

矩阵元股权交易 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
2017-09-13	V1.0	顾秋艳	姜珍	新建

目录

- 第 1 章 产品简介..... 5
- 第 2 章 产品主要功能说明..... 6
 - 2.1 PC 端主要功能..... 6
 - 2.2 APP 端主要功能..... 6
- 第 3 章 PC 端功能详细说明..... 7
 - 3.1 注册..... 7
 - 3.1.1 文件证书账号注册..... 7
 - 3.1.2 U-Key 证书账号注册..... 10
 - 3.2 登录..... 13
 - 3.2.1 文件证书账号登录..... 13
 - 3.2.2 U-Key 证书账号登录..... 15
 - 3.2.3 配置链..... 17
 - 3.3 应用中心..... 19
 - 3.4 股权交易..... 21
- 第 4 章 APP 端功能详细说明..... 23
 - 4.1 注册..... 23
 - 4.1.1 文件证书账号注册..... 23
 - 4.1.2 U-Key 证书账号注册..... 27
 - 4.2 登录..... 27
 - 4.2.1 文件证书账号登录..... 28
 - 4.2.2 U-Key 证书账号登录..... 31
 - 4.2.3 配置链..... 35

4.3 应用中心.....	36
4.4 首页.....	37
4.5 设置流通股数.....	39
4.6 股权登记.....	39
4.7 非交易过户.....	41
4.8 我的账户地址.....	42
4.9 登记记录.....	43
4.10 过户记录.....	44

第 1 章 产品简介

矩阵元股权交易 Demo 是内置于矩阵元区块链客户端内的一个 DApp，该 DApp 演示了基于零知识证明及同态加密技术的股权登记和转让业务，是对区块链技术应用扩展的探索。

同态加密是一种无需对加密数据进行提前解密就可以执行计算的方法。它提供了一种急需的方法，能够在原有基础上使用区块链技术。通过使用同态加密技术在区块链上存储数据可以达到一种完美的平衡，不会对区块链属性造成任何重大的改变。也就是说，区块链仍旧是公有区块链。然而，区块链上的数据将会被加密，因此照顾到了公有区块链的隐私问题，同态加密技术使公有区块链具有私有区块链的隐私效果。

同态加密技术不仅提供了隐私保护，它同样会允许随时访问公用区块链上的加密数据进行审计或其他目的。换句话说，使用同态加密在公用区块链上存储数据将能够同时提供公有和私有区块链的最好的部分。

使用同态加密的以太坊智能合约能够提供相似的特点和更强的掌控，同时完整地保留以太坊的优点。

“零知识证明” - zero-knowledge proof，指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

零知识证明并不是数学意义上的证明，因为它存在小概率的误差，欺骗者有可能通过虚假陈述骗过证明者。换句话说，零知识证明是概率证明而不是确定性证明。但是也存在有技术能将误差降低到可以忽略的值。

第 2 章 产品主要功能说明

股权交易 Demo 是内置于矩阵元区块链客户端应用中心的一款 DApp，矩阵元区块链客户端提供了 PC 端及 App 端两个端的功能，您可以通过登录矩阵元区块链客户端，登录成功之后进入应用中心，来使用股权交易 Demo。

2.1 PC 端主要功能

1. **登录/退出登录**：矩阵元客户端提供了文件证书账号、U-Key 证书账号两种登录方式，登录之前需要先配置连接的链，连接链成功之后才可以使用用户账号登录。
2. **应用中心**：应用中心集成了若干 DApp，点击某一个 DApp 可进入该并使用该 DApp 的相关功能。
3. **股权信息展示**：总股数、流通股、非流通股、股东等信息展示。

2.2 App 端主要功能

1. **登录/退出登录**：矩阵元区块链客户端 App 提供了文件证书账号、U-Key 证书账号两种登录方式，登录之前需要先配置链，连接链成功之后才可以使用用户账号登录。
2. **应用中心**：应用中心集成了若干 DApp，点击某一个 DApp 可进入并使用该 DApp 的相关功能。
3. **股权信息展示**：总股数、流通股、非流通股、股东等信息展示。
4. **股权登记**：用于管理员为普通用户登记股权。
5. **非交易过户**：用于用户之间转让股份。
6. **历史记录查询**：包括登记记录、过户记录查询。

第 3 章 PC 端功能详细说明

3.1 注册

矩阵元区块链客户端注册提供两种方式：

1、**用户自助注册文件证书账号**：用户在客户端登录页面，点击【注册用户】，进入文件证书账号注册流程；

2、**管理员签发 U-Key 证书账号**：管理员在管理后台创建 U-Key 证书账号，完成之后给到用户使用；

3.1.1 文件证书账号注册

文件证书账号注册流程：文件证书账号注册需要用户自助在客户端提交用户注册申请，管理员在管理后台进行审核，审核通过后，用户即可登录。

相关产品截图及操作说明如下：



在登录页面，点击【注册用户】

用户注册

×

用户账号注册流程

① 填写用户信息并提交申请
录入用户信息并设置登录密码

② 管理员审核
管理员对提交的用户注册申请进行审核

③ 注册完成
审核通过即可使用账号密码登录系统。

* 姓名

请输入姓名

* 密码

请设置密码

* 手机

请输入手机号

* 所属组织

请选择所属组织

请选择...

备注

请输入备注

* 用户名

请设置用户名

* 再次输入密码

请确认密码

* 邮箱

请输入邮箱

取消

确定

填写用户注册信息，完成后点击【确定】

用户注册

×

用户账号注册流程

① 填写用户信息并提交申请
录入用户信息并设置登录密码

② 管理员审核
管理员对提交的用户注册申请进行审核

③ 注册完成
审核通过即可使用账号密码登录系统。

✔ 用户注册申请提交成功，请等待管理员审核！

用户注册申请提交之后，管理员对用户提交的注册申请进行审核。审核页面如下：

矩阵元客户端 应用中心 控制台 开发工具 个人中心

控制台

用户注册审核

待审核 已审核

请输入姓名进行查询 请输入手机进行查询 账户类型 全部 查询

序号	用户名	姓名	所属组织	账号类型	手机	申请时间	状态	操作
1	guqiyuan	顾秋艳	矩阵元产品部	文件证书账号	15820499053	2017-09-13 10:35	待审核	审核
2	guyuqi	顾雨琪	矩阵元产品部	文件证书账号	15938621475	2017-09-13 10:44	待审核	审核

共 2 条

当前连接的链：烟云链 系统时间：2017-9-13 10:58:08 当前登录用户：危月燕(文件证书账号)

管理员需要登录后进入控制台，用户注册审核页面，在待审核列表中，找到要审核的用户注册申请，在列表操作列点击【审核】进入审核页面：

矩阵元客户端 应用中心 控制台 开发工具 个人中心

控制台

用户注册审核

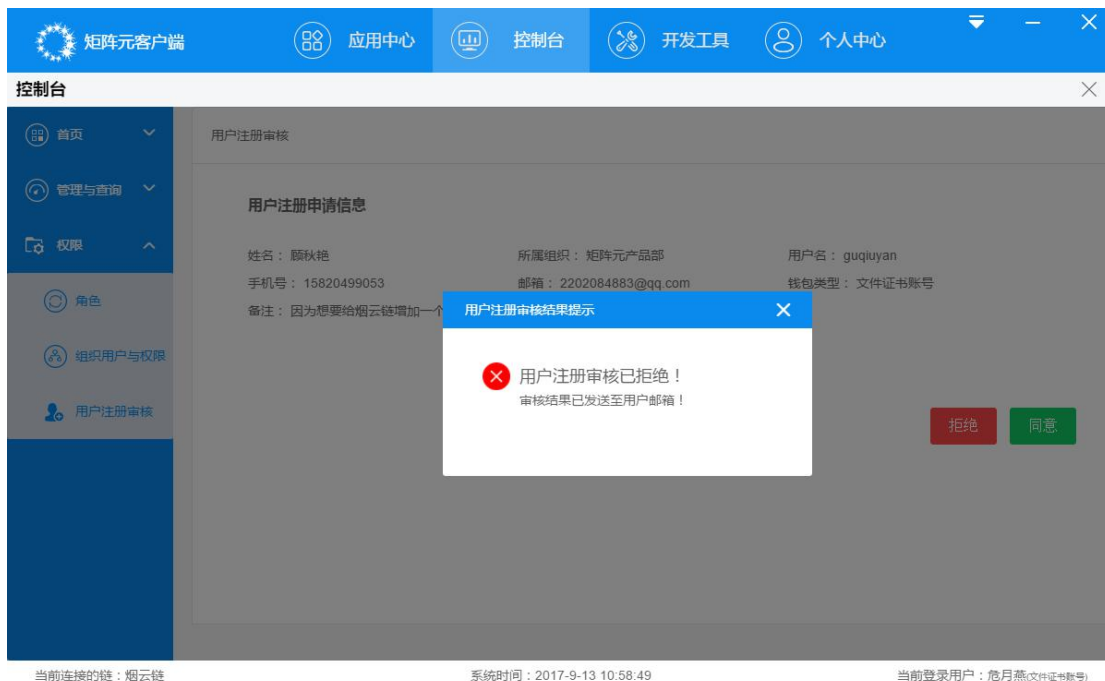
用户注册申请信息

姓名：顾秋艳 所属组织：矩阵元产品部 用户名：guqiyuan
 手机号：15820499053 邮箱：2202084883@qq.com 钱包类型：文件证书账号
 备注：因为想要给烟云链增加一个节点，所以需要先注册一个用户账号。

拒绝 同意

当前连接的链：烟云链 系统时间：2017-9-13 10:58:30 当前登录用户：危月燕(文件证书账号)

点击【同意】或【拒绝】



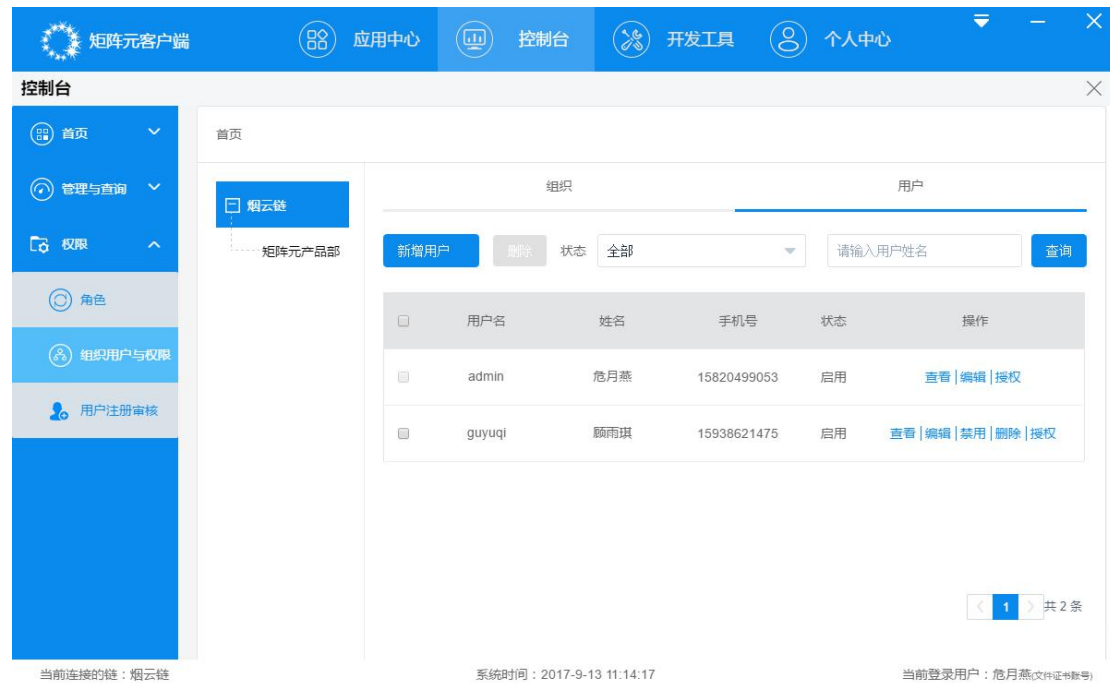
审核通过的用户可以使用用户账号登录系统了。

3.1.2 U-Key 证书账号注册

U-Key 证书账号注册：U-Key 证书账号是由管理员在管理后台统一创建，用户不可自行创建，管理员创建完成之后，将 U-Key 给到用户，用户使用 U-Key 证书账号首次登录

需要修改密码，修改之后可持续使用。

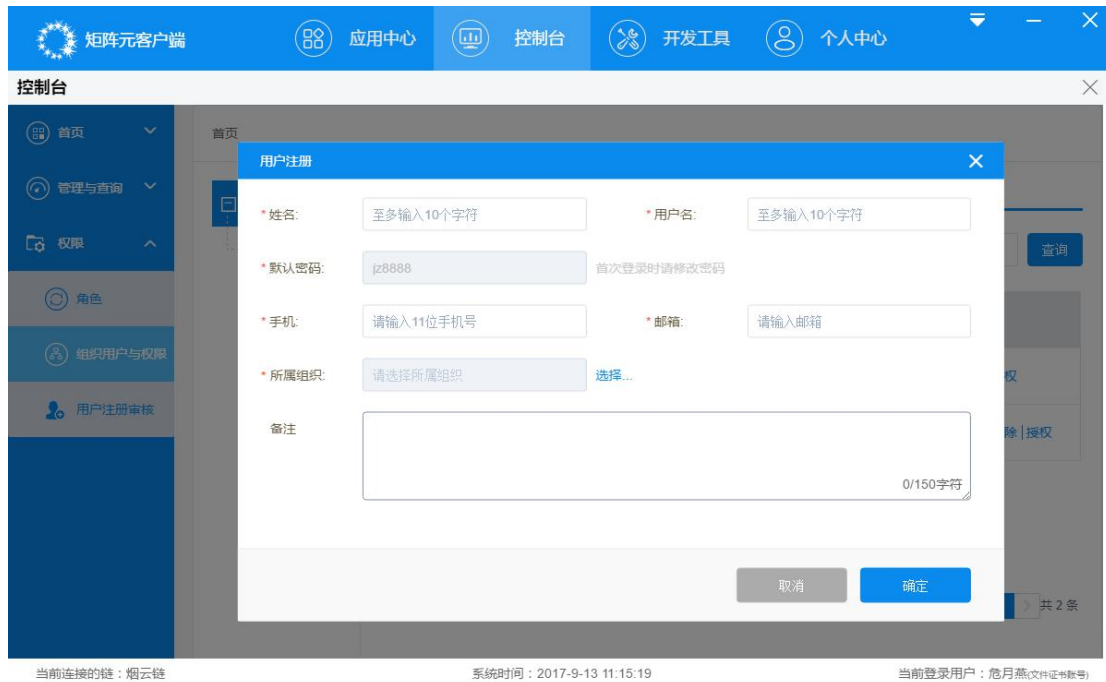
相关产品截图如下：



管理员进入管理控制台用户管理页面，点击【新增用户】

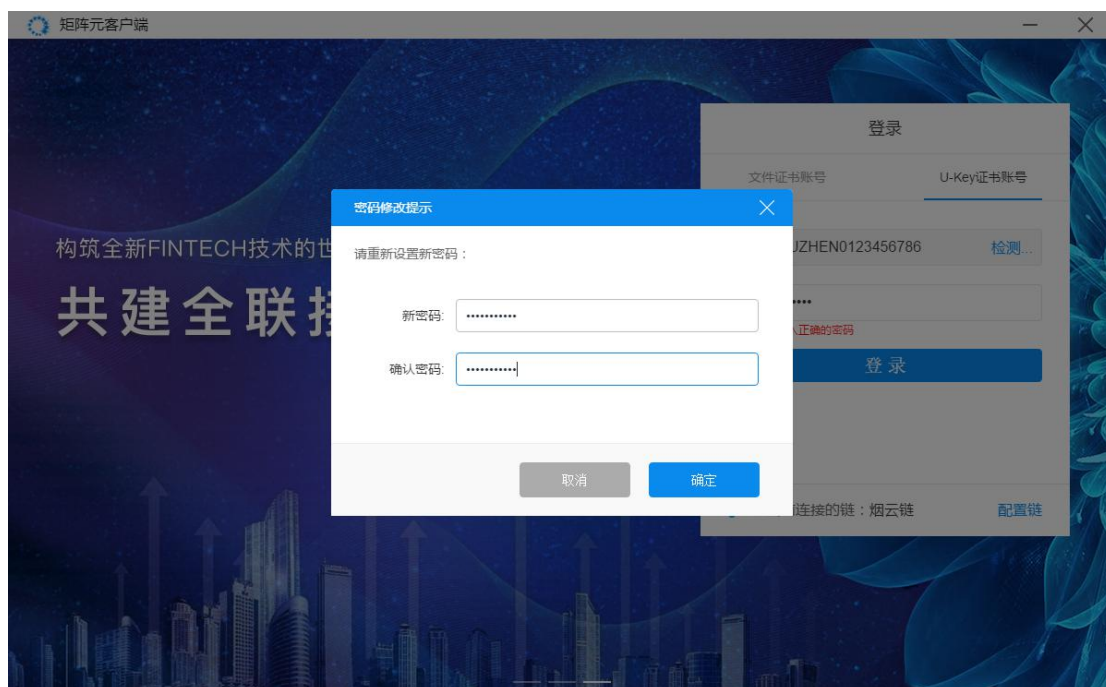


系统自动检测 U-Key 是否插入，选中要使用的 U-Key 后，点击【确定】



填写用户注册信息，完成后点击【确定】后，即完成注册，用户可使用该 U-Key 进行登录。

系统默认密码是：jz8888，用户首次登录时需要修改密码，见下图：



3.2 登录

使用股权交易需登录矩阵元区块链客户端，登录页面如下：



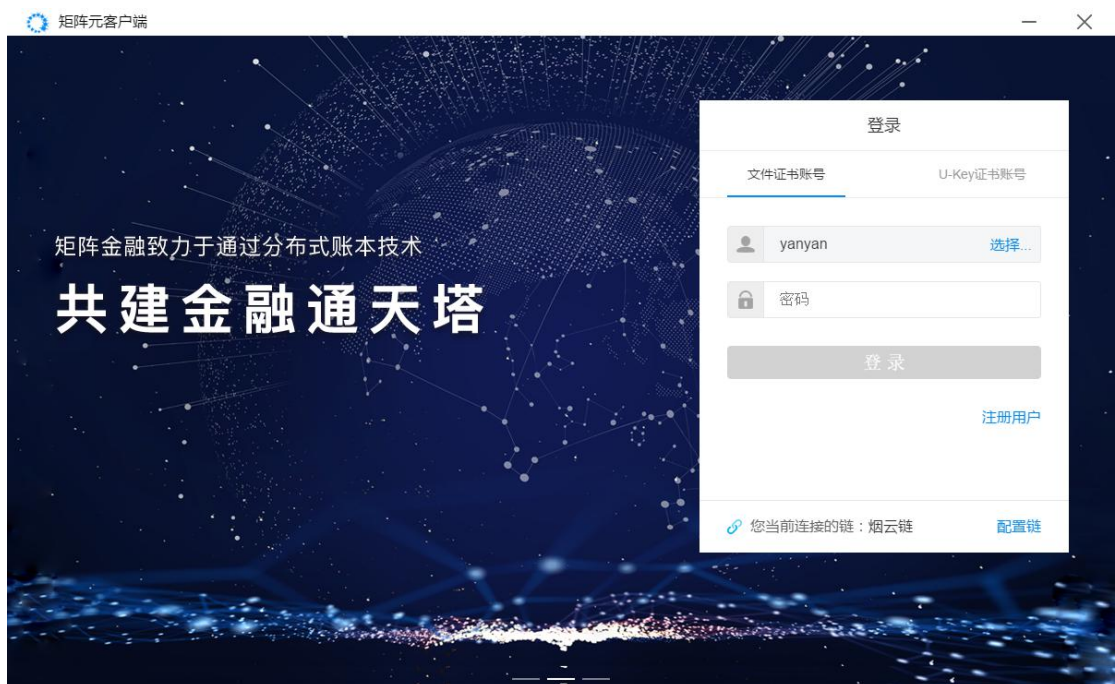
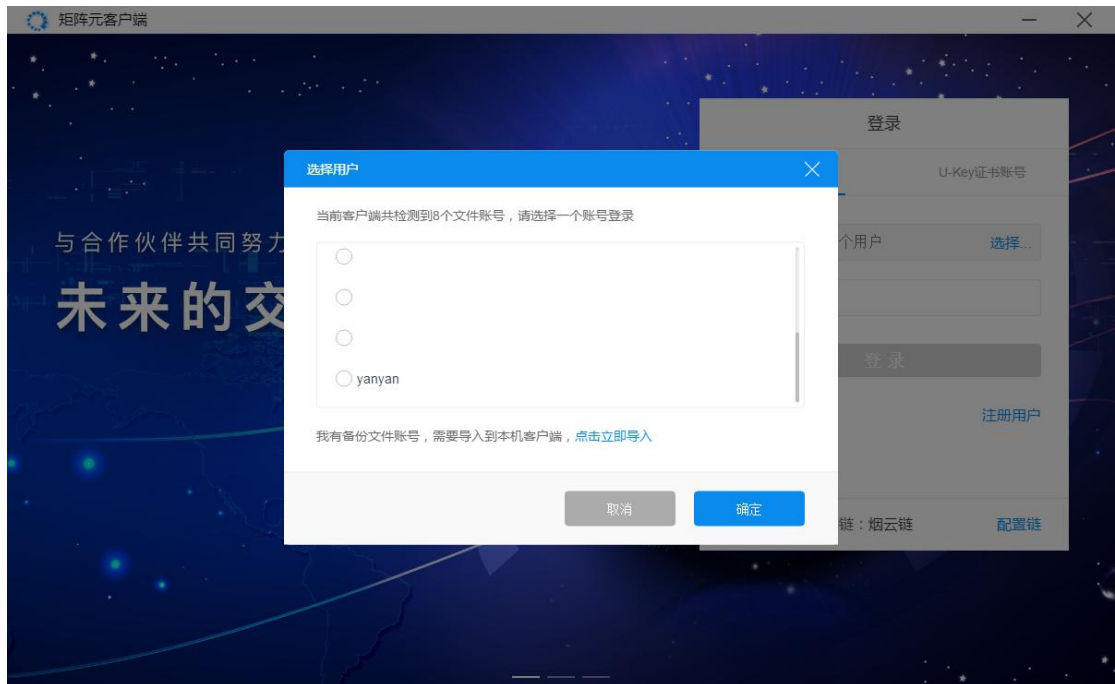
矩阵元客户端提供了两种登录方式：①文件证书账号登录；②U-Key 证书账号登录。

3.2.1 文件证书账号登录

文件证书账号登录流程：

1. 在登录页面，点击【选择用户】，弹出选择用户弹框；
2. 从用户列表中选择要登录的用户名，点击【确定】即可将该用户名填充至用户名输入框内；
3. 输入密码，点击【登录】即可登录；

产品截图如下：



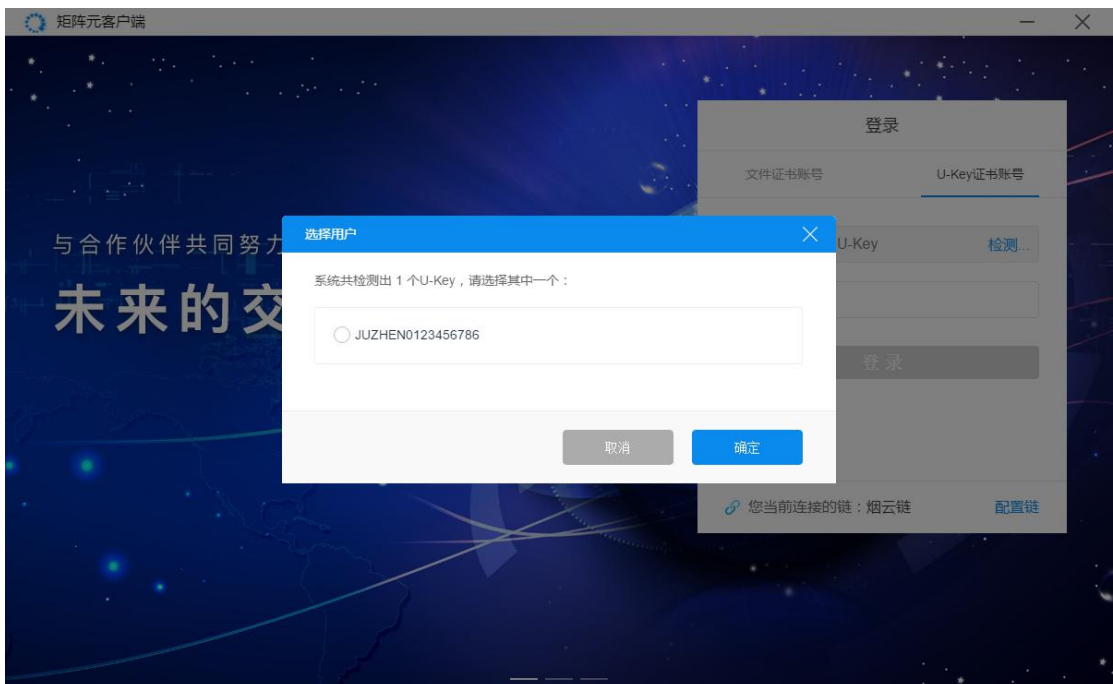


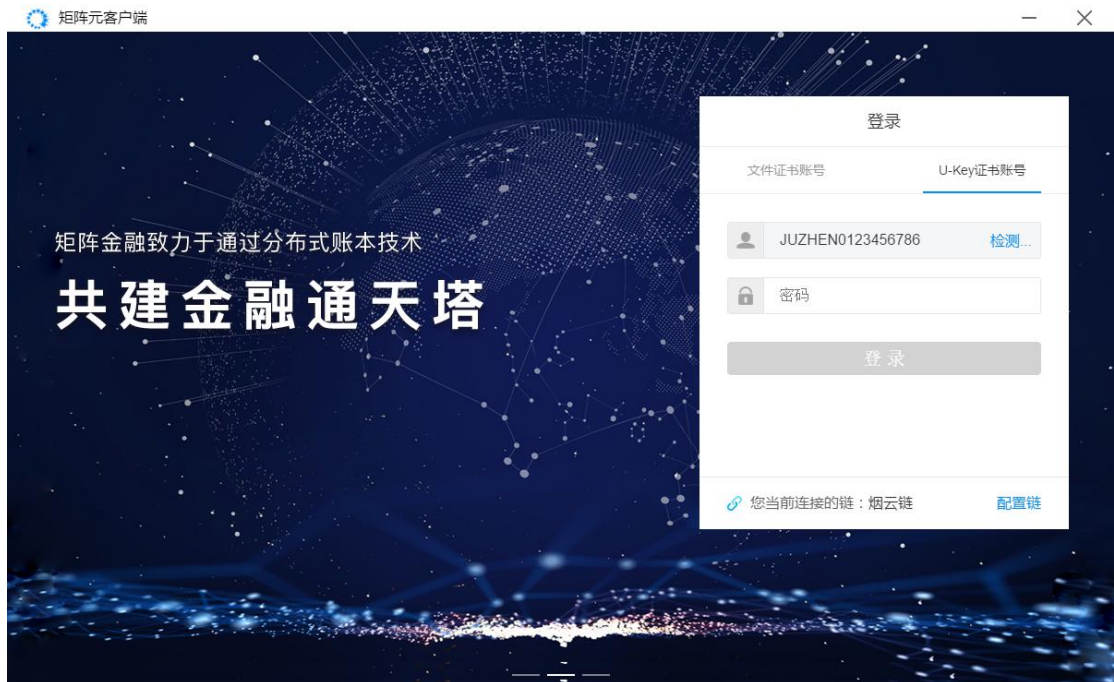
3.2.2 U-Key 证书账号登录

U-Key 证书账号登录流程：

1. 在登录页面，点击【检测】，系统自动检测 U-Key；
2. 从检测到的 U-Key 列表中选择要登录的 U-Key 证书账号，点击【确定】即可将该用户名填充至用户名输入框内；
3. 输入密码，点击【登录】即可登录；

产品截图如下：





3.2.3 配置链

登录前必须要配置链并能正常连接链，同时登录的用户名及密码正确或者 U-Key 证书账号正确方可正常登录。

配置链流程如下：

1. 在登录页面，点击【配置链】进入配置链页面；
2. 系统默认选中【企业联盟链】，输入要连接的链的 IP/域名及服务端口；
3. 点击【确定】即完成配置链；

说明：如果要连接的链不存在，则需要先创建链，【创建链】的功能此处暂不介绍。



目前仅提供矩阵元测试链及企业联盟链的连接，矩阵元公有链暂不提供。



3.3 应用中心

登录客户端成功之后即可进入应用中心，点击【股权交易】DApp，即可进入【股权交易】DApp 页面。

相关产品截图如下：

矩阵元区块链客户端

应用中心

控制台

开发工具

个人中心

发布DAPP

查询

控制台

内置合约权限配置器

版本：V1.0.0.1 2017-07-27

监控DAPP

监控DApp模块

版本：V1.0.0.1 2017-07-27

股权交易DApp

本应用演示了基于零知识证明及同态加密技术的股权登记和转让业务，是对区块链技术应用扩展的探索。

版本：V1.0.0.1 2017-07-27

当前连接的链：矩阵元

系统时间：2017-07-27 14:26

当前登录用户：危月燕（文件证书账号）

矩阵元区块链控制台

应用中心

控制台

开发工具

个人中心

股权交易

股权交易

流通股占比：28.73%

总股数：10000 份

流通股：2873 份

非流通股：7127 份

查询

序号	股东账户地址	账户余额 (份)
1	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
2	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
3	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
4	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
5	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
6	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL

<<

<

1

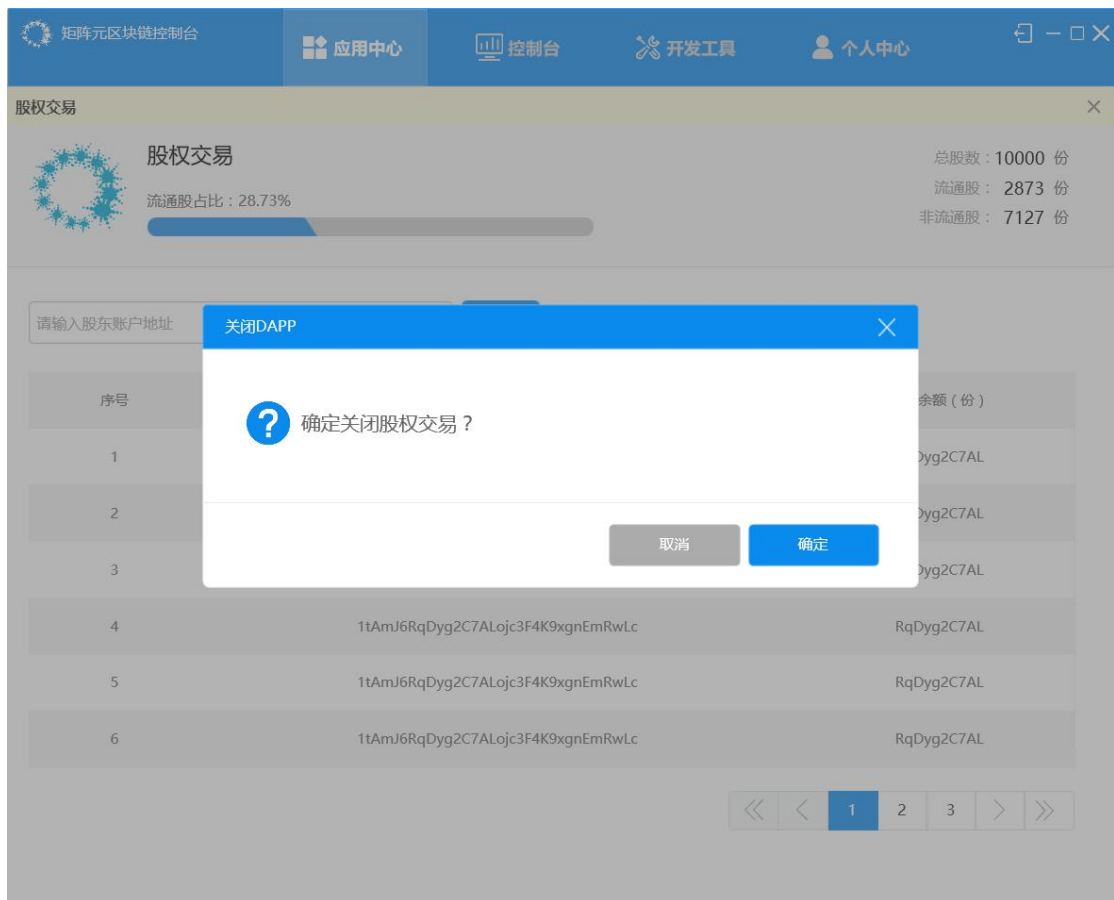
2

3

>

>>

点击【股权交易】DApp 页面右上角的【关闭】图标，弹出“关闭 DApp”确认弹框，确认之后，会回到应用中心。



3.4 股权交易

股权交易 DApp 主要包括两个方面的信息：

1、股权登记概要信息，包括：总股数、流通股数、非流通股数即流通股占比。总股数 = 流通股数 + 非流通股数。流通股数占比 = 流通股数 / 总股数 * 100%。

2、股东账户地址及其余额，支持按照股东账户地址进行查询。股东账户余额加密后密文显示。

矩阵元区块链控制台


应用中心

控制台

开发工具

个人中心

股权交易



股权交易

流通股占比：28.73%

总股数：10000 份

流通股：2873 份

非流通股：7127 份

请输入股东账户地址

查询

序号	股东账户地址	账户余额 (份)
1	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
2	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
3	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
4	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
5	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL
6	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc	RqDyg2C7AL

<<

<

1

2

3

>

>>

第 4 章 App 端功能详细说明

4.1 注册

矩阵元区块链客户端 App 端用户注册提供两种方式：

- 1、**用户自助注册文件证书账号**：用户在客户端 App 登录页面，点击【注册新用户】，进入文件证书账号注册流程；
- 2、**管理员签发 U-Key 证书账号**：管理员在管理后台创建 U-Key 证书账号，完成之后给到用户使用；

4.1.1 文件证书账号注册

文件证书账号注册流程：文件证书账号注册需要用户自助在 App 端提交用户注册申请，管理员在管理后台进行审核，审核通过后，用户即可登录。

在登录页面，点击【注册新用户】进入注册新用户申请流程。

矩阵元

文件证书账号 U-Key证书账号

Bonyee

请输入登录密码

忘记密码？

登录

导入文件账号

注册新用户

配置链

注册新用户申请流程如下：

第 1 步：填写用户注册信息；

第 2 步：设置用户名及密码；

第 3 步：新用户注册信息提交；

产品截图如下：





 矩阵元

1 录入信息

2 创建账号

3 等待审核

 请输入您的真实姓名

 请输入您的手机号码

 请输入您的电子邮箱

 点击选择您所属的组织

下一步

[已有账号登录](#)

[配置链](#)



 矩阵元

1 录入信息

 —

2 创建账号

 —

3 等待审核



请设置您的用户账号名（字母、数字组成）



请设置您的登录密码



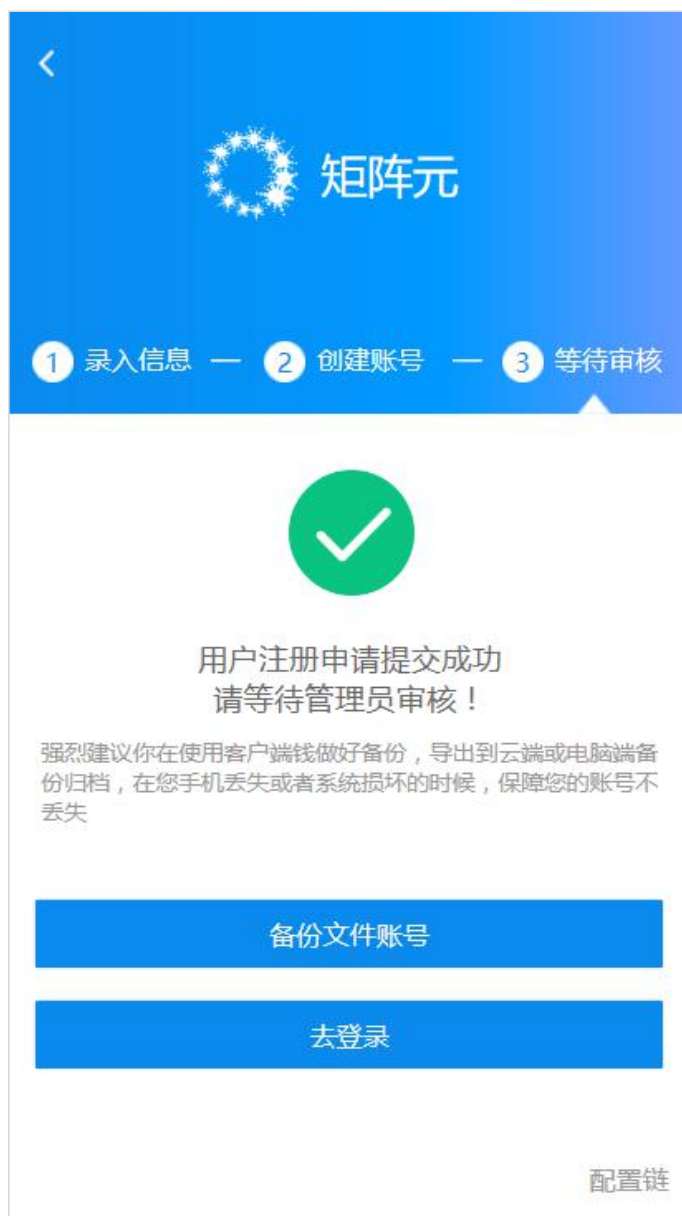
请再次输入登录密码

提交

<上一步

已有账号登录

配置链



新用户注册申请提交成功之后，管理员在管理后台对新用户注册申请进行审核，审核功能介绍请见 3.1.1 章节第 9 页、第 10 页。

4.1.2 U-Key 证书账号注册

U-Key 证书账号注册功能介绍请见 3.1.2 章节。

4.2 登录

矩阵元区块链客户端 App 提供了两种登录方式：①文件证书账号登录；②U-Key 证书

账号登录。U-Key 证书登录是通过蓝牙登录。

4.2.1 文件证书账号登录

文件证书账号登录流程：

1. 在登录页面，点击用户图标，弹出选择用户弹框；
2. 从用户列表中选择要登录的用户名，即可将该用户名填充至用户名输入框内；
3. 输入密码，点击【登录】即可登录；

产品截图如下：

 矩阵元

文件证书账号U-Key证书账号

 Bonyee

 请输入登录密码

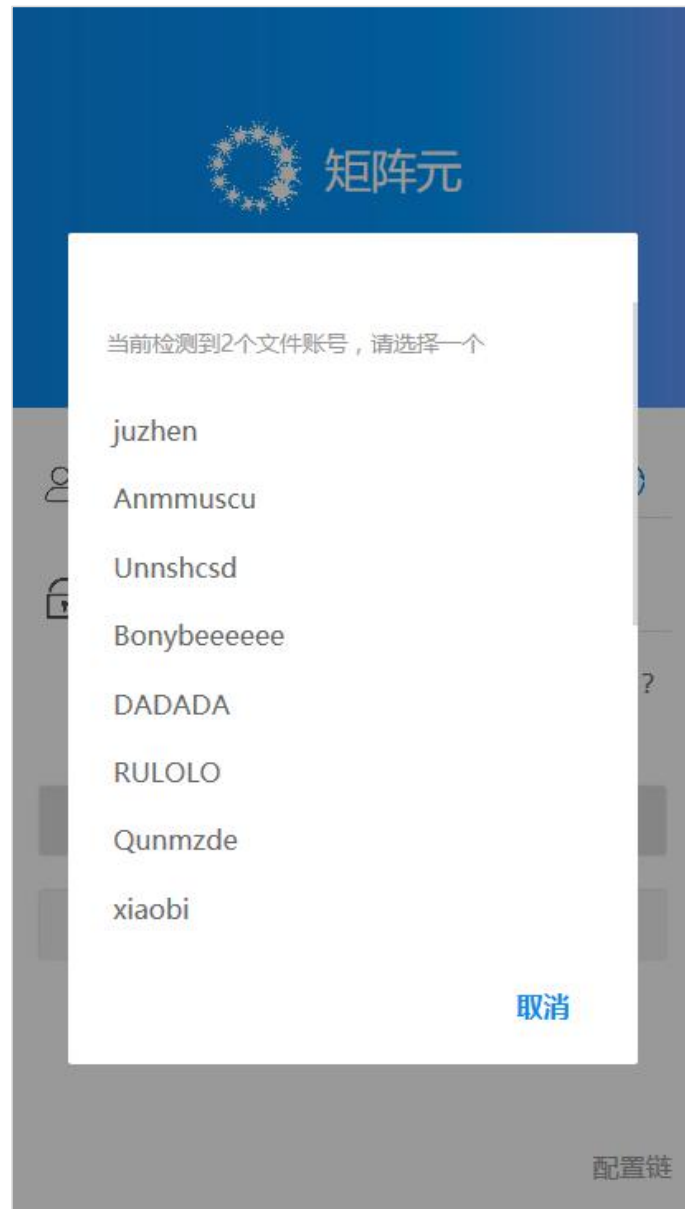
忘记密码？

登录

导入文件账号

注册新用户

配置链



矩阵元

文件证书账号 U-Key证书账号

Bonyee

忘记密码？

登录

导入文件账号

注册新用户

配置链

4.2.2 U-Key 证书账号登录

U-Key 证书账号登录流程：

1. 在登录页面，点击【检测】，系统自动检测 U-Key；
2. 从检测到的 U-Key 列表中选择要登录的 U-Key 证书账号，点击【确定】即可将该用户名填充至用户名输入框内；
3. 输入密码，点击【登录】即可登录；

产品截图如下：

 矩阵元

文件证书账号

U-Key证书账号



请开启蓝牙检测





请输入登录密码

忘记密码？

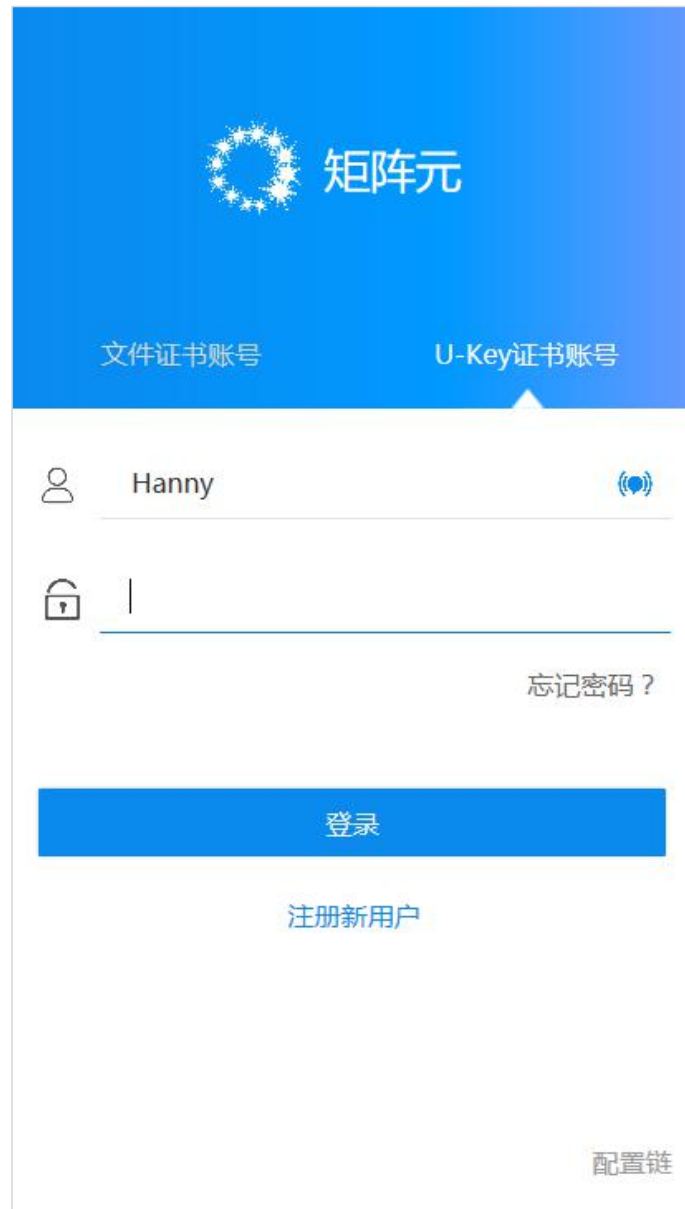
登录

注册新用户

配置链







The image shows a login interface for '矩阵元' (Matrix Element). At the top, there is a blue header with the company logo and name. Below the header, there are two tabs: '文件证书账号' (File Certificate Account) and 'U-Key证书账号' (U-Key Certificate Account). The 'U-Key证书账号' tab is currently selected. The main login area has a white background. It contains a username field with the text 'Hanny' and a blue speaker icon on the right. Below the username field is a password field with a lock icon on the left and a blue underline. To the right of the password field is a link that says '忘记密码?' (Forgot Password?). Below the password field is a large blue button with the text '登录' (Login). Below the login button is a link that says '注册新用户' (Register New User). At the bottom right of the interface is a link that says '配置链' (Configure Chain).

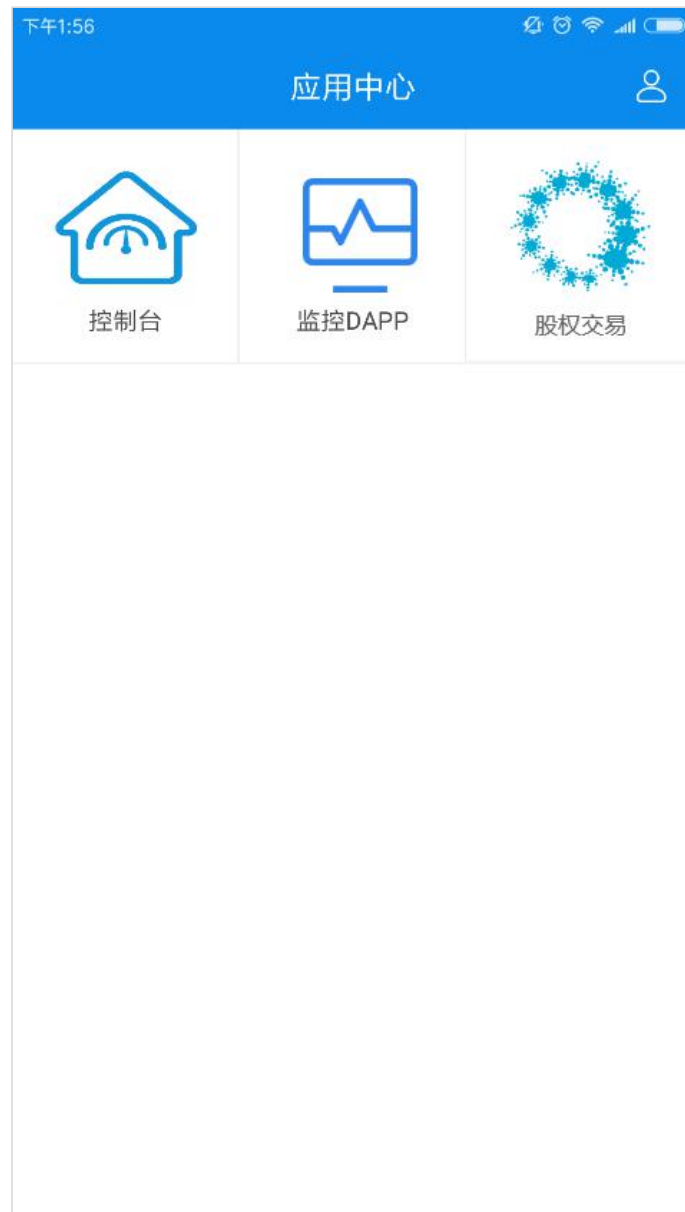
4.2.3 配置链

登录前必须要配置链并能正常连接链，同时登录的用户名及密码正确或者 U-Key 证书账号正确方可正常登录，配置链页面如下：



4.3 应用中心

登录矩阵元区块链客户端成功之后即可进入应用中心，点击【股权交易】DApp，即可进入【股权交易】DApp 页面。



4.4 首页

点击【股权交易】DApp 即可进入股权交易 DApp 首页，见下图：



股权交易 DApp 首页包含了以下功能：

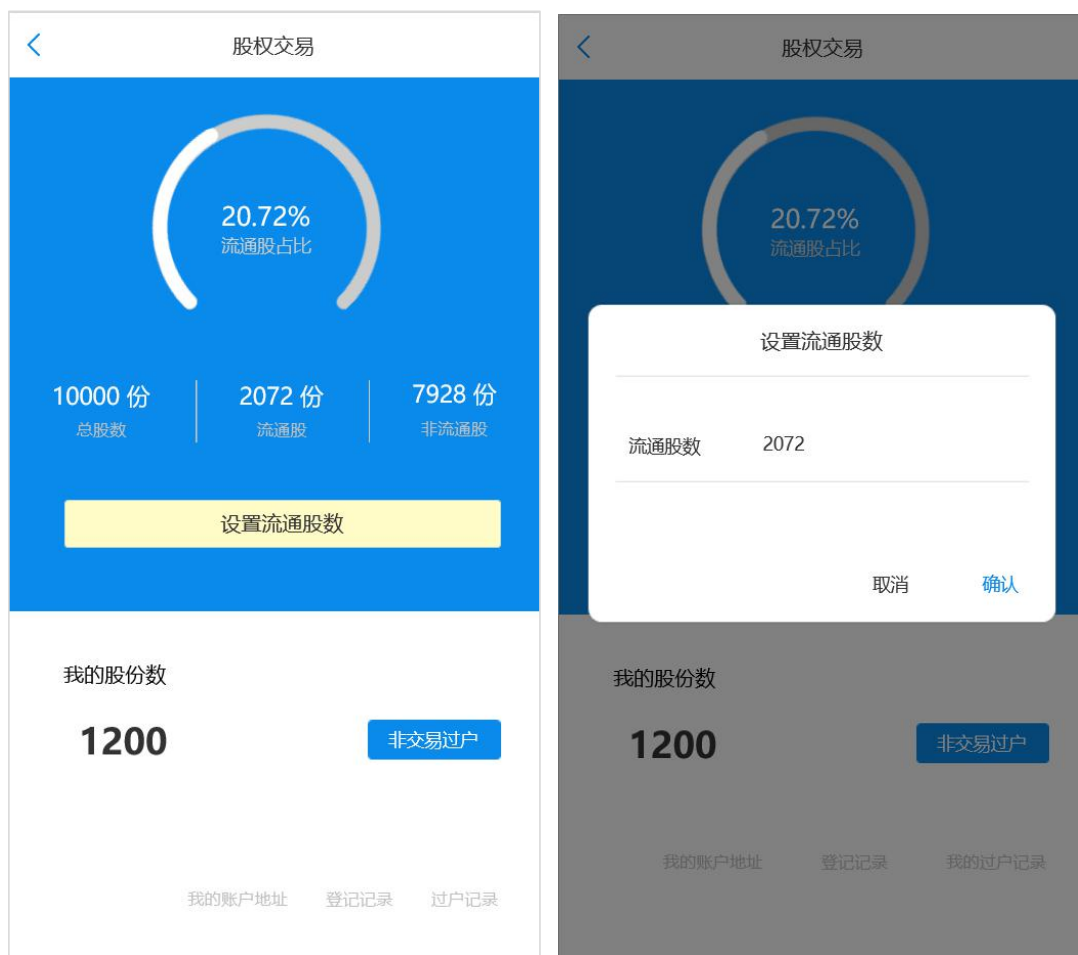
(1) 展示股权登记概要信息，包括：总股数、流通股数、非流通股数即流通股占比。其中， $\text{总股数} = \text{流通股数} + \text{非流通股数}$ ， $\text{流通股占比} = \text{流通股数} / \text{总股数} * 100\%$ 。

(2) 展示用户的股份数，即用户个人资产余额。 $\text{用户个人资产余额} = \text{个人已登记股份数} + \text{转入的股份数总和} - \text{转出的股份数总和}$ 。

(3) 集成各个功能入口，包括：设置流通股数、股权登记、非交易过户、查看个人账户地址、查看登记记录、查看过户记录。点击各个功能入口进入各个子功能页面，点击返回即可返回首页。

4.5 设置流通股数

【设置流通股数】功能用于初始化系统可登记股数的初始值。该功能是提供给管理员使用。管理员登录后的初始化页面才会显示，设置之后便不再显示该功能入口。



4.6 股权登记

【股权登记】功能用于登记股权。该功能是提供给管理员使用。管理员设置完初始流通股数之后可进入该页面，管理员可为普通用户登记股份。

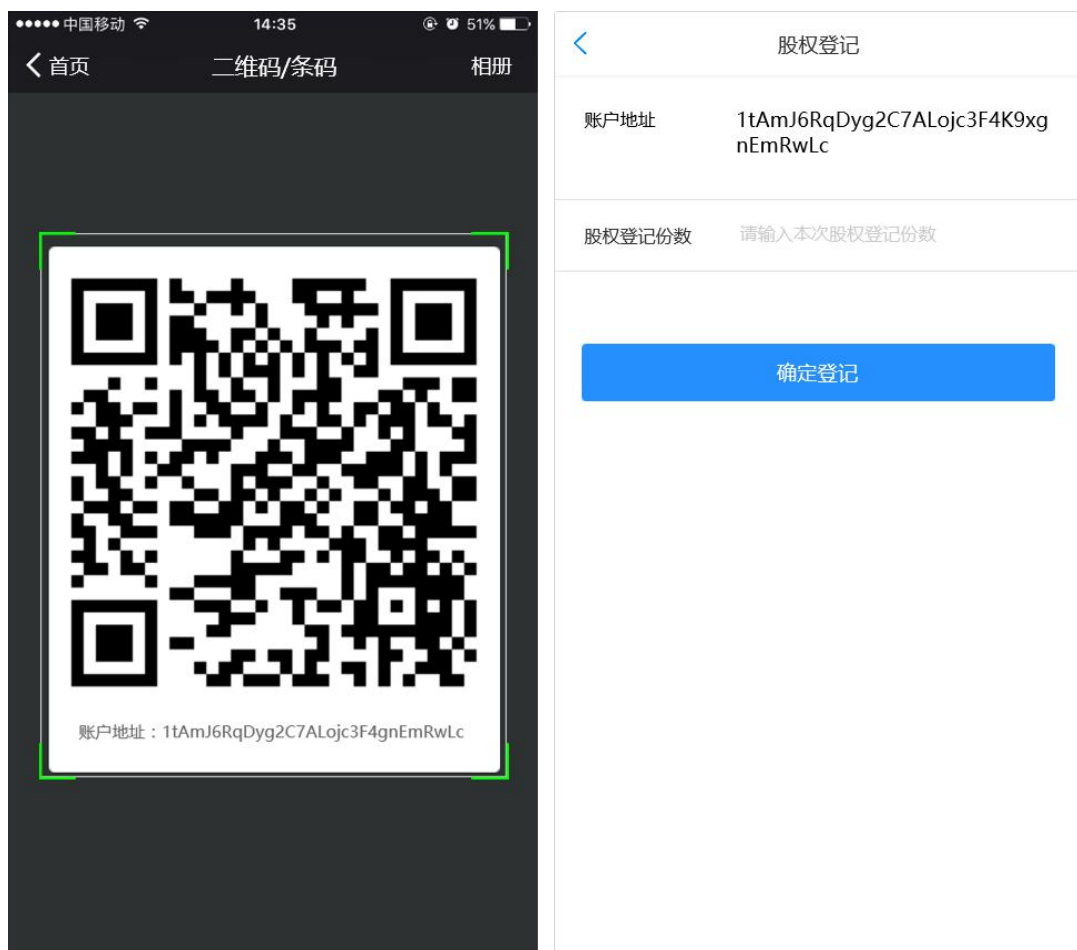


管理员进行股权登记的操作流程如下：

第 1 步：点击【股权登记】按钮，扫描要登记用户的账户地址的二维码；

第 2 步：系统识别出用户的账户地址后，输入要登记的股份数量，登记的股份数不可超过可登记的股份总数；

第 3 步：点击【确定登记】后，提交登记结果。登记成功后，流通股数减去本次登记股份数，被登记用户增加本次登记的股份数；



4.7 非交易过户

【非交易过户】功能用于用户之间股份转让，用户可使用该功能将自己的股份转让给对方。转让的操作流程如下：

第 1 步：点击【非过户交易】按钮，扫描要转让用户的账户地址二维码；

第 2 步：系统识别对方的账户地址后，输入要转让的股份数量，转让的股份数量不可超过可转让的股份数量，可转让的股份数量为个人资产余额；

第 3 步：点击【确定过户】后提交过户结果。过户成功后，个人股份数减去本次转让股份数，被转让用户的股份数则增加本次转让的股份数；

产品相关截图如下：



4.8 我的账户地址

【我的账户地址】可查看用户自己的账户地址二维码及明文地址。可用于股权登记或非交易过户时，让对方扫描。



4.9 登记记录

【登记记录】功能用于查看股权登记记录，包括登记地址、登记数量、登记时间等信息。管理员可查看所有登记记录。普通用户仅可查看自己的登记记录，即管理员为自己登记股权的登记记录。

相关产品截图如下：

<div> <div><</div> <div>登记记录</div> </div>	
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-15 08:09
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-16 08:09
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-18 08:09
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-19 08:09
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-25 08:09
登记地址	1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc
登记数量	1000
登记时间	2017-09-26 08:09

4.10 过户记录

【过户记录】功能用于查看股份转让记录，即非交易过户记录。既包括用户转给别人的转出记录也包括别人转让给用户的转入记录。转出/转入记录主要包括：转出/转入地址、转出/转入数量、转出/转入时间等。

管理员可查看所有过户记录。普通用户仅可查看自己的过户记录。

相关产品截图如下：

<div> <div><</div> <div>过户记录</div> </div>	<div> <div><</div> <div>过户记录</div> </div>
<div> <div>转出记录</div> <div>转入记录</div> </div>	<div> <div>转出记录</div> <div>转入记录</div> </div>
<div> <div>转出地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转出数量</div> <div>1000</div> <div>转出时间</div> <div>2017-09-15 08:09</div> </div>	<div> <div>转入地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转入数量</div> <div>1000</div> <div>转入时间</div> <div>2017-09-15 08:09</div> </div>
<div> <div>转出地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转出数量</div> <div>1000</div> <div>转出时间</div> <div>2017-09-16 08:09</div> </div>	<div> <div>转入地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转入数量</div> <div>1000</div> <div>转入时间</div> <div>2017-09-20 08:09</div> </div>
<div> <div>转出地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转出数量</div> <div>1000</div> <div>转出时间</div> <div>2017-09-18 08:09</div> </div>	<div> <div>转入地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转入数量</div> <div>1000</div> <div>转入时间</div> <div>2017-09-25 08:09</div> </div>
<div> <div>转出地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转出数量</div> <div>1000</div> <div>转出时间</div> <div>2017-09-19 08:09</div> </div>	<div> <div>转入地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转入数量</div> <div>1000</div> <div>转入时间</div> <div>2017-08-15 08:09</div> </div>
<div> <div>转出地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转出数量</div> <div>1000</div> <div>转出时间</div> <div>2017-09-25 08:09</div> </div>	<div> <div>转入地址</div> <div>1tAmJ6RqDyg2C7ALojc3F4K9xgnEmRwLc</div> <div>转入数量</div> <div>1000</div> <div>转入时间</div> <div>2017-08-25 08:09</div> </div>
<div> <div>上拉查看更多...</div> </div>	<div> <div>上拉查看更多...</div> </div>