去中心化交易所开发文档

1.引言

1.1目的

本文档提供了去中心化交易所(DEX)开发所需的详细信息，包括功能模块、用户界面设计、后端服务架构以及安全性设计。

1.2范围

本文档涵盖以下主要部分:

功能模块描述

用户界面(UI)设计

后端服务架构

安全性设计

2.功能模块

2.1首页

轮播图:用于广告宣传。

币种涨幅榜:展示币种波动情况，如AU、UTO、BTC、USDT、ETH。

快捷按钮:提供帮助中心、自选、充值、提现等快速入口。

公告栏:展示最新公告。

2.2领空投

项目方发布空投:项目方可以发布空投活动，并填写合约地址。

用户领取空投:用户可以领取空投，需要填写钱包地址并通过去中心化身份验证。

2.3币种涨跌幅：我们将实时监控并更新币种的价格变动和涨跌幅数据，为用户提供即时的市场动态信息。

热门榜：代币通过将Uto代币转入黑洞的方式获得上榜资格，转入金额的大小直接影响其在热门榜上的排名，金额越大，排名越靠前。

审查榜(人工审查)：代币需支付一定的审查费用，提交至DAO组织委员会进行审查，以确定其是否符合平台标准，避免割韭菜等不正当行为。

主流币榜：(自动评估)

审查榜(自动审查)(一般模板开发或者是上架的都会自动通过)(检测是否有老鼠仓、公共储备资金和流动性池有没有上锁、上永久的是自动上榜)

上架要求：上架前，必须燃烧至少1枚Uto代币并转入黑洞，作为上架的基本条件。

排行机制：

燃烧数量：代币燃烧的Uto代币数量是决定其在热门榜、审查榜。行中位置的主要因素，燃烧数量越多，排名越高。

时间顺序：若代币燃烧的Uto代币数量相同，则按照燃烧时间的先后顺序进行排名，新近燃烧的代币将获得更高排名。

审查流程：所有代币在上架前需经过DAO组织委员会的严格审查，确保其合法性和安全性，防止不正当行为。

费用支付：代币上架前需支付审查费用，以支持DAO组织委员会的运营和审查工作。

透明度：所有上架代币的燃烧记录和审查结果将在平台上公开，保证整个过程的透明度和公正性。

持续监管：代币上架后，平台将持续对其进行监管，确保其持续符合平台的标准和要求，任何违规行为都可能导致代币被下架。

3.用户界面设计

3.1首页设计

首页应包含所有快捷操作入口，以及实时更新的市场信息。

应有清晰的导航栏，方便用户快速找到所需功能。

3.2领空投界面

界面应提供简单的表单填写，以便用户领取空投。

需要有明确的提示信息，指导用户完成领取流程。

3.3行情界面

行情界面应提供实时的数据更新和图表展示。

应有筛选和排序功能，使用户能够根据需要查看不同币种的信息。

3.4交易界面

交易界面应简洁明了，方便用户快速下单。

应提供详细的交易对信息和交易历史记录。

3.5行情走势

曲线图（分时）:展示市场深度和实时成交情况。

K线图:提供市场深度和成交信息，以及币种的发行时间、发行总量、流通总量等简介。

3.6 UtoSwapv1去中心化代币价值交换系统

UtoSwapv1的去中心化代币价值交换系统。该系统借鉴了Uniswap v4的架构，并引入了若干创新机制，旨在优化流动性和定价策略。以下是对该系统运行原理的详尽解析。

初步理解

UtoSwapv1采用了一种修改自Uniswap v4的流动性池模型。Uniswap v4以其自动做市商（AMM）而著称，通过恒定乘积公式\[ x \times y = k \]来管理代币交换，确保流动性的高效利用。UtoSwapv1在此基础上进行了扩展，引入了更复杂的池子结构和动态调整机制，以优化流动性和定价策略。

关键组件解析

1. 流动性池（LP）：作为系统的核心，LP池负责管理代币交换所需的流动性。LP池中的代币遵循恒定乘积公式，以维持价格的稳定性和流动性。

2. 代币池：代币池持有代币的供应量，用户可以向其中添加代币以获得流动性池的收益，或在需要时从池中移除代币。

3.对付储备金：该池管理用户在交换代币时存入的资金。这些资金根据预设的比例分配至LP池和代币池，以平衡流动性和代币价值。

4. 动态容差调整系统：该系统根据代币的流通量动态调整容差值，以控制代币价值的增长，确保其与市场条件相匹配。

1. 混合定价机制：结合了LP池和支付准备金池的输入，通过动态调整比例来确定代币的买入和卖出价格，从而优化定价策略。

https://github.com/Uniswap/v4-core

https://docs.uniswap.org/concepts/protocol/oracle

运行原理:

1.对付储备金与流通量:

代币的最低价值由对付储备金除以流通数量决定

2.代币池子输入:(默认权限直接锁黑洞)

用户可以向代币池子输入代币数量，同时添加新发行的代币。

对付储备金池子输入:(默认权限直接锁黑洞)

多币储备金池(可以添加多个币或者单个币作为对付储备金池)(按照USDT总价值计算)

用户可以向对付储备金池子输入代币数量(建议添加99.9%)(场外没有币)

添加LP流动性(初始价格相同)(默认权限直接锁黑洞)

设置(买入和卖出回流百分比 )范围是从最低值精确到18位小数，到最高值5%。

买入滑点( ) % U回流对付储备金池

卖出滑点( ) % U和币同时回流LP流动池

定价权

对付储备金池÷全网用户持有流通数量包含LP池子里面代币、不含主代币池、不含黑洞地址+每枚代币动态容差)=买入的价格

对付储备金池÷全网用户持有流通数量包含LP池子里面代币、不含主代币池、不含黑洞地址=卖出的价格

根据您的描述和搜索结果，以下是关于买入资金权重和卖出资金权重的计算公式，以及LP流动池和储备金池的资金分配机制的整理：

买入和卖出资金权重的计算

在DeFi流动性池中，资金权重的分配通常基于LP流动池和储备金池中的资产比例。权重的计算公式可以参考以下逻辑：

买入资金权重

当用户买入时，资金会按照LP流动池和储备金池的资产比例分配。权重计算公式为：

• LP流动池权重：

\[

\text{LP Pool Weight}=\frac{\text{LP Pool Assets}}{\text{LP Pool Assets}+\text{Reserve Pool Assets}}

\]

• 储备金池权重：

\[

\text{Reserve Pool Weight}=\frac{\text{Reserve Pool Assets}}{\text{LP Pool Assets}+\text{Reserve Pool Assets}}

\]

其中，LP Pool Assets表示LP流动池中的资产价值，Reserve Pool Assets表示储备金池中的资产价值。

卖出资金权重

卖出时的资金分配权重与买入时相同，也根据LP流动池和储备金池的资产比例计算。

资金分配机制

在买入或卖出时，资金会根据上述权重分配到LP流动池和储备金池：

• 买入资金分配：

• 分配到LP流动池的资金=买入资金×LP流动池权重

• 分配到储备金池的资金=买入资金×储备金池权重

• 卖出资金分配：

• 从LP流动池提取的资金=卖出资金×LP流动池权重

• 从储备金池提取的资金=卖出资金×储备金池权重。

应用场景

这种机制广泛应用于流动性引导池（LBP）和自动做市商（AMM）模型中。通过动态调整LP流动池和储备金池的资金分配，可以优化交易效率，减少滑点，并灵活应对市场变化。

1.权重比计算公式

权重比（Weight Ratio）是通过比较LP流动池中的代币数量与代币池中的代币数量来计算的。公式如下：

权重比=LP流动池代币数量/代币池代币数量

用数学公式表示为：

\(\text{Weight Ratio}=\frac{\text{LP Pool Tokens}}{\text{Token Pool Tokens}}\)

公式解释

• LP Pool Tokens：LP流动池中的代币数量。这个数量会随着交易的变化而动态更新。

• Token Pool Tokens：代币池中的代币数量。这个数量也会随着交易的变化而动态更新。

• 权重比：表示LP流动池与代币池之间的相对比例。权重比越高，说明LP流动池在整体中的占比越大；权重比越低，则说明代币池的占比更大。

2.动态变化的公式

在每次交易中，代币池和LP流动池的代币数量会根据交易量（Transaction Amount）增加或减少。具体公式如下：

增加代币

• 代币池更新公式：

\(\text{Token Pool Tokens}{\text{new}}=\text{Token Pool Tokens}{\text{old}}+\text{Transaction Amount}\)

• LP流动池更新公式：

\(\text{LP Pool Tokens}{\text{new}}=\text{LP Pool Tokens}{\text{old}}+\text{Transaction Amount}\)

减少代币

• 代币池更新公式：

\(\text{Token Pool Tokens}{\text{new}}=\text{Token Pool Tokens}{\text{old}}-\text{Transaction Amount}\)

• LP流动池更新公式：

\(\text{LP Pool Tokens}{\text{new}}=\text{LP Pool Tokens}{\text{old}}-\text{Transaction Amount}\)

3.权重比的动态变化

每次交易后，权重比会根据新的代币数量重新计算。新的权重比公式为：

\(\text{New Weight Ratio}=\frac{\text{LP Pool Tokens}{\text{new}}}{\text{Token Pool Tokens}{\text{new}}}\)

4.特殊情况处理

• 如果代币池中的代币数量为0（即\(\text{Token Pool Tokens}=0\)），为了避免除以零的错误，权重比可以定义为无穷大（\(\infty\)）。

• 如果LP流动池中的代币数量为0，权重比为0。

5.公式总结

以下是完整的公式总结：

• 权重比公式：

\[

\text{Weight Ratio}=\frac{\text{LP Pool Tokens}}{\text{Token Pool Tokens}}

\]

• 增加代币时的更新公式：

\[

\text{Token Pool Tokens}{\text{new}}=\text{Token Pool Tokens}{\text{old}}+\text{Transaction Amount}

\]

\[

\text{LP Pool Tokens}{\text{new}}=\text{LP Pool Tokens}{\text{old}}+\text{Transaction Amount}

\]

• 减少代币时的更新公式：

\[

\text{Token Pool Tokens}{\text{new}}=\text{Token Pool Tokens}{\text{old}}-\text{Transaction Amount}

\]

\[

\text{LP Pool Tokens}{\text{new}}=\text{LP Pool Tokens}{\text{old}}-\text{Transaction Amount}

\]

• 特殊情况：

• 如果\(\text{Token Pool Tokens}=0\)，则\(\text{Weight Ratio}=\infty\)。

• 如果\(\text{LP Pool Tokens}=0\)，则\(\text{Weight Ratio}=0\)。

6.应用场景

这些公式可以用于模拟流动性引导池（LBP）或类似的动态权重机制。通过动态调整权重比，可以根据交易量的变化灵活地控制两个池子之间的比例关系，从而实现更灵活的流动性管理和交易机制。

示例

初始条件：

中文名称：乌托邦币

英文简称：Uto

总供应量：1亿枚

锁仓0.9亿枚自动释放到代币池子

权限黑洞代币池子：1000万枚Uto 兑付储备金：1.01枚USDT

权限黑洞LP流动池 :1枚Uto 1.01枚USDT

初始价值1.01U

动态容差：1～5%(线性增加)每枚

容差代币区间:2～1000万枚

1000万以上容差保持5%

买入滑点0.5% U流回对付储备金池

卖出滑点0.5% U和币同时回流LP流动池

容差设置的动态计算

5.容差设置:(模式一可设定容差)

用户可以设置每一枚币容差值，容差值越大，代币价值的涨幅越快。

静态容差容:差值的范围是从最低值精确到18位小数，到最高值5%。

动态容差调整系统

运行原理

动态容差调整系统根据代币的市场流通量（用户持有的数量加上LP池子的数量）动态调整容差值。随着流通量的增加，容差值从起始容差线性增加到最终容差；相反，随着流通量的减少，容差值从最终容差线性减少到起始容差。这种机制确保了代币价值的涨幅与市场流通量成比例，同时保持了市场的灵活性和响应性。

参数定义

起始容差：代币市场流通量初始时的容差值。

最终容差：代币流通量达到一定阈值时的容差值。

流通量：用户持有的代币数量加上LP池中的代币数量。

运行公式

1. 每枚代币容差增加量：

\text{每枚代币容差增加量} = \frac{\text{最终容差} - \text{起始容差}}{\text{最多代币容差} - 1}

其中，\text{最多代币容差} 是达到最终容差时的代币数量。

2. 任意代币 x 的容差计算：

T(x) = \text{起始容差} + \left( \frac{\text{最终容差} - \text{起始容差}}{\text{最多代币容差} - 1} \right) \times (x - 1)

对于流通量减少的情况，公式调整为：

T(x) = \text{最终容差} - \left( \frac{\text{最终容差} - \text{起始容差}}{\text{最多代币容差} - 1} \right) \times (\text{最多代币容差} - x)

3. 简化公式：

T(x) = \text{起始容差} + \frac{(\text{最终容差} - \text{起始容差}) \times (x - 1)}{\text{最多代币容差} - 1}

对于流通量减少的情况：

T(x) = \text{最终容差} - \frac{(\text{最终容差} - \text{起始容差}) \times (\text{最多代币容差} - x)}{\text{最多代币容差} - 1}

注意事项

如果 x 超过 \text{最多代币容差}，容差将保持在最终容差不变。

如果 x 低于起始流通量，容差将保持在起始容差不变。

确保 x 不超过总发行量。

示例设置

起始容差：0.01%

最终容差：5%

最多代币容差：根据每种代币的发行量和自定义区间设置。

应用

该系统适用于需要根据市场流通量动态调整容差的代币经济模型，确保代币价值的稳定增长，同时适应市场流通量的变化。通过这种动态调整，系统能够更好地响应市场的需求和供应变化，保持代币价值的稳定性和市场的活力。

4.2API设计

API应提供完整的端点，以支持前端的所有功能。

应有安全措施，如认证和授权，保护API端点。

4.3服务器和网络

服务器应有足够的处理能力和存储空间。

网络应设计为高可用性和安全性。

5.安全性设计

5.1加密和认证

所有敏感数据应进行加密处理。

用户认证应采用多因素认证方式。

5.2防御机制

系统应具备防止DDoS攻击的能力。

应有定期的安全审计和漏洞扫描。

5.3合规性

平台应遵守相关的法律法规和行业标准。

应有透明的隐私政策和用户协议。

6.7安全性考虑

认证授权:确保只有订单的所有者可以查看、修改或取消订单。

数据加密:订单数据在传输和存储过程中应进行加密，以防止数据泄露。

6.8用户界面设计

直观展示:订单簿应直观展示所有挂单，包括价格、数量、订单状态等信息。

操作便捷:用户应能轻松地进行挂单、取消和修改操作。