UtoDePIN开发文档

1.区块链网络

1.1L1节点

功能描述：处理区块链主网事务的节点。

1.2区块链网络

Fork以太坊：Fork以太坊（Ethereum），再根据项目需求进行优化和改造。

1.3创世区块

独立公链：创世节点独立分发。

开源：开源，2进制核对开源系统。

1.4网络切换

正式网络：正式网络。

测试网络：测试网络。

2进制核对开源系统：2进制核对开源系统。

1.5USDT跨链

第三方跨链系统接入公链底层：第三方跨链系统接入公链底层。

测试网络：测试网络。

2进制核对开源系统：2进制核对开源系统。

2.语言支持

繁体中文：繁体中文。

英文：英文。

2进制核对开源系统：2进制核对开源系统。

3.DAPP应用层

3.1模块

功能：模块功能描述。

原理：模块原理描述。

2进制核对开源系统：2进制核对开源系统。

3.2前端托管机制

允许DApp前端代码托管在区块链上：通过智能合约地址访问。

前端资源通过智能合约进行存储和分发：提供了一种去中心化的前端托管方案。

2进制核对开源系统：2进制核对开源系统。

3.3去中心化(DNS)DAAP

允许用户通过智能合约地址直接访问DApp：无需传统DNS。

DAAP协议通过区块链网络解析智能合约地址：实现去中心化的域名解析服务。

2进制核对开源系统：2进制核对开源系统。

3.4智能合约动态节点绑定

允许用户通过智能合约地址直接访问DApp：无需传统DNS。

智能合约根据后端节点的IP变动自动更新地址映射：保持用户访问的稳定性。

2进制核对开源系统：2进制核对开源系统。

3.5去中心化应用访问协议（DAAP）

允许用户通过智能合约地址直接访问DApp：无需传统DNS。

DAAP利用区块链网络提供去中心化的路由服务：增强了DApp的安全性和抗审查性。

2进制核对开源系统：2进制核对开源系统。

3.6区块链IP托管服务（BIHS）

将IP地址托管在区块链上：通过智能合约管理IP地址的分配和更新。

BIHS通过智能合约实现IP地址的动态管理：保障DApp后端的高可用性。

2进制核对开源系统：2进制核对开源系统。

3.7智能合约IP同步器

实时监测和同步智能合约关联的动态IP地址：同步器作为DApp的一部分，确保用户请求总是被导向最新的服务节点。

2进制核对开源系统：2进制核对开源系统。

3.8动态后端智能合约托管（DBSCH）

结合智能合约稳定性和动态IP灵活性：提供DApp托管解决方案。

DBSCH允许DApp在没有中心化后台服务的情况下运行：由智能合约自动管理后端功能。

2进制核对开源系统：2进制核对开源系统。

4.UTO区块浏览器

4.1主页

搜索框内容：输入地址/交易哈希值/区块哈希值/区块号/代币查询/钱包下ip/ip查询钱包/流量明细等数据。

首页顶部：UTO价格。

表格：UTO交易量（近7天）、流通总量、总市值、销毁总量、质押总量、验证人数。

最新区块：最新区块、区块号、出块时间、打包者、交易数。

查看更多：查看更多。

4.2最新交易

交易哈希值：最新交易。

从到：最新交易。

查看更多：查看更多。

4.3底部导航栏

开发者中心：开发者中心。

产品：UTO钱包、UTOwallet。

UTO：UTO、官网。

页面顶部的区块列表：区块列表（中文改为区块）、共xx条记录。

4.4区块列表

表格：时间、交易数、手续费。

打包者：奖励、时间、手续费。

4.5交易列表

页面顶部：交易列表（中文改为交易）、共xx条记录。

表格状态类型：已确认、打包中、成功、失败。

结果：发送人、接收人、金额、手续费。

4.6地址详情页

表格：时间、从到、状态、金额、手续费。

合约：合约概览、创建者、数量、其他资产、交易、基本信息、合约名称、合约代码、合约ABI、字节码。

4.7合约详情页

合约详情：基本信息、编译器版本、合约代码、合约ABI、字节码。

4.8交易详情页

概览：交易哈希值、发送人、时间、手续费、状态、接收人、转账金额、所在区块、GasPrice、GasLimit、Nonce、InputData。

4.9区块详情页

区块详情：区块哈希值、区块大小、区块高度、出块奖励、创建时间、出块者、交易、Gas消耗、GasLimit。

4.10代币详情页

代币详情页：代币详情页比合约详情页增加‘持有者’部分、前500名持有者、序号、地址、数量、占比、价值。

5.L2节点

5.1扩展节点

功能描述：处理快速结算与数据缓存。

6.模块功能描述

6.1发布任务

创建任务：创建任务。

铸造担保合约：铸造担保合约。

领取任务：领取任务。

锁定PCDN节点：任务开始。

任务结算：释放PCDN节点、执行担保合约、任务详情。

6.2后台系统

任务查询：任务查询。

6.3第三方PCDN

任务查询：模块、节点管理、添加节点、删除节点、节点详情。

6.4挖矿程序

识别用户ip：挖矿程序（算法整理钱包地址下的ip集）识别用户ip。

识别用户填入挖矿地址：ip流量显示。

该钱包地址收益明细展示：大数据整理求和数据。

6.5API对接数据

日总收益：AI系统接入计算。

IP流量明细：破解第三方广告程序集。

6.6IP对应钱包

大数据整理求和数据：链与第三方数据进行链侨对接。

6.7第三方破解

破解第三方广告程序集：自动签到、自动派发收益。

6.8第三方计费规则权重计算产量

破解第三方广告程序集：自动签到、自动派发收益。

6.9接口对接

链与第三方数据进行链侨对接：自动签到、自动派发收益。

7.区块链云盘板块

7.1功能描述

上传：用户可以将本地文件上传到云盘，支持断点续传和大文件上传。

下载：用户可以下载云盘中的文件，支持多线程下载以提高速度。

播放视频：云盘内的视频文件可以直接在线播放，无需下载。

外链分享：用户可以生成文件的外链，方便分享给其他人。

版本控制：云盘支持文件版本控制，可以查看和恢复旧版本的文件。

加密存储：所有文件在上传前都会进行加密处理，确保数据安全。

智能分类：云盘可以自动识别文件类型，并进行智能分类。

多设备同步：

智能搜索：提供强大的搜索功能，可以快速找到需要的文件。

多媒体预览：支持图片、音频和视频文件的预览功能。

回收站：删除的文件会被放入回收站，用户可以在一定时间内恢复。

对接基金公司与Au币发行

功能名称：黄金挂钩数字货币（Au币）发行与交易机制

运行原理：

1. 基金公司资产管理：

基金公司通过其专业的资产管理服务，为投资者提供多样化的资产配置方案，增加资产的增值潜力。

2. 黄金作为资产配置：

黄金作为一种传统资产，以其稳定性和价值储存功能，被纳入基金的投资组合中，用以平衡风险。

3. Au币的发行：

Au币是与黄金价值挂钩的数字货币，每枚Au币代表一克实物黄金的所有权。

4. 买入滑点与LP分红：

交易Au币时，设置1%的买入滑点，其中一部分用于流动性提供者（LP）的分红，以激励LP参与并维护流动性池的稳定性。

5. 流动性池交易支持：

Au币支持流动性池交易，允许用户通过提供Au币和基础货币（如USDT）的流动性来获得交易费分成。

6. 挂单买卖机制：

用户可以在订单簿上进行挂单买卖，挂单可以设置期望的买入或卖出价格，当市场价格达到预设价格时自动成交。

7. 订单簿与流动性池的独立性：

挂单交易可以独立于流动性池进行，为用户提供更多的交易灵活性和控制权。

8. 基金公司交互对现：

用户可以选择将Au币直接兑换为实物黄金或现金，通过基金公司完成交互对现操作。

9. Au币转入黑洞机制：

为了确保Au币的稀缺性和价值稳定性，部分Au币可以被转入黑洞地址，实现永久性销毁。

功能细节：

1. Au币的铸造与赎回：

用户可以通过基金公司购买Au币，同时，持有Au币的用户也可以选择赎回回黄金或现金。

2. 交易对与市场深度：

Au币将支持与多种主流货币的交易对，通过流动性池提供充足的市场深度。

3. 价格发现机制：

通过市场供需关系，Au币的价格将实时反映其与黄金价值的挂钩关系。

4. 风险管理：

基金公司将实施风险管理策略，包括但不限于仓位限制、价格波动监控等，以保护投资者利益。

功能名称：晚高峰日95计费系统

运行原理：

1. 时段定义：系统将每天的18:00至23:59定义为晚高峰时段，共计7小时。

2. 取样点记录：系统每5分钟记录一次带宽使用量，全天共记录288个点，晚高峰时段记录84个点。

3. 晚高峰时段处理：在晚高峰时段的84个带宽使用量点中，进行降序排列。

4. 数据筛选：从晚高峰时段的带宽使用量点中，去掉前5%（即4个点）。

5. 计费带宽量确定：在剩余的带宽使用量点中，选择最高的一个点的带宽使用量作为计费带宽量B。

6. 系数应用：使用运营商系数C和设备系数D，以及设备在线时长T，来计算日积分。

7. 日积分计算：根据日95计费公式\text{日积分} = B \times C \times D \times \left(\frac{T}{24}\right)进行计算。

8. 权重分配：晚高峰时段的权重设置为最高，通常超过90%，以确保收益最大化。

9. 在线时长要求：设备需要保持全天在线，以确保计费的准确性。

具体计算步骤：

1. 记录带宽使用量：系统每5分钟记录一次带宽使用量，全天共记录288次。

2. 晚高峰时段记录：在晚高峰时段（18:00至23:59）内，记录84次带宽使用量。

3. 排序带宽使用量：将晚高峰时段的84个带宽使用量点按照降序排列。

4. 去除前5%点：从排列好的带宽使用量点中去除前4个点。

5. 选择最大带宽使用量：选择去除后的带宽使用量点中的最大值作为B。

6. 计算日积分：使用公式\text{日积分} = B \times C \times D \times \left(\frac{T}{24}\right)计算日积分。

7. 计算收益：根据日积分和晚高峰权重，计算设备在晚高峰时段的收益。

8. 保持在线：确保设备在非晚高峰时段也保持在线，以满足计费需求。

8.代币铸造合约

8.1节点(95计费)

显示节点当天现金收益

初始汇率1元=100000枚：79%转入公共储备金并铸造UtoT代币19%转入做市储备金，1%转入公共映射储备金，1%转入开拓者映射储备金。

公共储备金÷数量=铸造价格=销毁兑现价格=映射价格：

做市储备金 转入公共储备金，增加公共储备金的总量提高铸造价格销毁兑现价格。

9.做市储备金开始释放

9.1数学公式：

持有地址100以上 每日做市储备金总金额50%释放公共储备金每分钟释放一次00:00截止。

持币地址50万以上 每日做市储备金总金额60%释放公共储备金每分钟释放一次00:00截止。

持币地址100万以上每日做市储备金总金额70%释放公共储备金每分钟释放一次00:00截止。

持币地址200万以上每日做市储备金总金额80%释放公共储备金每分钟释放一次00:00截止。

持币地址300万以上每日做市储备金总金额90%释放公共储备金每分钟释放一次00:00截止。

10.减产模型

10.1减产触发条件

减产触发条件：当流通量达到1000万枚时，系统将自动触发减产机制，以调整代币的发行速率。

10.2减产后的资金分配

减产开始后：每增加1枚代币流通量，将按照新的分配比例执行：\(79\%N\)的资金将被打入公共储备金，而\(19\%+N\)的资金将被打入做市储备金，1%将转入映射储备金。1%转入开拓者映射储备金。

公共储备金与做市储备金的动态调整：随着流通量的增加，公共储备金的比例将逐渐递减，而做市储备金的比例相应增加，以保持两者的平衡。

流通量与储备金比例的目标调整：减产逻辑将持续执行，直至流通量接近5000万枚，此时目标是将公共储备金的比例调整至约49%，做市储备金的比例调整至约49%，映射储备金保持为1%。

11.贡献值与自动燃烧机制

11.1贡献值的获取

汇聚网络用户：每获得一枚UtoT币，用户将累积一点贡献值(UtoCCT)。

专线网络用户：每获得一枚UtoT币，用户将累积一点贡献值(UtoCCY)。

11.2贡献值的分类

系统区分两种贡献值：专线节点贡献值和普通节点贡献值，分别对应不同的合约地址。

专线节点贡献值：适用于使用专线的用户。

普通节点贡献值：适用于使用普通宽带的用户。

兑换比例：2枚UtoCCY兑换10枚UtoCCT。

11.3节点贡献值管理机制：多节点平衡扣除系统（MNBDS）

公平性：每个节点的产出和贡献值扣除与其在线状态和产出量成正比。

透明性：所有扣除和奖励过程公开可追踪。

激励性：鼓励用户保持节点在线，以维护网络健康。

11.4操作步骤

节点产出统计：统计每个节点i在正常运行时产出的代币量\(T\_i\)。

总产出计算：计算所有节点的总产出量\(T\_{\text{total}}=\sum\_{i=1}^{n}T\_i\)。

节点在线状态记录：记录每个节点的在线状态，在线记为\(O\_i=1\)，离线记为\(O\_i=0\)。

节点产出比例确定：对于每个节点，计算其产出量占总产出的比例\(P\_i=\frac{T\_i}{T\_{\text{total}}}\)。

贡献值计算：每个节点的贡献值\(UtoCCT\_i\)等于其产出的代币量\(T\_i\)。

贡献值扣除规则：如果节点i离线，则根据产出比例\(P\_i\)从用户的总贡献值\(UtoCCT\_{\text{total}}\)中扣除相应的贡献值：\(\text{扣除的贡献值}\_i=P\_i\timesUtoCCT\_{\text{total}}\)。

总贡献值更新：用户的总贡献值更新为：\(UtoCCT\_{\text{total,new}}=UtoCCT\_{\text{total}}\sum\_{i=1}^{n}(\text{扣除的贡献值}\_i)\)。

自动燃烧与储备金兑换：如果用户的贡献值被扣至零或以下，用户的临时代币将自动燃烧，等值资金转化为储备金并转入用户钱包。

周期性评估：每个评估周期（如每日或每周）结束时，重复以上步骤，确保贡献值的扣除与节点状态同步。

用户界面展示：用户界面应清晰展示每个节点的产出量、在线状态、贡献值以及扣除情况，使用户能够轻松跟踪和管理自己的节点。

11.5注意事项

所有操作应符合UtoDePIN网络网络规则和当地法律法规。

用户应确保所有节点的合规运行，以最大化贡献值的积累和网络的稳定性。

通过MNBDS，UtoDePIN

网络能够实现对用户节点贡献的精确管理和公平激励，促进网络的健康发展和用户的积极参与。

12.贡献值挂单卖出机制（CVPSM）

12.1功能描述

流动池支持：平台提供了流动池功能，允许用户将资产存入流动池中，以提供流动性。用户可以通过提供流动性来获得交易费的分成，同时支持交易对的流动性，确保交易的顺畅进行。

12.2挂单交易

挂单交易：平台支持用户进行挂单交易，即用户可以设置一个期望的交易价格，并在该价格达到时自动成交。挂单交易不会直接进入流动池，而是在订单簿中等待匹配，这样用户可以更灵活地控制交易时机和价格。

卖单挂单

用户可以设置一个卖单挂单，即在希望卖出的价格上挂出订单。这允许用户在不立即交易的情况下，等待市场达到预期的价格。

买单挂单

同样，用户也可以设置买单挂单，即在希望买入的价格上挂出订单。这为用户提供了一种策略，以等待市场下跌至其期望的买入价格。

12.3优化交易体验

为了提高交易效率和用户体验，平台对挂单交易机制进行了优化。这包括但不限于改善订单匹配算法，减少交易滑点，以及提供更直观的交易界面。

13.双币流动性自动添加与合约地址转换机制

13.1转化流程

1.用户界面操作：用户在平台上选择“双币流动性添加”功能，并输入他们希望添加的UtoCCT和UtoT代币数量。

2.合约地址识别：用户指定UtoCCT代币的合约地址，并选择目标UtoCC代币的合约地址。

3.自动转换设置：用户发起请求，按照1:1的比例将UtoCCT代币转换为UtoCC代币。

4.智能合约触发：用户提交请求后，智能合约自动触发UtoCCT到UtoCC的转换过程。

5.代币转换：智能合约调用UtoCCT合约的`transferFrom`函数，将用户账户中的UtoCCT代币转移到UtoCC合约地址。

6.流动性池添加：转换后的UtoCC代币与用户指定的Uto代币一起被添加到流动性池中。

7.汇率应用：智能合约根据预设的汇率（例如UtoCC币100:1Uto）计算并添加相应的Uto代币到流动性池。

8.流动性代币分配：智能合约根据用户添加的流动性比例，分配相应的流动性代币（LPToken）给用户。

9.交易确认：所有交易步骤在区块链上确认，确保转换和添加流动性的过程透明、安全。

10.收益分享：用户作为流动性提供者，根据持有的LPToken份额，分享交易费用收益。

13.2运行原理

智能合约自动化：智能合约自动执行所有步骤，包括代币转换、流动性添加和LPToken分配。

代币转换逻辑：智能合约内置逻辑，确保UtoCCT代币能够按照1:1的比例转换为UtoCC代币。

流动性池管理：智能合约管理流动性池资产，根据用户添加的流动性自动调整池内资产比例。

交易费用分配：智能合约根据用户持有的LPToken份额，自动分配交易费用作为收益。

风险控制：智能合约实现风险控制逻辑，如滑点保护和资产价值波动预警。

用户交互：用户通过图形界面与智能合约交互，提交转换和添加流动性的请求。

透明度保障：所有操作记录在区块链上，用户可以随时查看交易记录和流动性池状态。

13.3撤销流动性流程

1.用户发起撤销请求：用户在平台上选择撤销流动性，并指定希望撤销的LPToken数量。

2.智能合约处理：智能合约根据用户请求的LPToken数量，计算并返回相应的UtoCC和Uto代币。

3.代币转换：智能合约调用Uto合约的`transferFrom`函数，将中的UtoT合约地址代币转移到UtoT用户账户地址。

4.直接燃烧UtoCC：如果合约设置为撤销流动性时直接燃烧UtoCC代币，智能合约将自动执行燃烧操作。

5.UtoT份额分配：用户收到计算出的UtoT份额，而燃烧的UtoCC代币则从流动性池中移除。

6.流动性池更新：智能合约更新流动性池的UtoCC和UtoT代币数量，以反映撤销后的资产状态。

7.交易记录：撤销操作和燃烧记录在区块链上，确保整个过程的透明性和不可篡改性。

Uto永久代币交易规则和机制：

1.铸造与销毁价格机制\*\*

铸造价格、销毁兑现价格、映射价格以及最低买入价值均相等，由以下公式确定：

\[

\text{铸造价格} = \text{销毁兑现价格} = \text{映射价格} = \text{最低买入价值} = \frac{\text{公共储备金}}{\text{数量}}

\]

2.初始底池设置\*\*

初始底池由1,000,000枚Uto代币和10,000 USDT组成。

3.买卖滑点设置\*\*

买入滑点\*\*：设定为10%，其中8%的代币用于销毁并兑换黄金，1%的代币用于燃烧，1%的代币作为流动性提供者（LP）分红。

扣除手续费后，剩余90%金额全部转入公共储备金，10%转入流动性池。

随着流动性价格接近系统最低价值，分配比例调整为50%转入公共储备金，50%转流动性池。

4.卖出滑点\*\*

卖出滑点\*\*：设定为1.5%，其中0.5%的代币转入映射储备金，1%作为LP分红。

若为单独转账，额外有1%的代币销毁并兑换黄金。

5.卖出最低价\*\*

最低价值\*\*：\( \text{最低价值} = \frac{\text{公共储备金}}{\text{流通数量}} \)

代币转入黑洞，直接与公共储备金交互。

6.8%Uto销毁与黄金兑换规则\*\*

兑换黄金价值\*\*：\( \text{兑换黄金价值} = \frac{\text{公共储备黄金} + \text{做市储备黄金}}{\text{流通数量}} \)

根据计算结果，从做市储备金和公共储备金中按份额扣除相应的黄金并进行兑换。

7.最低挂单价与系统保护最高价\*\*

最低挂单价\*\*：\( \text{最低挂单价} = \frac{\text{公共储备黄金数量}}{\text{流通数量}} \)

系统保护最高价\*\*：\( \text{系统保护最高价} = \frac{\text{（公共储备黄金 + 做市储备黄金）}}{\text{流通数量}} \)

8.涨停价格的设定\*\*

涨停价格\*\*：在系统保护最高价的基础上，再增加5倍（500%），公式简化为：\( P\_{\text{limit up}} = P\_{\text{max}} \times 6 \)

9.超额风险提示与泡沫风险警示\*\*

当市场价格超过系统保护最高价，提示投资者可能出现泡沫，泡沫破裂可能导致投资者遭受大约83.33%的损失。

10.买入操作后的流动性池处理\*\*

在买入操作中，除了滑点分配外，剩余的90%金额转入公共储备金，而10%转入流动性池。

流动性池对Uto代币的分配\*\*：当买入操作发生时，流动性池会根据交易需求，提供相应的Uto代币以满足市场流动性。

流动性池的这一机制确保了在买入操作中，有足够的Uto代币供应，以维持交易的顺畅和市场的稳定性。

流动池与挂单交易支持：

流动池支持：平台提供了流动池功能，允许用户将资产存入流动池中，以提供流动性。用户可以通过提供流动性来获得交易费的分成，同时支持交易对的流动性，确保交易的顺畅进行。

1、挂单交易：平台支持用户进行挂单交易，即用户可以设置一个期望的交易价格，并在该价格达到时自动成交。挂单交易不会直接进入流动池，而是在订单簿中等待匹配，这样用户可以更灵活地控制交易时机和价格。

卖单挂单：用户可以设置一个卖单挂单，即在希望卖出的价格上挂出订单。这允许用户在不立即交易的情况下，等待市场达到预期的价格。

买单挂单：同样，用户也可以设置买单挂单，即在希望买入的价格上挂出订单。这为用户提供了一种策略，以等待市场下跌至其期望的买入价格。

优化交易体验：为了提高交易效率和用户体验，平台对挂单交易机制进行了优化。这包括但不限于改善订单匹配算法，减少交易滑点，以及提供更直观的交易界面。

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行情

币种涨跌幅:实时获取币种价格和涨跌幅。

热门榜:向公共储备金转入一定金额可以上热门，金额越多排行越高。

审查榜:需要支付审查费用，通过DAO组织委员会审查是否是割韭菜体系。

2.4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。

2.5买入卖出

限时买入/卖出:用户可以设置期望的交易价格和数量，以及支付方式。

交易对:展示可交易的币种对。

挂单交易:用户可以查看已提交的买单或卖单列表。

2.6Swap

兑换:用户可以兑换不同币种。

做市:创建市场，加入流动性。

奖励:展示流动性提供者的奖励。

2.7流动性赎回机制

排队自动赎回:赎回请求按先来先服务原则处理。

赎回内容:用户赎回其最初添加到流动池中的代币和相应的黄金份额。

剩余资产处理:如果用户赎回后流动池中仍有剩余资产，将按比例分配给其他流动池。

2.8公共储备金兑付

兑付合约地址:公共储备金除以流通数量等于最低价值。

铸造代币手续费:手续费转入公共储备金，或者代币转入黑洞。

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。

3.5Swap界面

Swap界面应提供兑换功能和流动性池的管理。

应有清晰的指引，帮助用户理解如何加入和取回流动性。

4.后端服务架构

4.1数据库设计

需要设计一个能够处理高并发请求的数据库。

数据库应支持快速查询和数据更新。

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.挂单交易订单簿

6.1概述

挂单交易订单簿是交易平台的核心功能之一，它允许用户根据市场条件设置买卖订单。用户可以指定交易的价格和数量，订单将按照用户设定的条件在订单簿中排队等待成交。

6.2功能描述

挂单交易:用户可以设置一个期望的交易价格，并在该价格达到时自动成交。

订单匹配:挂单交易不会直接进入流动池，而是在订单簿中等待匹配。

灵活性:用户可以更灵活地控制交易时机和价格。

6.3卖单挂单

设置卖单:用户可以设置一个卖单挂单，即在希望卖出的价格上挂出订单。

等待成交:订单将保留在订单簿中，直到市场价格达到用户设定的卖出价格。

市场条件:此功能允许用户在不立即交易的情况下，等待市场达到预期的价格。

6.4买单挂单

设置买单:类似地，用户也可以设置买单挂单，即在希望买入的价格上挂出订单。

市场下跌策略:这为用户提供了一种策略，以等待市场下跌至其期望的买入价格。

6.5订单管理

查看订单:用户可以在订单簿中查看所有当前挂单的状态，包括自己的挂单。

取消订单:用户可以随时取消未成交的挂单。

订单更新:用户可以修改已有挂单的价格和数量，以适应市场变化。

6.6技术实现

数据库设计:订单数据需要存储在高性能的数据库中，以支持快速的查询和更新。

前端展示:订单簿应在前端以列表或图表的形式展示，方便用户查看和操作。

后端逻辑:后端服务需要处理订单的创建、匹配、成交和取消等逻辑。

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。

钱包功能开发文档

1.引言

1.1目的

本文档旨在为去中心化交易所的钱包功能开发提供详细指南。钱包功能是用户管理其加密资产的核心工具，需要确保安全性、易用性和功能性。

1.2范围

本文档包括钱包功能的以下主要部分：

钱包创建与管理

导入与导出钱包

转账功能

资产管理

安全性设计

2.钱包创建与管理

2.1创建钱包

功能描述:用户可以创建新的钱包，生成钱包名称、密码和备份助记词。

用户界面:提供简洁明了的界面，引导用户完成创建过程。

安全性:助记词需安全生成和备份，密码需加密存储。

2.2钱包管理

功能描述:用户可以管理其钱包，包括查看钱包地址、余额和交易历史。

用户界面:提供清晰的钱包信息展示和操作选项。

安全性:确保所有敏感信息都经过加密处理。

3.导入与导出钱包

3.1导入钱包

功能描述:用户可以通过助记词或私钥导入已有钱包。

用户界面:提供导入选项，引导用户输入助记词或私钥。

安全性:确保导入过程中的敏感信息安全。

3.2导出钱包

功能描述:用户可以导出其钱包的助记词或私钥，以便在其他设备上使用。

用户界面:提供导出选项，允许用户选择导出格式。

安全性:导出过程中需提醒用户注意信息安全。

4.转账功能

4.1发起转账

功能描述:用户可以向其他地址转账，输入转账金额、收款地址和矿工费。

用户界面:提供直观的转账表单，包括地址验证和交易确认。

安全性:交易前需进行多重验证，确保交易安全。

4.2交易历史

功能描述:用户可以查看其钱包的交易历史记录。

用户界面:以列表形式展示交易历史，包括交易详情和状态。

安全性:交易历史信息需加密存储，确保用户隐私。

5.资产管理

5.1资产概览

功能描述:显示用户钱包中的所有资产及其价值。

用户界面:提供资产列表，包括资产名称、数量和价值。

安全性:资产信息需实时更新，确保数据准确性。

5.2资产操作

功能描述:用户可以进行资产的划转、冻结和解冻等操作。

用户界面:提供操作选项，引导用户完成相应操作。

安全性:所有资产操作需进行身份验证和权限检查。

6.安全性设计

6.1加密技术

功能描述:使用行业标准的加密技术保护用户数据。

技术实现:采用AES、RSA等加密算法对敏感数据进行加密。

6.2认证机制

功能描述:实施多因素认证，确保用户身份安全。

技术实现:结合密码、短信验证码、生物识别等多种认证方式。

6.3交易安全

功能描述:确保交易过程的安全，防止欺诈和盗窃。

技术实现:交易过程中进行多重验证，如交易密码、电子邮件确认等。

6.4安全审计

功能描述:定期进行安全审计，发现并修复潜在的安全漏洞。

技术实现:采用自动化工具和手动审计相结合的方式。

14.人民币提现入口(DAPP)

14.1运行原理

1.用户界面操作：用户通过UtoDePIN网络的客户端或网页界面，选择“人民币提现”功能，输入希望兑换的Uto代币数量，并选择与他们提现需求相关的特定任务。

2.身份验证：系统执行KYC（了解你的客户）流程，以验证用户身份，确保提现操作的合法性和安全性。

3.提现信息填写：用户填写支付宝账号或银行卡号等提现信息，并指定接收人民币的账户。

4.Uto代币燃烧：用户输入的Uto代币数量将被系统自动转入黑洞地址进行燃烧，确保代币被永久移除出流通。

5.黄金兑换与担保池存储：燃烧的Uto代币价值等额兑换成黄金，并自动存入担保池。

6.燃烧价值计算：系统计算每一枚Uto代币的燃烧价值，公式为：\[\text{燃烧价值}=\frac{\text{公共储备金总额}}{\text{Uto代币总流通量}}\]

7.人民币份额计算：系统根据任务池中的黄金价值和用户兑换的Uto数量，计算用户应得的人民币份额。

8.官方打款：官方根据计算结果，通过支付宝或银行转账的方式，将相应金额的人民币打款到用户指定的账户。

9.担保池与任务池的黄金转移：用户提现人民币后，系统将等值的黄金从担保池转入用户选择的任务池，以维持任务池的黄金价值与用户提现的人民币价值相匹配。

10.交易记录与反馈：系统实时更新交易记录和提现状态，并通过客户端或网页界面反馈给用户。

11.安全性保障：所有提现操作均通过加密技术保护，确保用户数据安全和操作的不可篡改性。

12.透明度与合规性：所有交易和提现操作记录在区块链上，确保操作的透明度，并符合相关法律法规的要求。