JADE POOL

瑶池宣传手册

JADEPOOL.iO

BACKGROUND

自 2008 年诞生以来，区块链因其独特的去中心化概念和开源技术成为全世界的焦点。随着区块链生态和市场的快速发展，不断有交易所和钱包由于对加密数字资产的保护不善被黑客攻击而导致大量资产丢失。因此监管政策对相关方面加强重视，例如 SEC “Dodd Frank”法案规定，任何存储用户加密数字资产总额超过 $150,000 的企业必须将资产托管在合格的托管机构。由此，加密数字货币托管应需诞生，以用来安全存储和管理企业的加密数字资产。

WHAT IS JADEPOOL

瑶池，英文名 Jadepool，又称热钱包，是拓链（上海）科技有限公司（NBLTrust）针对企业级客户开发的用于安全存储和快速提取多种加密数字货币的资产托管系统。瑶池系统具有高安全性，需要配备硬件钱包，用户存放在瑶池的加密数字资产总额可根据客户需求设定以一定比例被安全分离存储在冷钱包中，其余则是用于应对用户提取存款的流动资产。另外，瑶池可与 NBLTrust 开发的密码机 HSM 对接，形成一套完整的具有更高安全性的资产托管体系，以全方位保障客户的资产安全。瑶池现已支持以下加密数字资产：BTC, USDT, ETH, ERC20, EOS, XRP, LTC, XLM, NEO, NEP5, VET, QTUM, ZCASH, CYB。

FEATURES

密码机 HSM

密码机 HSM 是 NBLTrust 开发的专为瑶池业务打造的应用层数据密码机，是物理安全的硬件，承担保管私钥、验证交易和签名的角色。HSM 与瑶池对接可形成一套完整的具有更高安全性的加密资产托管系统，以最大限度保障瑶池私钥和交易的安全。

冷热分离

瑶池作为热钱包，需另外配备硬件冷钱包。客户可根据需求调整存放在瑶池和冷钱包中的资产比例。冷钱包用以保障存放在瑶池大部分资产的安全，其余则是用于应对用户提取存款的流动资产。

支持多种加密资产

瑶池支持多种加密数字资产的托管。每种加密数字货币的区块链都有其特殊性，所以瑶池是一个能够高效兼容多个区块链的通用系统。瑶池可应客户需求增加对更多资产的支持。

高性能

在微服务架构的基础上，瑶池支持分布式多机部署，也就是一台机器可以只处理对于一条区块链的监测和充值提现请求。这样不仅分散安全风险，更大幅提高处理请求效率。

支持高并发

在高并发请求的环境下，瑶池仍然能够安全、有序、无阻塞地处理用户的充值提现请求。

独立部署

每个客户需独立部署一套瑶池系统，所有配置和数据由客户掌控。另外，瑶池部署使用 DOCKER，整个部署过程简单快捷。

可视化管理

瑶池 Admin 是专门为瑶池系统开发的一款后台管理系统，可以协助客户全方位掌控瑶池运行状态。不同角色和账户可在被超级管理员限制权限的基础上对瑶池进行读写操作，例如查看余额、修改配置、管理用户、查看运营和审计情况等等。

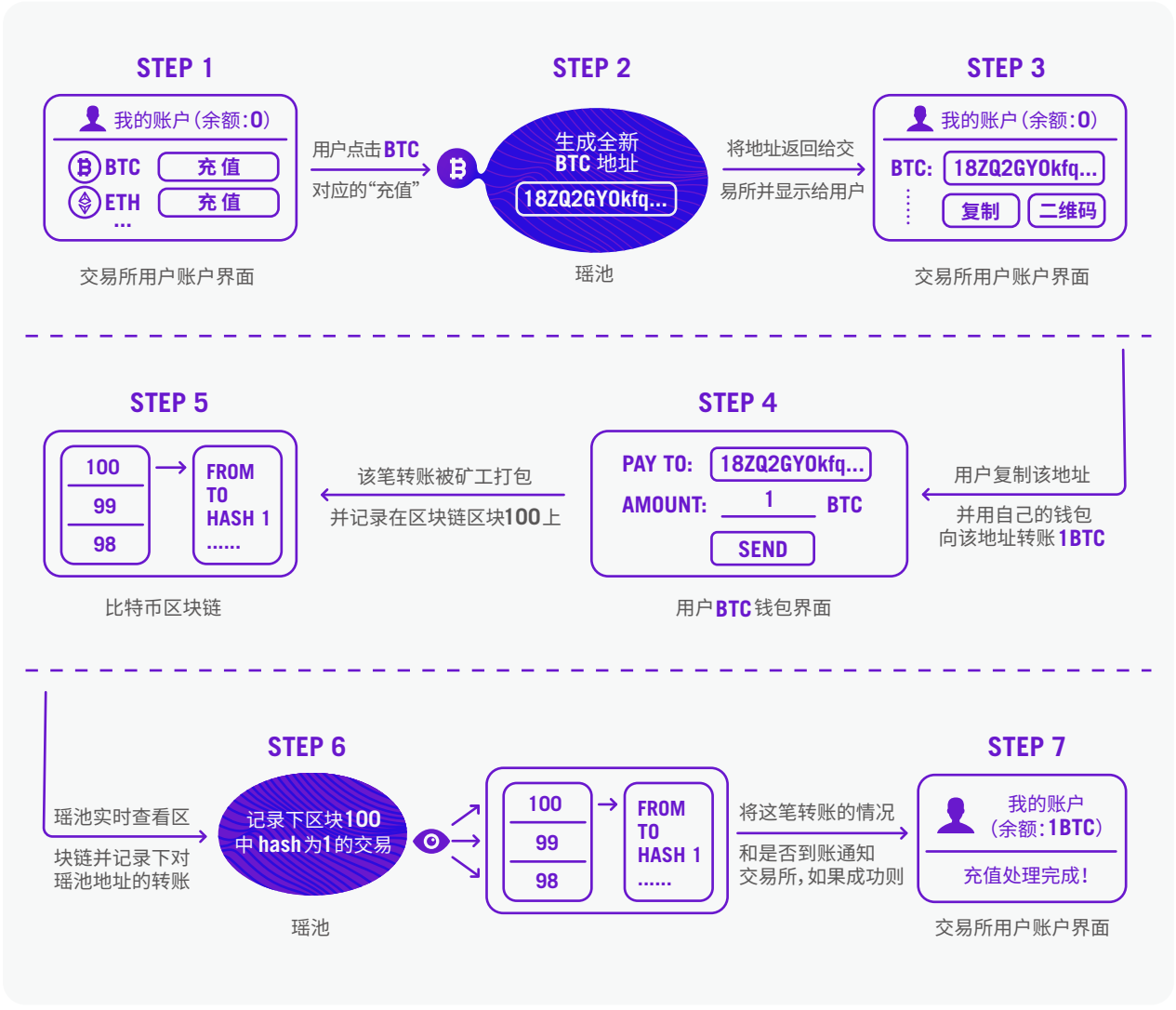
PRODUCT DETAILS

充值业务

当用户向瑶池内存放某加密数字货币，只需通过客户系统在瑶池获取一个该币种的地址，然后用自己的钱包向该地址转账即可。随着充值交易被区块链记录并确认，瑶池会通知客户系统该笔充值的到账情况。

充值示意图：

用户向自己在交易所的账户内存放 1 个比特币，所有步骤如图所示。



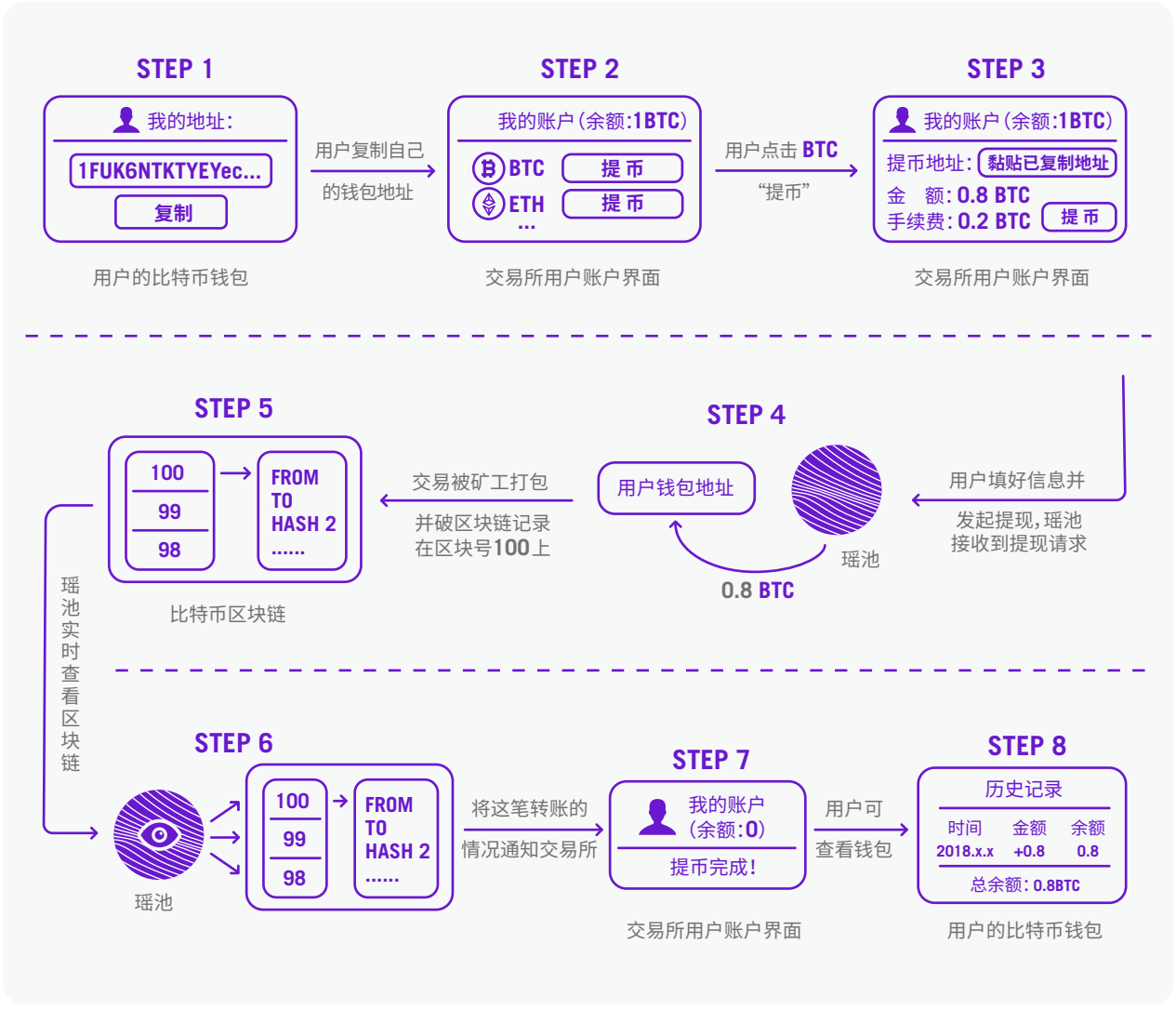
PRODUCT DETAILS

提现业务

当用户在瑶池中存放的资产大于可提取金额(对接客户对用户收取的提现手续费或者设定的提现最低金额),用户可通过客户系统发起提现。瑶池会处理用户的提现请求并向用户的钱包地址发起转账。随着交易被区块链记录并确认,瑶池会通知客户系统该笔提现的到账情况。

提现业务示意图:

用户从交易所提现 1 个比特币到自己的钱包,所有步骤如图所示。

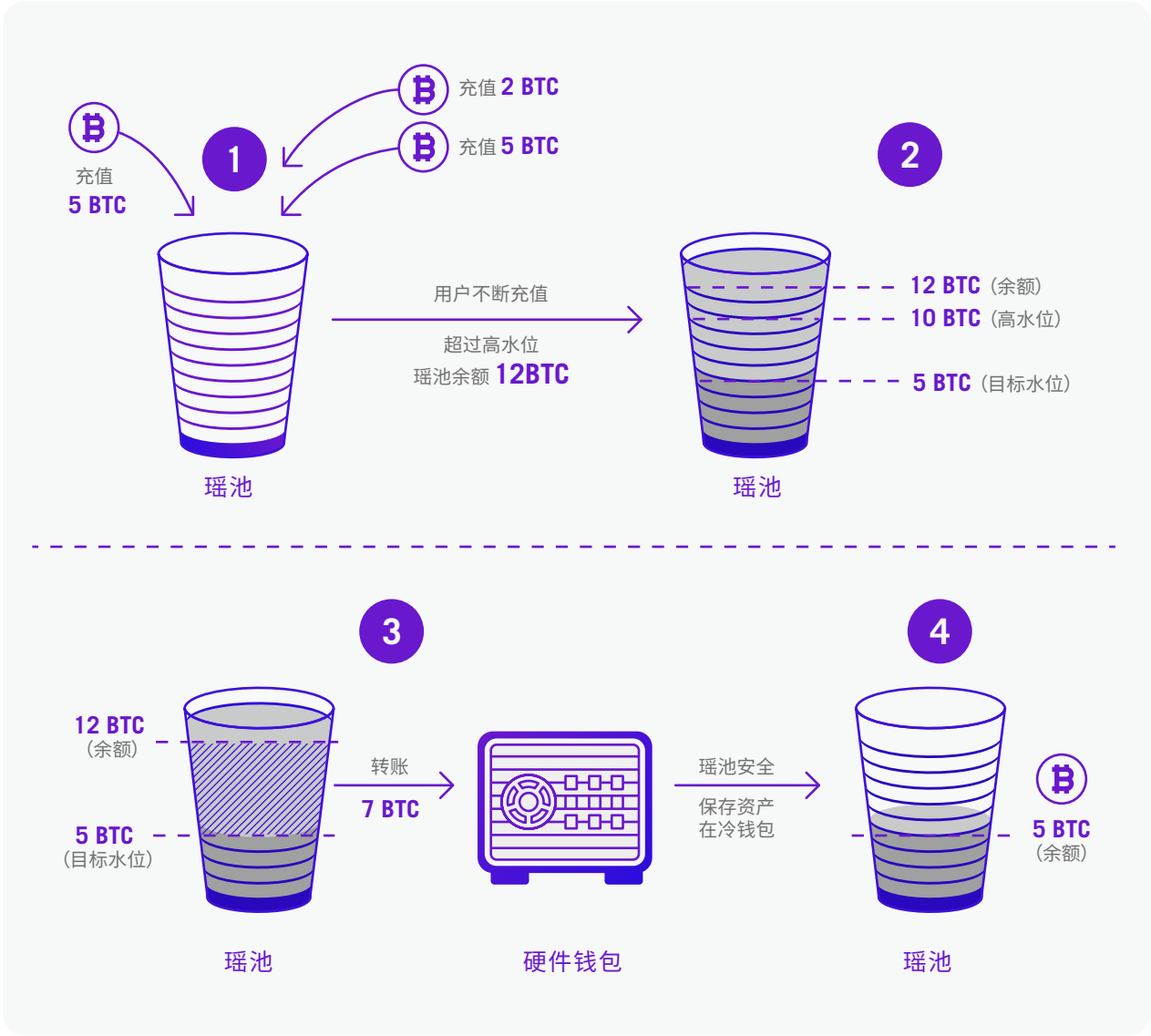


PRODUCT DETAILS

热转冷

为了保障客户的资产安全，瑶池需要对接硬件钱包形成完整的高安全性资产管理系统。硬件钱包，即冷钱包，是安全的离线设备，可以离线存储私钥免受黑客攻击。客户可以通过瑶池Admin后台管理系统对每种加密数字货币设定合理的水位，当加密数字货币的金额超过其高水位，瑶池会自主发起一笔热转冷交易。

热转冷示意图：

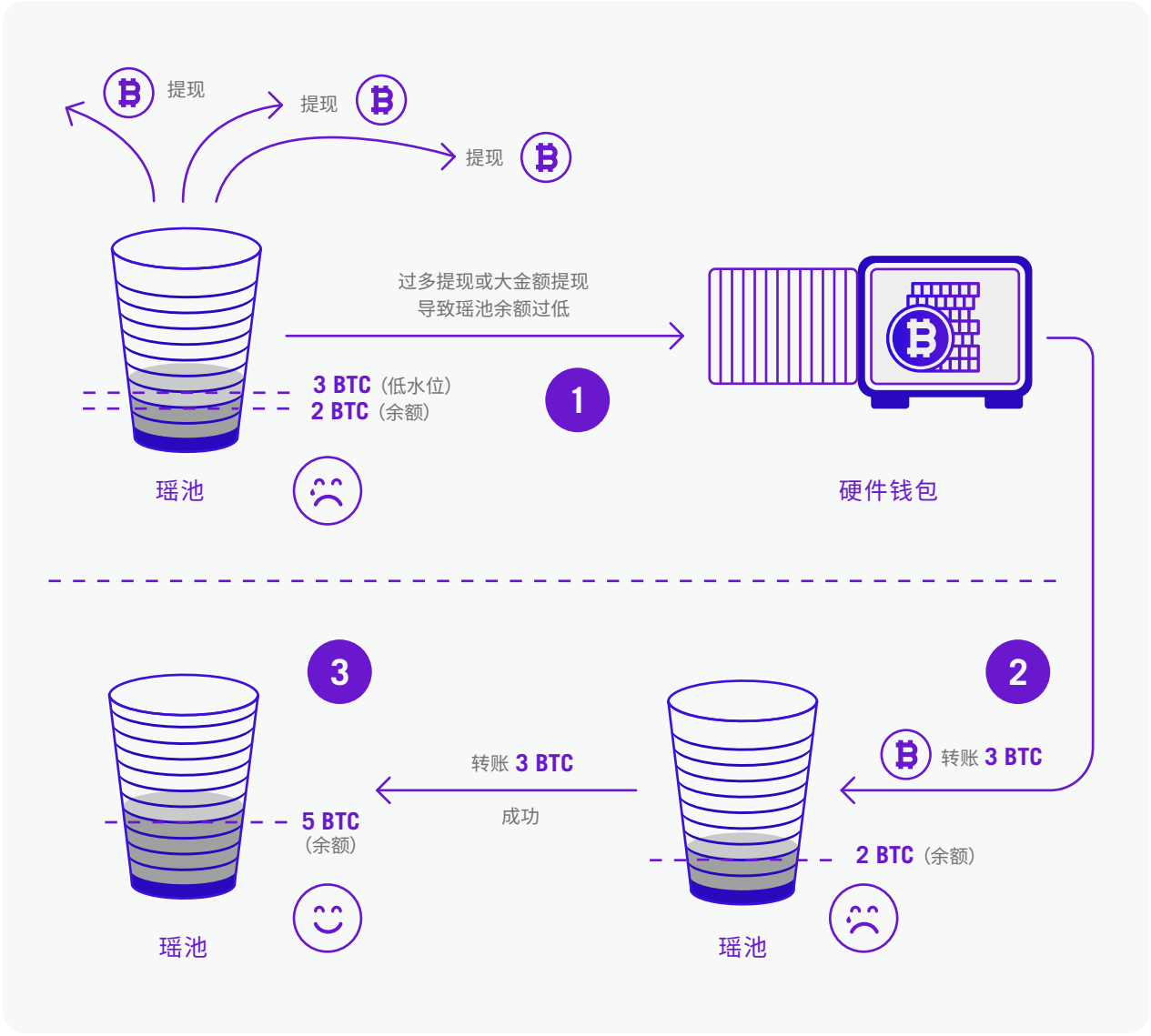


PRODUCT DETAILS

冷转热

若瑶池内某加密数字货币余额低于其低水位，瑶池会向客户发送余额告警邮件。客户可按运营需求通过与瑶池对接的硬件钱包向瑶池发起“冷转热”转账操作，以保证有足够的流动资产应对用户的提现请求。因硬件钱包是离线设备且并不属于瑶池系统，所以“冷转热”操作必须由人工手动发起。

冷转热示意图：



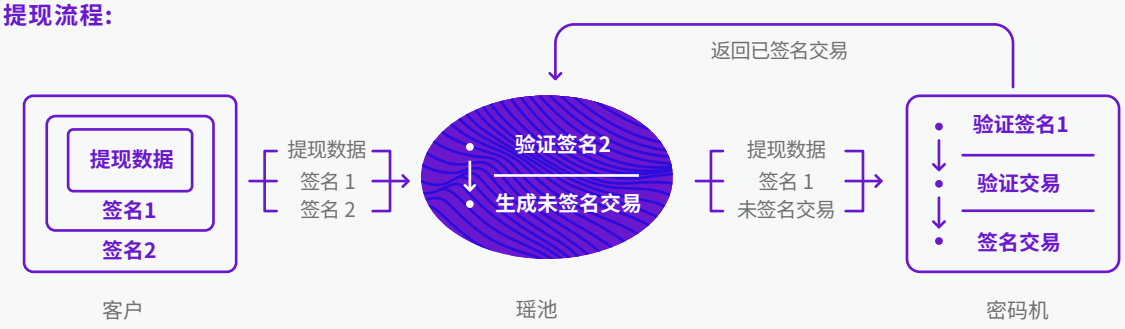
PRODUCT DETAILS

密码机 HSM

密码机 HSM 是一款专为瑶池业务打造的应用层数据密码机，是物理安全的实体，承担和瑶池业务安全相关的所有核心功能，例如生成 SEED、生成和还原衍生地址私钥、验证交易真实性和签名等，还将瑶池的“热转冷”逻辑整合于其中，保证了热钱包向冷钱包转账过程的资产安全。此外，密码机使用多签加密 USB KEY 进行配置管理（例如私钥备份、修改密码、增加 / 修改 / 查询数据等），配置管理需要一定数量以上的加密 USB KEY 授权才可以进行。密码机还配置了启动加密 USB KEY，启动密码机需加密 USB KEY 授权才能正常工作。

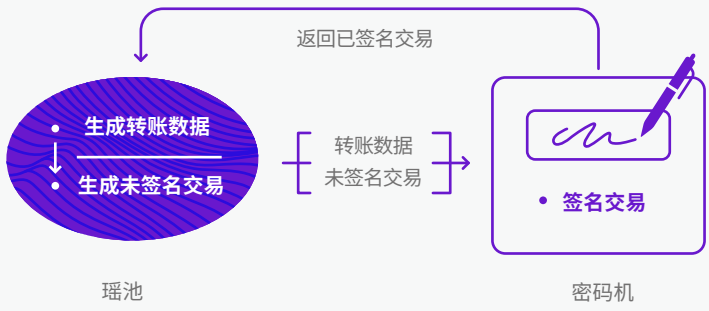
密码机示意图：

提现流程：



1. 客户对提现数据进行签名生成签名 1，再对提现数据 + 签名 1 进行签名生成签名 2
2. 将提现数据、签名 1、签名 2 传给瑶池
3. 瑶池验证签名 2，生成未签名交易
4. 将客户原始提现数据、签名 1 和未签名交易传给密码机
5. 密码机验证签名 1，解析未签名交易，根据提现数据验证未签名交易，验证通过后对未签名交易进行签名
6. 将已签名交易返回给瑶池
7. 瑶池发布交易

热转冷/内部转账流程：

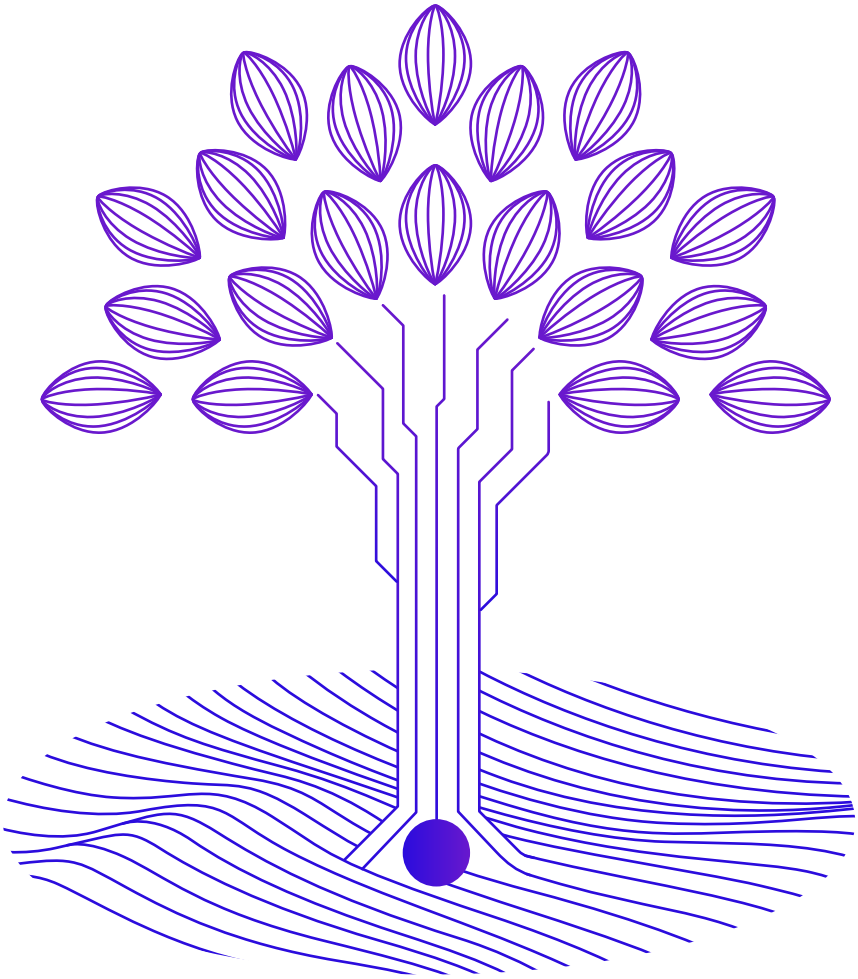


1. 瑶池根据业务逻辑生成热转冷 / 内部转账数据，生成未签名交易
2. 将转账数据和未签名交易传给密码机
3. 密码机对未签名交易进行签名
4. 将已签名交易返回给瑶池
5. 瑶池发布交易

PRODUCT DETAILS

SEED VAULT

SEED VAULT 软件是 NBLTrust 开发的密码机 HSM 的可选择替代解决方案。该软件可生成 SEED，其被用来和瑶池生成的衍生路径结合生成和还原私钥和衍生地址。SEED 被加密存储于服务器本地，通过客户设置密码保护和设置白名单的方式以保证其安全性。另外，SEED VAULT 也是一个数据保险箱，会存储很多瑶池重要数据，客户也需设置被瑶池用来组成交易的重要数据，例如冷钱包地址，这些数据都会被加密存储于服务器本地。与 SEED VAULT 相比，密码机 HSM 安全性明显更高，但若需要支持新的加密数字资产，SEED VAULT 软件升级会比 HSM 的固件升级更快。



对于每一种加密数字货币，瑶池都利用其独特的衍生路径和 SEED 结合生成和还原衍生地址和其对应私钥。

= 地址 + 公钥 + 私钥　= SEED

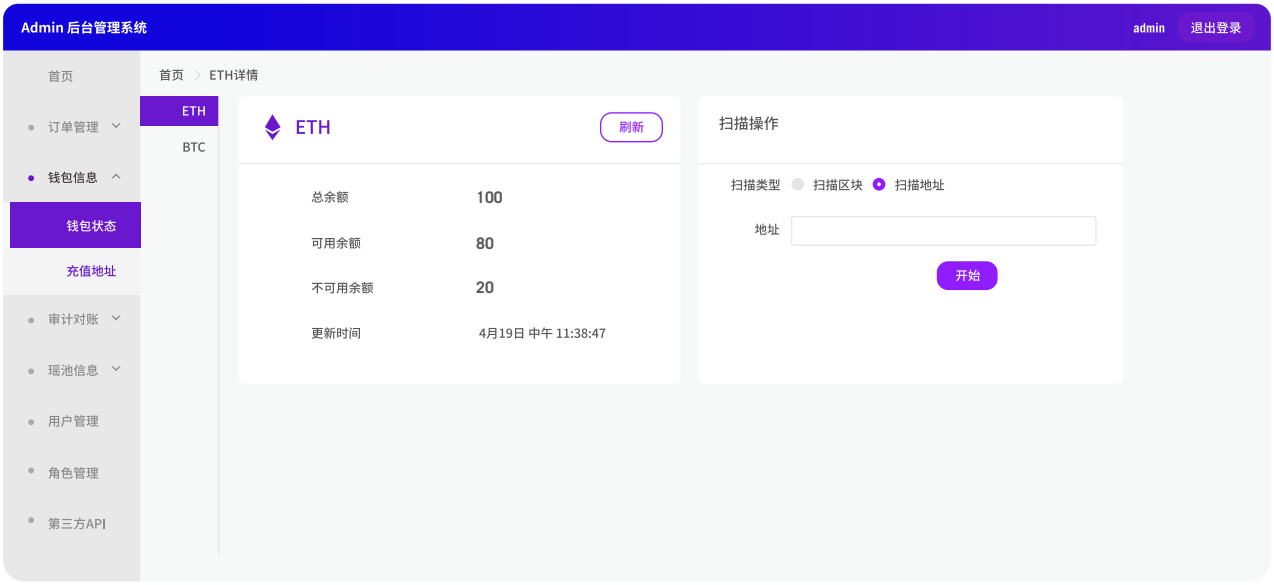
= 衍生路径　= JADEPOOL

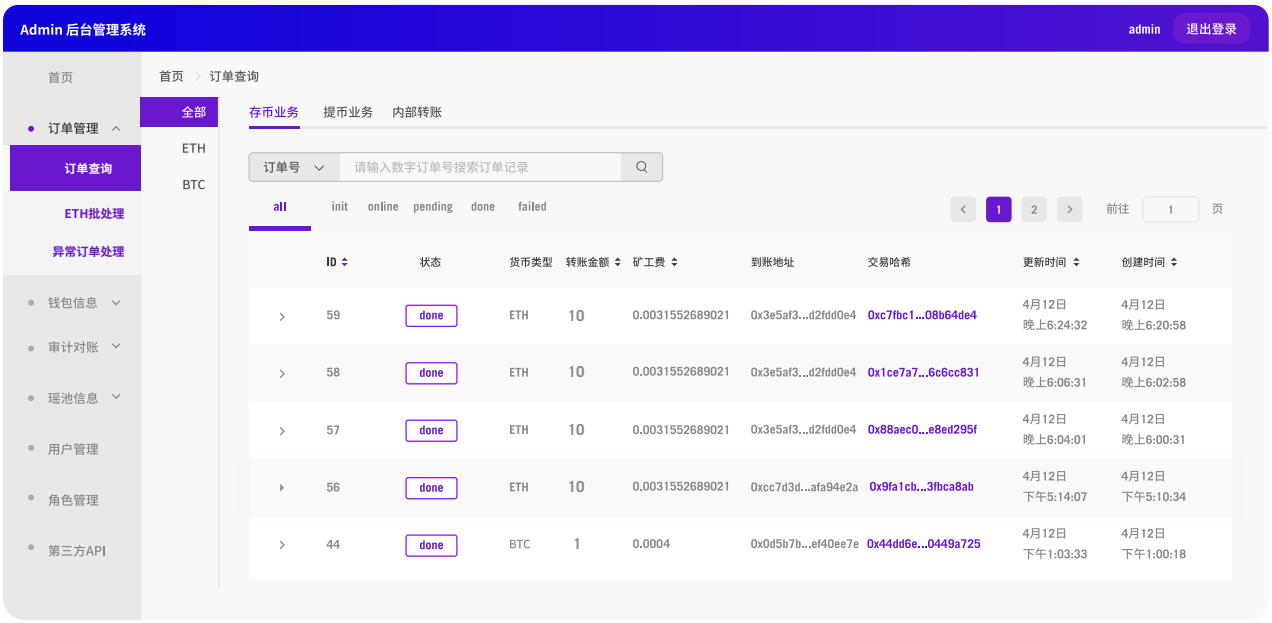
PRODUCT DETAILS

Admin 后台管理系统

Admin 是专门为瑶池系统开发的一款后台管理系统。Admin 不仅可以有效辅助客户的运营人员掌握瑶池信息，比如订单查询、余额状态、区块链高度等等，还可以在限制权限的基础上对瑶池进行修改操作，例如更改瑶池配置、管理用户和重新扫描交易等等。

Admin 界面示意图：





BUSINESS PARTNERS

Cybex

Cybex 是去中心化加密数字资产交易所。瑶池作为 Cybex 的官方合作伙伴，良好支持了 Cybex 官方发行加密数字货币 CYB，更为 Cybex 提供了高安全性、高稳定性的加密数字资产托管服务。

HashKey Pro

HashKey Pro 是位于香港的全功能数字资产交易平台。HashKey Pro 高度重视资产安全，与瑶池长期保持合作关系。

HashQuark

HashQuark 是专注于 POS、DPOS 以及其他共识机制公链的新一代区块链矿池，具有一支背景专业，经验丰富的技术团队。HashQuark 团队在安全、透明、高效的基础上，为用户提供挖矿服务。

everiToken

everiToken 是世界上第一个以 token 为中心而架构的公有链项目，具有高 TPS，高安全性和高标准化三大技术特点。everiToken 对自身合规性要求极高，特使用瑶池进行资产内控管理。

Saphirstein

Saphirstein 是位于苏黎世的新兴金融机构，专为传统银行及资产管理公司提供专业的数字资产投资服务。作为紧密的合作伙伴，NBLTrust 为 Saphirstein 提供全套数字托管系统，包括瑶池与硬件钱包设备。Saphirstein 预计在 2019 年初获得瑞士银行牌照。

ChaiNext

ChaiNext 专业指数团队由国内证券行业顶级专家和工程师组成，是区块链和通证市场指数及投资分析工具提供商，致力于打造区块链和通证市场的 MSCI。依托自身在金融产品设计、底层系统架构方面的优势，致力于打造区块链和数字代币领域的全产业链基础服务设施。

JADE POOL

JADEPOOL.IO