矩阵元 MPC Demo 用户手册

矩阵元技术（深圳）有限公司

文档控制

更改记录

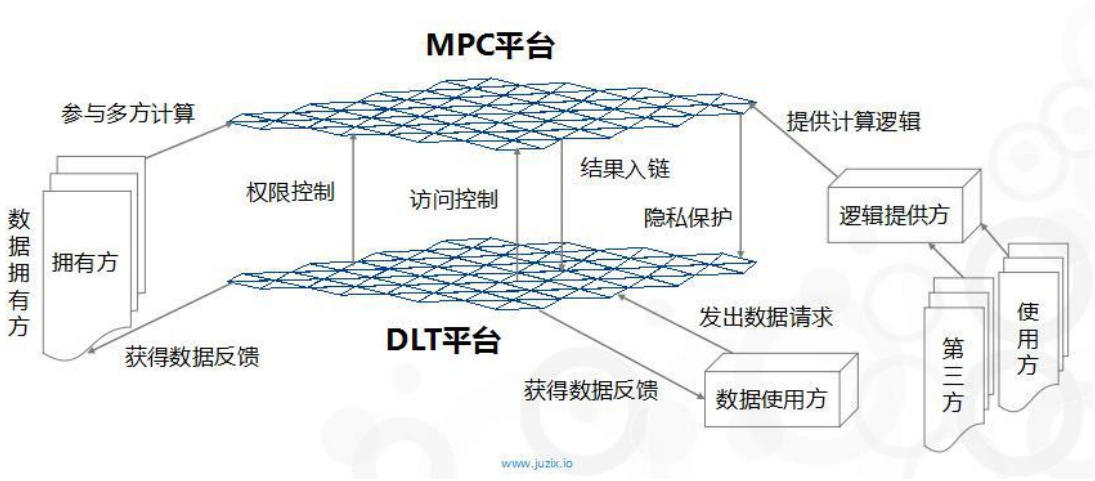
日期	版本	更改人	审批人	更改条款及内容
2017-09-12	V1.0	毕淦欣	姜珍	新建

目录

第 1 章 产品简介

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC 是在该价值理念下的解决方案与工程实现。借助矩阵元的 MPC 框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

矩阵元将 MPC 与区块链两种数据治理方案进行结合，让区块链基于隐私保护、权限控制、不可伪造篡改等特性为 MPC 提供可信的数据计算参与方；MPC 平台基于 OT 协议完成可信的数据计算并将结果入链作为存证。



本 Demo 基于 MPC（多方安全计算）实现了一个区块链私钥的安全备份方案

1. 通过人脸识别等生物特性实现对账户私钥的加密存储与备份

2. 通过人脸识别等生物特性实现对账户私钥的快速恢复

第 2 章　产品主要功能说明

2.1 注册用户

用户注册时在本地生成账户私钥，并进行人脸识别，将自己的生物特征（人脸特征）作为 MPC 输入与业务系统进行 MPC 计算，对私钥进行加密，私钥加密结果保存在安全的业务系统中。

2.2 恢复私钥

用户在私钥丢失或者不小心删除之后，可通过人脸识别，将自己的生物特征（人脸特征）作为 MPC 输入与业务系统进行 MPC 计算，对私钥进行解密，解密成功，客户端即可获取丢失的私钥

第 3 章　产品详细操作说明

3.1 注册用户

用户下载并安装完 App 后，启动 App 进入 MPC 应用首页，点击【注册用户】，进入注册流程。

注册流程：

1、输入账户信息：姓名、身份证号、手机号、登录密码

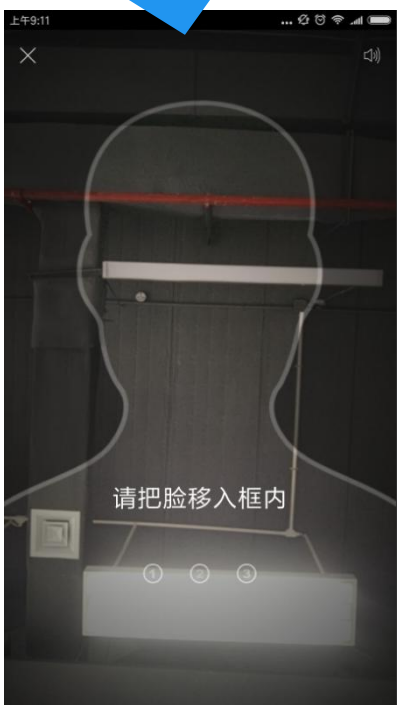
2、人脸识别：按照操作引导，进行人脸识别

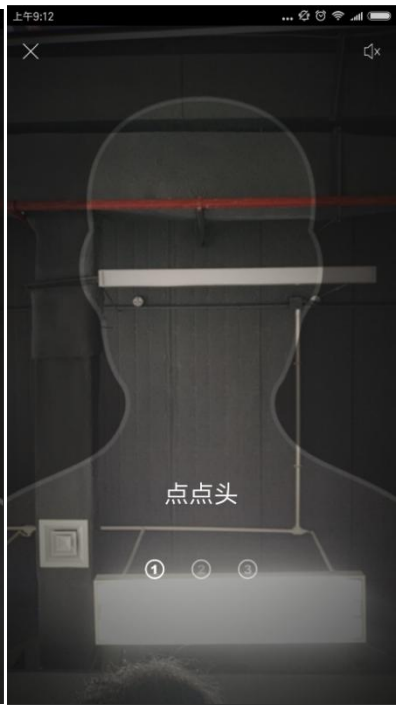
3、完成注册

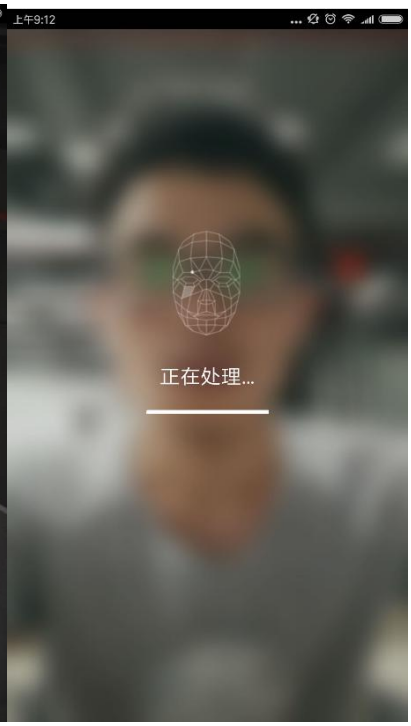
输入账户信息：姓名、身份证号、手机号、登录密码

点击【开始识别】按钮进入人脸识别流程

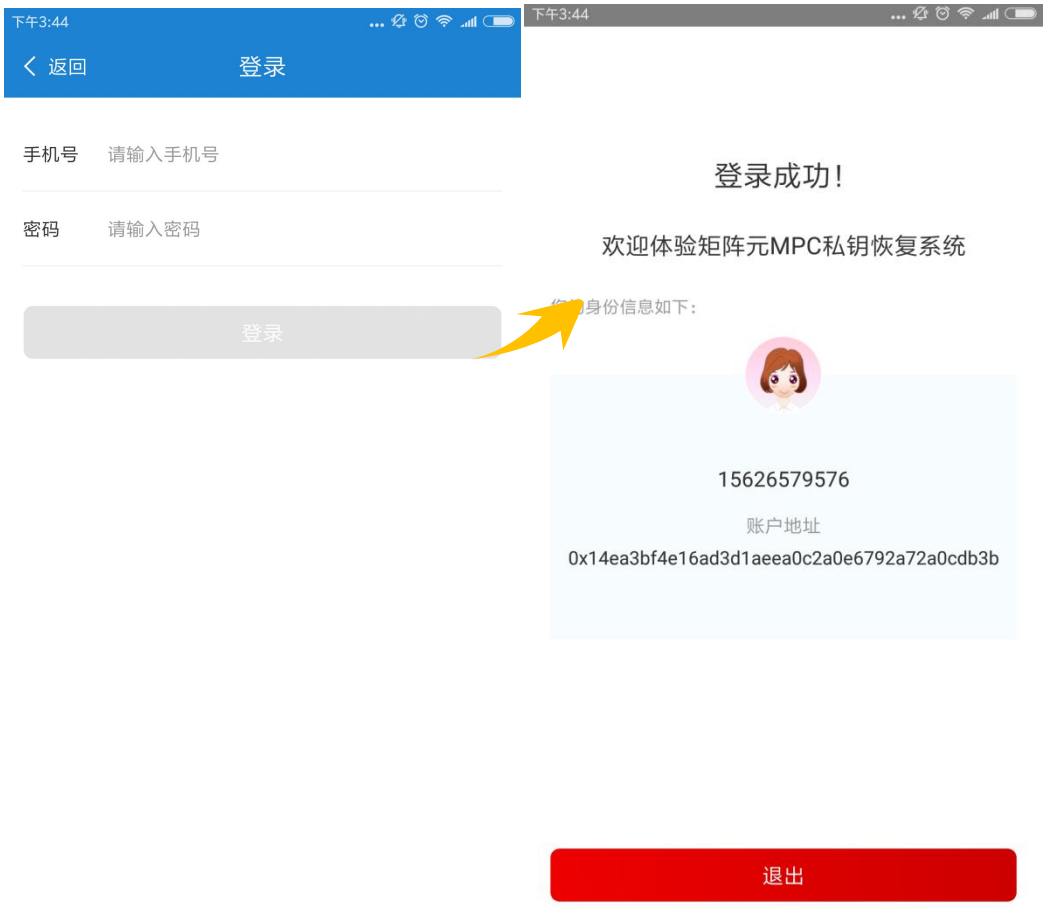
按照操作引导，完成人脸识别







注册完成可进行登录验证，点击【去登录】进入登录页面，输入刚注册的手机号、登录密码，点击【登录】，如果成功进入“登录成功欢迎页面”，则表示注册成功！



3.2 删除私钥

为体验 MPC 私钥恢复，在当前注册手机上，点击【删除私钥】，在弹出的确认提示框中，点击【确认】，即可删除本地手机所有私钥文件；

PS：如果有两部手机，可以直接在另一部手机上进行【恢复私钥】操作

点击【删除私钥】，弹出确认框

点击【确认】，即可删除本地私钥

删除完成，可点击【登录】进入登录页面，输入手机号、密码，点击【登录】可以验证当前私钥文件已不存在，无法登录！

3.3 恢复私钥

在删除私钥或者更换新手机之后，点击【恢复私钥】，在弹出的确认提示框中，点击【确认】，进入私钥恢复流程：

点击【恢复私钥】，弹出确认框

点击【确认】，进入恢复私钥流程

私钥恢复流程：

1、输入用户信息：姓名、身份证号、手机号

2、人脸识别：按照操作引导，进行人脸识别

3、设置新密码

4、完成私钥恢复

点击【开始识别】，进入人脸识别流程

人脸识别成功后，设置新的登录密码

恢复成功可进行登录验证，点击【去登录】进入登录页面，输入手机号、新的登录密码，点击【登录】，如果成功进入“登录成功欢迎页面”，则表示恢复成功！