

团 体 标 准

T/ZADT XXXX-XXXX

数字贸易 基于区块链的大宗散货仓单 系统应用指南

Digital Trade – Application Guideline for Blockchain-based
Bulk Cargo Warehouse Receipt System

(征求意见稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

浙江省国际数字贸易协会 发布

ZADOT

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语	1
4 业务参考架构	1
5 相关参与方	2
5.1 货主	2
5.2 仓储公司	2
5.3 贸易商	2
5.4 监管机构	2
5.5 平台方	2
6 大宗散货仓单系统基础功能要求	2
6.1 基础模块	2
6.2 业务服务模块	3
7 底层区块链系统的功能要求	4
7.1 智能合约功能要求	4
7.2 存储功能要求	4
7.3 运维功能要求	4
8 应用原则	5
8.1 合规性原则	5
8.2 安全性原则	5
8.3 权限分级原则	5
8.4 可扩展性原则	5
8.5 业务高可用原则	5
8.6 可追溯原则	5

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由宁波舟山港集团有限公司、浙江大学、杭州趣链科技有限公司提出。

本文件由浙江省国际数字贸易协会归口。

本文件起草单位：。

本文件主要起草人：。

ZADT

数字贸易 基于区块链的大宗散货仓单系统应用指南

1 范围

本文件为基于区块链的大宗散货仓单系统的建设和使用提供指导建议，具体建议了基于区块链的大宗散货仓单系统的业务参考架构、相关参与方、基础功能要求和应用原则等。

本文件适用于基于区块链的大宗散货仓单系统的建设和使用，为相关开发、使用组织、机构提供应用指南与建设参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18354 物流术语
ISO 22739:2021 Blockchain and distributed ledger technologies – Vocabulary

3 术语

下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加而形成的分布式账本。

注：区块链旨在防止篡改并创建最终的，确定的和不变的账本记录。

[来源：ISO/WD 22739:2021, 3.6]

3.2

共识 consensus

分布式账本节点间达成的协议，即交易已验证并且分布式账本包含已验证交易的一致性集合和顺序。

注1：共识不等同于所有节点同意。

注2：分布式账本设计之间关于共识的细节有所不同，这是一种设计和另一种设计之间的区别特征。

[来源：ISO/WD 22739:2021, 3.6]

3.3

智能合约 smart contract

存储在分布式账本中的计算机程序。

注：用于程序化的记账或自动化交易执行，其共识执行结果都记录在分布式账本中。

3.4

仓单 warehouse receipt

仓单保管人在与存货人签订仓储保管合同的基础上，按照行业惯例，以表面审查、外观查验为一般原则，对存货人所交付的仓储物品进行验收之后出具的权利凭证。

[来源：GB/T 18354-2006, 3.22]

4 业务参考架构

基于区块链的大宗散货仓单系统的业务参考架构如图1所示，从底向上可分为基础服务层、业务服务层。货主、贸易商、仓储公司、监管机构等参与机构可以使用移动客户端或浏览器等设备通过API接口技术接入系统进行各项业务操作。

其中基础服务层为系统提供必要的底层设施服务，包含区块链技术服务，利用区块链多中心化、防篡改、可追溯等技术特点来保障大宗散货仓单的真实性和唯一性。

业务服务层为用户提供业务功能服务，并在操作过程中，将业务数据、文件信息、操作行为等重要信息存储在区块链上。

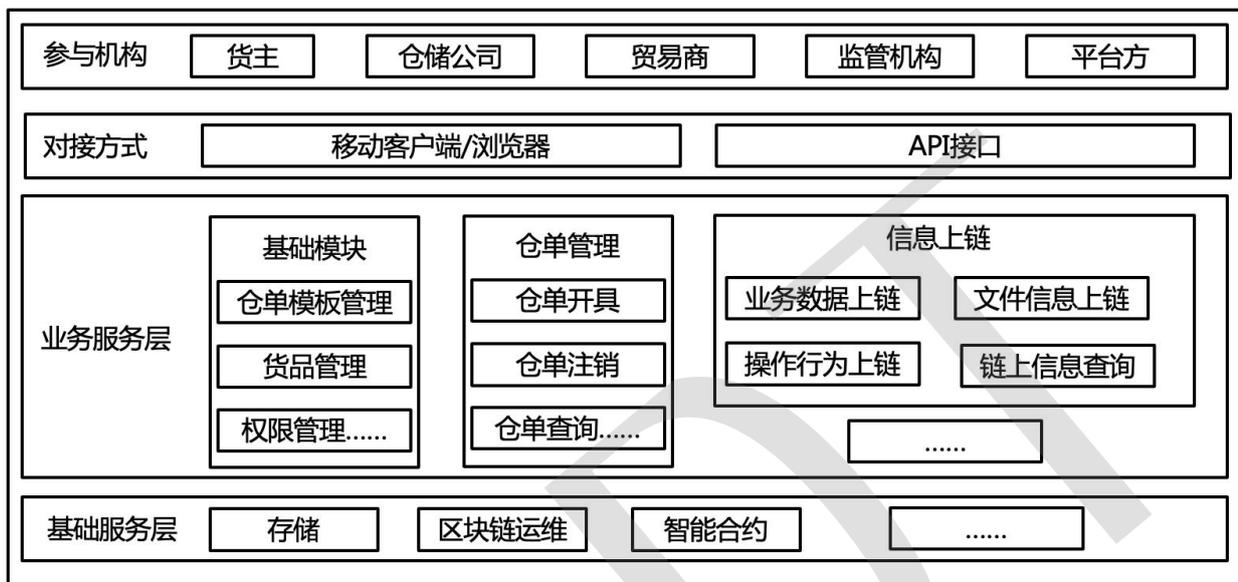


图1 基于区块链的大宗散货仓单系统参考架构

5 相关参与方

5.1 货主

货主即存货方，货物所有权的拥有人或机构。

5.2 仓储公司

为用户提供货物仓储与运输服务的服务商。

5.3 贸易商

进行大宗散货的交换或买卖活动的人或机构。

5.4 监管机构

对区块链大宗散货仓单系统的仓单交易进行监管审计和干预。包括质检单位、证书签发单位等机构。

5.5 平台方

为区块链大宗散货仓单系统提供基础功能模块的管理与运维服务。

6 大宗散货仓单系统基础功能要求

6.1 基础模块

基于区块链的大宗散货仓单系统的基础模块宜包含仓单模块管理、货品属性管理、审批流程管理、业务关系管理等。

6.1.1 仓单模块管理

- 支持用户对仓单模板的全生命周期进行管理，全生命周期可包含但不限于仓单模板的新建、编辑、删除等操作；
- 支持用户在列表查看创建的仓单模板，可支持对历史版本的查看。

6.1.2 货品属性管理

- 支持用户对货品属性进行管理，可包含但不限于：货品属性的新增、编辑、自定义添加、删除查看等操作；
- 支持用户在列表查看创建的货品属性，可支持对历史版本的查看。

6.1.3 审批流程管理

- 支持用户对仓单签发、仓单注销等流程的审批过程进行配置，可根据实际业务需求设置监管方和审批流程；
- 支持用户对创建的审批流程进行停用操作，停用的审批流程无法再被业务关联；
- 支持用户对已停用的审批流程重新开始使用，重新开启使用的审批流程可被业务关联。

6.1.4 业务关系管理

- 支持用户对业务关系进行配置，可根据实际业务需求将各方用户与仓单模板、审批流程等进行关联形成配套业务体系；
- 支持用户对创建的业务关系进行停用操作，停用的业务关系无法再被使用；
- 支持用户对已停用的业务关系重新开始使用。

6.2 业务服务模块

基于区块链的大宗散货仓单系统业务服务模块宜包含基础模块、用户管理、仓单管理、信息上链等。

6.2.1 用户管理

- 基于区块链的大宗散货仓单系统的用户管理功能宜包含但不限于：
- 支持不同相关方的用户注册系统，并根据自身用户类型提交相应材料；
 - 支持平台管理员对用户提交材料进行审核，审核通过用户才可使用系统；
 - 支持用户修改维护用户信息和密码；
 - 支持用户对自己的密钥进行管理，可下载拥有的密钥；
 - 支持管理员用户配置不同的角色；
 - 支持管理员用户为不同角色配置不同的权限；
 - 支持管理员用户为不同的用户分配不同的角色，相应角色的用户只能拥有相应权限。

6.2.2 仓单管理

基于区块链的大宗散货仓单系统的用户管理功能宜包含但不限于：

6.2.2.1 仓单签发

- 支持货主用户提交仓单签发申请，仓单签发信息可包含但不限于：货主信息、仓储场所等基本信息，货品名称、存货量、货品规格等存货信息，填货信息和质量检测证书附件信息等必要的申请信息；
- 支持监管方对货主提交的仓单签发申请进行审批，审批通过才可签发成功；
- 支持平台方在监管方进行签发审批时使用Ukey等技术手段保证审批的安全性；
- 支持货主用户提交的仓单申请信息、监管方的审批操作等重要信息存储在区块链上。

6.2.2.2 仓单注销

- 支持用户对已签发的仓单申请进行注销操作；
- 支持监管方对仓单注销申请进行审批，审批通过才可注销成功；
- 支持平台方在监管方进行注销审批时使用Ukey等技术手段保证审批的安全性；
- 支持平台方将仓单注销流程操作记录存储在区块链上。

6.2.2.3 仓单查询

- 支持用户查看申请的仓单列表；
- 支持用户根据列表字段对仓单进行模糊搜索；
- 支持用户查看仓单状态；
- 支持用户对仓单流转过程进行溯源查询，显示正确的溯源结果；
- 支持用户对仓单进行冻结操作，被冻结的仓单不能再被使用；
- 支持用户对冻结的仓单进行解冻操作，被解冻的仓单可以继续被使用。

6.2.3 信息上链

基于区块链的大宗散货仓单系统的上链信息宜包括但不限于：

- 平台支持仓单的业务数据上链；
- 平台支持各角色用户上传的文件信息上链；
- 平台支持各角色用户的操作行为上链；
- 平台支持对链上信息的查询和校验，查验数据是否被篡改。

7 底层区块链系统的功能要求

7.1 智能合约功能要求

底层区块链系统的智能合约，宜考虑以下条件：

——宜支持智能合约的触发和执行。使用者可通过某种编程语言定义智能合约逻辑，发布到区块链上之后，根据智能合约条款的逻辑，由使用者签名或者其他的事件触发执行，完成交易结算等智能合约的逻辑。

——宜支持智能合约验证功能。上层应用能根据实际业务需求，将业务执行规则编码成智能合约脚本，继而将智能合约部署在底层区块链系统，由记账节点负责在安全的容器环境中运行，给出运行结果。

——宜支持分布式多方共识记账功能。参与方在通过智能合约对业务进行验证后，使用共识算法对运行结果的正确性进行投票，最终将投票的结果记录到分布式账本中，同时分布式账本通过哈希链的方式将交易包含在数据块中，降低数据篡改的可能性。

——系统应具有跨平台特性，支持不同的操作系统，如：Windows、Linux等，实现一次开发，多端调用。

7.2 存储功能要求

底层区块链系统的存储功能，宜考虑以下条件：

——系统应支持本地数据库存储、文件系统存储以及云存储多种方式。本地存储应支持冷热分离，数据库存储应支持分库分表的模式，云存储应支持无损扩容，支持按照云的集群规则无限扩展。

——系统的数据存储宜采用链数据库与状态数据库的双数据库方式进行存储。链数据库保存链数据，所有的业务数据都存在此数据中，让数据有源可溯。状态数据库用于保存当前的状态值，以避免遍历所有的交易日志去计算当前的状态值。双数据库方案在保存所有交易历史证据的同时，可以极大提升数据查询的速度。

7.3 运维功能要求

底层区块链系统的运维功能，宜考虑以下：

——系统应提供全面、实时、可视化的运维管理系统，快速识别系统状态，满足多个层级的运营管理需求；

——系统应提供可视化的服务交付。从代码编译、测试、灰度环境验收到正式环境部署，整个服务交付流程实现可视化管理。

——系统应提供可视化的服务度量。对数据进行标准化的分层归类，从基础设施、上层组件、应用服务到使用者侧，基于应用的拓扑架构，收集各类指标，统一到一个分析平台中展现。

——系统应提供通用高效的信息采集组件，把机器的系统信息（如CPU，内存、硬盘、网络等状态）、节点使用状态（如节点访问量、访问耗时、节点健康状态等）以及业务使用情况（业务访问量、成功率、耗时分布等）实时展示到监控界面上，便于整个系统的管理。

——系统宜支持数据态势呈现功能。系统通过对账本中的数据进行提取分析，形成数据的当前世界状态和历史记录，继而通过界面进行呈现，同时也可对当前系统节点的运行状态进行监控。

8 应用原则

8.1 合规性原则

大宗散货仓单系统及配套设施的建立、运行等应满足合规性要求，宜考虑以下条件：

- 设计文档中对于账本系统的职责、权限等规范明确，使账本系统的运作有规范可循；
- 系统对于用户个人信息采取加密保护和安全管理措施；
- 遵循独立性、系统性、全员参与、强制性、管理地位与职责明确的科学管理原则进行合规管理。

8.2 安全性原则

大宗散货仓单系统需满足安全性原则，宜考虑以下条件：

- 具备系统的保密与安全防护、私钥密钥算法的选取、系统各层数据的传输安全保障等条件；
- 具备安全保障机制，配有可不断完善、改进的应急处理机制与实际措施；
- 确保加入节点的各方身份安全可靠，资产真实合法，节点权限可控；
- 确保数据的生成、传输、存储、调用的数据安全，宜将密钥与数据分离，确保其保密性。

8.3 权限分级原则

大宗散货仓单系统的权限划分、授予、收回等宜纳入系统生命周期管理中，宜考虑以下条件：

- 建立并完善相关方的账户管理体系，如账户管理、相关方管理、权限管理、授权范围等；
- 减少非必要信息采集，采取最小权限原则和多角色授权方案；
- 根据相关方级别授予对应权限，不越权、划分明确，不同级别相关方获取对应的数据访问权限。

8.4 可扩展性原则

大宗散货仓单系统满足可拓展性的要求，宜考虑以下条件：

- 大宗散货仓单系统的建立与评价考虑到其系统内部功能的可拓展性，充分考虑系统未来的成长；
- 系统的建设宜对未来发展趋势做科学预判，系统架构组件设计具有延展性，能够满足未来新的需求与发展；
- 设计文档对系统的模块化、组件化等宜进行充分考量与规划，设计良好的代码以允许更多的功能被添加到适当的位置。

8.5 业务高可用原则

考虑到分布式账本的应用领域，高可用性是账本系统宜充分规划的特性之一，宜考虑以下条件：

- 大宗散货仓单系统时刻保持提供有效服务时间，防止服务器故障等问题导致服务不可用；
- 避免和减少运营维护操作以及突发应急的系统崩溃、受攻击所导致的停机时间；
- 具备高应对处理能力，在面对高并发流量时，能够保障其核心功能需求；
- 具有自动备份与还原能力，系统崩溃或受攻击可还原至最近备份点；
- 具有灾备处理能力，如建立同城双活中心、异地容灾数据中心等。

8.6 可追溯原则

大宗散货仓单系统系统基于区块链技术，应具备数据可追溯能力，宜考虑以下条件：

- 对全生命周期产生的资产相关的数据进行唯一性标识和存证；
- 可追溯数据考虑包括：数据生成时间、数据类型、数据来源方、数据查询方信息、授权信息、权属变更、追溯历史记录、数据更改与访问记录等；
- 系统、用户、授权信息等数据的追溯宜根据数据的敏感程度和重要性划分，根据性质的不同采取对应的追溯方案；
- 系统根据数据的敏感程度和重要性依次展示类型不同的数据量，用以满足不同的追溯需求。