DeepStone RWA 多签平台技术说明

1. 概览

DeepStone RWA（Real World Assets，现实世界资产）多签平台是一个面向机构级用户的 **通用型 RWA 管理与托管基础平台**。平台支持包括黄金、房地产、债券等多种现实世界资产的数字化与合规托管。系统结合分布式密钥生成（Distributed Key Generation，DKG）、EIP-712 签名标准、Ledger 硬件钱包和 Safe 多签合约，为金融机构和企业提供 **安全、合规、可扩展** 的多资产管理方案。

- **应用场景**：各类 RWA 代币托管、跨境结算、合规审计、多签协作
- **目标用户**：金融机构、资产管理公司、交易平台、合规托管方
- **核心优势**：
  - 多层安全：DKG + Ledger + Safe 多签
  - 金融级合规：支持 KYC（Know Your Customer，了解你的客户）/AML（Anti-Money Laundering，反洗钱） 与 ERC3643 等标准
  - 模块化架构：可扩展至多种 RWA 类型与多链部署
  - 现代化体验：React 前端、即时通信、Ledger 集成

2. 系统架构

平台采用分层架构：

- **前端**（React + wagmi）：多签控制台、交易提案、实时通知
- **API 网关**：认证、提案、签名、交易执行
- **业务逻辑层**：多签钱包、DKG 协调、交易路由
- **密码学引擎**：Curv DKG、EIP-712 验证、Shamir Secret Sharing（秘密共享）
- **存储层**：PostgreSQL + Redis
- **外部集成**：Ledger、以太坊/多链网络、SMTP 邮件

3. 技术栈

后端

- **语言**：Rust（Actix-Web + Tokio）
- **数据库**：PostgreSQL + Redis
- **密码学库**：secp256k1, ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）, SHA-2/SHA-3, AES-GCM

- **区块链交互**：ethers-rs，JSON-RPC，WebSocket

前端

- **框架**：React + TypeScript
- **Web3 集成**：wagmi, ethers.js, viem
- **UI**：Material-UI, Framer Motion, Lottie 动画
- **硬件钱包支持**：Ledger WebUSB 集成

区块链集成

- **多签合约**：基于 Gnosis Safe
- **合约标准**：ERC3643 等合规 RWA 代币标准
- **支持网络**：Ethereum、Base 及测试网
- **扩展性**：跨链部署与多资产托管

---

4. 核心功能演示

1. 用户注册与登录

登录 www.wallet.deepstonetech.com，进入多签系统登录界面，本系统的账号管理采用 JWT（JSON Web Token）+ 2FA（Two-Factor Authentication，双因子认证）方式登录认证，实时变更登录码，确保账号不被泄露。

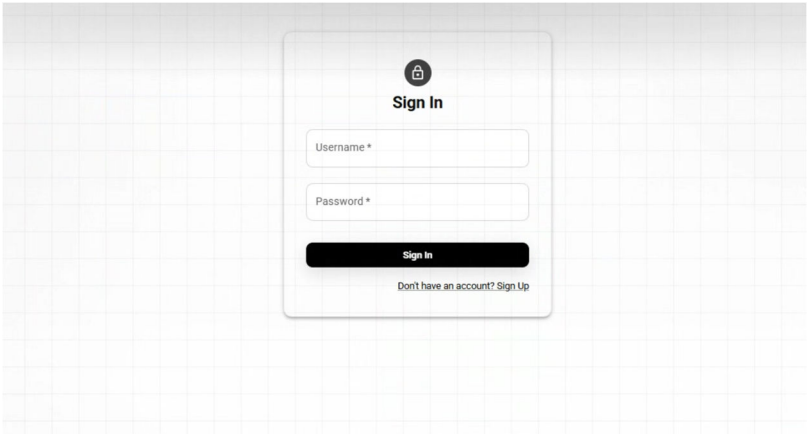

图 1 登录界面

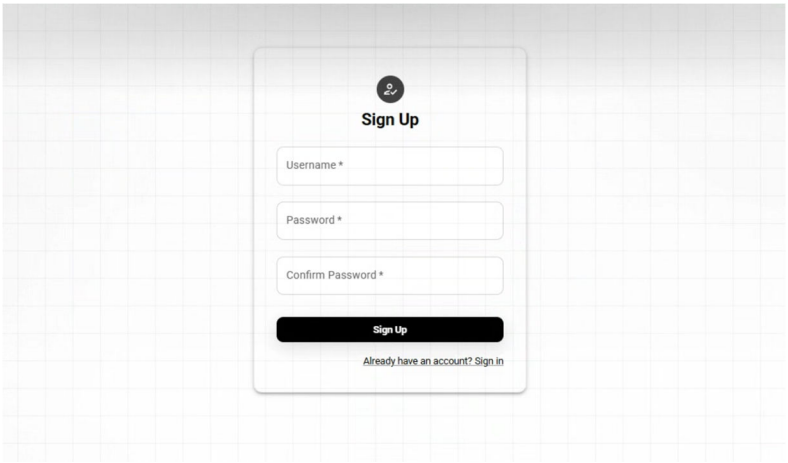

图 2 注册界面

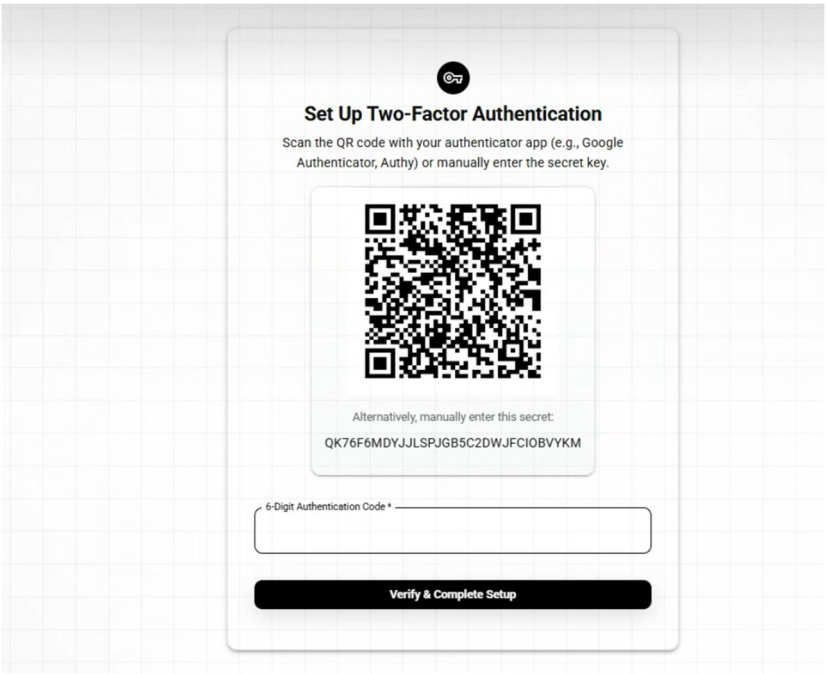

图 3 Authenticator 验证

2. 多签钱包系统

使用注册过的账号登录多签钱包系统，通过 Authenticator APP 获取验证码后进入多签系统主界面。

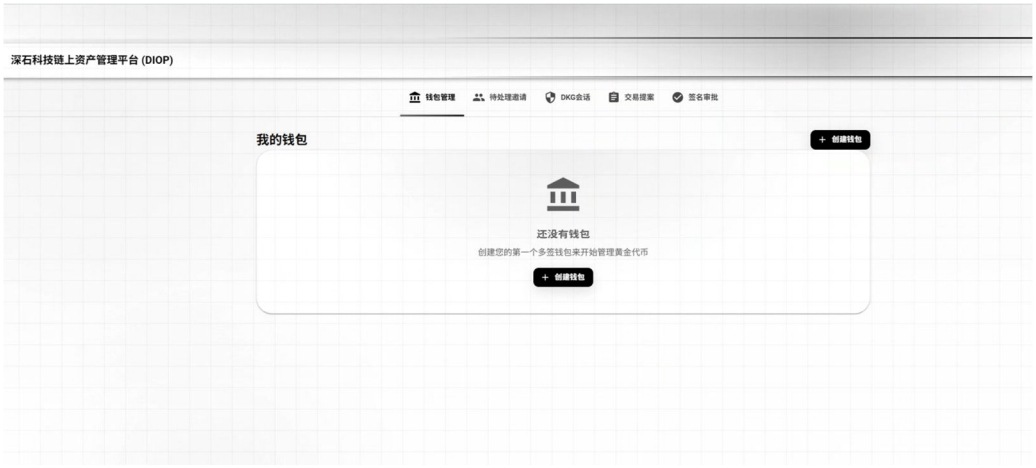

图 4 多签钱包系统主界面

（1）创建钱包

首先，点击创建钱包，输入自定义的钱包名称并选取签名阈值（2-of-3、3-of-5 等）。

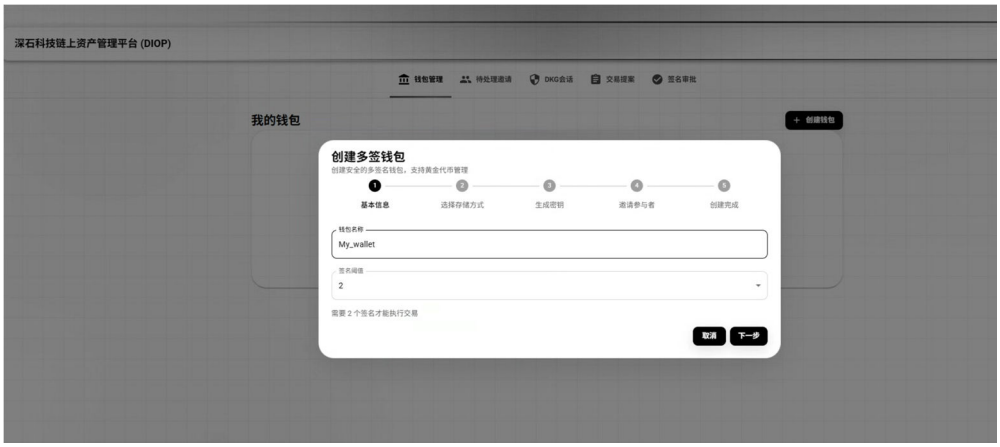

图 5 创建钱包

接下来选择存储钱包私钥的方式，本平台支持三种储存方式：
①自定义密码
②Ledger 硬件钱包储存（专用路径隔离（BIP32））
③密码+Ledger 硬件钱包双重储存

图 6 选择储存方式

通过分布式密钥生成（DKG）生成秘钥。该生成过程包含了 Merkle Tree 构建与根哈希验证；zk-SNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge，零知识简洁非交互式知识论证）证明生成与验证。

图 7 生成秘钥

接下来，邀请参与者审批，创建钱包（示例为邀请一位参与者）。

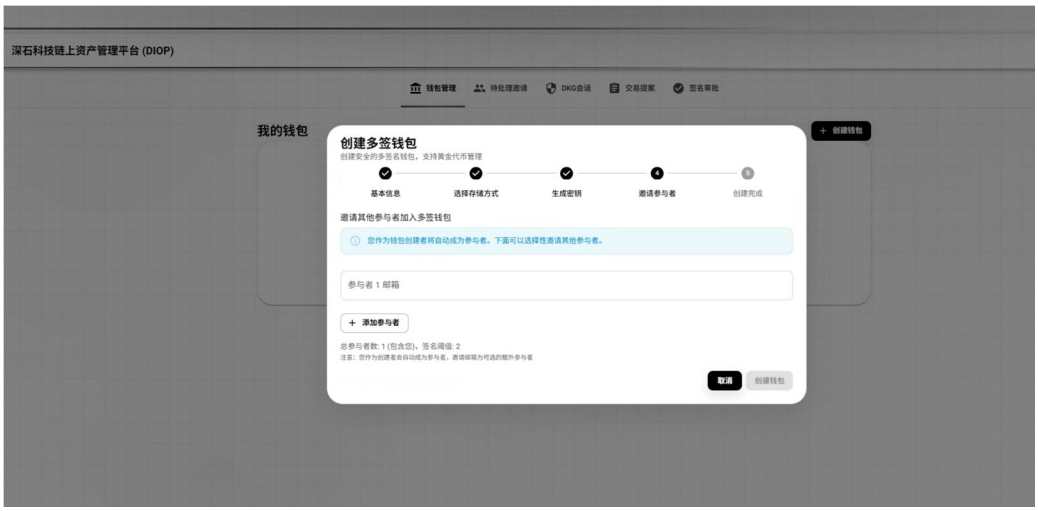

图 8 邀请参与者

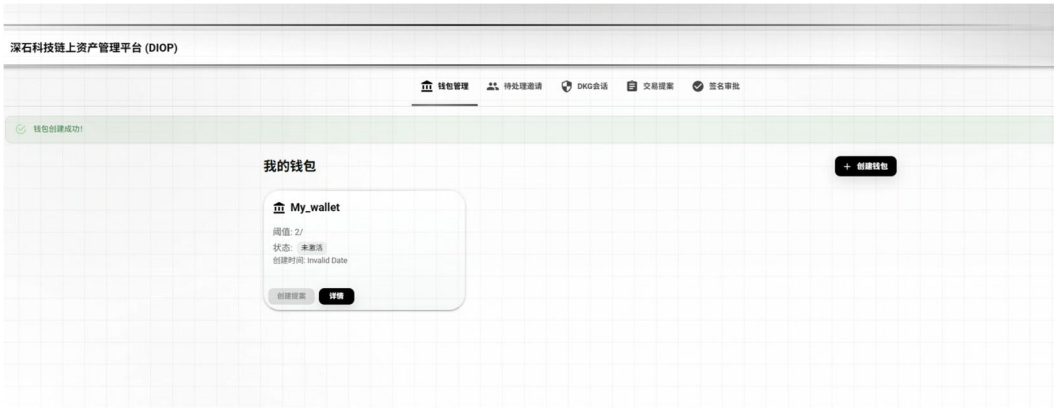

图 9 待参与者审批状态

此时，被邀请者需要登录多签系统，进入待处理邀请选项选择加入钱包，同时也需要选择秘钥储存方式、进行 DKG。

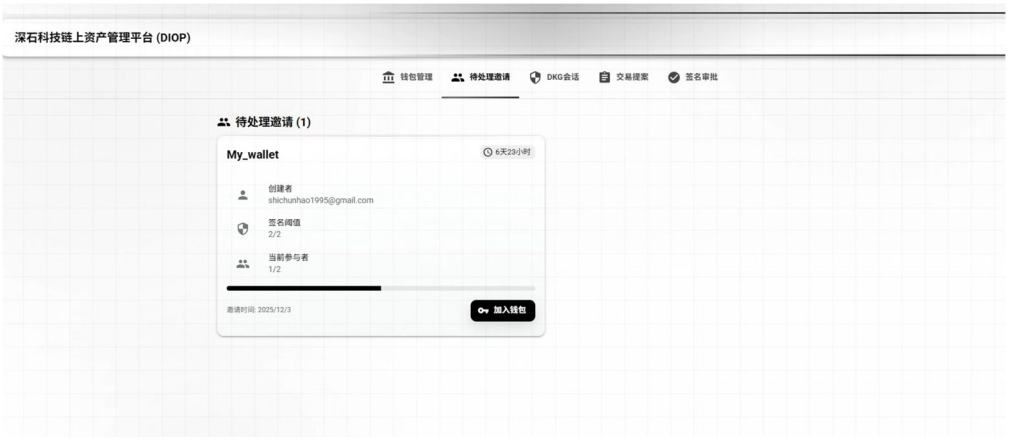

图 10 参与者审批、加入钱包

至此，多签钱包已创建完成。

（2）交易提案

创建钱包成功后，钱包的参与者可发起需被审批的提案。首先选择钱包、选择操作类型（铸造、销毁、添加或移除白名单）、铸造数量、接收地址以及 RWA Token ID。

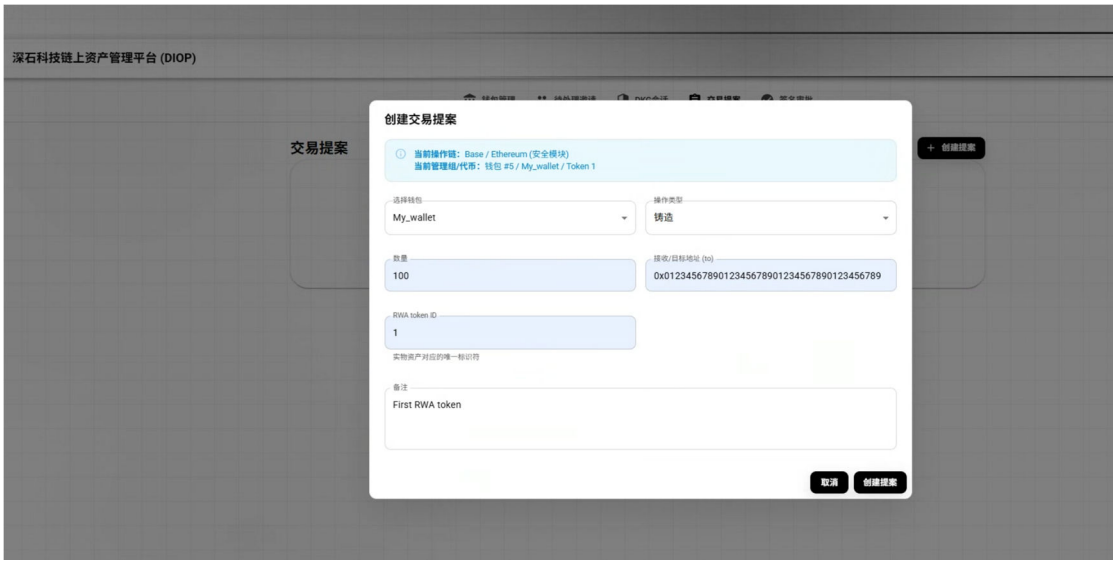

图 11 创建提案

此时该提案已被创建，需要创建钱包时的参与者进行签名，签名通过方可完成提案请求。

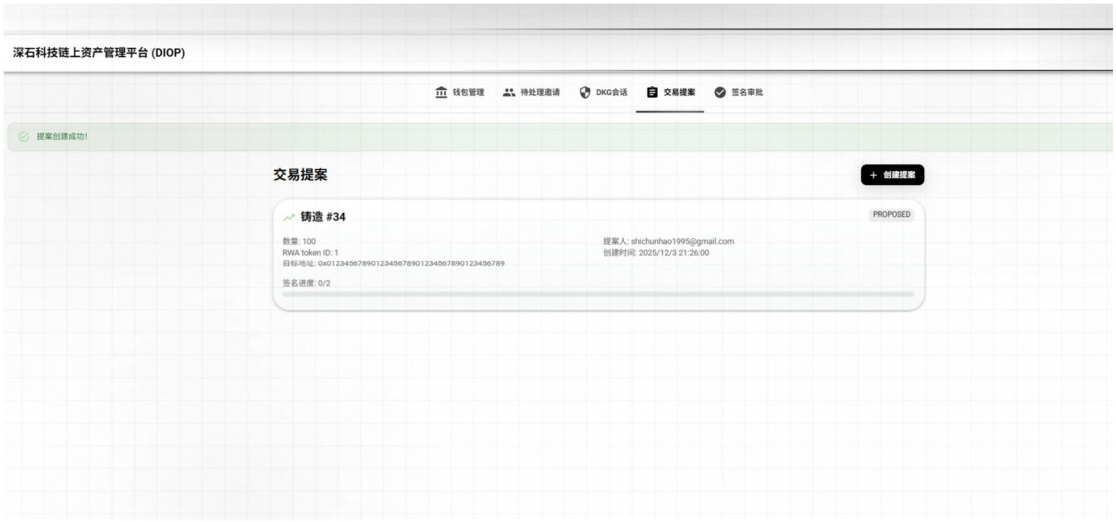

图 12 待签名的提案

钱包的其他参与者在多签系统中进入签名审批选项，可以看到待处理签名的提案。

图 13 签名审批

待参与者签名通过后，该提案方可通过。

图 14 通过提案

5. 联系方式

- 技术支持：deepstonetech@gmail.com
- GitHub：https://github.com/DeepStoneTech