

基于区块链技术的供应链平台 ——账户及 workflow 管理系统

[需求规格说明书]

目录

| | |
|----------------------|----|
| 1. 概述..... | 4 |
| 1.1 用户简介..... | 4 |
| 1.1.1 供应商..... | 4 |
| 1.1.2 核心企业..... | 4 |
| 1.1.3 金融机构..... | 4 |
| 1.2 项目的目的与目标..... | 4 |
| 1.2.1 目的..... | 4 |
| 1.2.2 目标..... | 5 |
| 1.3 术语定义..... | 5 |
| 1.4 参考资料..... | 5 |
| 1.5 相关文档..... | 5 |
| 1.6 版本更新信息..... | 5 |
| 2. 目标系统描述..... | 5 |
| 2.1 角色定义..... | 5 |
| 2.2 工作流程..... | 5 |
| 2.3 单据、账本和报表..... | 6 |
| 2.3.1 单据..... | 6 |
| 2.3.2 账本..... | 6 |
| 2.3.3 报表..... | 6 |
| 2.4 可能的变化..... | 6 |
| 3. 目标系统功能需求..... | 6 |
| 3.1 功能模块总体设计..... | 6 |
| 3.2 功能模块详细设计..... | 7 |
| 3.3 用例详细说明..... | 8 |
| 3.3.1 账户管理系统..... | 8 |
| 3.3.2 工作流管理系统..... | 13 |
| 4. 目标系统性能需求..... | 14 |
| 5. 目标系统界面与接口需求..... | 15 |
| 5.1 界面需求..... | 15 |
| 5.2 接口需求点列表..... | 15 |
| 6. 目标系统的其他需求..... | 15 |
| 6.1 安全性..... | 15 |
| 6.2 可靠性..... | 15 |
| 6.3 灵活性..... | 16 |
| 6.4 特殊需求..... | 16 |
| 7. 目标系统的假设与约束条件..... | 16 |

1. 概述

1.1 用户简介

基于区块链技术的供应链平台的使用者有 3 类，分别是供应商、核心企业和金融机构。

1.1.1 供应商

- <1> 供应商是生产货物并出售来获取利润的企业。
- <2> 使用本系统的供应商，其客户无法一次付清货款，需要借助贷款来完成。
- <3> 供应商希望收货方受到货物后能立刻得到货款。
- <4> 供应商不希望因购买方信用问题遭受损失。

1.1.2 核心企业

- <1> 核心企业是本系统服务的对象。
- <2> 核心企业要购买供应商提供的货物，但无法一次付清货款。
- <3> 核心企业要找一个第三方金融机构贷款来购买货物。

1.1.3 金融机构

- <1> 金融机构根据供应商和核心企业之间的贸易合同，向供应商发放贷款，向核心企业索要本金和利息的机构。
- <2> 金融机构有自定义产品利率的权利，以便获取利润。
- <3> 金融机构需要对供应商和核心企业进行审批，防止任何一方失信。

1.2 项目的目的与目标

1.2.1 目的

供应链金融（应收账款）系统，针对以核心企业为圆心，根据交易中构成的链条关系、行业特点和各业务自有流程，设计特有的融资方案，提供上下游多个企业提供的全面金融服务。并结合金融资产账户管理系统，与银行端对接，实现银行金融级账户应用及资金安全，

从而形成交易信息与资金信息的精准，反映整条供应链上的资产、负债和权益等的增减，实现真正意义上的有效资产管理。

本模块是属于网站后端，实现部分数据管理和业务逻辑，为前端提供接口，使用区块链模块提供的接口，在整个系统中起到重要作用。

1.2.2 目标

- (1) 本模块功能完整，接口友好
- (2) 整个系统可以稳定高效运行
- (3) 保证数据安全可靠

1.3 术语定义

- [1] 供应商：出售货物，使用该系统进行融资的企业。
- [2] 核心企业：购买货物，使用该系统的支付应收账款的企业。
- [3] 金融机构：使用该系统根据供应商和核心企业的贸易合同发放贷款的机构。

1.4 参考资料

- [1] 吕云翔.软件工程实用教程.北京：清华大学出版社，2015.

1.5 相关文档

- [1] 《软件开发计划书》
- [2] 《软件设计说明书》

1.6 版本更新记录

| 版本号 | 创建者 | 创建日期 | 维护者 | 维护日期 | 维护纪要 |
|------|-----|------------|-----|------|------|
| V1.0 | 陈思言 | 2019/04/28 | — | — | — |
| | | | | | |

2. 目标系统描述

2.1 角色定义

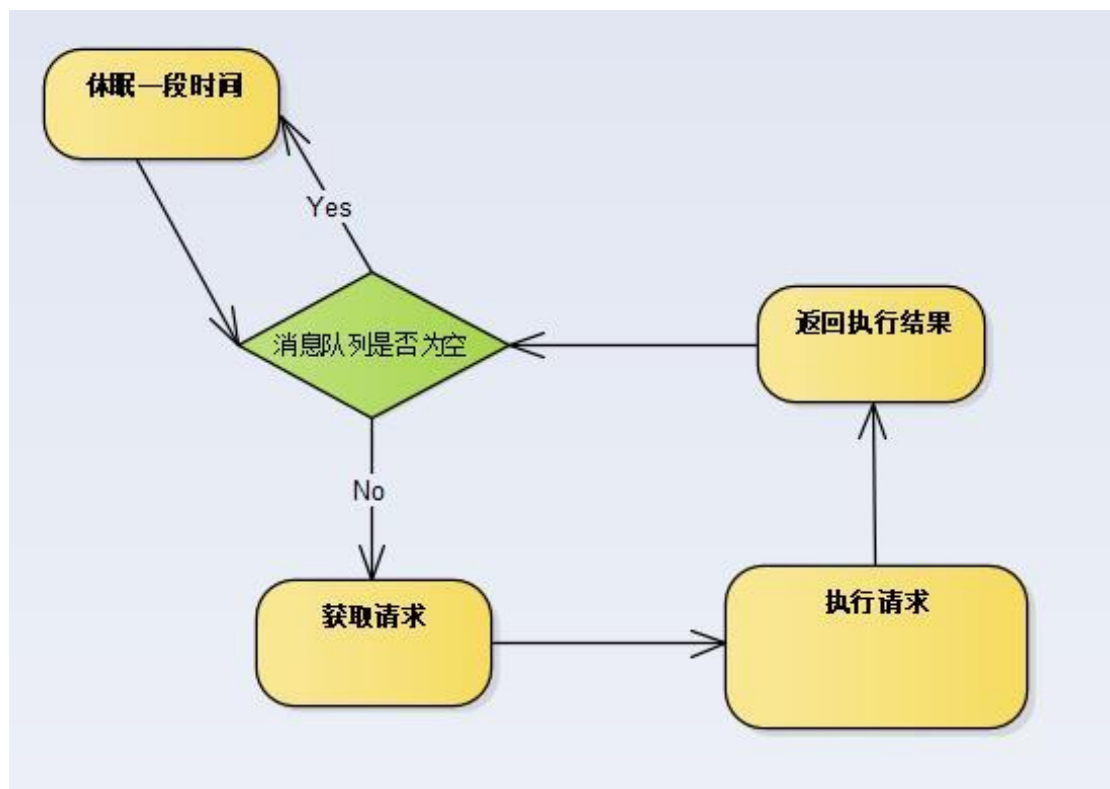
表 2.1 角色定义

| 编号 | 角色 |
|----|------|
| 01 | 供应商 |
| 02 | 核心企业 |
| 03 | 金融机构 |

2.2 工作流程

服务器在正常情况下将不停地按此图所描述的方式对前端发送来的请求进行处理：

图 2.1 服务器工作流程图



考虑到并发和编程难度问题，遇到区块链操作时候使用阻塞式同步操作，服务器的当前线程阻塞直到区块链操作完成，因此需要很多个线程来处理请求防止因一个操作阻塞导致其他请求响应长。每个服务线程的工作方式完全相同。没有请求是线程休眠一段时间，具体休眠时间依当前休眠线程数量确定，当前已有的休眠线程数量多时可以适当延长休眠时间。

2.3 单据、账本和报表

2.3.1 单据

暂无。

2.3.2 账本

暂无。

2.3.3 报表

暂无

2.4 可能的变化

根据前端的需要增加一些接口和用例

3. 目标系统功能需求

3.1 功能模块总体设计

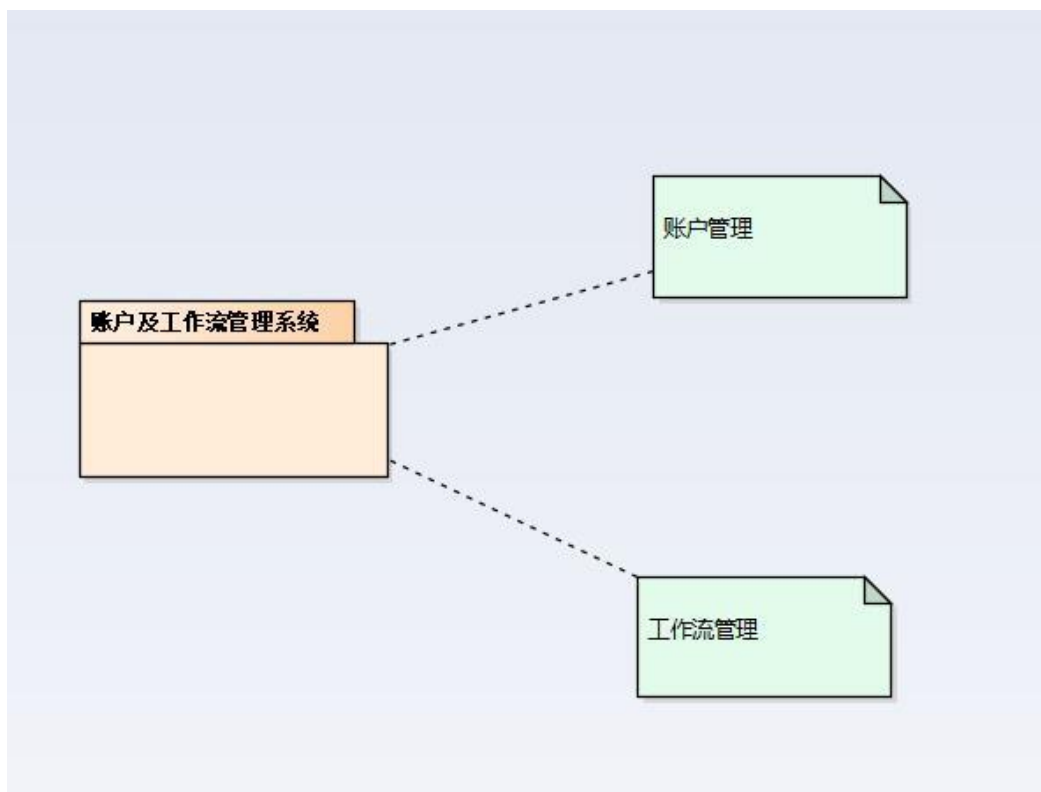


图 3.1 功能模块总体设计

3.2 功能模块详细设计

账户管理部分包含对 3 种不同账户的增删改查操作。普通账户信息存储在数据库中，实名信息和转账记录存储在区块链中，登录状态存储在内存中。

workflow 管理部分根据业务来对 workflow 进行增删改查操作。workflow 相当于一个状态机，记录当前交易处于从签订合同完成发货，到融资申请和放款，再到最后还款的整个过程的哪个状态，中间各种审批操作则是对状态的修改，如下图所示：

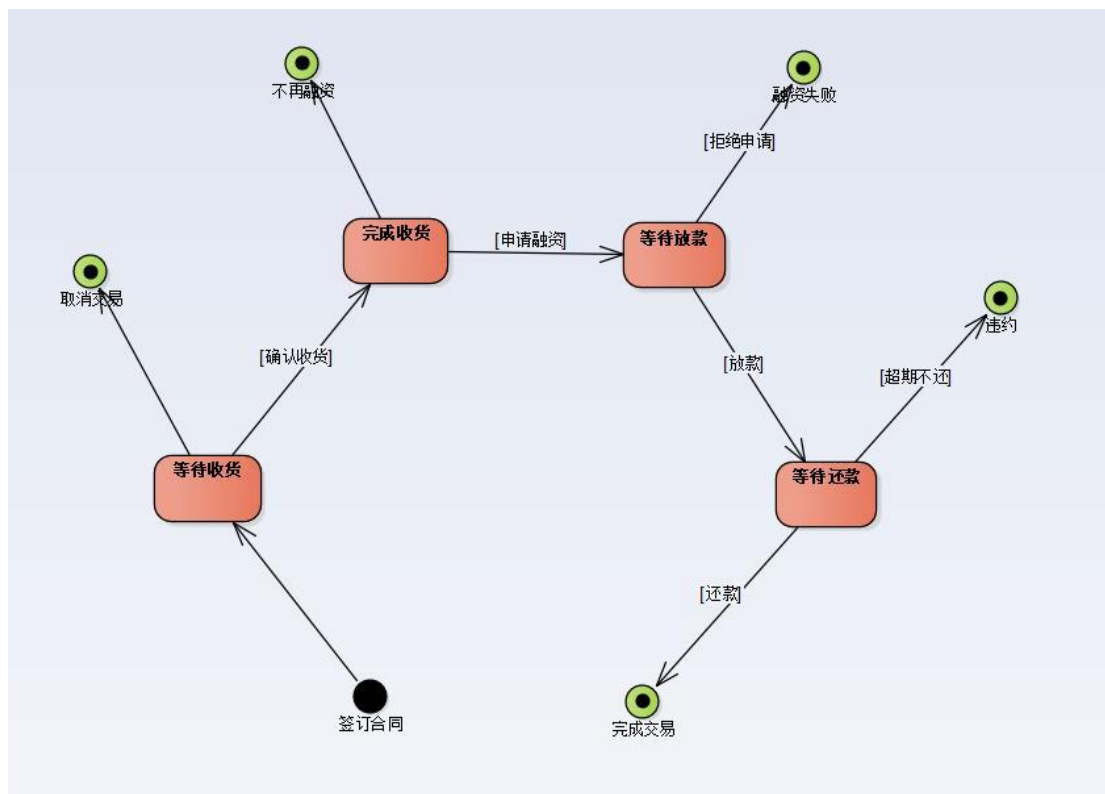


图 3.2 工作流示意图

3.3 用例详细说明

3.3.1 账户管理系统

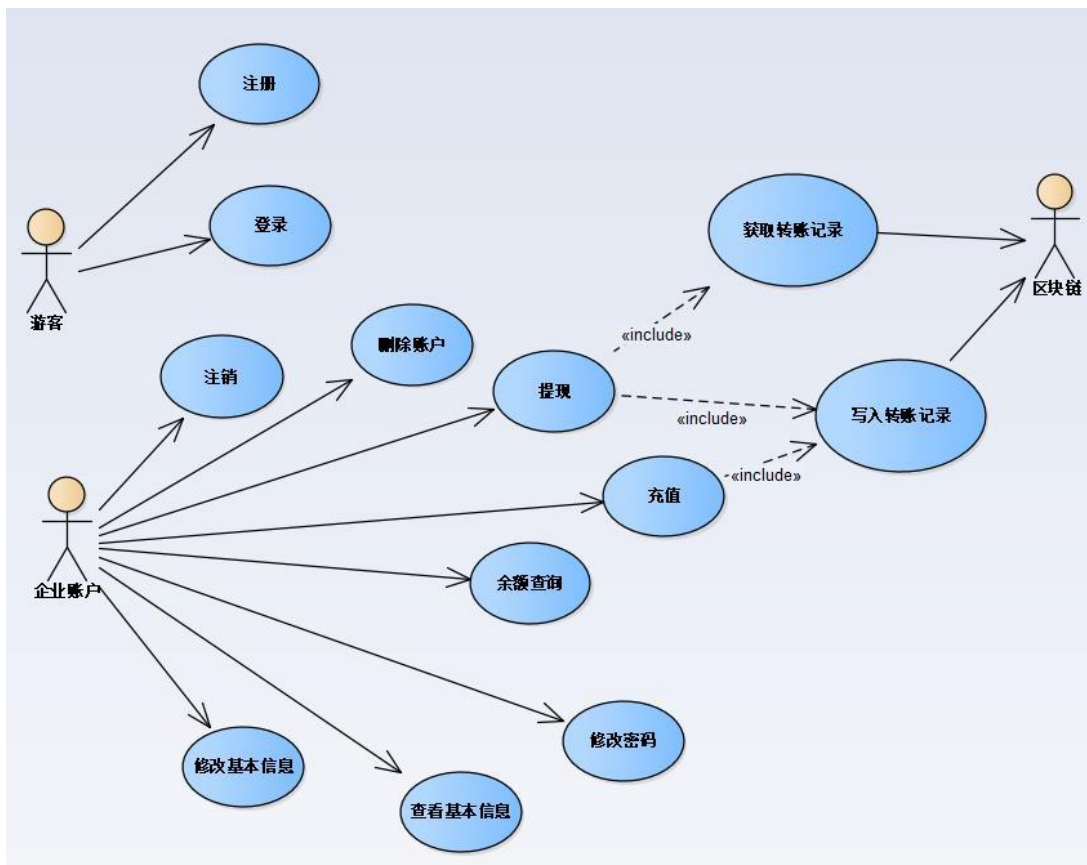


图 3.3 账户管理系统用例图

对用例的说明如下：

| | | | |
|------|--|------|-----------------------------------|
| 编号 | 101 | 用例名称 | 企业账户创建 |
| 使用人员 | 游客 | 扩展点 | 防止恶意注册 |
| 输入 | 企业身份（供应商、核心企业、金融机构），基本信息，实名信息 | | |
| 系统响应 | 在数据库中写入基本信息，实名信息存储在区块链 | | |
| 输出 | 通知前端注册成功或失败 | | |
| 前置条件 | 游客申请注册 | 后置条件 | 注册成功，成为供应商、核心企业、金融机构三者之一，但处于未实名状态 |
| 活动步骤 | 1. 从消息队列中得到注册请求 2. 在数据库中写入基本信息，需要对密码进行 SHA 处理 3. 调用区块链接口写入实名信息，等待实名认证审核 4. 账户余额初始化为 0，其他信息初始化为空 5. 通知前端注册成功并自动登录 | | |
| 异常处理 | 1. 请求格式不对（可能是伪造请求），忽略请求 2. 系统忙或故障，提醒用户稍后再试 | | |

| | | | |
|------|---------------|------|--------|
| 编号 | 102 | 用例名称 | 查看账户信息 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名 | | |

| | | | |
|------|---|------|---|
| 系统响应 | 从数据库中查找账户基本信息及状态 | | |
| 输出 | 返回账户基本信息及状态 | | |
| 前置条件 | 无 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到查询请求 2. 从数据库中查找账户基本信息及状态 3. 返回账户基本信息及状态给前端 | | |
| 异常处理 | 1. 用户名不存在，提示用户检查是否输错 2. 系统忙或故障，提醒用户稍候再试 | | |

| | | | |
|------|---|------|---------|
| 编号 | 103 | 用例名称 | 登录 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名、密码、校验码 | | |
| 系统响应 | 检验用户名和密码，如果成功记住登录状态 | | |
| 输出 | 该用户此次登录的密钥 | | |
| 前置条件 | 此账户已经注册过 | 后置条件 | 改为已登录状态 |
| 活动步骤 | 1. 从消息队列中得到登录请求 2. 检验用户名是否存在，密码是否正确 3. 修改登录状态 4. 生成 RSA 密钥 5. 提醒前端登录成功并返回密钥 | | |
| 异常处理 | 1. 用户名不存在或密码错误，提示用户检查是否输错 2. 系统忙或故障，提醒用户稍候再试 | | |

| | | | |
|------|--|------|------|
| 编号 | 104 | 用例名称 | 修改信息 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和修改后的信息 | | |
| 系统响应 | 在数据库中修改相应信息 | | |
| 输出 | 修改成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到修改请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 在数据库中修改相应信息 4. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍候再试 | | |

| | | | |
|------|---------------|------|------|
| 编号 | 105 | 用例名称 | 删除账户 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码 | | |
| 系统响应 | 在数据库中删除该账户的信息 | | |

| | | | |
|------|---|------|---------|
| 输出 | 删除成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 该账户不再存在 |
| 活动步骤 | 1. 从消息队列中得到删除请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 在数据库中删除相应信息 4. 删除与该账户相关的其他信息如工作流，余额自动提现 5. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍后再试 | | |

| | | | |
|------|---|------|------------|
| 编号 | 106 | 用例名称 | 注销 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 长时间无操作自动注销 |
| 输入 | 用户名，加密了的校验码 | | |
| 系统响应 | 修改为未登录状态 | | |
| 输出 | 注销成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 此账户变成未登录状态 |
| 活动步骤 | 1. 从消息队列中得到注销请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 修改为未登录状态 4. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip | | |

| | | | |
|------|--|------|------|
| 编号 | 107 | 用例名称 | 修改密码 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和新的密码 | | |
| 系统响应 | 在数据库中修改该账户的密码 | | |
| 输出 | 修改成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到修改请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 在数据库中修改该账户的密码 4. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍后再试 | | |

| | | | |
|------|-----------------|------|---------------------------|
| 编号 | 108 | 用例名称 | 余额查询 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 在确保余额不变的情况下可缓存余额数据，加快查询速度 |
| 输入 | 用户名，加密了的校验码 | | |
| 系统响应 | 从区块链中获取转账信息计算余额 | | |
| 输出 | 余额 | | |

| | | | |
|------|--|------|---|
| 前置条件 | 此账户是登录状态 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到查询请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 从区块链中获取转账信息计算余额 4. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍后再试 | | |

| | | | |
|------|--|------|--------|
| 编号 | 110 | 用例名称 | 充值 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 自动余额查询 |
| 输入 | 用户名，加密了的校验码和充值金额 | | |
| 系统响应 | 调用银行接口转账，转账记录写入区块链 | | |
| 输出 | 充值成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到充值请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 调用银行接口转账，从充值方的账户转入自己的账户 4. 转账记录写入区块链 5. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，通知管理员进行调查（若证实恶意操作将依法追究其法律责任） 2. 系统忙或故障，提醒用户稍后再试 3. 转账失败（银行账户余额不足）给出错误提示 | | |

| | | | |
|------|--|------|----|
| 编号 | 111 | 用例名称 | 提现 |
| 使用人员 | 供应商、核心企业、金融机构 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和提现金额 | | |
| 系统响应 | 调用银行接口转账，转账记录写入区块链 | | |
| 输出 | 提现成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 无 |
| 活动步骤 | 1. 从消息队列中得到提现请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 进行余额查询和检验 4. 调用银行接口转账，从自己的账户转入提现方的账户 5. 转账记录写入区块链 6. 返回成功提示给前端 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，通知管理员进行调查（若证实恶意操作将依法追究其法律责任） 2. 系统忙或故障，提醒用户稍后再试 3. 余额不足返回错误信息 | | |

3.3.2 工作流管理系统

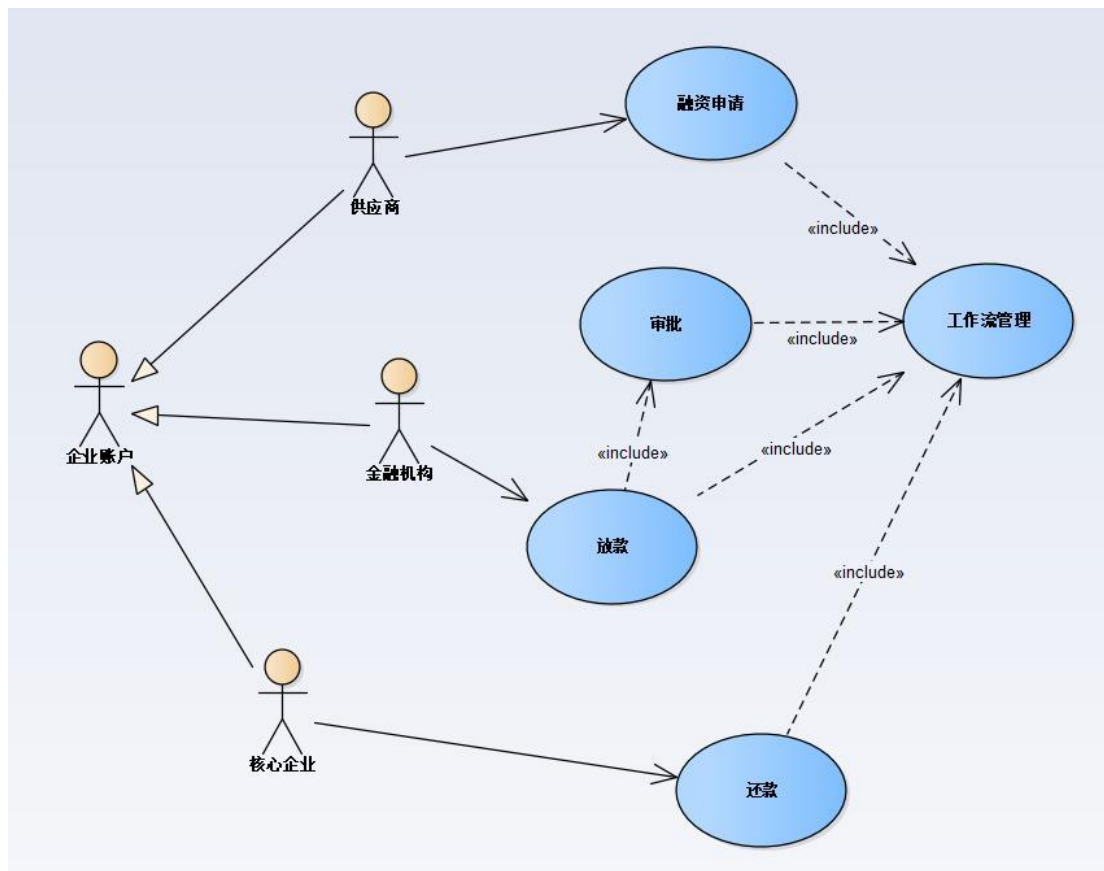


图 3.3 工作流管理系统用例图

对用例的说明如下：

| | | | |
|------|---|------|----------|
| 编号 | 201 | 用例名称 | 融资申请 |
| 使用人员 | 供应商 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和金融产品编号及融资金额 | | |
| 系统响应 | 工作流创建 | | |
| 输出 | 等待审批 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 新建了一个工作流 |
| 活动步骤 | 1. 从消息队列中得到融资申请请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 创建一个工作流并初始化为等待审批和放款状态 4. 通知前端等待审批 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍后再试 | | |

| | | | |
|----|-----|------|------|
| 编号 | 202 | 用例名称 | 发放贷款 |
|----|-----|------|------|

| | | | |
|------|---|------|-----------|
| 使用人员 | 金融机构 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和工作流编号 | | |
| 系统响应 | 工作流修改 | | |
| 输出 | 放款成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 修改此工作流的状态 |
| 活动步骤 | 1. 从消息队列中得到发放贷款请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 修改此工作流为等待还款状态 4. 转账信息存入区块链 5. 通知前端操作成功 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍候再试 | | |

| | | | |
|------|---|------|--------|
| 编号 | 203 | 用例名称 | 支付贷款 |
| 使用人员 | 核心企业 | 扩展点 | 无 |
| 输入 | 用户名，加密了的校验码和工作流编号 | | |
| 系统响应 | 工作流删除 | | |
| 输出 | 支付成功 | | |
| 前置条件 | 此账户是登录状态 | 后置条件 | 删除此工作流 |
| 活动步骤 | 1. 从消息队列中得到支付贷款请求 2. 使用对应该用户名的密钥进行解密，然后校验 3. 删除此工作流（完成了整个流程） 4. 转账信息存入区块链 5. 通知前端操作成功 | | |
| 异常处理 | 1. 用户名不存在或校验失败，认为这是伪造请求，暂时封锁该 ip 2. 系统忙或故障，提醒用户稍候再试 | | |

4. 目标系统性能需求

表 4.1 性能需求点列表

| 编号 | 性能点名称 | 使用部门 | 性能描述 | 输入 | 系统响应 | 输出 |
|----|--------------|------|---------------|-----------|-----------------|-----------|
| 1 | 企业账户信息查询 | 企业人员 | 查询账户基本信息及状态 | 企业账户的相关信息 | 在 1 秒内列出记录 | 输出符合要求的记录 |
| 2 | 工作流的创建、修改、删除 | 金融机构 | 在数据库中录入、修改、删除 | 工作流的相关信息 | 在 1 秒内进行录入、修改和删 | 输出提示信息 |

| | | | | | | |
|---|------|----|------------------------|----|--|---------------|
| | | | 相 应 的 信 息 | | 除, 并输出 提示信息 | |
| 3 | 支付系统 | 企业 | 查询余额, 订单验证, 安全防护 | 订单 | 在 1 秒内 检 查 用 户 状 态, 余 额, 订单合 法性, 进行 操 作 并 返 回 提 示 信 息 | 输 出 提 示 信息 |

5. 目标系统界面与接口需求

5.1 界面需求

本模块是纯后端，不需要界面。

5.2 接口需求点列表

需要银行结算系统。

6. 目标系统的其他需求

6.1 安全性

本项目应尽量提高数据传输的安全性，要对用户的请求进行加密防止恶意伪造请求。

6.2 可靠性

本项目应保证企业用户访问网站时都能正常操作。

6.3 灵活性

本项目应支持多种客户端登录，并且支持后续更新。

6.4 特殊需求

暂无。

7. 目标系统的假设与约束条件

该平台目前阶段异常处理还不够完善，只考虑一般问题导致的异常，暂不考虑因硬件 bug、有预谋的黑客攻击或不可抗力因素引起的数据错误。