

软件需求规格说明书

**项目名称：** 基于区块链的校园交易平台

学生姓名 卢良强

学 号 202202532

学 院 区块链学院

年 级 2022级

专 业 区块链技术

指导教师 邹林薏

完成日期 2024年9月25日

目 录

[1 引言 1](#_Toc21829)

[1.1 开发背景及目的 1](#_Toc26933)

[1.2 术语和缩写词 1](#_Toc5642)

[1.3 参考资料 1](#_Toc18697)

[1.4 版本信息 2](#_Toc26948)

[2 系统描述 2](#_Toc27613)

[2.1 用户简介 2](#_Toc19809)

[2.2 业务流程 2](#_Toc29529)

[3 系统功能需求 4](#_Toc20121)

[3.1 功能总体需求 4](#_Toc3927)

[3.2 用例建模 4](#_Toc26575)

[4 非功能性需求 10](#_Toc32678)

[4.1 性能需求 10](#_Toc13767)

[4.2 易用性 10](#_Toc2809)

[4.3 安全性与可靠性 10](#_Toc8469)

**基于区块链的校园交易平台需求规格说明书**

**1 引言**

## 1.1 开发背景及目的

随着校园二手商品交易需求的增长，传统的二手商品交易模式面临诸如交易安全性不足、信息不透明和流程复杂等问题，导致许多学生和教师难以高效、安全地进行物品交易。为了解决这些问题，本项目旨在开发一个基于区块链技术的校园交易平台。平台将利用区块链的去中心化、不可篡改、透明等特性，结合NFT（非同质化代币）技术，确保交易信息和商品的所有权得到确权，商品交易的每一个步骤透明可信。此外，通过智能合约，系统可以自动化处理商品交易的资金与物品转移，大幅提升交易的效率与安全性。

本项目的目的在于：

1）提供一个基于区块链的安全、高效、透明的校园交易平台；

2）实现商品的数字化确权，确保商品的真实性和唯一性；

3）通过去中心化的身份认证和支付系统，简化注册与支付流程；

4）通过自动化智能合约，提高交易效率，减少纠纷。

## 1.2 术语和缩写词

（1）NFT: Non-Fungible Token，即非同质化代币，代表商品的唯一性，应用于数字资产的确权与交易。

（2）智能合约: 通过区块链自动执行的合约，保证交易的安全性和透明性。

（3）区块链: 一种去中心化的分布式账本技术，记录不可篡改的交易历史，确保交易的透明性和安全性。

（4）IPFS: InterPlanetary File System，分布式文件存储系统，用于存储NFT元数据。

（5）MetaMask: 一个基于浏览器的区块链钱包插件，用户可以通过它进行区块链交易和身份验证。

（6）ERC-721: 以太坊区块链上的标准，用于NFT的实现。

（7）ETH: 以太坊区块链的原生加密货币，用于支付和交易。

## 1.3 参考资料

[1]王明明.区块链技术与应用[M].北京：人民邮电出版社，2019

[2]张云飞.区块链开发入门与实战[M].北京：机械工业出版社，2020

[3]宋新宇.区块链技术原理与应用[M].北京：清华大学出版社，2020

[4]李伟,王晓东.区块链智能合约设计与开发实战[M].北京：电子工业出版社，2021

## 1.4 版本信息

本文档的版本更新信息如下表1-1所示。

|  |  |  |  |
| --- | --- | --- | --- |
| 文档版本 | 发布时间 | 更新人 | 更新内容 |
| V1.0 | 2024年9月25日 | 卢良强 | 首次完成文档。 |
| V2.0 | 2024年9月29日 | 卢良强 | 完善文档用例图 |
| ... | ... | ... | ... |

表 1-1 文档版本

**2 系统描述**

## 2.1 用户简介

本系统面向不同的用户群体，分别为游客、注册用户和管理员。

1）游客：游客无需注册即可浏览平台上的商品和NFT，查看相关的详细信息。但游客无法进行购买、发布商品或生成NFT等操作。若游客需要使用更多功能，可以通过注册成为正式用户。

2）学生用户：学生用户通过注册后，可以使用区块链钱包MetaMask登录系统。学生用户可以发布商品、生成NFT、购买商品和NFT，并能够查看自己的交易记录。通过区块链技术，学生用户发布的商品和NFT会得到确权和交易安全保障。

3）教师用户：教师用户的权限与学生用户类似，能够发布商品、生成NFT、购买和出售商品或NFT，管理自己的交易记录。教师用户还可以参与平台功能的验收与测试，以帮助系统持续优化和改进。

4）系统管理员：系统管理员负责平台的整体管理和维护工作。他们可以管理用户权限、监控系统状态、部署和维护系统，并审核发布的商品和NFT内容。管理员还负责管理平台的区块链交易，确保系统运行的安全性与合规性。

## 2.2 业务流程

(1）用户注册与登录

用户通过MetaMask钱包进行去中心化身份认证，登录平台时无需使用传统的用户名和密码。

新用户首次访问平台时，需要安装并配置MetaMask钱包，完成身份验证后方可进入系统。MetaMask将自动生成唯一的区块链钱包地址，用于用户身份标识和平台交互。

(2）商品发布与NFT生成

用户登录后，可以发布商品信息。发布商品时，用户可以选择将该商品铸造成NFT，商品的元数据（如名称、描述、图片、价格等）将存储在去中心化存储平台（如IPFS）。

生成的NFT将通过区块链进行确权，确保商品的唯一性和安全性，发布的信息将显示在平台供其他用户浏览和购买。

(3）商品和NFT购买

用户可以浏览商品和NFT列表，选择想要购买的商品后，通过区块链智能合约进行支付和交易。支付过程通过MetaMask完成，用户选择数字货币作为支付方式。智能合约自动执行资金和商品/NFT所有权的转移，交易完成后，相关信息会更新到区块链，确保交易的透明性和不可篡改性。

(4）交易历史与确权查询

每个商品和NFT的交易记录都会保存在区块链上，任何用户都可以通过平台查询商品的确权历史和交易过程。区块链确保商品和NFT的所有权信息公开透明，不可篡改，保障商品和NFT来源的真实性和唯一性。

(5）系统管理与监控

系统管理员通过后台对用户权限进行管理，审核商品发布内容，确保商品和NFT的合法性。管理员还负责监控系统运行状态，如服务器性能、网络流量、交易处理情况等，保障平台的稳定性和安全性。

(6）智能合约管理

管理员可对智能合约进行部署、更新和维护，确保交易的安全性和合法性。智能合约确保所有交易都按照预定规则s执行，无需人工干预，同时保障了平台交易过程的透明性和自动化。

**3 系统功能需求**

## 3.1 功能总体需求

本系统的功能总体需求如下图3-1所示。

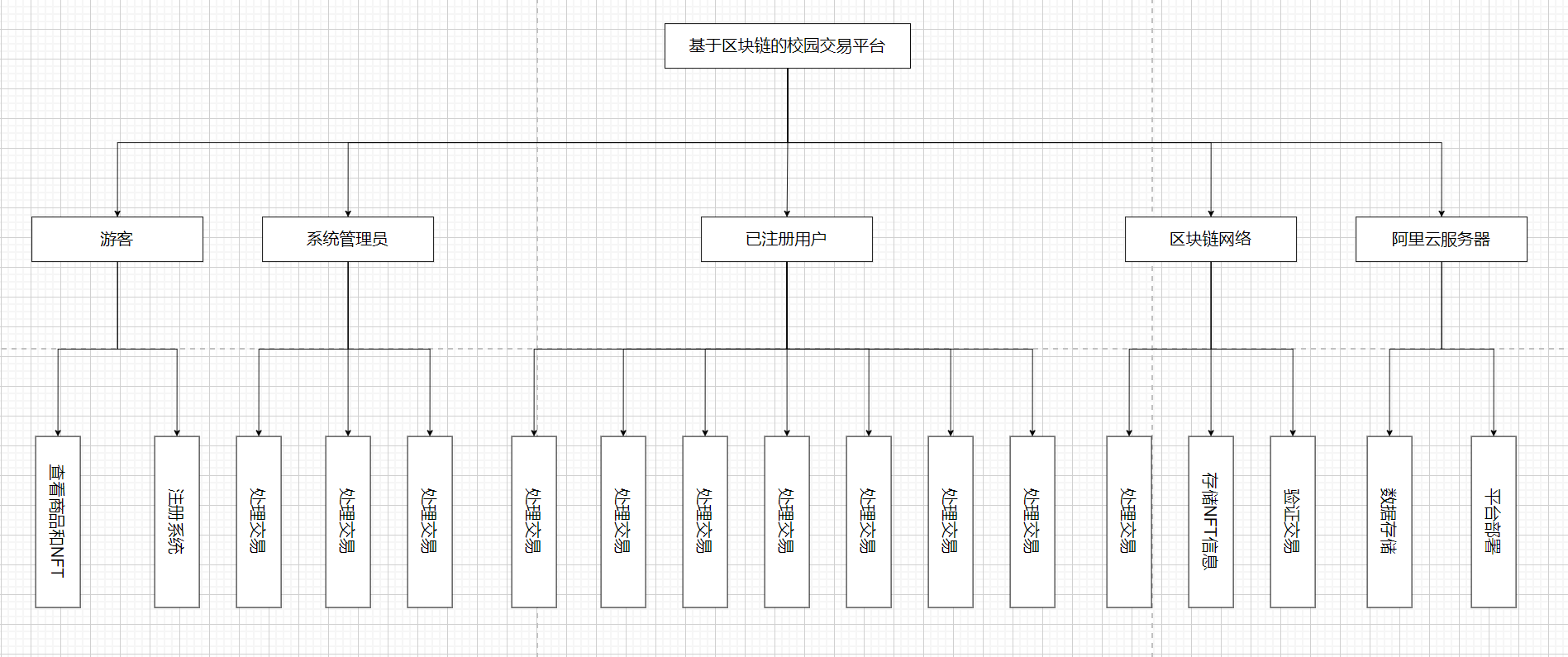


图 3-1 功能总体需求

## 3.2 用例建模

**3.2.1 已注册用户模块**

已注册用户模块用例图如图3-2所示。

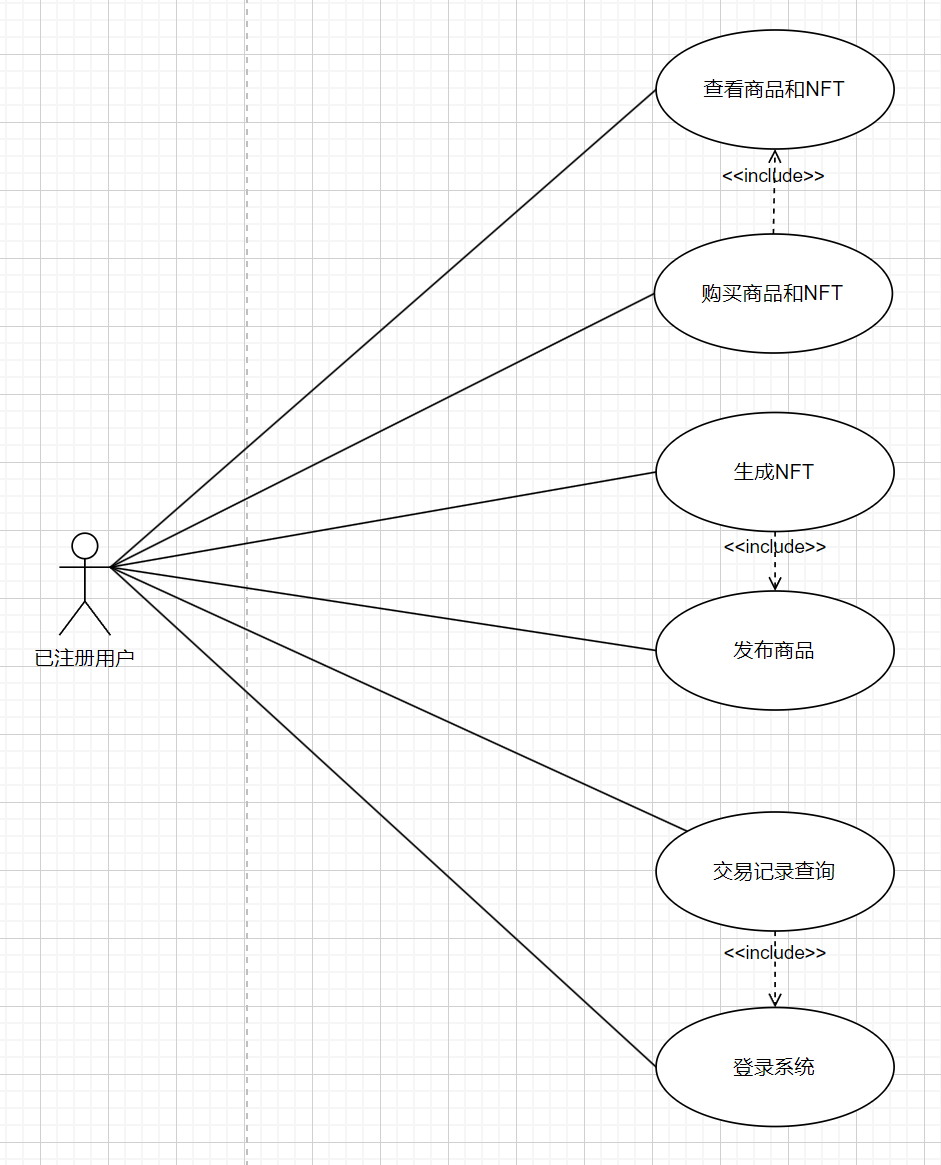
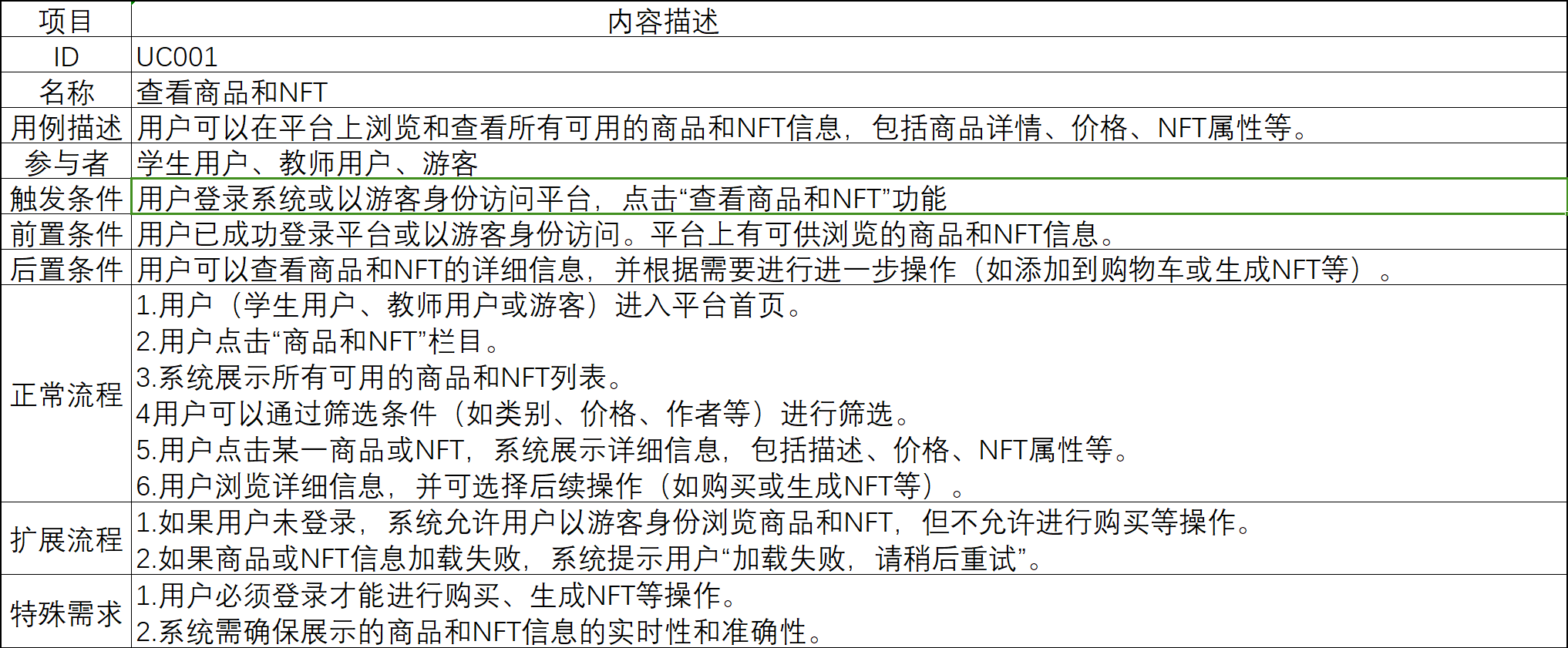


图 3-2 已注册用户模块用例图

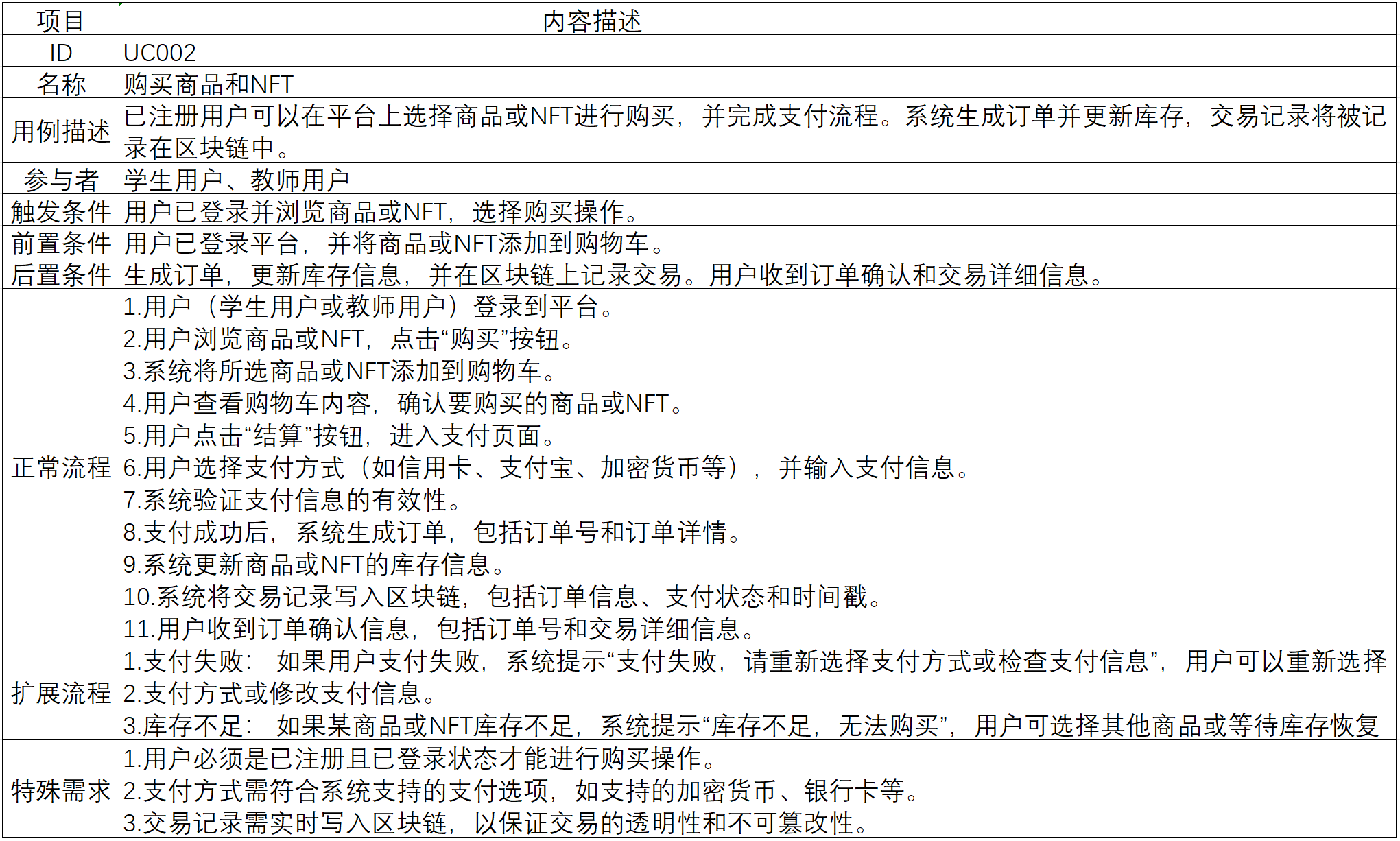
查看商品和NFT用例介绍表如表3-3所示。

表 3-3 查看商品和NFT用例介绍表



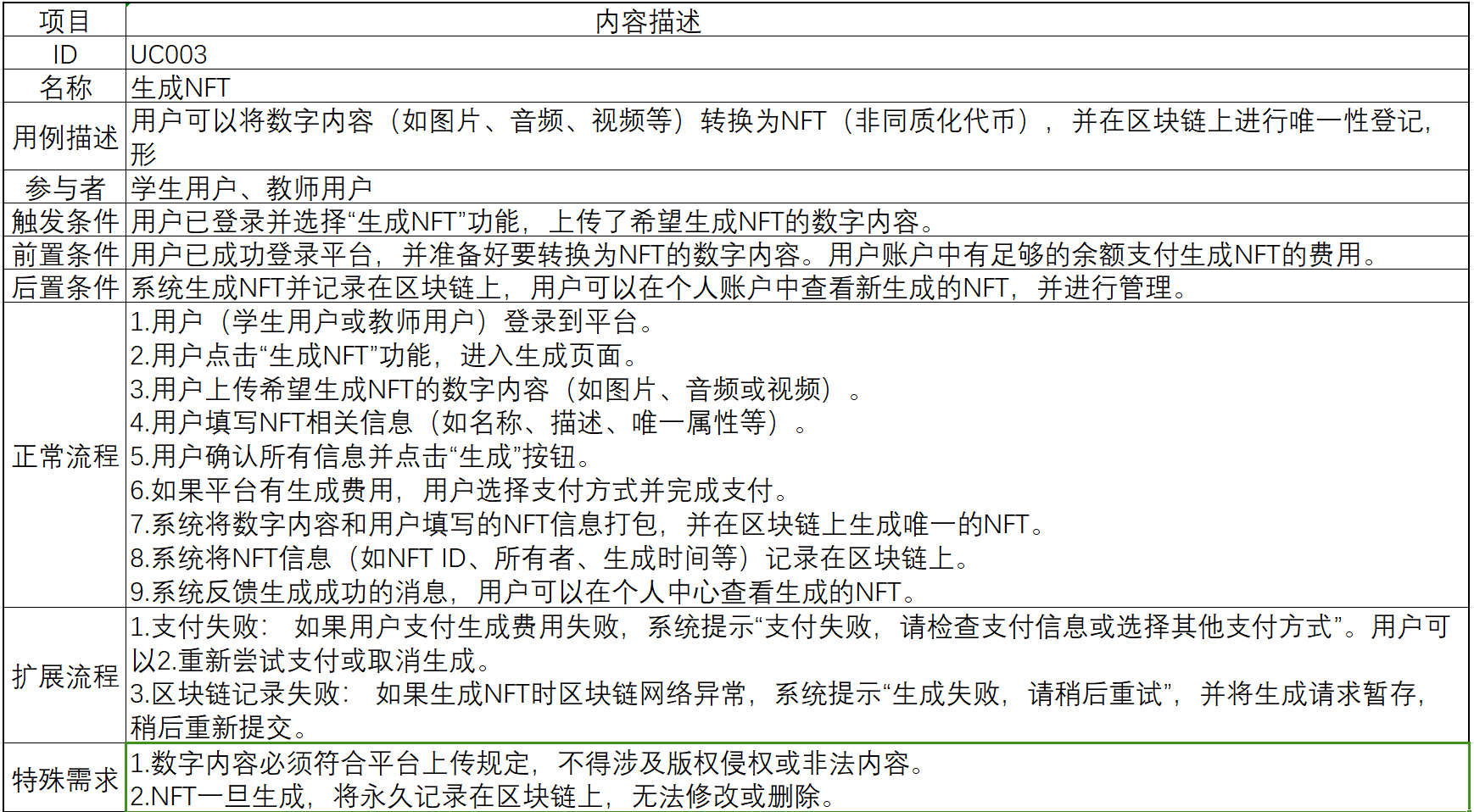
购买商品和NFT用例介绍表如表3-4所示。

表 3-4 查看商品和NFT用例介绍表



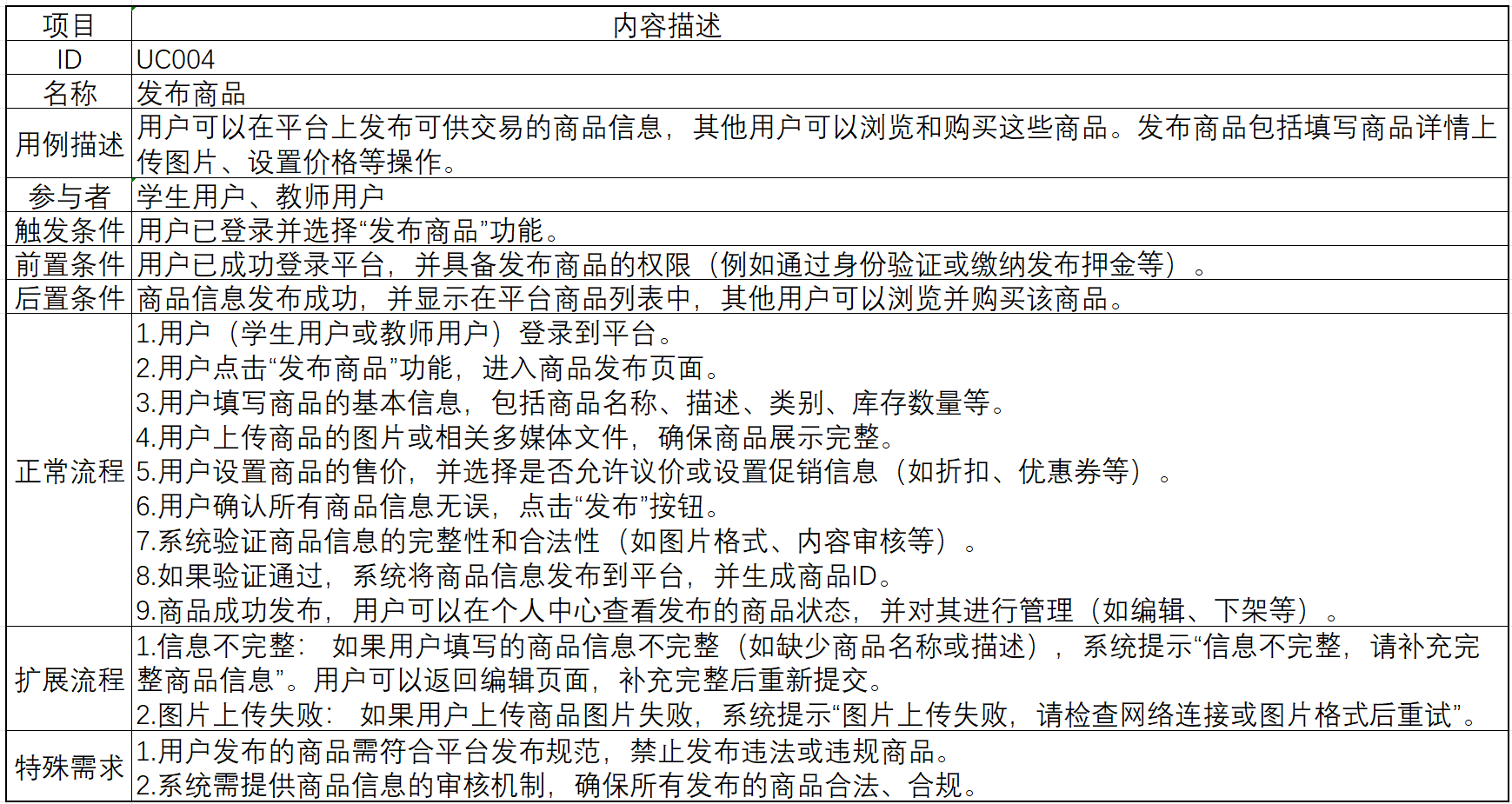
生成NFT用例介绍表如表3-5所示。

表 3-5 生成NFT用例介绍表



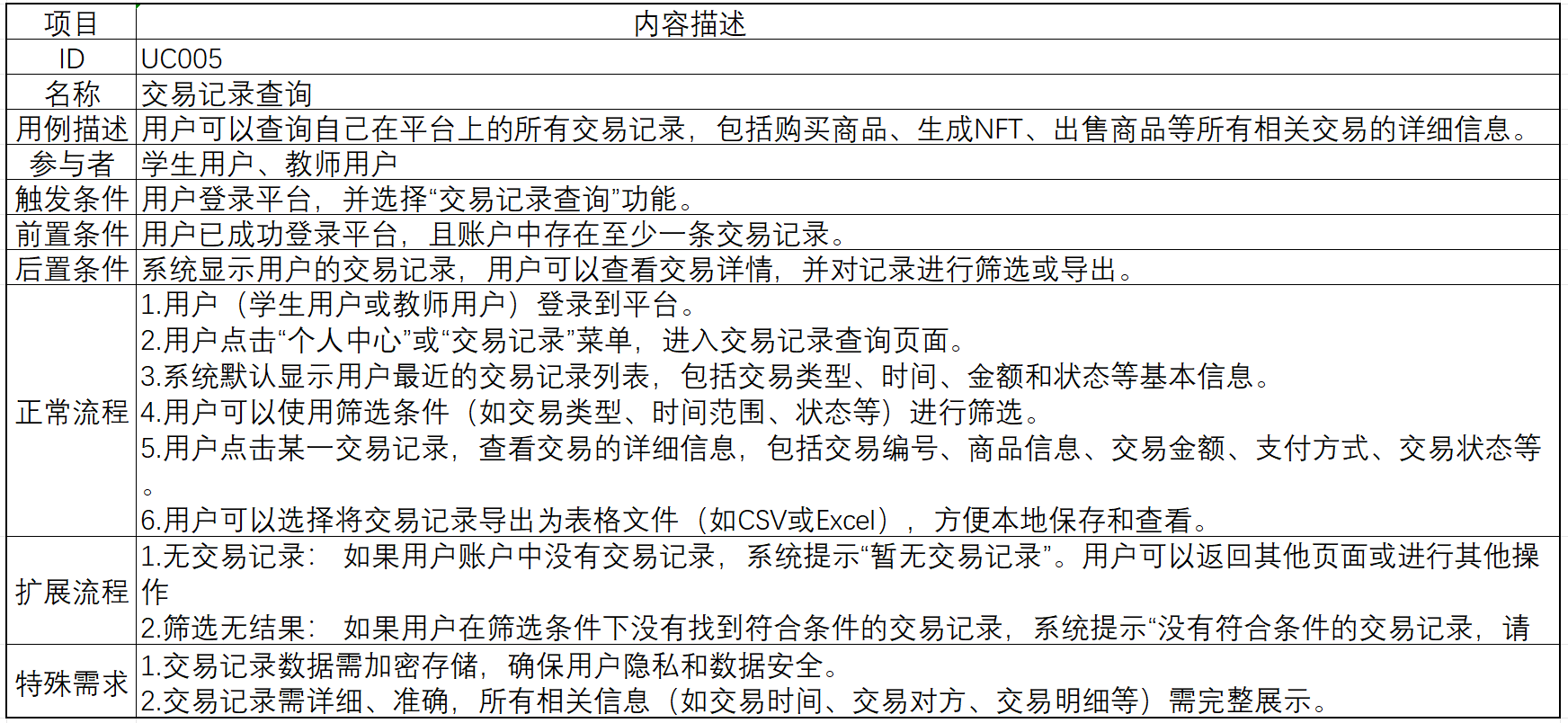
发布商品用例介绍表如表3-6所示。

表 3-6 发布商品用例介绍表



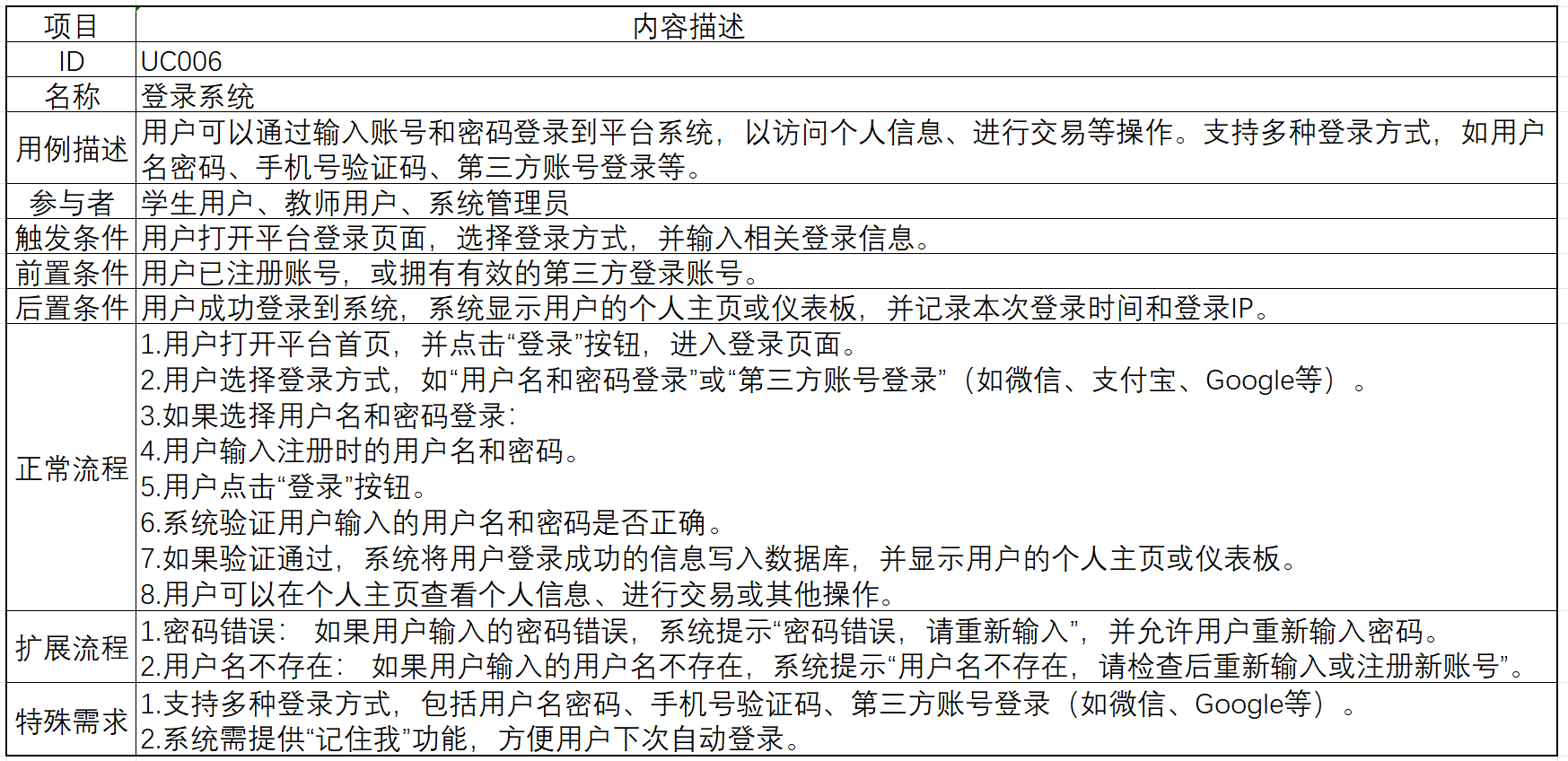
交易记录查询用例介绍表如表3-7所示。

表 3-7 交易记录查询用例介绍表



登录系统用例介绍表如表3-8所示。

表 3-8 登录系统用例介绍表



**3.2.2 区块链网络模块**

区块链网络模块用例图如图3-9所示

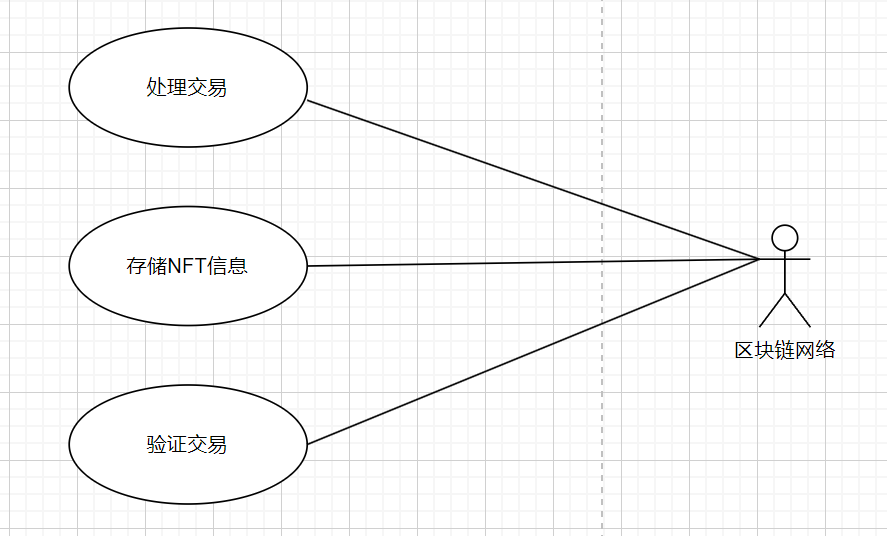
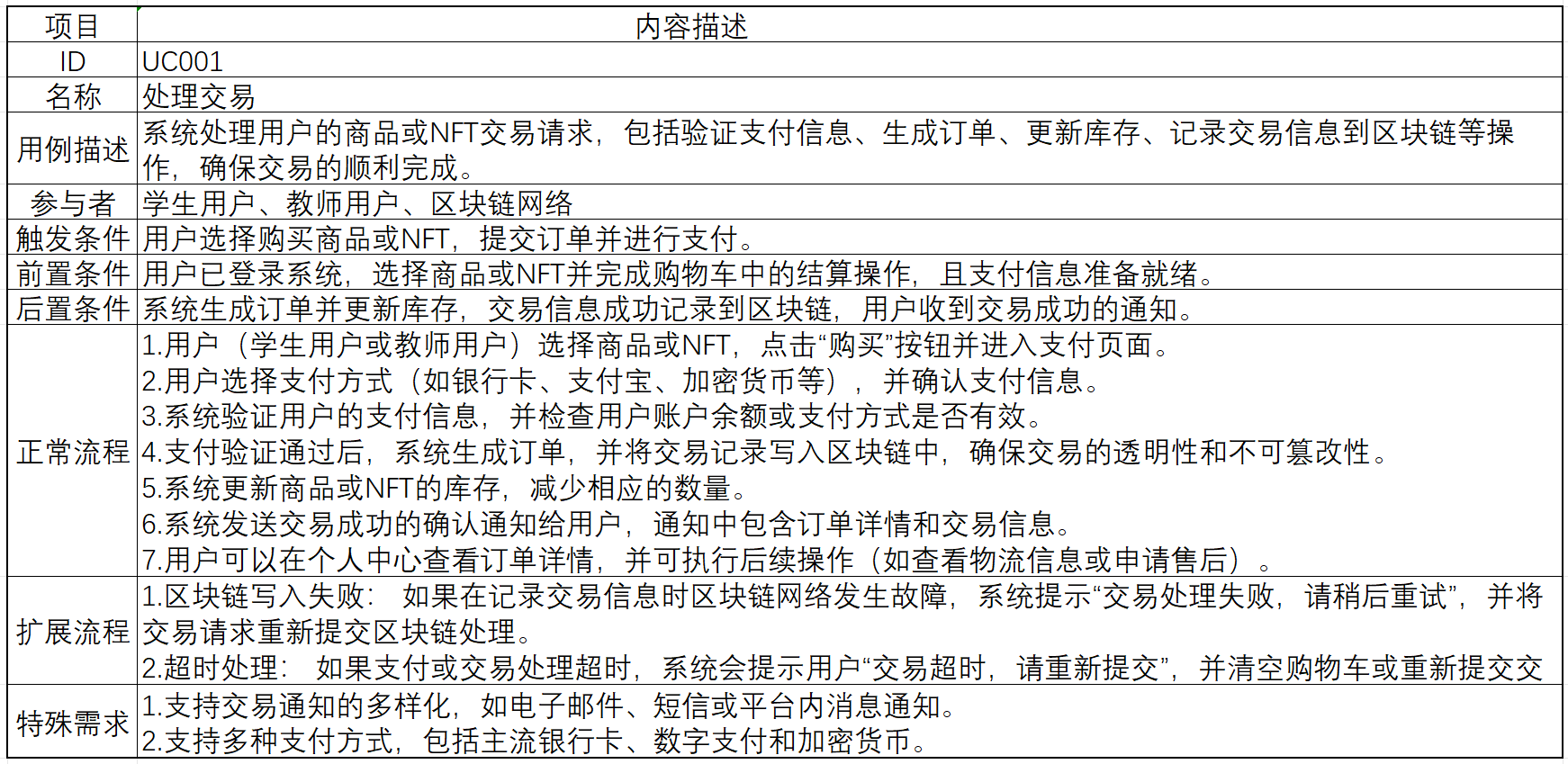
****

图 3-9 区块链网络模块用例图

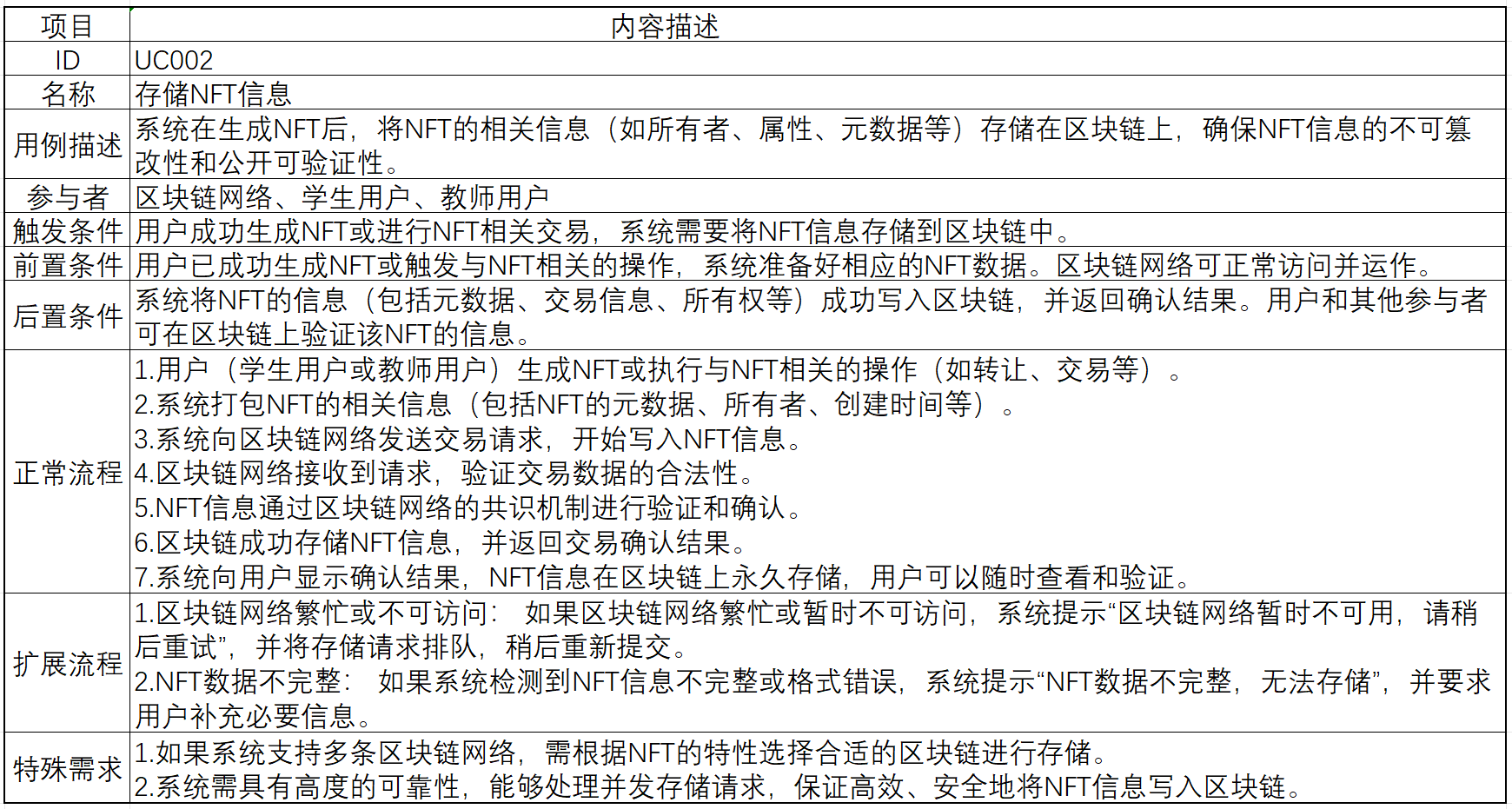
处理交易用例介绍表如表3-10所示。

表 3-10 处理交易用例介绍表



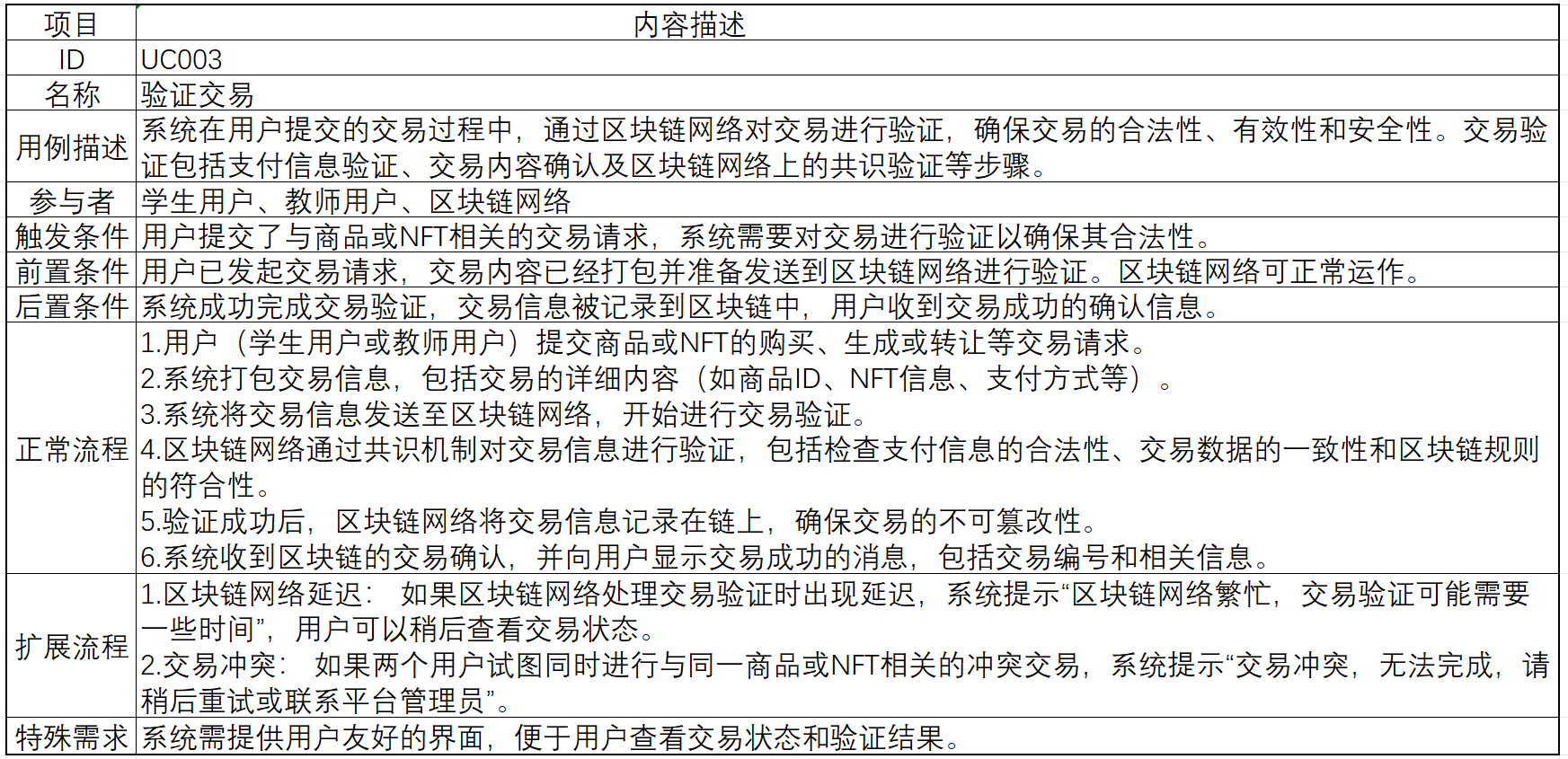
存储NFT信息用例介绍表如表3-11所示。

表 3-11 存储NFT信息用例介绍表



验证交易用例介绍表如表3-12所示。

表 3-12 验证交易用例介绍表



**3.2.3 系统管理员模块**

系统管理员模块用例图如图3-13所示

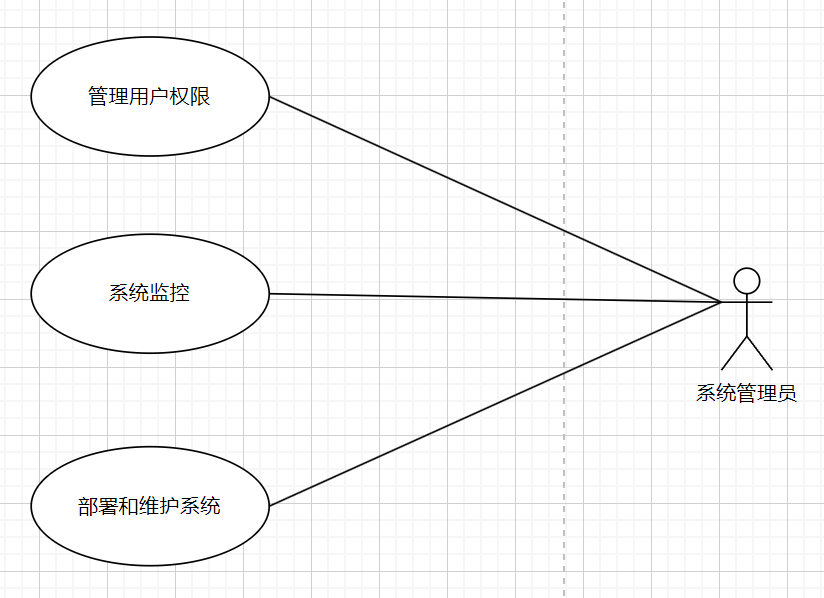
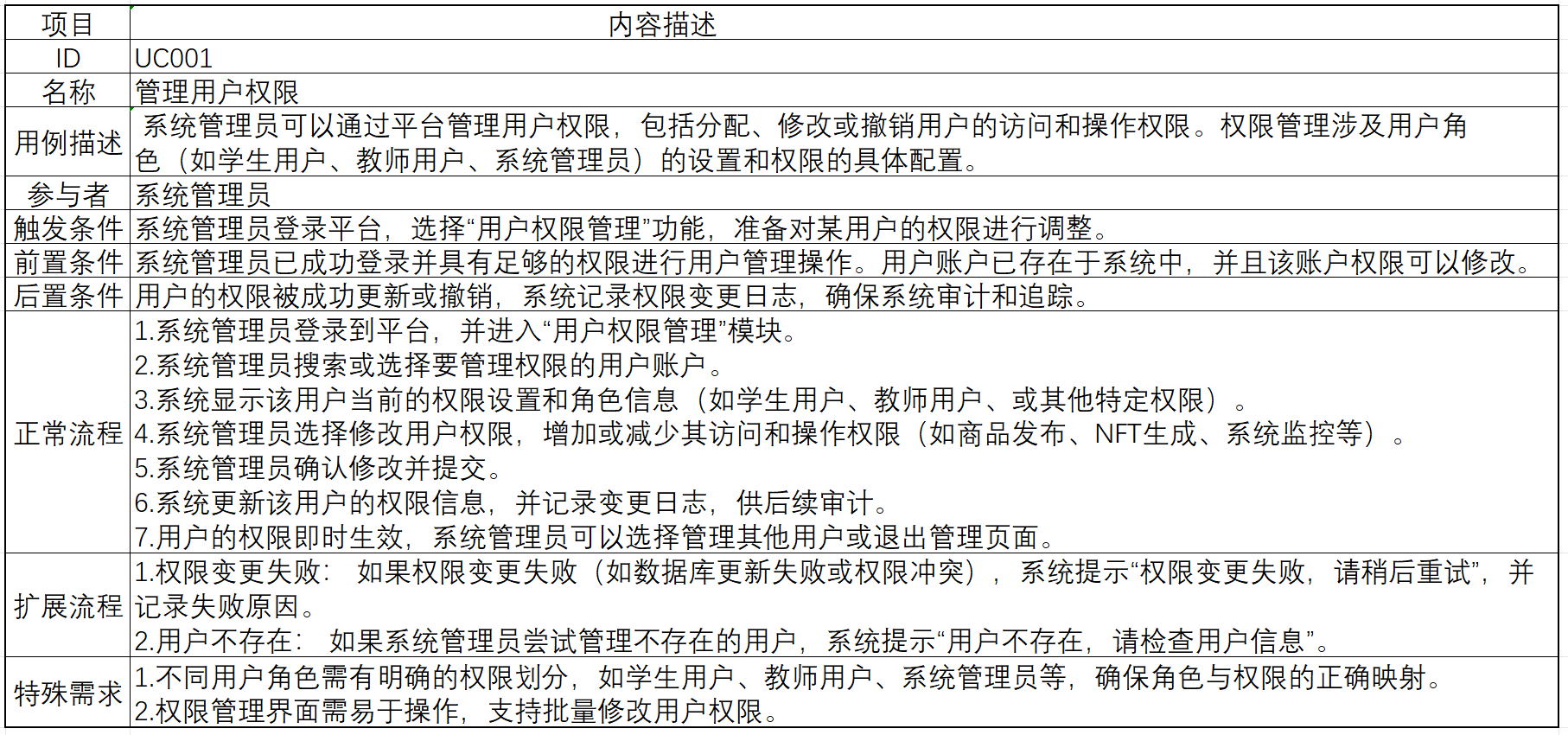
****

图 3-13 系统管理员模块用例图

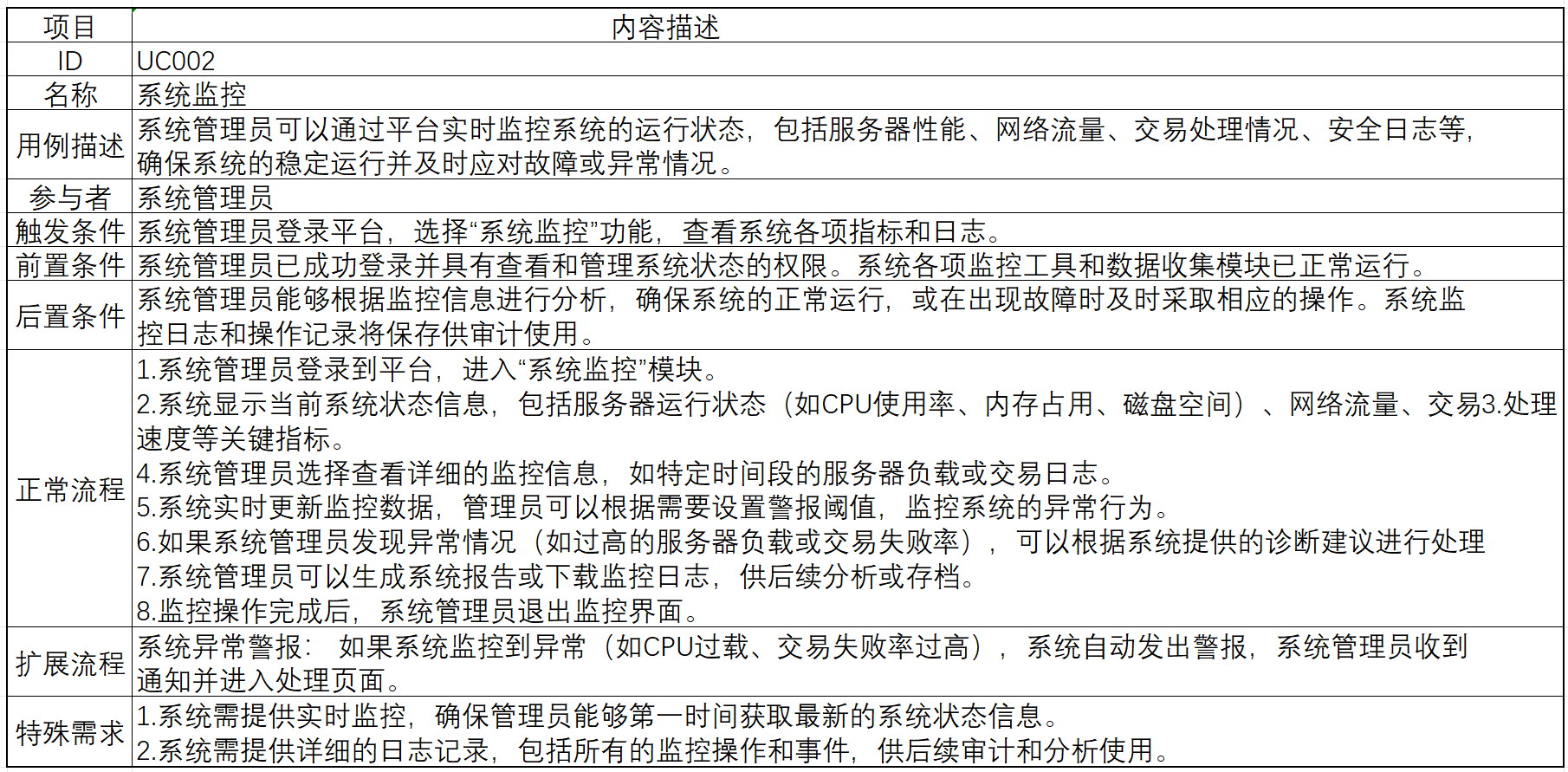
管理用户权限用例介绍表如表3-14所示。

表 3-14 登录系统用例介绍表



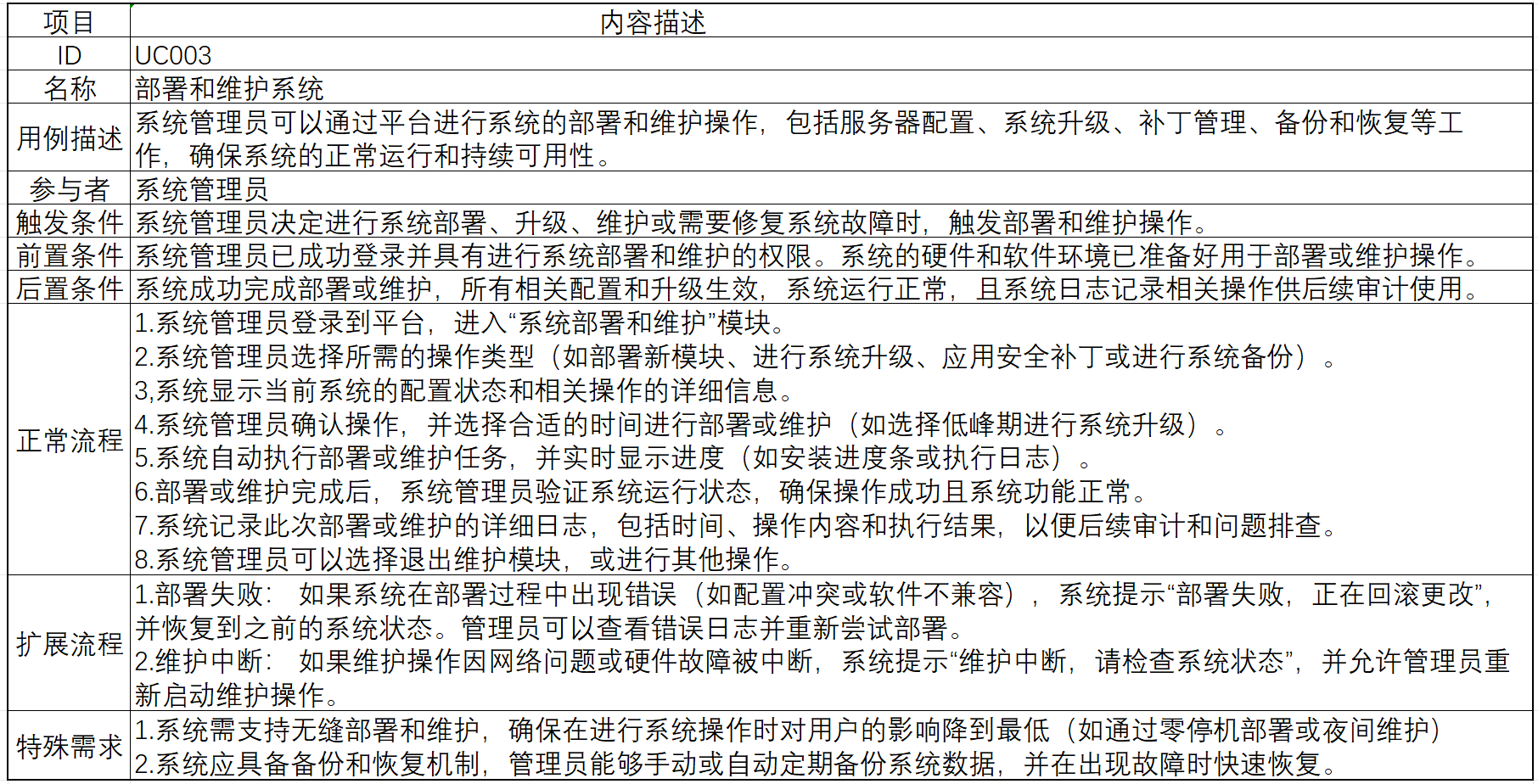
系统监控用例介绍表如表3-15所示。

表 3-15 系统监控用例介绍表



部署和维护系统用例介绍表如表3-16所示。

表 3-16 部署和维护系统用例介绍表



**4 非功能性需求**

## 4.1 性能需求

系统的性能需求主要包括以下方面。

1. 响应时间：对于常规操作，如浏览商品、查询交易记录等，系统的响应时间应在1秒内完成。

对于较复杂的操作，如生成NFT、调用智能合约等，系统的响应时间应在5秒内完成。

2）并发支持：系统需支持至少5000名用户的并发使用，且系统性能不应受到明显影响。

3）数据处理能力：系统需支持同时展示2000件商品，且查询商品时，检索时间不应超过30秒。

交易记录查询需要在1-2秒内返回结果。

## 4.2 易用性

软件易于使用是用户对软件的一个最基本的需求。为实现软件的易用性，软件应满足以下需求：

1. 简洁直观的用户界面：平台界面设计应简洁易用，初次使用的用户能够快速上手，所有功能都应易于访问和理解。
2. 响应式设计：系统需支持在不同设备上使用，包括桌面端和移动端，确保良好的用户体验。
3. 操作指导：对于首次登录的用户，平台需提供简单的操作指导，帮助用户快速了解如何发布商品、铸造NFT、购买商品等关键功能。
4. 错误提示与纠正：在用户执行错误操作时，系统应提供明确的错误提示，并引导用户正确操作。

## 4.3 安全性与可靠性

由于系统涉及交易与用户隐私，需保障平台的安全性与可靠性：

用户隐私保护：用户的身份信息、钱包地址、交易数据等敏感信息需加密存储，保证数据的隐私性。

交易安全：所有交易通过智能合约进行，确保资金和商品所有权的转移在链上完成，交易记录公开透明且不可篡改。

防止欺诈与攻击：系统需具备防止常见网络攻击（如DDoS攻击、SQL注入等）的能力，保障平台的安全性。

崩溃恢复与备份：系统应具有数据备份和恢复机制，确保在发生系统崩溃或故障时，能够迅速恢复系统功能，保障交易和数据不丢失。