



🔟 audit.json	2021/10/13 14:52	JSON 源文件
[] config.yaml	2021/10/11 14:28	Yaml 源文件
🔟 input.json	2021/10/13 14:54	JSON 源文件
🔟 proof.json	2021/10/14 16:39	JSON 源文件
📧 zkchain.exe	2021/10/11 14:36	应用程序
📧 zkprove.exe	2021/10/13 11:58	应用程序
审计包.zip	2021/10/13 14:52	ZIP 文件

注:运行对应的工具包即可出现相应的命令提示。

PS C:\Users\peersafe\Desktop\test1> .\zkchain.exe
zkchain.go:34 16:46:00.110 [zkchain] DEBU : Usage : ./zkchain -configPath=configFilePath 🛛 🖉 🚈 😎
user.go:102 16:46:00.166 [zkchain] DEBU : default user already exist
zkchain.go:59 16:46:00.167 [zkchain] DEBU :zkchain cmd
zkchain.go:60 16:46:00.167 [zkchain] DEBU : eg: ./zkchain -func help
zkchain.go:61 16:46:00.167 [zkchain] DEBU : eg: ./zkchain -func maketx -value
zkchain.go:62 16:46:00.167 [zkchain] DEBU : eg: ./zkchain -func getlist
zkchain.go:63 16:46:00.167 [zkchain] DEBU : eg: ./zkchain -func getdata -txid xxxx
PS C:\Users\peersafe\Desktop\test1> .\zkprove.exe
zkprove cmd err 验证交易金额
eg: ./zkprove -prove help
eg: ./zkprove -prove value
eg: . /zkprove -prove blacklist
eg: ///wwwwww.all

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