ICS XX.XXX.XX
CCS X XX

T/CCLJS

江 苏 省 冷 链 学 会 团 体 标 准

T/CCLJS XXX—2026

基于区块链的果蔬供应链追溯技术规范

Technical Specification for Blockchain-based Fruit and Vegetable Supply Chain Traceability

（征求意见稿）

2026－XX－XX 发布　　2026－XX－XX 实施

江苏省冷链学会　　发 布

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专利的责任。

本文件由陕西科技大学提出。

本文件由江苏省冷链学会归口并组织实施。

本文件起草单位：陕西科技大学、北京工业大学、延安自然搭档农业发展有限公司、陕西农产品加工技术研究院。

本文件主要起草人：姚丽姗、莫海珍、胡梁斌、刘振彬、李红波、徐丹、田露、严海蓉、田锐、宋文章、方浩、王新、潘霞

基于区块链的果蔬供应链追溯技术规范

1 范围

本文件规定了基于区块链技术的果蔬供应链追溯系统的术语和定义、系统架构、追溯数据采集规范、跨链数据同步规范、隐私保护规范以及实施与安全要求。

本文件适用于苹果、猕猴桃、柑橘、葡萄等果蔬产品在异构联盟链（如 Hyperledger Fabric、FISCO BCOS）环境下的供应链追溯系统设计、开发与实施。

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。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 14881—2013 食品安全国家标准食品生产通用卫生规范
GB/T 38155—2019 重要产品追溯追溯术语
GB/T 38159—2019 重要产品追溯追溯体系通用技术要求
GB/T 35273—2020 信息安全技术个人信息安全规范
GB/T 32918.1—2016 信息安全技术SM2椭圆曲线公钥密码算法
GB/T 32918.2—2016 信息安全技术SM2椭圆曲线公钥密码算法
GB/T 32905—2016 信息安全技术SM3密码杂凑算法
Y/T 1431—2021 农产品追溯编码导则
T/CIIA 043—2023 区块链跨链交互协议

3 术语和定义

下列术语和定义适用于本文件。

3.1

追溯标识符 traceID

用于唯一标识果蔬产品从种植到销售全生命周期的编码标识，由产地编码、批次编码和校验码组成。

3.2

跨链消息包 XC-Packet

用于在异构区块链网络间传输追溯数据的标准化数据结构，包含路由信息、追溯标识、业务载荷和验证签名。

3.3

可验证声明 Verifiable Claim

基于零知识证明技术生成的声明，允许验证者在不获取原始数据的情况下验证某一陈述的真实性。

3.4

轻节点 Light Node

仅存储区块头信息而不存储完整区块数据的区块链节点，用于实现跨链状态验证。

3.5

注册表合约 Registry Contract

部署在区块链上用于管理链身份注册、验证和状态同步的智能合约。

3.6

验证者合约 IVerifier Contract
用于链上验证零知识证明有效性的智能合约接口。

4 缩略语

下列缩略语适用于本文件。

缩略语	英文全称	中文含义
ZKP	Zero-Knowledge Proof	零知识证明
SM2	ShangMi 2	国密 SM2 非对称加密算法
SM3	ShangMi 3	国密 SM3 杂凑算法
DID	Decentralized Identifier	分布式标识符
API	Application Programming Interface	应用程序接口

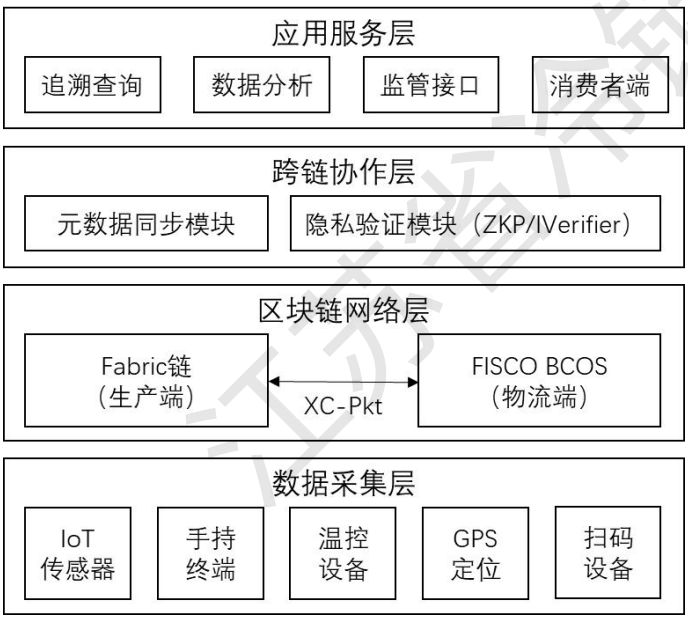
5 系统架构

5.1 总体架构

基于区块链的果蔬供应链追溯系统应采用分层架构设计，自下而上分为四层：

a. 数据采集层：通过物联网传感器、移动终端、扫码设备等采集果蔬供应链各环节的追溯数据；
b. 区块链网络层：由一个或多个联盟链组成，负责追溯数据的分布式存储和共识验证；
c. 跨链协作层：实现异构联盟链之间的元数据同步、消息路由和隐私数据验证；
d. 应用服务层：提供追溯查询、数据分析、监管接口和消费者服务等业务功能。

5.2 架构图



5.3 各层职责

5.3.1 数据采集层

数据采集层应具备以下能力：

a. 支持多种采集终端接入，包括物联网传感器、智能手持终端、二维码/RFID扫码设备；
b. 采集数据应包含时间戳、设备标识、操作人员标识；
c. 数据传输应采用加密通道，支持断网续传。

5.3.2 区块链网络层

区块链网络层应满足以下要求：
a. 采用联盟链架构，准入节点需经过身份认证；
b. 共识机制应支持每秒不少于 1000 笔交易的处理能力；
c. 数据存储应采用链上存证+链下存储的混合模式。

5.3.3 跨链协作层

跨链协作层应实现：
a. 异构链间的轻节点区块头同步；
b. 基于 traceID 的跨链消息路由；
c. 隐私数据的可验证声明生成与验证。

5.3.4 应用服务层

应用服务层应提供：
a. 面向消费者的追溯码查询接口；
b. 面向监管机构的批量数据导出接口；
c. 面向企业的追溯数据分析仪表盘。

6 追溯数据采集规范

6.1 全生命周期节点定义

果蔬供应链追溯应覆盖以下关键环节：

环节	主要采集数据	采集时限
种植	产地、品种、种植日期、施肥/用药记录	操作后 24 小时内
采收	采收日期、批次号、硬度/糖度检测值	采收后 12 小时内
预冷	预冷开始/结束时间、预冷温度	实时采集
仓储	入库时间、库位编号、温湿度记录	实时采集
运输	车辆编号、GPS 轨迹、车厢温度、振动频率	间隔≤5 分钟
销售	销售时间、销售渠道、销售批次关联	销售后 24 小时内

6.2 traceID 编码规则

traceID 应按照以下结构编码：

traceID = [产地编码(6 位)] + [生产主体编码(8 位)] + [批次日期(8 位)] + [流水号(4 位)] + [校验码(2 位)]

示例：330102-12345678-20260109-0001-A7

6.3 数据质量要求

6.3.1 温度数据精度应达到 ±0.5℃。

6.3.2 湿度数据精度应达到 ±3%RH。

6.3.3 GPS 定位精度应优于 10 米。

6.3.4 振动频率检测阈值应设置为 3G。

7 跨链数据同步规范

7.1 元数据同步机制

7.1.1 轻节点区块头格式

跨链元数据同步应采用轻节点区块头格式，包含以下字段：

字段名	数据类型	说明
chainId	string	源链唯一标识
blockHeight	uint64	区块高度
blockHash	bytes32	区块哈希值
stateRoot	bytes32	状态树根哈希
timestamp	uint64	区块时间戳
validatorSigs	bytes32	验证节点签名集

7.1.2 注册表合约

各参与链应部署注册表合约，实现：

a. 链身份的注册与注销；
b. 轻节点区块头的提交与验证；
c. 跨链消息的路由查询。

7.2 可靠通信机制

7.2.1 XC-Packet 数据结构

跨链消息包应包含以下字段：

```
{
  "version": "1.0",
  "sourceChain": "fabric-production",
  "targetChain": "fisco-logistics",
  "traceID": "330102-12345678-20260109-0001-A7",
  "messageType": "TRACE_DATA",
  "payload": { /* 业务数据 */ },
  "timestamp": 1736409600,
  "signature": "0x..."
      }
```

7.2.2 原子提交模型

跨链通信应采用”请求-响应-确认”三阶段提交模型：
请求阶段：源链发起跨链消息，锁定相关状态；
响应阶段：目标链验证消息，执行业务逻辑并返回结果；
确认阶段：源链收到响应后解锁状态或执行回滚。
消息确认超时时间应设置为不超过 30 秒。

8 隐私保护规范

8.1 隐私保护原则

数据最小化：仅采集和共享追溯功能所必需的数据；
选择性披露：数据主体可选择公开或隐藏特定属性；
可验证性：隐藏的数据仍可通过密码学方式验证其合规性。

8.2 可验证声明机制

8.2.1 声明结构

基于零知识证明的可验证声明应包含：

字段	说明
claimType	声明类型（如：农药合规、温控达标）
publicInputs	公开输入参数（如：标准阈值）
proof	ZKP 证明数据
issuerDID	声明签发者分布式标识
ssuedAt	签发时间戳

8.2.2 典型应用场景

场景	隐私需求	验证内容
农药合规性	不公开具体配方	证明用药符合安全间隔期要求
冷链质控	不公开完整温度日志	证明运输温度保持在 2℃～8℃ 范围内
质检分级	不公开库存明细	证明特级果占比不低于 60%

8.3 IVerifier 合约接口

链上验证合约应实现以下接口：

```
interface IVerifier {
    // 验证零知识证明
    function verify(
        bytes32 claimHash,
        bytes calldata publicInputs,
        bytes calldata proof
    ) external view returns (bool);

    // 查询声明验证记录
    function getVerificationRecord(bytes32 claimHash)
        external view returns (uint256 timestamp, bool result);
    }
```

验证合约应兼容国密 SM2/SM3 算法。

9 实施与安全要求

9.1 部署要求

9.1.1 硬件要求

组件	最低配置	推荐配置
区块链节点	8 核 CPU/16GB 内存/500GB SSD	16 核 CPU/32GB 内存/1TB SSD
跨链网关	4 核 CPU/8GB 内存/100GB SSD	8 核 CPU/16GB 内存/200GB SSD
应用服务器	4 核 CPU/8GB 内存/200GB SSD	8 核 CPU/16GB 内存/500GB SSD

9.1.2 网络要求

区块链节点间网络带宽应不低于100Mbps；
跨链网关应部署在独立网络区域，与各链节点保持低延迟连接；
应用层与区块链层之间应设置防火墙隔离。

9.2 性能要求

单链追溯数据写入TPS应不低于500；
跨链消息确认延迟应不超过10秒；
追溯查询响应时间应不超过2秒；
系统可用性应达到99.9%。

9.3 安全审计

智能合约上线前应通过第三方安全审计；
系统应每季度进行一次安全渗透测试；
跨链密钥应采用硬件安全模块（HSM）存储；
操作日志应保留不少于3年。

附录 A（资料性） 智能合约接口示例

A.1 追溯数据上链接口

```
interface ITraceRegistry {
    // 记录追溯数据
    function recordTrace(
        string calldata traceID,
        string calldata stage,                    // 环节：PLANT/HARVEST/STORAGE/TRANSPORT/SALE
        bytes calldata dataHash,      // 数据哈希
        uint256 timestamp
    ) external returns (bool);

    // 查询追溯记录
    function queryTrace(string calldata traceID)
        external view returns (TraceRecord[] memory);
}
```

A.2 跨链消息发送接口

```
interface ICrossChainGateway {
    // 发送跨链消息
    function sendPacket(
        string calldata targetChain,
        string calldata traceID,
        bytes calldata payload
    ) external returns (bytes32 packetId);

    // 确认跨链消息
    function confirmPacket(bytes32 packetId) external;
}
```

参考文献

[1]. 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

[2]. 农业农村部. 农产品质量安全追溯管理办法