**UniswapV3Ink-产品软件总体设计**

1. 2022.03.02 V1.0 WeiYong create by wangdong

# 概述及需求

在substrate链上创建一个基础的金融swap服务.该服务主要提供以下几点服务:

* 1. 该服务可以使普通用户作为流动性提供者提供资金流动性.并且流动性具有较高的资金使用率.
  2. 提供抽离流动性服务.可以部分抽取流动性.
  3. 提供的swap功能和当前价格的查询服务.根据用户提供的交易量和交易价格swap出不低于最小量的token.
  4. 提供交易的路由服务.提供一种token swap另一种token的交易路由.
  5. 提供最新价格服务.

# 系统结构

uniswapV3ink 的系统结构如下图所示：

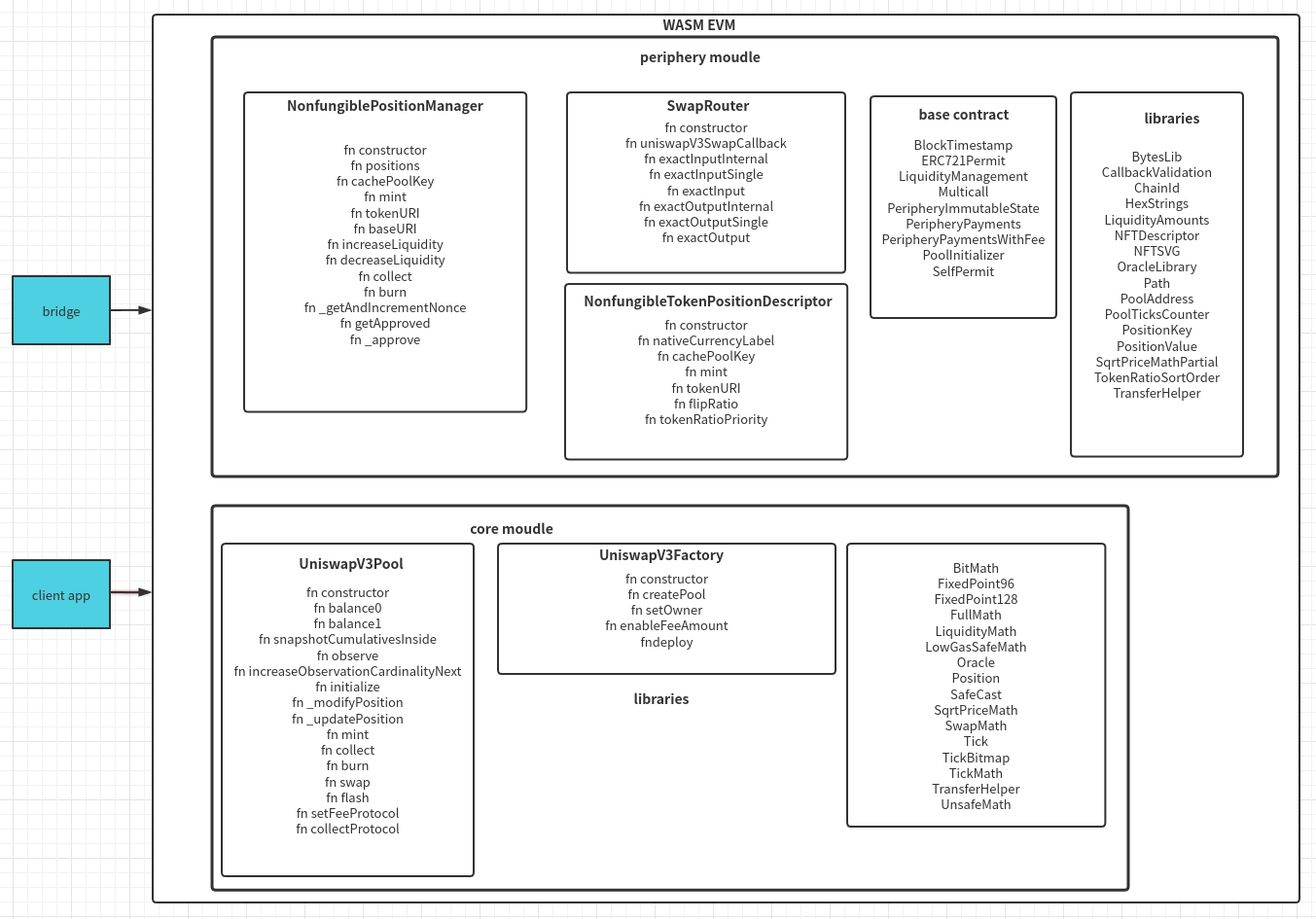


图1. uniswapV3ink系统结构

# 系统模块和功能

功能的具体流程图和计算公式见uniswap v3 白皮书,网址:https://www.jinse.com/news/blockchain/1057182.html

## 代码架构主要分为两个大的集合:

**core moudle**

**periphery moudle**

core 仓库的功能主要包含在以下 2 个合约中：

* **UniswapV3Factory**: 提供创建 pool 的接口，并且追踪所有的 pool
* **UniswapV3Pool**: 实现代币交易，流动性管理，交易手续费的收取，oracle 数据管理。接口的实现粒度比较低，不适合普通用户使用，错误的调用其中的接口可能会造成经济上的损失。

peirphery 仓库的功能主要包含在以下 2 个合约：

* **SwapRouter**: 提供代币交易的接口，它是对 UniswapV3Pool 合约中交易相关接口的进一步封装，前端界面主要与这个合约来进行对接。
* **NonfungiblePositionManager**: 用来增加/移除/修改 Pool 的流动性，并且通过 NFT token 将流动性代币化。使用 ERC721 token（v2 使用的是 ERC20）的原因是同一个池的多个流动性并不能等价替换（v3 的集中流性动功能）。

### ****NonfungiblePositionManager**** Module

* + 1. 初始化流动性池.

factory根据token0,token,fee判断该pool是否已经存在,如果不存在,则使用factory创建一个pool,并根据价格初始化该pool.

如果该pool已经存在,再检查该pool是否已经初始化.如果没有初始化,则调用pool的initialize进行初始化.

3.1.2 创建流动性

根据给定的factory和poolkey计算出pool的地址.获取pool的当前价格,计算出ticker的最高价和最低价.再根据这些参数我们能够计算出得到的流动性的值.

调用pool内的mint方法实现流动性的添加.修改用户的头寸.通过oracle获取ticker的累计值以及流动性累计平均秒数,再更新tickerLower和tickerUpper对应的tickerInfo.更新位图,调用position的update方法进行更新.

判断当前价格是否低于tickLower,如果是,则只需要计算amount0的值.

判断当前价格是否处于tickLowner和tickUpper内,如果是则更新oracle信息,计算amount0,amount1和增加后liquid的总量.

判断当前价格高于tickUpper,则计算需要的amount1的量.至此更新用户的头寸完毕.

回调****NonfungiblePositionManager**** 合约进行amount0和amount1的转账.

增发一个erc721的token转给增加流动性的用户.

* + 1. 添加流动性.

根据已有的erc721的tokenId添加对应的流动性.

流程与新增流动性差不多.后期不再增发一个ERC721的token.

* + 1. 抽离流动性.

根据tokenId获取存储的postion信息.检查头寸中的postion的liquid是否足够扣减.根据计算出来的poolkey计算出pool的地址.调用pool的burn方法减少流动性并得到减少流动性可以获得的amount0和amount1.

计算头寸的positionKey,通过pool的positions重新计算postion的累计手续费和liquid.

### ELC Basic Module

* + 1. ERC20 Fun

实现ELC token 基本的ERC20 标准功能

### Democracy Module

* + 1. Proposal Fun

实现提案提交， 排序， rELP锁定功能

* + 1. Vote Fun

实现投票提交，rELP锁定， 计票， 执行提案功能

### rELP Module

* + 1. ERC20 Fun

实现rELP token 基本的ERC20 标准功能

* + 1. CoinDay Fun

实现计算持有人的币天的统计，和各个奖励的清算。并统计已清算总奖励数。

* + 1. Reward Fun

实现ELC增发奖励到rELP持有人， 记录奖励数，及时间戳，并统计总奖励数。

实现rELP持有人提取奖励， 并统计总提取数。

* + 1. Liquidity Fun

实现rELP持有人获得流动性挖矿，获得ELP。 矿池总量：2,000,000 ELP， 首日总出矿量：20,000 ELP，每日递减系数：1%，

分30年分配。 每日从矿池转入，奖励给rELP持有人。

* + 1. Lock Fun

实现锁定功能，包括approveLock， lockFrom， unlock， lockInfo等功能， 并记录锁定人，锁定时间，锁定数量。

### ELC Stablization Module

* + 1. Token Swap

实现兑换功能，根据负债率LR（30%，70%，90%）等条件实现不同的兑换， 实现ELP兑换成ELC和rELP（LR<30%), ELP兑换成rELP（LR>=30%)，ELP兑换成固定价格的rELP（LR>=90%)。

ELC和rELP组合兑换ELP（LR<90%)。ELC和rELP组合不能兑换ELP（LR>=90 抗清算机制）。

* + 1. Supply Expanding

当ELC加权平均价格>ELCaim时，实现ELC供应量扩张功能，a. 将储备金中ELC释放出去， b. 将风险准备金中ELC释放出去，c. 直接增发ELC（要求LR<70%）， 其中5%放入风险准备金，并释放出去。其中95%直接释放奖励给rELP持有人，根据持有人的币天值分配。

每次数量<=价格冲击0.1%的数量。 外部服务调用监控时间间隔5分钟。

* + 1. Supply Thrinking

当ELC加权平均价格<ELCaim\*0.98时，实现ELC供应量紧缩功能，a. 将风险准备中ELP换出去，收回ELC， b. 将储备金中ELP换出去，收回ELC，每日使用ELP<=储备金数量的2%。

每次数量<=价格冲击0.1%的数量。 外部服务调用监控时间间隔5分钟。

* + 1. Risk Reserve Fun

实现风险准备金池功能，记录和使用池中ELC和ELP。

* + 1. Anti Inflation Fun

实现放通胀功能，根据通胀因子k，调整ELCaim，ELCaim初始值为$1, 在BSC，每隔20,000块将ELCaim的值提升k，调整ELCaim=ELCaim\*（1+k).