ICS 65.020.01
CCS B 07

DB22

吉 林 省 地 方 标 准

DB22/T 3033.3—2023

畜禽产品质量安全追溯 第3部分：区块链技术应用规程

Traceability of quality and safety of livestock and poultry products
The three part Blockchain technical regulations

地方标准信息服务平台

2023-09-28 发布　　2023-11-16 实施

吉林省市场监督管理厅　　发 布

地方标准信息服务平台

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。

本文件是 DB22/T 3033《畜禽产品质量安全追溯》的第3部分。DB22/T 3033 已经发布了以下部分：

——第 1 部分：信息编码技术规程；

——第 2 部分：操作技术规程；

——第 3 部分：区块链技术应用规程；

——第 4 部分：技术服务规范。

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。

本文件由吉林省畜牧业管理局提出并归口。

本文件起草单位：吉林省畜产品安全协会、吉林省森祥科技有限公司、吉林省牧业信息中心、吉林省动物疫病预防控制中心、吉林省畜禽定点屠宰管理办公室。

本文件主要起草人：赵安妮、柳林、王春发、柴方红、潘荣辉、贺亮、冯凯、程晓辉、宋岩、杨静、田忠华。

地方标准信息服务平台

地方标准信息服务平台

畜禽产品质量安全追溯 第3部分：区块链技术应用规程

1 范围

本文件确立了畜禽产品质量安全区块链技术应用程序，规定了身份注册与验证、创建声明、获取声明、生成溯源数据、溯源查询等阶段的操作指示，以及上述阶段之间的转换条件。

本文件适用于区块链技术在畜禽产品质量安全追溯管理中的应用。

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 38155 重要产品追溯 追溯术语

DB22/T 3033.1 畜禽产品质量安全追溯 第 1 部分：信息编码技术规程

DB22/T 3033.2 畜禽产品质量安全追溯 第 2 部分：操作技术规程

3 术语和定义

GB/T 38155 界定的以及下列术语和定义适用于本文件。

3.1

区块链 block chain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

[来源：GB/T 37043—2018，2.5.8]

3.2

联盟链 consortium block chain

由一组利益相关的参与者使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的一类区块链部署模型。

3.3

智能合约 smart contract

一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

[来源：JR/T 0184—2020，3.20]

3.4

非对称加密 asymmetric cryptography

非对称加密算法是一种密钥的保密方法。非对称加密算法需要两个密钥：公开密钥（public key：简称公钥）和私有密钥（private key：简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密。

地方标准信息服务平台

3.5

畜禽产品质量安全追溯区块链平台 traceability of quality and safety of livestock and poultry products block chain platform

采用联盟链模型构建的网络信息服务平台（以下简称“平台”），具备可信追溯数据上传和存储功能，提供畜禽产品追溯数据信息发布和共享机制，为畜禽产品提供来源可溯、去向可查、真实可信的追溯数据信息。

3.6

分布式数字身份标识符 distributed digital identity identifier, DID

是一种去中心化、可验证、唯一的标识符，由字符串组成，用来代表一个数字身份。

3.7

声明 declaration

标识 DID 某些属性的数据文件。

3.8

参与方 participant

完成身份注册的养殖、收购、屠宰、流通、消费、监管等环节的参与者，拥有 DID 和声明。

3.9

业务对象 business object

畜产品质量安全追溯过程中由参与方创建的业务实体（如畜禽活体、畜禽产品、票据等）， 拥有 DID 和声明。

4 程序确立

区块链技术应用程序包括 5 个阶段。业务流程如图 1 所示。

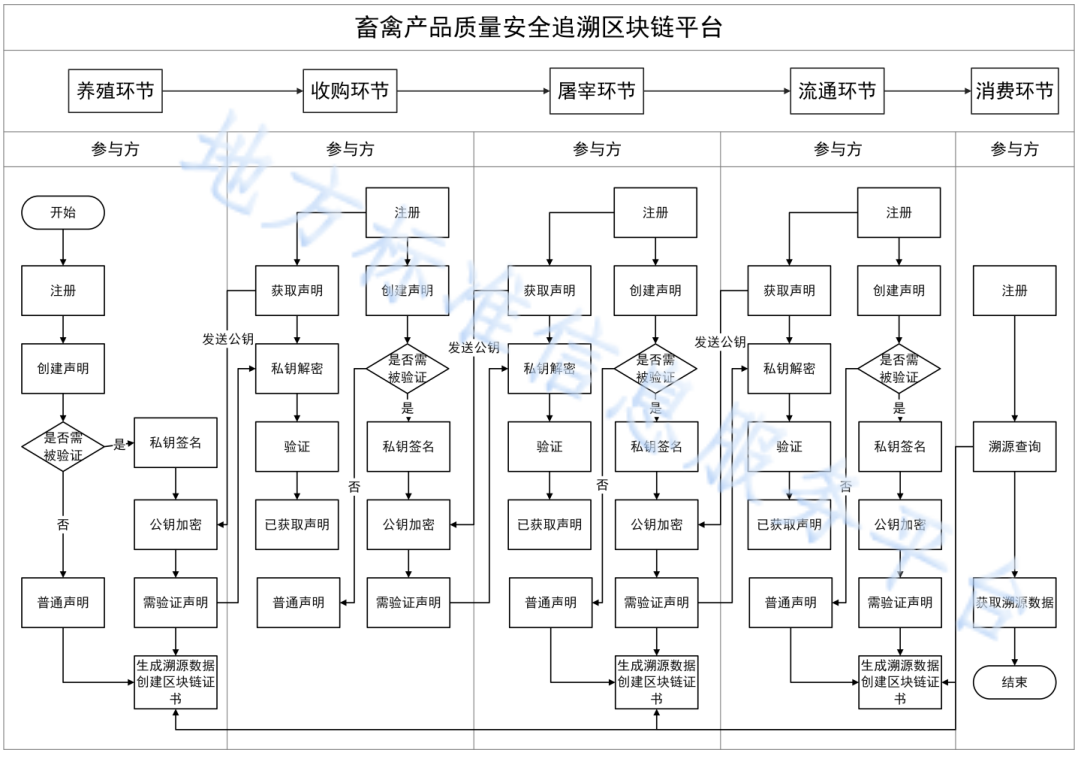


图1　区块链技术应用流程图

5 身份注册与验证

5.1 养殖、收购、屠宰、流通、消费等环节参与方通过平台进行 DID 注册：

a) 自然人参与方使用有效身份证件进行实名注册；

b) 机构参与方使用统一社会信用代码及法人有效身份证件进行实名注册。

5.2 平台基于非对称加密技术为实名注册的参与方 DID 创建私钥和公钥。

5.3 平台监管参与方为 5.1 中需要验证的参与方 DID 颁发可信的声明，广播到区块链网络中。

5.4 参与方在创建声明、获取声明前应完成身份注册。

6 创建声明

6.1 参与方为业务对象创建声明，声明需被验证时，用私钥对声明进行签名。

6.2 声明需要发送给指定参与方，使用该指定参与方公钥对声明内容加密，声明内容包括并不限于：

a) 声明 ID；

b) 声明主体（业务对象 DID）；

c) 声明内容（举例：“产地信息”）；

d) 声明类型（举例：“养殖过程”）；

e) 签名者 DID（参与方 DID）；

f) 签名者公钥（参与方公钥）；

g) 签名时间；

h) 声明过期时间（举例：“never”）；

i) 签名（参与方的签名）；

j) 签名算法（参与方签名所使用的算法）；

k) 意见（举例：“support”“revoke”）；

l) 加密算法（声明内容使用的加密算法）；

m) 摘要（声明内容的摘要）；

n) 摘要算法（参与方摘要所使用的算法）。

6.3 参与方为业务对象创建声明后，业务对象持有该声明。

6.4 创建声明的参与方可通过将声明意见值改为“revoke”的方式来撤销已创建声明。

6.5 应按照 DB22/T 3033.1 规定创建声明内容编码。

6.6 应按照 DB22/T 3033.2 规定创建声明内容。

7 获取声明

7.1 参与方在获取并使用其他参与方创建的声明前，先验证该声明，声明内容包括：

a) 是否在区块链上；

b) 是否过期；

c) 是否已被撤销；

d) 验证签名确认声明创建者身份未被篡改；

e) 验证摘要确认声明内容未被篡改。

7.2 若该声明内容加密，参与方通过己方私钥对该声明解密。

8 生成溯源数据

吉林省社会信用信息服务平台

8.1 平台通过智能合约为满足追溯条件的业务对象生成溯源数据，并创建区块链证书，证书内容包括并不限于：

a) 证书所载区块信息；
b) 时间信息；
c) 畜禽产品 DID；
d) 畜禽产品认证信息。

8.2 平台按照 DB22/T 3033.1 要求为业务对象 DID 创建溯源二维码，完成溯源二维码和业务对象 DID、区块链证书关联。

8.3 若溯源数据中包含已撤销声明，应在数据源数据中标识该声明为撤销状态。

8.4 不应在畜禽产品追溯信息中公开各环节参与方未允许公开的声明。

9 溯源查询

可通过业务对象 DID 查询或扫描追溯二维码获得畜禽产品追溯数据、区块链证书等信息。

地方标准信息服务平台

参 考 文 献

[1] GB/T 37043—2018 智慧城市 术语

地方标准信息服务平台