瑶池使用前须知

瑶池团队
contact@jadepool.io
上海市虹口区乍浦路 512 号
SOHO 3Q

目录

瑶池使用前须知

什么是订单？

订单是瑶池处理请求和记录交易的基本单位。是瑶池所有逻辑的根本依据。

订单有哪些类型？

1. 充值(DEPOSIT)：检测到用户向瑶池的充值地址转账正确币种类型而生成的订单类型。
2. 提现(WITHDRAW)：收到提现请求后生成的订单类型。
3. 热转冷(SWEEP)：余额高于高水位设置，自动触发热转冷转账而生成的订单。
4. 冷转热(RECHARGE)：检测到从冷钱包地址向热主地址转账而生成的订单类型。
5. 异常入账(RECHARGE_UNEXPECTED)：检测到内部地址以外的地址向热主地址转账，或者充值地址收到错误类型币种的转账而生成的订单类型。
6. 空投(AIRDROP)：检测到从设置的空投地址发起的转账而生成的订单类型。空投来源地址可以设置多个。
7. 内部出账(SWEEP_INTERNAL)：对于某些币种（例如ETH）来说，瑶池需要将散落在充值地址的金额汇总到热主地址，即内部地址向内部地址转账，该类型是转出而生成的订单。
8. 内部入账(RECHARGE_INTERNAL)：为审计结果的准确性，每个内部出账订单对应一笔内部入账订单。
9. 特殊入账(RECHARGE_SPECIAL)：目前只有NEO的claim gas行为应用此订单类型。

订单有哪些状态？状态流转过程是什么？

1. 未处理(init)：指瑶池已收到提现请求，但还未开始处理。
2. 预处理(holding)：将交易发上链前的预处理状态，订单长时间处于holding状态会被认为是异常订单并需要人工介入。
3. 已发送(online)：指瑶池已成功向节点发送交易（出账类订单）。
4. 已上链(pending)：指交易已成功上链并已被打包在某一区块中，但仍需一定数量的新区块产生以确认交易不可逆。
5. 不可逆(done)：订单最终状态，指交易已达到足够的区块确认数，交易不可逆。
6. 失败(failed)：订单最终状态，指交易失败。

状态机请参照“入账状态机示意图”和“出账状态机示意图”。

什么情况下订单会失败（failed）？

交易上链失败：瑶池发送的交易可能会被节点抛弃。

区块链拥堵：该情况在以太坊常见。

智能合约执行失败：该情况在以太坊常见。以太坊交易成功但内部智能合约执行失败，也

就是交易付ETH矿工费成功但并没有转账代币成功。发生该情况可能由于gas不够或者执行违反合约操作（合约报错），例如转账超出余额的金额。

区块链分叉：该情况针对入账交易。瑶池已通过配置“防分叉检测间隔”避免因为分叉而检测错误的入账交易，但不能完全消除这种可能性。如果在软分叉期间在弱势链上检测到入账交易，但交易没被打包在强势链上，分叉结束后交易并不存在链上，订单失败。

什么情况下会生成异常入账（RECHARGE_UNEXPECTED）订单？

对于EOS和CYB来说，如果转账来自于除冷钱包以外账户并且交易memo不是瑶池提供，会生成异常入账订单。对于其他链，除冷钱包地址和充值地址以外的地址向热主地址转账都属于异常入账。如果链除了主币以外还开启有其他代币，向充值地址充值错误类型的币种也属于异常入账。

什么情况下订单会停留在 holding 状态？

当瑶池将交易发送至节点（上链）报错，订单会停留在holding状态。但上链报错不代表交易一定发送失败，所以holding订单需要人工介入，在链上确认交易是否发送成功并做出相应的处理。

什么是高水位、低水位和目标水位？设置三个水位的依据是什么？有没有参考值？

高水位：瑶池热钱包内可存放的金额上限，超过该水位则和“目标水位”参数搭配控制转入冷钱包的金额。

目标水位：当瑶池热钱包内该币种金额超过高水位，转一部分金额去冷钱包后在瑶池剩余的目标金额。例如：若高水位为0.4BTC，目标水位为0.2BTC，现瑶池热钱包有0.5BTC，则应转0.3BTC到冷钱包，剩余0.2BTC在瑶池热钱包。

低水位：瑶池热钱包的金额下限，若余额低于此配置，则会发送告警邮件。

没有参考值。三个水位设置应根据应用方的用户流量、风险控制等级、每个币种对应法币价值等因素综合考虑。

对于高水位来说，设置越高则热转冷被触发的概率就越小，大量资产放在热钱包会面临高风险。若设置过低，则会频繁触发热转冷增加无端内耗。

对于目标水位来说，若设置太低，则会导致热转冷被触发后瑶池内余额太低，没有足够金额应对用户提现，反之若设置离高水位数值太近，则会导致不必要的频繁触发热转冷，导致消耗大量矿工费。

低水位的设置应仍足够用户提现，留充裕时间向热钱包补充。

提现超过高水位会发生什么？

会被瑶池拒绝处理（API报错）。

余额低于低水位会发生什么？

瑶池检测到某币种的余额低于低水位，会向在admin上开通了告警权限并设置邮箱的用户发送告警邮件。收到告警邮件后应立即向热钱包补充余额。

余额不足的情况下提现会发生什么？

瑶池仍然会接收提现请求。如果余额不足处理提现订单，订单会一直处于init状态，直到余额足够为止。余额不足处理的提现订单不会阻塞余额足够处理的小额提现订单。

什么是汇总？为什么汇总？

汇总是把用户向充值地址充值的金额转移到热主地址。以ETH为例，ETH的每个地址都有nonce（出账交易的递增序列号），并且交易转账来源地址只能有一个。瑶池为了方便管理地址和交易，将热主地址作为出账交易（提现和热转冷）的唯一来源地址。所以只有在热主地址的余额才是真正可以被使用的金额，充值地址的余额被汇总到热主地址以后才能被使用。

什么是热主地址？

热钱包主要地址。热主地址不是充值地址，不会提供给用户充值（除EOS和CYB以外，详情见“区块链相关常见问题”），一般被用来汇总、找零或补充热钱包余额。

什么是可用余额？什么是不可用余额？

可用余额：可以用作出账的金额。

不可用余额：即不可以用作提现的余额。以ETH为例，不可用余额等于散落在所有充值地址的金额总和。

瑶池判断订单完成（done）的依据是什么？

订单完成的标准是交易在链上不可逆。每个链都有交易不可逆区块确认数。以BTC为例，BTC的交易不可逆区块确认数是6，交易上链被打包进区块是第一个区块确认，之后再出五个区块就是对这笔交易的五次确认，加起来一共达到了六个区块确认，所以该交易不可逆，订单完成。

瑶池知不知道每个用户有多少资产？

不知道。瑶池没有用户的任何信息。用户信息、资产情况和用户与充值地址的关系只存在于应用方数据库中。

用户申请提现所产生的矿工费由谁承担？

实际由用户来承担。例如：用户在交易所（瑶池）存放了1BTC，当用户想提现时，最高只能提现0.9BTC，这时交易所向瑶池请求提现0.9BTC，交易所实际从用户手里扣掉了0.1BTC，除去提现消耗的矿工费以外其余则是交易所盈利。所以，应用方应该制定合理的用户提现手续费。

订单如果失败用户的钱有没有损失？

用户的钱是否损失取决于应用方。瑶池没有用户的信息。订单失败后瑶池会以回调方式通知应用方。只要应用方的处理逻辑正确，用户的钱不会损失。

瑶池的所有订单都是上链的吗？

所有订单均上链并在链上可查。可以通过admin查看订单并点击哈希跳转区块链浏览器查看交易详情。

瑶池是以什么顺序处理提现请求的？

按接收请求的顺序依次处理。但如果余额不足处理排在前面的提现，则会跳过该提现而优先处理后续的小额提现 。

瑶池怎么检测充值（入账类订单）？

在瑶池系统中启动的每条区块链都需要配置节点，随着节点不断和链的最高区块同步，瑶池会通过扫描节点最新同步到的区块中被打包的每笔交易进行判断，然后根据不同情况区分转账类型并将交易的信息以订单形式存储数据库。

什么是回调？

回调即瑶池通知应用方订单状态和审计结果的方式。对于每一个服务（appid），应用方可对每种订单类型设置回调通知地址。

审计的机制是什么？

瑶池审计的基本原理是按照应用方调用审计API传入的时间戳在数据库中找出出块时间最相近的区块，找出区块号（交易被打包的区块）在该区块之前并达到最终状态的所有订单并进行计算，也就是说瑶池数据库中的审计订单数据都是历史累计数据，审计结果是两次审计相减得出的。以目前的实现，如果通过调用审计接口进行审计，得到的审计回调是差值，只有充值和提现审计结果，未来会优化。在admin下载的审计报表中的数据也是差值，包含所有类型订单和对应费用的审计结果。

瑶池有没有提供 SDK？

有。目前只提供JAVA和NODE JS版本。

JAVA版本：https://github.com/nbltrust/jadepool-sdk-java
NODE JS版本：https://github.com/nbltrust/jadepool-sdk-nodejs

瑶池有哪些启动模式？有什么区别？

有dev、staging、production三种模式。dev和staging都使用测试链。dev是测试环境，ECC不开启，staging是预生产环境，ECC开启并且默认配置和生产环境的标准一样。production是正式生产环境，ECC开启并使用正式链。

瑶池是怎么保管私钥的？

瑶池所有地址的私钥均不存储在任何地方。0.12版本起瑶池可支持SEED和密码机两种模式，之前版本只支持SEED模式。如果使用SEED模式，瑶池需要seed和衍生路径两个部分才能使用私钥。seed被加密存储在部署SEED的服务器本地，充值地址的衍生路径存储在瑶池数据库，瑶池需要获取seed并结合地址衍生路径才能还原私钥并使用。如果使用密码机模式，seed和衍生路径根被存储在密码机中，密码机需要瑶池传入充值地址的衍生唯一序列号才能还原出私钥并对交易签名。

瑶池的防分叉机制是什么？

考虑到区块链的分叉可能性，瑶池为防止错误记录分叉期弱势链上的交易，对每个链都设置了符合该链情况的“防分叉检测间隔”参数。也就是说，瑶池只扫描当前最高区块头减去“防分叉检测间隔参数”的高度以下的区块。

什么是 ECC?

ECC是瑶池为保证通信安全而在内部各组件之间还有和应用方之间通信使用的加密算法。作为信息发送方的组件应有私钥对信息签名，而作为接收方的组件则需要有消息发送方的公钥以对信息进行验签。以瑶池和应用方的通信为例，两方都需要发送并接收信息，所以瑶池应配有应用方的公钥，应用方也应配有瑶池的公钥。瑶池的公钥可以在admin“系统配置”获得，配置应用方公钥也可以在同一个页面完成。

瑶池防止双提（同一个提币请求）的机制是什么？

0.12.0版本之后，提现接口增加sequence字段，每次请求提现传入该字段必须是唯一的数字，如果不唯一将会被拒绝处理。