

# Kloud-数字资产交易平台需求规格说明书



作者 19281030-张云鹏

## 引言

### 编写目的

在项目启动之前，对同类型产品的市场进行了前期调查，与多位软件设计者和使用者进行了探讨和分析，

之后由软件项目小组向系统分析人员与软件设计人员提出了这份需求规格说明书。

为明确软件需求、规划项目、确认进度、组织软件开发并测试而撰写本文档。

同时，详细分析项目总体需求，可以作为软件开发工作的基础和依据以及确认测试和验收的依据。

### 项目背景

- 项目委托单位：北京交通大学计算机与信息技术学院
- 开发单位：北京交通大学计算机与信息技术学院Kloud项目组
- 主管部门：北京交通大学计算机与信息技术学院计科Kloud项目组
- 项目概述：本项目名称为“Kloud数字资产交易平台”。系统功能主要包括：能够存储用户的数字资产，提供主流数字货币的便捷交易，支持对主流交易对的限价单，市价单委托、用户还可以通过API接口获取实时行情数据信息授权访问，以及Okx和Binance的交易大数据。

### 定义

Go: Go（又称 Golang）是 Google 的 Robert Griesemer，Rob Pike 及 Ken Thompson 开发的一种静态强类型、编译型语言。Go 语言语法与 C 相近，但功能上有：内存安全，GC（垃圾回收），结构形态及 CSP-style 并发计算。

MongoDB: MongoDB是一个基于分布式文件存储的数据库。由C++语言编写。旨在为WEB应用提供可扩展的高性能数据存储解决方案。

## 参考资料

1. 张海藩.《软件工程导论》.人民邮电出版社.2006年1月
2. jammy928. Bizzan. CoinExchange

## 需求概述

### 目标

本项目名称为“Kloud数字资产交易平台”。系统功能主要包括：能够存储用户的数字资产, 提供主流数字货币的便捷交易, 支持对主流交易对的限价单, 市价单委托、用户还可通过API接口获取实时行情数据信息授权访问, 以及Okx和Binance的交易大数据.

具体包括以下需求点:

### 客户端

1. 币币交易-限价委托
2. 币币交易-市价委托
3. 法币C2C交易
4. 法币OTC交易
5. 交易撮合
6. 币种钱包RPC-充值
7. 币种钱包RPC-提现
8. 资产管理
9. 流水账单

### 管理端

1. 币币管理-新建/修改交易对
2. 币币管理-设置交易引擎
3. 交易数据-分时交易额
4. 交易数据-分时充值/提现流水
5. 行情引擎-币种数据

## 运行环境

参见可行性分析报告的运行环境

## 用户类和特征

最终的用户是运营和客户, 平台运营负责数据的更新, 具备一定的专业知识。客户是普通用户, 具备一定的计算机操作知识即可。

## 条件和限制

由于缺少并发编程经验，本交易系统尚不支持高频交易，整个系统的管理员与用户的安全性有待进一步完善。

## 系统功能需求

### 客户端

1. 币币交易对的多关键字检索查询
2. 币币交易限价和市价委托
3. 交易流水和历史订单查询
4. 用户注册, 信息修改和注销
5. 提供Okx和Binance交易数据API

### 数据保存

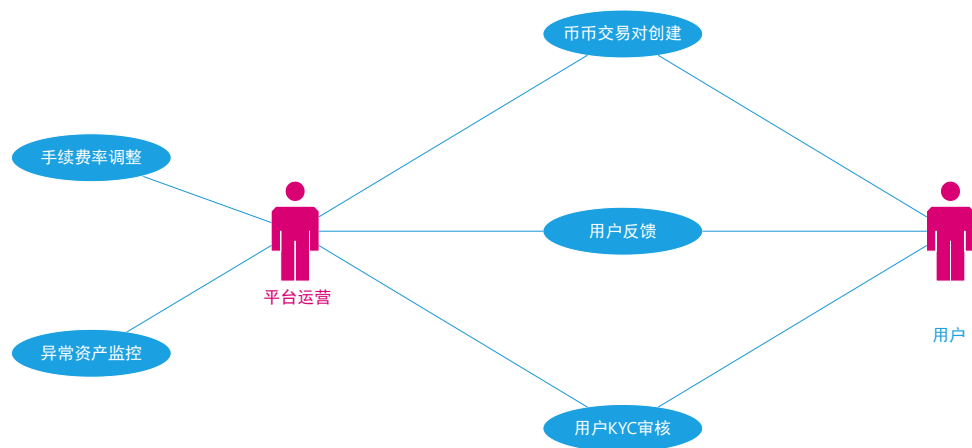
1. Redis每隔12小时持久化保存
2. 币币交易对信息
3. 账户信息
4. 历史账单
5. 交易流水

### 确定执行者

确定用户和平台运营为系统的执行者.平台运营负责系统的主要功能. 用户从系统中获取所需的信息。

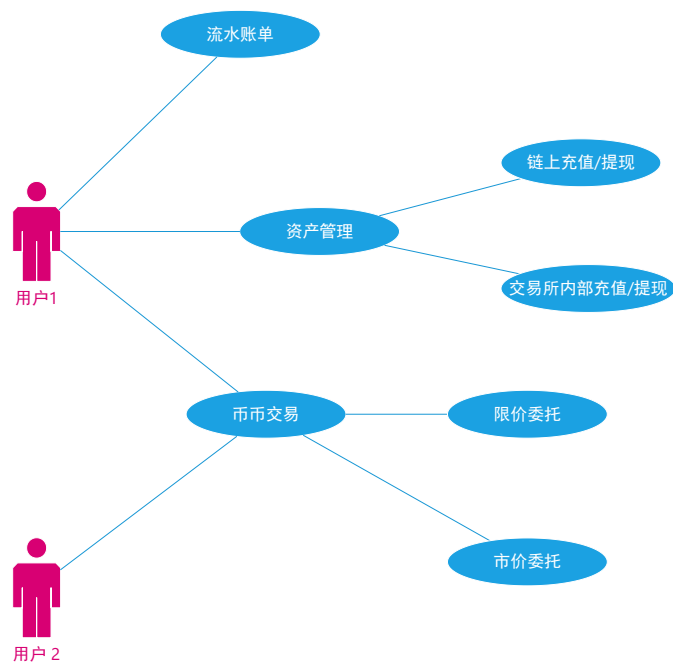
### 确定用例

1. 运营管理用例图. 平台运营创建用户可交易的交易对信息. 审核用户KYC, 同时监察异常的资产情况以保证资金安全, 防止黑钱洗钱等行为. 根据商业策略调整有吸引力的手续费率, 以保证平台的竞争力



## 2. 用户币币交易用例图.

用户通过平台创建的交易对与其他用户进行币币交易. 委托的类型可分为限价单和市价单. 同时访问平台的数据库, 查询流水账单. 通过区块链RPC外部充值/提现或者平台内部账号的转账.



## 编写用例文档

### 1. 平台运营管理用例

- 执行者: 平台运营
- 入口条件: 运营获得权限
- 事件流: 当有新的币币交易对上架时, 运营在录入界面输入交易对信息. 点击提交按钮, 将交易对的信息保存再MongoDB数据库中. 当某一个交易的信息需要修改时, 运营通过输入查询条件, 搜索出该交易对时, 点击修改按钮, 系统在可编辑状态显示交易对的当前信息, 运营修改具体信息, 点击保存按钮, 系统将更新数据库中该交易对的信息; 当需要删除一个或多个交易对时, 平台查找到需要删除的交易对记录, 点击删除按钮, 系统提示“确实要删除?”对话框, 当运营选择“是”, 系统将删除数据库中相应交易对的信息, 反之, 则不进行任何操作。
- 出口条件: 系统将数据库中的信息进行相应的操作: 添加交易对信息时, 将新的交易对信息保存在数据库中; 修改交易对信息时, 将数据库中该交易对的信息做相应的更新操作; 删除交易对信息时, 则删除数据库中的相应交易对记录。
- 异常事件: 在交易对进行修改和删除时, 先查出需要进行处理的交易对记录, 如果数据库中不错在符合条件的记录, 查询无结果时, 则无法进行修改和删除操作。

### 2. 用户币币交易用例

- 参与执行者: 用户
- 入口条件: 用户已经登陆到该系统中。
- 事件流: 当有新的用户时, 用户在录入页面输入平台的信息, 点击提交按钮, 系统将平台的信息保存到数据库中; 当某一平台的信息需要修改时, 用户通过输入查询条件, 搜索出该平台信息时, 点击修改按钮, 系统在可编辑状态显示会员的当前信息, 用户修改具体信息, 点击保存按钮, 系统将更新数据库中该平台的信息; 当需要删除一个或多个平台时, 用户查找到需要删除的平台记录, 点击删除按钮, 系统提示“确实要删除?”对话框, 当管理员选择“是”, 系统将删除数据库中该平台的信息, 反之, 则不进行任何操作。
- 出口条件: 系统将数据库中的会员信息进行相应的操作: 添加平台信息时, 将新的平台信息保存在数据库中; 修改平台信息时, 将数据库中该平台的信息做相应的更新操作; 删除平台信息时, 则删除数据库中的相应平台记录。
- 异常事件: 在进行修改和删除会员信息时, 先查出需要进行处理的平台记录, 如果数据库中不错在符合条件的记录, 查询无结果时, 则无法进行修改和删除操作。

## 非功能性需求

### 性能需求

Kloud数字资产交易平台的目標使用者是平台运营和用户。对于运营的管理工作, 性能要求不是很严格, 但需要备份操作。对于用户的一般浏览和下单功能, 对性能要求较高, 一般要达到并发数1000以上。

## 安全性需求

由于Kloud的交易量会非常大，所有在对这些交易对导入和查询时要保证速度。在交易对购买过程中又要保证事务的完整性。对于整个系统，需要完整的权限控制，防止某些人恶意的攻击系统，修改原始记录。同时对于数据库中的数据需要定时备份，防止系统数据丢失。此外，系统要求用户在登陆时需要身份验证。

## 故障处理

在正常情况下，应不出错。一旦发生意外，比如掉电、网络不通等，应保证系统数据不会丢失。为此，会定期的对整个数据库进行备份并且进行日志的记录，一但发生故障，则通过日志恢复事务。

系统首先可以进行用户订单表达导出，管理员可以在前端通过按钮去选择对整个数据库的备份。同时在后台，设置了每天的00:00进行数据库的备份。在任务栏中添加了每天定点备份数据库的任务。

## 数据描述

### 静态信息

- 币币交易对信息: 标的币种, 本位币种, 最小交易单位, 首次发行时间, 首次发行价, 创始团队, 投资机构, 币种基本信息, 官网链接, 白皮书, 区块浏览器.
- 用户个人资料: UID, 用户邮箱, 用户名, 登录密码, 真实姓名, 联系电话, 身份证.
- 费率等级信息. 用户费率等级, 挂单成交手续费, 吃单成交手续费, 24小时提现额度.

### 动态数据

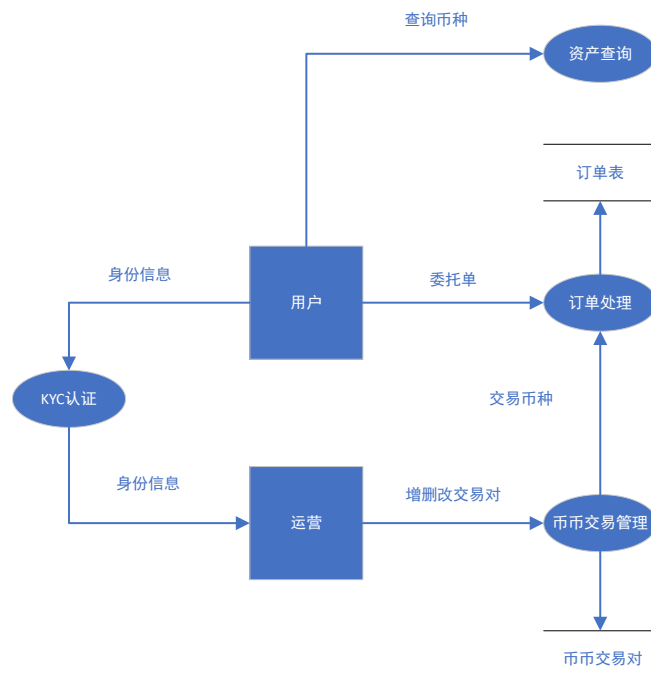
- 币币交易对信息: 当前价格, 24小时涨跌幅度, 币种市值, 24小时最高价, 24小时最低价, 24小时交易量
- 订单表: 买入/卖出方向, 币种数量, 价格, 最新成交数量, 最新成交价格.
- 资金账单: 账单币种类型, 转账数量, 充值/提现/转入/转出. 币种余额, 手续费.

## 数据库描述

数据库采用MongoDB

## 数据流图和数据词典

### 数据流一层图



## 数据源点及汇点描述

- 名称: 币币交易对
- 简要描述: 修改, 查看
- 有关数据流: 交易币种信息

### 数据流名词条描述:

- 数据流名: 委托订单
- 说明: 委托订单描述了用户交易的方向, 金额
- 数据流来源: 用户
- 数据流去向: 交易引擎, 费率等级
- 数据流组成: 委托订单 = 交易对名称 + 委托类型+ 买卖方向+ 数额

编号	字段名称	数据类型	长度	说明
1	ExchangePair	String	2-5	交易对名称
2	OrderType	String	1-10	订单委托类型
3	OrderSide	String	3-4	买卖方向
4	OrderAmount	Int	$1 - 2^{64} - 1$	订单数额

- 数据流名: 资金转账
- 说明: 说明了用户的充值/提现金额和币种
- 数据流来源: 区块链RPC
- 数据流去向: 用户钱包
- 数据流组成: 资金转账 = 币种名称 + 充值/提现方向+ 数额

编号	字段名称	数据类型	长度	说明
1	CoinName	String	2-5	币种名称
3	TransferSide	String	3-4	转账方向
4	Amount	Int	$1 - 2^{64} - 1$	转账数额

## 功能需求

### 功能划分

该软件具有如下主要功能

1. 数字资产交易
2. 链上充值/提现
3. 资金账单查询
4. 交易行情数据

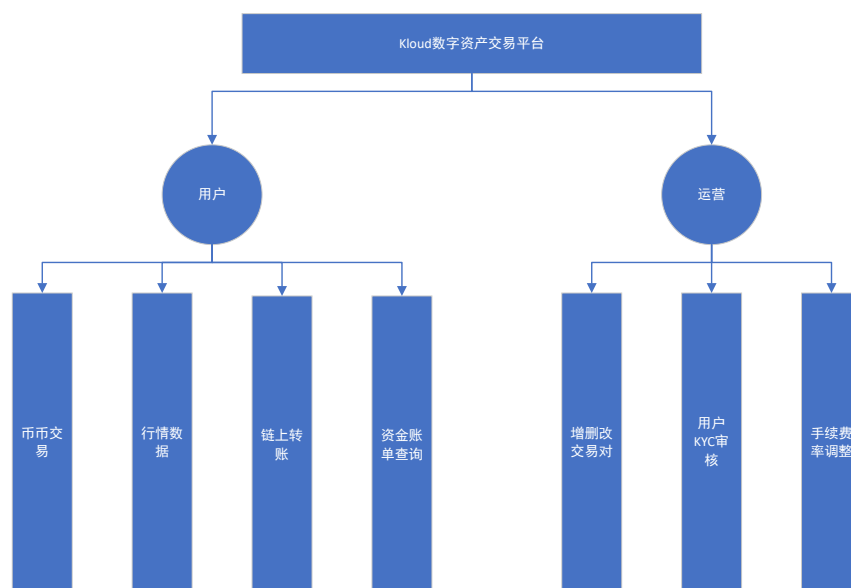
### 功能描述



## 系统各功能概述

1. 数字资产交易
  - 币币交易限价委托
  - 币币交易市价委托
2. 链上充值/提现
  - 区块链钱包
  - 链上RPC调用确认转账
3. 资金账单查询
  - 历史订单
  - 历史转账
4. 交易行情数据
  - 主流交易对行情数据
  - 交易大数据

## 系统功能结构图



## 用户使用系统

### 用户信息管理

1. 会员注册
  - 用户点击注册按钮，打开注册页面；
  - 用户输入注册信息，包括用户名、登录密码、常用邮箱、手机等；
  - 点击发验证码，验证无误后即可注册

- 注册信息输入完成后，点击提交按钮；
- 若有不合格项目，例如两次输入密码不一致、邮箱格式不正确等，则系统提示错误信息，请重新输入；
- 若注册信息正确无误，则提示注册成功，页面跳转到登录界面。

## 2. 忘记密码

- 在登陆页面选择忘记密码；
- 页面跳转到忘记密码的页面；
- 用户填写相关信息（安全提问），系统给用户的常用邮箱或手机发送验证信息，用户输入验证密码正确后，可以重新设置密码；
- 若用户输入信息不正确，系统提示错误信息；

## 3. 记住密码

- 点击记住密码，下次直接登录，可跳过输入账号和密码阶段。

## 4. 个人信息

- 用户进入主页后可点击个人中心进行个人信息的修改  
页面显示当前的用户注册信息，并填写名字，性别等；
- 系统记录新的用户信息，并提示注册信息修改成功。

# 币币交易

## 1. 搜索框交易对查询

客户可根据要查询的交易对进行模糊搜索，在搜索框中填入关键字按回车或者点击搜索图标，进行搜索，页面跳转到查询结果页面，显示交易对。

## 2. 交易对种类查询

点击页面上交易对分类的标签，例如公链, Defi, NFT概念等等，在这下方还设置有二级查询，比如PoS, PoW等等，点击相应分类跳转到相应界面

## 3. 交易对信息浏览

点击对应交易对图片即可查看交易对的详细信息，包括价格，创始团队, 市值等等

## 4. 历史记录浏览

用户可以在历史记录中查看历史浏览交易对。

## 5. 推荐交易对浏览

用户在查看一款交易对的同时，在交易对详细信息下边会显示推荐交易对，点击推荐交易对就可以进入到推荐交易对的详细信息页面。

# 后台管理系统

## 交易对信息管理

### 1. 交易对添加

- 点击添加交易对后，先选择添加交易对的类别，之后填写交易对名称，市值, 行业等信息。
- 填写完后点击下一步，进入交易对属性填写页面，填写交易对的名称，最小交易单位等。
- 最后选择关联交易对，在用户浏览该交易对的时候将推荐交易对推荐给用户。

### 2. 交易对信息修改

- 交易对的信息有变化时（比如最小交易单位）运营进入交易对详细信息页面，

- 点击编辑即可编辑交易对信息

## 费率等级管理

### 1. 用户KYC审核

- 用户提交身份证信息
- 从KYC审核界面下载用户的身份证照片和人脸照片, 确认为同一人后点击审核确认按钮,
- 用户的资质从Lv0提升至Lv1.

### 2. 费率等级管理

- 会议确认调整费率后, 授予运营调整费率权限
- 选择费率等级列表, 输入新的费率.
- 交易额较大的客户或做市商, 进入用户管理界面, 单独调整用户费率.

## 故障处理

在正常情况下, 应不出错。一旦发生意外, 比如掉电、网络不通等, 应保证系统数据不会丢失。为此, 会定期的对整个数据库进行备份并且进行日志的记录, 若发生故障, 则通过日志恢复事务。

系统首先可以进行用户订单表达导出, 管理员可以在前端通过按钮去选择对整个数据库的备份。同时在后台, 设置了每天的00:00进行数据库的备份。在任务栏中添加了每天定点备份数据库的任务。

## 性能需求

### 数据精确度

查询时应保证查全率, 所有在相应域中包含查询关键字的记录都应能查到, 同时保证查准率。

### 时间特性

在网速正常的情况下, 一般操作的响应时间应在0.5秒钟之内。

### 适应性

满足运行环境在允许操作系统之间的安全转换和与其他应用程序的独立运行要求。

## 运行需求

## 用户界面

使用用户的语言，而非技术的语言;界面清晰明了;有清楚的错误提示;让用户知道自己当前的位置，使其做出下一步行动的决定;完善视觉的清晰度,条理清晰；图片、文字的布局和隐喻不要让用户去猜。

## 硬件接口

由于我们使用的通信协议是TCP/IP，因此这里的硬件接口问题主要就是TCP/IP层中的网络接口层，他负责数据帧的发送和接收，帧是独立的网络信息传输单元。网络接口层将帧放在网上，或从网上把帧取下来。这就要求IP使用网络设备接口规范NDIS向网络接口层提交帧，并且IP支持广域网和本地网接口技术。在系统运行时要注意关闭那些容易受攻击和入侵的端口号，在能保证带宽的前提下仅开通系统运行所必须的端口

## 软件接口

1. 手动下载 mongodb-driver，下载其依赖项 bson 和 mongodb-driver-core
2. 安装MongoDB 3.4.2 版本；通过 Github 网站下载驱动包，分别为 mongodb-driver-3.4.2.jar、mongodb-driver-core-3.4.2.jar、bson-3.4.2.jar