doi:10.6041/j.issn.1000-1298.2022.08.039

基于智能合约的果蔬区块链溯源数据存储方法研究

孙传恒[1]　于华竟[1]　罗　娜[2,3]　徐大明[2,3]　邢　斌[2,3]　杨信廷[2,3]

(1. 上海海洋大学信息学院, 上海 201306; 2. 国家农业信息化工程技术研究中心, 北京 100097;
3. 农产品质量安全追溯技术及应用国家工程实验室, 北京 100097)

摘要: 随着区块链农产品溯源技术的发展,果蔬产品质量安全得到保障。由于我国果蔬产品溯源跨度大、追溯周期长、涉及面广,并且区块链网络数据账本由全网节点共同记账备份,海量溯源数据存储压力大,同时所有数据透明共享,造成供应链溯源数据无法全部上链,引起产品数据上下游溯源企业共享不及时、追溯数据安全性难以得到保障、监管部门无法实时监管全部溯源数据,出现农产品质量安全问题时,责任无法定位、产品难以找到问题源头。基于上述问题,设计基于区块链多链架构的果蔬产品溯源框架,设计溯源数据存储模型,并通过智能合约实现溯源数据分类链上加密存储、链间授权访问、基于授权凭证解密查询,保证果蔬全供应链溯源隐私数据密文上链,减缓区块链存储压力、实现上下游溯源企业隐私数据无孤岛授权共享。基于联盟链 Hyperledger Fabric 通道技术实现多链溯源系统,经过扩散性测试,由对称加密与椭圆曲线混合加密的"链上加密存证、链间基于授权凭证共享、链上解密查询"智能合约方案,隐私数据密文变化率达 95% 以上,密钥密文变化率达 94% 以上,具备较高的安全性和混淆性;经过性能测试,所设计并实现的多链架构溯源系统公开溯源数据查询平均时延为 56.9 ms,基于授权凭证的隐私溯源数据平均解密查询时延为 62.87 ms,处理企业节点发起数据上链请求的平均时延为 2.16s,能够满足果蔬产品追溯实际的应用需求。

关键词: 果蔬产品; 溯源; 区块链; 多链; 智能合约; 数据存储

中图分类号: TP309.2; TS201.6　**文献标识码**: A　**文章编号**: 1000-1298(2022)08-0361-10　**OSID**:

Blockchain Traceability Data Storage Method of Fruit and Vegetable Foods Supply Chain Based on Smart Contract

SUN Chuanheng[1]　YU Huajing[1]　LUO Na[2,3]　XU Daming[2,3]　XING Bin[2,3]　YANG Xinting[2,3]

(1. *College of Information Technology*, *Shanghai Ocean University*, *Shanghai* 201306, *China*
2. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
3. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*)

Abstract: With the development of blockchain agricultural foods traceability technology, the quality and safety of fruits and vegetables are guaranteed. As the traceability of fruits and vegetables in China has a large span, long traceability cycle and wide coverage, and the blockchain network data ledger is backed up by the joint network nodes, the storage of massive traceability data is under great pressure, while all traceability data are transparently shared, resulting in the data not being able to be all upstream and downstream traceability enterprises to share in a real time, the safety of data is difficult to be effectively guaranteed, and the regulatory departments cannot regular traceability data efficiently. When there is a problem of agricultural foods quality and safety, the responsibility cannot be located and the source of the problem can hardly be found. Based on the above problems, a traceability framework for fruits and vegetables was designed based on blockchain multi-chain architecture, a data storage model was designed, and encrypted storage on the chain of traceability data classification, authorized access between chains and decrypted query based on authorized credentials were realized through smart contracts to ensure the privacy of whole traceability supply chain. Data encryption on the chain can reduce the

收稿日期: 2021-08-23　修回日期: 2021-09-08

基金项目: 国家自然科学基金面上项目(31871525)和广东省重点研发计划项目(202103000033)

作者简介: 孙传恒(1978—),男,研究员,博士,主要从事农产品追溯技术研究,E-mail: sunch@nercita.org.cn

通信作者: 杨信廷(1974—),男,研究员,博士,主要从事农产品智慧供应链研究,E-mail: yangxt@nercita.org.cn

pressure of storage and realize the sharing of privacy data of upstream and downstream traceability enterprises without silo authorization. Based on the Hyperledger Fabric channel technology of consortium chain, the multi-chain traceability system was realized. After proliferation test, the smart contract scheme of on-chain encryption and evidence storage, inter-chain sharing based on authorized credentials and on-chain decryption query, which was composed of symmetric encryption and elliptic curve hybrid encryption, had a private trace-data cipher text change rate of more than 95% and a key cipher text change rate of more than 94%, which possesses high security and confusion. After performance testing, the average time delay of public traceability data query was 56.9 ms, the average time delay of privacy traceability data decryption query was 62.87 ms, and the average time delay of processing data upload was 2.16 s, which can meet the actual application requirements of fruits and vegetables traceability system. The research result can provide a feasible reference solution for the classification and storage of traceability data of fruits and vegetables in China.

Key words: fruits and vegetables foods; traceability; blockchain; multi-chain; smart contract; data storage

0 引言

传统果蔬产品追溯通过企业中心化数据库存储溯源信息,在海量数据基础上数据易被篡改、企业间流通困难、监管即时性差、遍历查询效率低[1]。区块链集成点对点分布式网络、默克尔树数据结构、加密链式区块、智能合约自动化触发机制[2-3],保证追溯数据一经共识验证上链完成就无法篡改,适用于保障果蔬产品溯源过程追溯数据的安全可靠[4]。

我国果蔬农产品全产业链追溯链条长、周期长、数据海量异构[5-6],区块链基于链式区块存储追溯数据,通过全网节点共识备份数据账本,造成区块链网络数据存储压力大[7]。在缓解链上存储压力方面,部分学者提出通过链上链下数据协同验证减缓区块链存储压力,文献[8]设计基于区块链的稻米供应链溯源监管模型,溯源数据通过链下 MySQL 中心数据库存储,链上存储溯源数据密文,稻米追溯数据链上链下协同扩容并保证数据的真实性。文献[9]综合分析区块链技术在稻米溯源中的应用场景,提出将溯源数据分类存证,公开溯源数据直接上链存储,隐私数据存储在企业链下数据库,由哈希算法计算信息摘要上链,链上链下协同保证数据安全、未经篡改。文献[10]深入考虑区块链技术与农产品的综合应用,提出一种数据链下存证、链上验证的存储模型,减轻区块链溯源网络的存储压力,保证数据的安全可靠。但是,链上链下协同架构通过存储信息摘要的方式验证数据真实性,无法保证链下数据的安全,在链下数据被篡改时仅能发现篡改,无法恢复原始溯源数据。部分学者通过多链架构扩充区块链溯源总体容量,文献[11]在水产品方面应用区块链多链溯源系统,使用从链存储企业追溯数据,将部分可公开数据上传至主链用于溯源,通过主从多链的架构缓解溯源数据存储压力。文献[12]设计并实现的基于区块链多链架构的农产品溯源系统,通过链下中心化数据库与链上多链协同缓解存储压力。以上研究深入分析多链架构在农产品溯源方面价值,并未进一步考虑链上数据的高效共享。我国果蔬产品全供应链追溯每个环节涉及多企业,溯源数据海量异构,因此,研究在多链架构扩充总体容量的基础上减少单条数据存储压力,研究链上数据的分类存储和隐私数据的无孤岛共享具备重要的意义。

通过分析果蔬产品溯源流程,本文设计基于区块链智能合约的溯源数据存储机制,为每个追溯环节设计一条溯源链,每个环节中一或多个溯源企业作为节点,通过区块链多链架构溯源,扩展区块链溯源总体容量,解决果蔬农产品跨地域、跨时空的溯源数据存储的真实可信,缓解区块链网络海量数据的存储压力。通过编写智能合约,由全网节点背书安装实例化完成后共同维护合约逻辑,实现数据上链时的自动分类以及隐私溯源数据的混合加密上链,通过密钥授权凭证实现链间数据共享与监管部门的穿透式全溯源数据监管。

本文设计并实现的果蔬产品全供应链溯源系统,分析每个环节采集的溯源数据,并划分为公开与隐私数据;通过智能合约实现对称加密与椭圆曲线混合加密隐私数据密文上链,并通过密钥授权实现链上密文解密共享;果蔬区块链多链溯源系统存储公开溯源明文数据与隐私数据密文数据,缓解单条溯源数据的存储压力;并通过果蔬应用案例进行分析验证。

1 关键技术

区块链是在对等网络环境下,通过透明和可信规则,构造不可篡改、不可伪造、数据正向记录、逆向溯源的链式存储结构,以密码学的技术保证以及实

现链上数据的真实可信，通过分布式网络保证数据的安全备份[13-14]。根据网络的准入机制，区块链可划分为：公有链、私有链、联盟链[15]。公有链所有人均可参与，交易数据全部节点公开；私有链为个人或组织参与，交易数据私密存储；联盟链由全网节点审计准入参与，链上通过智能合约自动化执行联盟成员制定的合约逻辑，通过节点授权实现网络账本的读写[16]。本文实现的果蔬产品溯源系统基于联盟链 Hyperledger Fabric，由通道技术建立多链追溯架构，保证溯源数据隔离存储；由链上证书管理机构审计节点身份、节点交易授权；通过 Kafka 共识机制[17]实现多链间数据共识备份；通过链外状态数据库 CouchDB 存储链上溯源记录。

智能合约是一段运行在区块链上的代码，在触发条件满足时可自动执行的合约逻辑，以信息化的方式传播、验证节点行为。智能合约大幅减少人工参与程度，保证了区块链的去中心化、数据的防篡改[18-19]。本文设计对称加密算法（Advanced encryption standard，AES）与椭圆曲线加密算法（Elliptic curve cryptography，ECC）混合加密智能合约，实现隐私溯源数据加密上链、基于密钥授权解密查询共享。

AES 采用单密钥的方式加密、解密，计算量小且加密效率高[20]，在果蔬全供应链溯源中用于加密企业隐私溯源数据，实现密文上链。ECC 通过离散对数问题保证逆向计算的难度[21]，并通过离散点的运算实现加密，使用 ECC 公钥加密 AES 密钥，生成密文上链。通过下发 ECC 私钥授权凭证的方式实现链上解密查询。椭圆曲线 $F_p(a,b)$ 为

$$y^2 = x^3 + ax + b(\mathrm{mod}\ p)\quad (4a^3 + 27b^2 \neq 0)$$

式中　a、b——椭圆曲线参数　　p——质数

mod——取模运算函数

椭圆曲线加密、解密的算法如下：

（1）用户 M 选定一条椭圆曲线 $F_p(a,b)$，并选取椭圆曲线上一点，作为基点 G，其中 n 为椭圆曲线的阶，即 $nG = \infty$。

（2）用户 M 选择一个随机数作为私有密钥 k，并根据离散点计算原则生成公钥 $K = kG$。

（3）用户 M 将椭圆 $F_p(a,b)$ 和点 G、K 传给用户 N。

（4）用户 N 接到信息后，将待传输的明文编码到 $F_p(a,b)$ 上的一点 A，并产生一个随机整数 r（$r < n$）。

（5）用户 N 通过椭圆曲线公钥 K 加密（密文 C 是一个点对）：$C_1 = A + rK$，$C_2 = rG$。

（6）用户 M 接收到密文 C 后，通过私钥 k 解密 $C_1 - kC_2$，计算 $A + rK - k(rG) = A$，对点 A 解码就可以得到明文。

2　基于智能合约的果蔬区块链溯源数据存储

2.1　果蔬产品多链溯源模型

本文基于联盟链通道技术构建区块链多链架构，实现数据隔离。面向果蔬生产、收购、仓储、加工、分销 5 个供应链环节，为每个环节建立一条溯源链，如图 1 所示。每个环节内的一或多个追溯企业作为节点发起溯源数据上链请求，不同的企业处于不同的溯源通道中，以通道的天然隔离性实现溯源数据的隔离存储。

从数据链内传递、链间传递、多链优势方面分析果蔬区块链溯源多链架构。溯源链内的同类多家企业节点共同备份溯源链数据账本，包括可公开溯源数据与隐私溯源数据密文，通过智能合约与操作更新链上数据。链内公开溯源数据通过智能合约直接调用传递，隐私溯源数据密文在获取

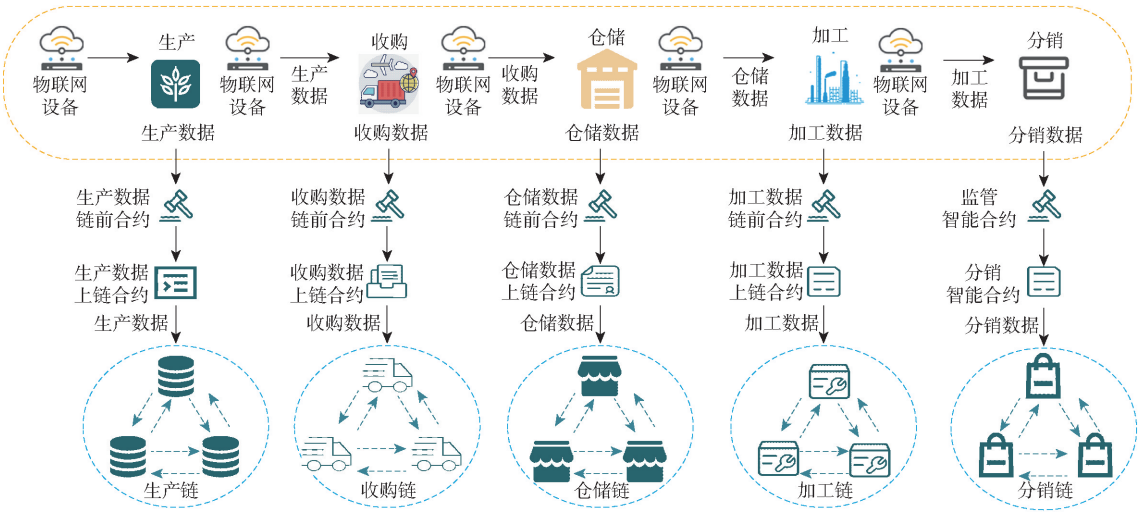


图 1　果蔬产品区块链溯源多链架构

Fig. 1　Blockchain multi-chain architecture for traceability of fruits and vegetables

数据所属企业密钥授权后,通过链上智能合约解密共享。溯源链间通过通道的天然隔离性保证数据独立存储,因此无法通过合约直接调用传递,本文为每条链封装账本操作接口,通过接口授权的方式限时提供链间数据传递。多链优势集中体现在应用业务和时间维度上,从应用业务上看,生产、收购、仓储、加工至分销等每个环节涉及多企业,供应链上下游数据流转在多类多个企业间无顺序关系,因此设计面向溯源环节建立区块链维护追溯数据;从时间长维度看,面向企业多年追溯数据存储,通过企业多链架构由同一类型企业维护一至多年追溯数据。综上所述,面向每个环节存在多企业、每个企业存在长时间维度追溯,本文建立果蔬产品多链追溯架构,每个环节独立维护溯源链,以多链的形式扩增追溯系统数据容量、独立存储溯源数据,提供追溯链间数据授权共享机制,降低商业隐私数据泄露风险。

2.2 溯源数据存储模型

果蔬产品溯源涉及多环节,每个追溯环节通过温湿度传感器、光敏传感器、北斗定位设备、氧气浓度传感器、摄像头、照相机等物联网设备实时采集产品生产、加工等数据。其中,并非所有数据可用于公开溯源,涉及商品成定价、存量等与质量无关的商业隐私数据,需在保证安全可靠的前提下通过区块链实现数据的防篡改,并进一步实现隐私数据的上下游授权访问以及监管部门的可管控。本文深入分析果蔬产品全供应链每环节的溯源数据,划分为可公开溯源数据与隐私商业数据,如表 1 所示。

表 1 果蔬产品溯源关键数据

Tab. 1 Traceability key information of fruits and vegetables

供应链环节	公开溯源数据	隐私溯源数据
生产	商品名称、生产周期、施肥记录、施药记录、负责人、采收时间、土壤情况、商品化验报告(黄曲霉素、农药残留、产品质量等)	种子价格、农药价格、肥料价格、采收成本、管理成本、单位面积收获数量、农场出货价格
收购	收购公司、收购批次、收购数量/批、收购时间、收购车次、车辆类型(是否冷藏)	收购成本、运输成本、出货价格
加工	加工企业、加工批次、加工数量、负责人员、加工过程检疫报告(生产卫生环境是否合格)、加工时间、加工配料	进厂价格、出厂价格、加工成本、加工数量
仓储	仓储企业、冷藏环境、温湿度、氧气浓度、二氧化碳浓度、仓储时间、仓储数量	进仓价格、出仓价格、存储成本
分销	销售企业、进货时间、进货数量	进货价格、销售价格、进货数量

企业节点以 Key-value 键值对的形式提交溯源数据,通过创建数据库键值索引代替遍历查询,减少数据查询时间开销。数据上链交易请求由企业节点构造交易背书提案,经过 Kafka 集群共识排序,生成新的区块,返回当前上链请求的交易哈希值与区块高度,详细信息如表 2 所示。

表 2 上链数据

Tab. 2 Key-value traceability data of blockchain

公开溯源数据	隐私溯源数据	交易哈希	区块高度
冷藏:false|产品批次:3703021220025716|产品名称:SXZZ 玫瑰香葡萄(散)|产品 Id:5519222E-7DB8-4AE3-8590-89781DAC32BE|上链节点 Id:370302122|节点名称:peer0.org1.example.com|销售市场:鲁中水果批发市场|进货时间:2021-08-13 00:00:00	进货价格:2.78 元/(500 g)|销售价格:4.5 元/(500 g)|进货数量:200 kg|负责人:张三	59995175a1be3c5320289 71b5fdcecc0dcd57acb569 b1f8ed823b497c556c5f4	678

本文分析供应链各环节关键数据,设计基于区块链的果蔬溯源数据存储模型,如图 2 所示。按照数据采集顺序,溯源系统正向记录从生产、收购、仓储、加工到分销等环节的数据。相应供应链节点提交数据上链请求时,通过智能合约将数据划分为公开溯源数据与商用隐私数据。其中,公开溯源数据直接上链存证;隐私溯源数据通过节点提交的对称加密算法 AES 密钥加密后,密文上链,保证隐私数据的安全不可见。智能合约自动化为当前节点生成椭圆曲线 ECC 密钥对,通过节点 ECC 公钥加密 AES 密钥,将密文上链。链上状态数据库 CouchDB 存储公开溯源数据、隐私溯源数据密文、对称加密 AES 密钥密文 3 类数据,上链请求经过 Kafka 共识达成上链交易后,返回当前节点的 ECC 私钥。在果蔬溯源过程产生的视频、图像以及音频等溯源数据,通过分布式数据库星际文件系统(Interplanetary file system,IPFS)存储,将返回的哈希值跟随公开溯源数据上传区块链网络。

面向消费者逆向溯源,通过智能合约直接查询链上数据账本获取公开溯源数据。链上隐私溯

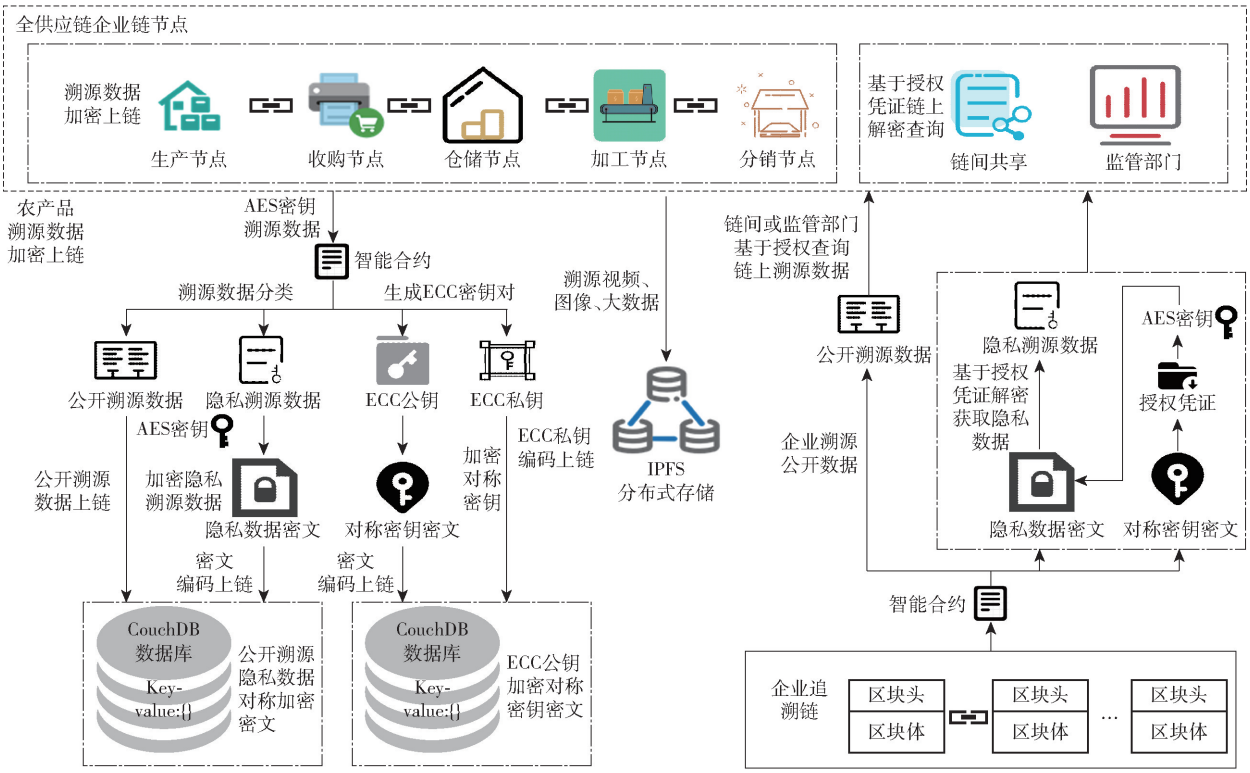


图 2　果蔬产品溯源存储模型

Fig. 2　Traceability data storage model of fruits and vegetables

源数据的安全性通过对称加密 AES 密钥和椭圆曲线 ECC 密钥保证，溯源上下游企业或监管部门获取隐私数据，需要向数据提交节点发起授权申请，获取节点下发的 ECC 私钥授权凭证后，通过智能合约获取链上隐私溯源数据密文、AES 密钥密文，通过溯源凭证 ECC 私钥解密 AES 密钥，基于 AES 密钥解密溯源隐私数据密文获取隐私数据明文，实现链上密文基于授权解密共享以及监管部门的全方面管控。

2.3　智能合约设计

针对果蔬隐私数据加密上链，设计数据加密上链智能合约、数据链上解密查询智能合约，通过追溯节点发起数据上链交易时自动触发智能合约业务逻辑，实现数据加密的自动执行，保证全产业链追溯环节每个追溯企业追溯数据的安全可靠、可溯、可信。企业节点提交溯源数据上链请求，通过节点 AES 密钥和智能合约自动化生成的 ECC 密钥对混合加密溯源隐私数据，如图 3 所示。

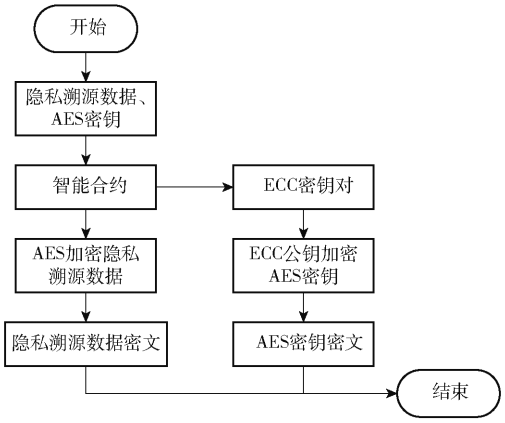


图 3　隐私溯源数据加密上链

Fig. 3　Private traceability data ciphertext written to blockchain

针对公开溯源数据消费者溯源需求、隐私溯源数据监管管控需求和上下游企业共享需求，本文设计数据加密智能合约、获取公开数据合约、通过授权凭证解密查询隐私溯源数据合约，具体的合约业务逻辑如表 3 所示。

表 3　合约业务逻辑设计

Tab. 3　Design of smart contract function

合约功能	合约业务逻辑	合约方法	描述
数据上链	公开溯源数据上链 隐私溯源数据加密上链	traceTrans( )	上链数据包括数据键值、公开溯源数据、隐私数据密文、对称密钥密文
数据查询	公开溯源数据查询	getPubdata(id)	通过产品溯源码查询产品公开溯源数据
	隐私溯源数据查询	getPubdata(id,key)	通过产品溯源码和授权凭证查询隐私溯源数据

本文通过智能合约实现溯源数据的加密上链、链间基于授权访问隐私数据、链上共享公开溯源数据,数据加密上链算法如下。

算法 1:隐私溯源数据加密上链智能合约算法

输入:企业发起交易节点 peer,合约名称 cc,通道名称 channel,公开溯源数据 pubData,隐私溯源数据 priData,AES 密钥 key

输出:隐私溯源数据密文、AES 密钥密文、ECC 私钥编码

```
1. //处于 channel 内的节点 peer 发起合约 cc 的 invoke 上链请求
2. if(! isnull(key))  //判断交易请求的 AES 密钥是否为空
3.   if(! getState(info. id)) //区块账本是否已经存在当前键值数据
4.     //使用 AES 密钥加密农产品溯源隐私数据
5.     EncryTraceData : = encryptAES(priData, key)
6.     //智能合约自动化生成上链节点 ECC 密钥对
7.     prk, err : = getKey()
     //溯源节点 ECC 私钥
8.     publicKey : = &prk. PublicKey
   //溯源节点 ECC 公钥
9.     //通过溯源节点 ECC 公钥加密 AES 密钥
10.    EccEncryAes : = ECCEncrypt(key, publicKey)
11.    //封装上链数据结构体
12.    traceObj : = &traceObj{id, pubData, EncryTraceData, EccEncryAes, eneccpubCode}
13.    //执行上链操作
14.    err = stub. PutState(id, marbleJSONasBytes)
15.    if(err ! = nil)
16.      return Error
17.  return dataExistsError;
18. return keyError;
```

通过溯源数据加密上链智能合约,区块账本经过共识备份公开溯源数据与隐私数据密文,执行成功后,链上返回当前请求数据上链交易哈希值、区块高度、数据哈希值等。

面向消费者、监管机构等提供公开数据透明访问、隐私数据授权查询,数据查询算法如下。

算法 2:公开与隐私溯源数据查询算法

输入:企业节点 peer,合约名称 cc,通道名称 channel,溯源数据溯源码 code,授权凭证 key

输出:公开溯源返回公开溯源数据、授权查询返回隐私溯源数据

```
1. //处于 channel 内的节点 peer 发起合约 cc 的 query 请求
2. //判断 query 方法//getPridata 方法
3. if(function = = getPubdata)
4.   if(! getState(code))  //判断溯源码有效性
5.     //查询全部数据
6.     traceinfo, err : = stub. GetState(code)
7.     //返回当前键值的公开溯源数据
8.     pubTracedata : = string(traceinfo. pubData)
9.     return pubData
10.  return codeError
11. else  // getPridata 方法
12.   if(! getState(id) && isnull(key))  //判断溯源码是否有效以及授权文件是否为空
13.     //获取隐私溯源数据密文
14.     priTraceEncrydata : = string(traceinfo. EncryTraceData)
15.     //获取 AES 密文
16.     aesEncry : = string(traceinfo. EccEncryAes)
17.     //通过授权凭证解密 AES 密文
18.     Aeskey, err : = ECCDecrypt(aesEncry, key)
19.     //通过 AES 密钥解密隐私溯源数据密文
20.     priTracedata : = decryptAES(priTraceEncrydata, Aeskey)
21.     return priData
22.  return dataError;
```

其中,第 1 ~ 10 行表示通过溯源码查询链上公开溯源数据,第 11 ~ 22 行表示通过授权凭证解密查询链上隐私溯源数据。

3 试验

3.1 测试环境

通过 Ubuntu 14.04.4 Linux 系统,基于 Hyperledger Fabric v1.4.4 建立果蔬多链溯源网络,存储容量 50 GB,运行内存 16 GB,试验数据来自于山东省淄博市鲁中水果批发市场溯源平台。区块链采用 Kafka 共识,所有节点均部署外部状态数据库 CouchDB,通过键值查询代替遍历查询,提升数据查询效率,具体配置如表 4 所示。

3.2 安全性测试

本文设计的果蔬全供应链溯源数据存储模型,采用对称加密 AES 与椭圆曲线加密算法 ECC 混合加密,保证隐私溯源数据安全、AES 密钥安全,通过离散对数求解保证授权凭证的安全,在隐私数据上链环节产生的密文如表 5 所示。

表 4　区块链配置

Tab. 4　Configuration of blockchain

设置	值	描述
共识机制	Kafka	Kafka 集群处理高并发的数据上链请求
Kafka 集群	kafka0、kafka1、kafka2、kafka3	接受节点请求，达成共识
排序节点集群	order0、order1、order2	链接 Kafka 集群与主节点，进行交易排序
Zookeeper 集群	zookeeper0、zookeeper1、zookeeper2	分布式协调服务，为 Kafka 集群提供一致性服务
通道数	6	主链提供 Kafka 共识，产购储加销 5 环节 5 条溯源链
节点数	10	每条链两个节点，保证数据完整性
数据库	CouchDB	通过链外状态数据库提供富查询
区块生成时间	1s	链上区块生成时间间隔
区块容量	20MB	每个区块容纳的最大容量
区块交易数	100	每个区块接受的最大交易数

表 5　隐私溯源数据上链密文

Tab. 5　Private traceability data ciphertext

数据	值
AES 密钥	qhgjisekoritdkcm
隐私溯源数据	进货价格:2.78 元/(500 g)|销售价格:4.5 元/(500 g)|进货数量:200 kg|负责人:张三
溯源数据密文	bksrZgPzLWESMnzBrst/ZZgxbxO/mAYQ1dhNtA7Yo/RnzpWZovYOW8/LHGwXpKin4SVuR+/u/bcPR/joB18WpLehWls8i4wesPxSioEJNTCDp5AtLDa3avKczWQQ09CK
ECC 密钥对	-----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEsouIgxUMSJC0OgFc+c6INvoHukFq en9gpHAHKpeShM09uihQl27nNPgqzWPIyF8peRcqABmk3xe1BS7ffQArNQ== -----END PUBLIC KEY----- -----BEGIN PRIVATE KEY----- MHcCAQEEIFPz9E8S2+FJODN+2zv5LaBNRZjT9K4iiDviipAqEMzgoAoGCCqGSM49 AwEHoUQDQgAEsouIgxUMSJC0OgFc+c6INvoHukFqen9gpHAHKpeShM09uihQl27n NPgqzWPIyF8peRcqABmk3xe1BS7ffQArNQ== -----END PRIVATE KEY-----
AES 密文	BJZFeedfGXAPiZWRdpyXgOXoJx5v5fXPITIpIJoJcIuJ5r2Rz8Sv9UmhsC8Q/u5o6JVsL0h7t4LGD4g7V5WBv06jFsBXL7Q3Pc5 YfKBrUOwpFbRXUPa6+yuL06ELOgajewGZ5gQ4V0kkHYwpxc9ERnw++MJ6V3yRQYdNKDoBD7Br
授权凭证	LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1IY0NBUUVFSUZQejlFOFMyK0ZKT0ROKzJ6djVMYUJOUlpqVDlLNGlpRHZ paXBBcUVNemdvQW9HQ0NxR1NNNDkKQXdFSG9VUURRZ0FFc291SWd4VU1TSkMwT2dGYytjNklOdm9IdWtGcWVuOWdw SEFIS3BlU2hNMDl1aWhRbDI3bgpOUGdxeldQSXlGOHBlUmNxQUJtazN4ZTFCUzdmZlFBck5RPT0KLS0tLS1FTkQgUFJJVkFU RSBLRVktLS0tLQo=

经扩散性测试，隐私溯源数据保持不变，改变 AES 密钥任意一位，引起的隐私溯源数据密文变化如图 4a 所示，密钥改变引起的隐私溯源数据密文平均变化率达到 95% 以上，经过 ECC 公钥加密 AES 密钥的密文变化如图 4b 所示，AES 密钥密文的平均变化率达到 94% 以上，具备较高的密文安全性与混淆性。

3.3　上链与查询性能分析

本文为合约封装上链外部接口，通过接口实现脚本文件高并发调用。在数据上链脚本文件中，指定发起数据上链交易的节点为 peer0.org1.example.com，封装组织 1 的上链授权证书，实现节点的身份认证，通过接口每轮次测试 60 次，数据上链平均时延如图 5a 所示。在数据查询接口中，通过接口每轮次测试60次，公开溯源数据、隐私溯源数据解密查

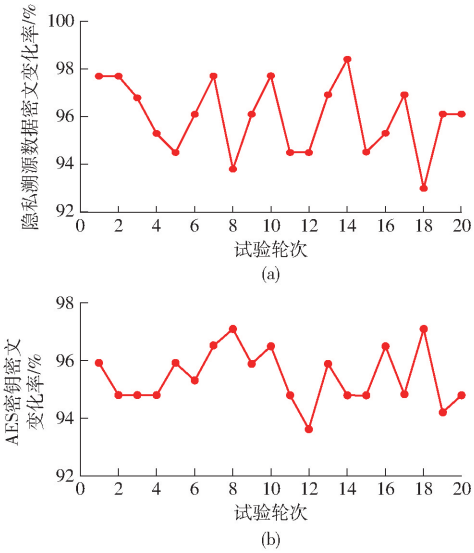


图 4　AES 与 ECC 加密安全性测试结果

Fig. 4　Security test of AES and ECC encryption

询所需的平均时延如图 5b 所示,溯源数据加密上链的平均时延为 2.16 s,公开溯源数据平均查询时延为 56.9 ms,隐私溯源数据平均查询时延为 62.87 ms,能够满足农产品溯源系统数据上链与查询需求。

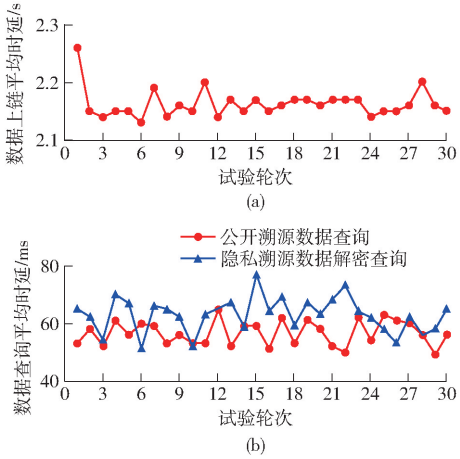


图 5 数据上链与查询性能测试

Fig. 5 Latency test of uploading and querying data from blockchain

3.4 存储性能分析

本文的核心在于利用区块链多链架构提升果蔬区块链溯源网络存储能力,通过将追溯网络划分为生产链、收购链、仓储链、加工链、分销链以及提供共识服务的共识链,每条链独立存储该类企业追溯节点的溯源数据,多链结构下每条链的存储容量、溯源节点以及单条溯源链的存储配置如表 6 所示。

表 6 溯源多链与单链存储配置

Tab. 6 Storage configuration of single and multi-chain

溯源链类型	名称	节点	IP 地址
单链	溯源链	生产节点、收购节点、仓储节点、加工节点、分销节点、排序节点、Kafka 集群、数据库节点、身份认证节点、浏览器节点	172.31.219.124
多链	生产链	生产节点、生产身份认证节点、数据库节点	172.16.61.109
	收购链	收购节点、收购身份认证节点、数据库节点	172.16.41.47
	仓储链	仓储节点、仓储身份认证节点、数据库节点	172.16.61.108
	加工链	加工节点、加工身份认证节点、数据库节点	172.16.61.107
	分销链	分销节点、分销身份认证节点、数据库节点	172.31.219.125
	共识链	Kafka 集群、排序节点、浏览器节点	172.31.219.123

多链结构的企业链性能配置取决于溯源企业,通过多环节不同企业链分布式独立存储溯源数据,缓解数据单链存储压力。链下追溯数据通过物联网设备采集,在一定的间隔时间内上传至区块链网络,其中,单条溯源数据为 0.34 kB,由企业节点授权背书,经过智能合约上链生成新的区块约 6 kB。单链式溯源网络在满足联盟链架构基础上难以负载千万吉字节数据存储需求,多链存储网络通过通道隔离数据,能够在满足多企业多产品海量溯源数据长时间内存储需求的基础上,实现数据的隐私保护、授权共享。

4 果蔬溯源系统实现

4.1 系统架构

基于联盟链通道创建的果蔬多链溯源系统,通过多链架构扩展总体溯源网络容量,通过链上智能合约自动分类溯源数据,实现公开数据明文与隐私数据加密上链、授权解密共享,解决上下游溯源企业数据无孤岛共享,监管部门全数据的穿透式管控,具体的系统架构如图 6 所示,共分为 4 层:存储层、服务层、接口层、应用层。

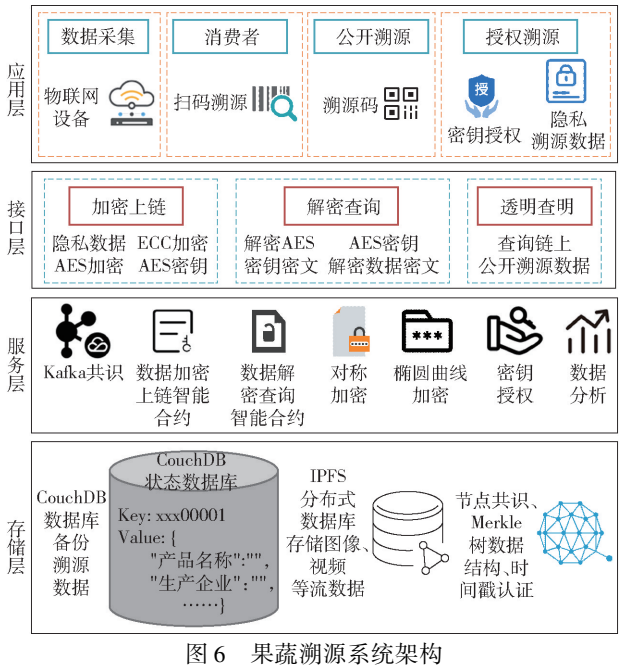


图 6 果蔬溯源系统架构

Fig. 6 Traceability system architecture of fruits and vegetables

存储层中溯源数据存储在链外状态数据库 CouchDB,构建 Key-value 键值索引,通过索引查询代替传统遍历查询,减少数据查询时间。产品生产过程由监控摄像设备、音频设备、照相机等采集的视频、音频数据通过分布式数据库 IPFS 存储,将返回的哈希值和公开溯源数据上传到区块链。

服务层中提供 Kafka 共识集群,以智能合约为

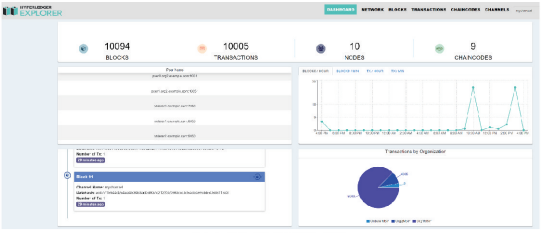
核心，保证数据加密上链请求与解密查询请求的自动处理。

接口层面向消费者封装公开溯源数据查询接口，通过产品溯源码扫码查询产品溯源数据；面向企业提供数据分类加密上链接口，提供授权解密共享接口，在保证链上全部数据的安全可靠的基础上，满足上下游数据共享需求与监管部门全溯源数据管控需求。

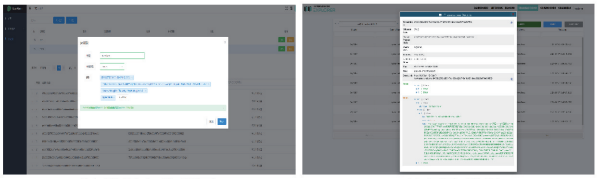
应用层通过物联网设备采集果蔬全供应链环节的溯源数据，为消费者与溯源企业提供不同应用服务。

4.2　应用案例分析

果蔬溯源区块链平台应用于山东省淄博市鲁中水果批发市场溯源平台，为市场果蔬提供产品全供应链环节溯源数据。目前，溯源区块链网络共处理数据上链请求 10 005 笔，生成区块 10 094 块，如图 7a所示。企业节点通过溯源平台填写当前溯源数据键值、公开溯源数据、隐私溯源数据、AES 密钥，提交数据上链请求，经过全网节点共识记账，返回交易哈希值，如图 7b 所示，关于具体区块的配置信息，包括交易哈希值、上链组织、合约名称、上链日期、上链的交易请求等如图 7c 所示。



(a) 区块链溯源网络



(b) 数据上链界面　　(c) 区块数据

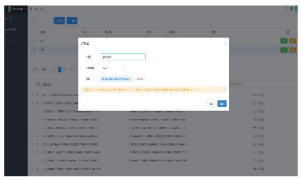
图 7　溯源数据上链请求

Fig. 7　Request of traceability data upload to blockchain

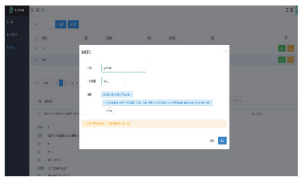
面向消费者逆向溯源，本文设计的溯源系统为市场果蔬提供溯源二维码，消费者通过扫码查询可获取产品溯源数据，如图 8a 所示。并提供计算机端公开溯源数据查询溯源界面，通过溯源码查询当前溯源数据的溯源结果，如图 8b 所示；为监管部门管控追溯数据提供计算机端界面，通过授权凭证解密查询数据，如图 8c 所示。



(a) 手机端扫码溯源界面



(b) 公开溯源数据查询界面



(c) 隐私溯源数据查询界面

图 8　溯源数据查询请求

Fig. 8　Request of traceability data query from blockchain

5　结论

(1)在果蔬区块链溯源系统中，对每个追溯环节构建溯源链，保证不同追溯环节内溯源企业数据的隔离存储，扩展溯源网络的总体容量。通过智能合约实现对称加密与椭圆曲线混合加密运算，能够有效保证链上隐私数据密文的安全性与密钥凭证的不可破解性，降低溯源数据的存储压力；链间基于密钥授权解密查询隐私数据，解决了溯源上下游多企业间数据共享孤岛难题，以及监管部门对全溯源数据的监管需求。

(2)本文所提出的基于智能合约的混合加密算法，能够实现隐私数据的安全存储。扩散性测试结果表明，隐私数据以及对称密钥的密文变化率分别为 95%、94% 以上，具备较高的安全性；系统性能测试结果表明，链上数据加密存储、隐私数据共享解密、公开数据透明访问的平均时延分别为 2.16 s、62.87 ms、56.9 ms，系统具备较高的性能，满足果蔬溯源过程中数据上链与查询的需求，为果蔬区块链溯源系统溯源数据分类存储提供一定的借鉴与参考。

参　考　文　献

[1] 孙传恒，于华竟，徐大明，等. 农产品供应链区块链追溯技术研究进展与展望[J]. 农业机械学报，2021，52(1)：1－13.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(1): 1－13. (in Chinese)

[2] SABERI S, KOUHIZADEH M, SARKIS J, et al. Blockchain technology and its relationships to sustainable supply chain management[J]. International Journal of Production Research, 2019, 57(7): 2117－2135.

[3] YANG X T, LI M Q, YU H J, et al. A trusted blockchain-based traceability system for fruit and vegetable agricultural products

[J]. IEEE Access, 2021, 9: 36282 - 36293.

[4] 郑艺,徐耀群,邱泽国. 基于区块链技术的生鲜农产品溯源研究[J]. 哈尔滨商业大学学报(自然科学版),2021,37(4):506 - 512.
ZHENG Yi, XU Yaoqun, QIU Zeguo. Research on fresh agricultural products traceability based on blockchain technology[J]. Journal of Harbin University of Commerce (Natural Sciences Edition), 2021, 37(4): 506 - 512. (in Chinese)

[5] 钟德福,艾红,张良国,等. 区块链技术及其在农产品质量安全追溯应用的研究进展[J]. 中国农学通报,2021,37(19):143 - 150.
ZHONG Defu, AI Hong, ZHANG Liangguo, et al. Research progress of blockchain technology and its application in agricultural product quality and safety traceability[J]. Chinese Agricultural Science Bulletin, 2021, 37(19): 143 - 150. (in Chinese)

[6] HARSHITHA M S, SHASHIDHAR R, ROOPA M. Block chain based agricultural supply chain—a review[J]. Global Transitions Proceedings, 2021, S2666 - 285X(21): 00069 - 8.

[7] 徐智,王岳,王欣. 结合区块链的非结构化大数据云存储优化研究[J]. 计算机仿真,2021,38(7):304 - 307,354.
XU Zhi, WANG Yue, WANG Xin. Research on cloud storage optimization of unstructured big data combined with blockchain[J]. Computer Simulation, 2021, 38(7): 304 - 307, 354. (in Chinese)

[8] 许继平,王健,张新,等. 区块链驱动的稻米供应链信息监管模型研究[J]. 农业机械学报,2021,52(5):202 - 211,101.
XU Jiping, WANG Jian, ZHANG Xin, et al. Information supervision modeling of rice supply chain driven by blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(5): 202 - 211, 101. (in Chinese)

[9] 于合龙,陈邦越,徐大明,等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报,2020,51(8):328 - 335.
YU Helong, CHEN Bangyue, XU Daming, et al. Modeling of rice supply chain traceability information protection based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(8): 328 - 335. (in Chinese)

[10] 杨信廷,王明亭,徐大明,等. 基于区块链的农产品追溯系统信息存储模型与查询方法[J]. 农业工程学报,2019,35(22):323 - 330.
YANG Xinting, WANG Mingting, XU Daming, et al. Data storage and query method of agricultural products traceability information based on blockchain[J]. Transactions of the CSAE, 2019, 35(22): 323 - 330. (in Chinese)

[11] 李梦琪,杨信廷,徐大明,等. 基于主从多链的水产品区块链溯源信息管理系统设计与实现[J]. 渔业现代化, 2021,48(3):80 - 89.
LI Mengqi, YANG Xinting, XU Daming, et al. Design and implementation of aquatic product blockchain traceability information manegement system based on master-slave multi-chain[J]. Fishery Modernization, 2021, 48(3): 80 - 89. (in Chinese)

[12] 张晓蝶,黄郑正,赵金辉,等. 基于区块链多链的农产品供应链追溯应用[J]. 重庆理工大学学报(自然科学),2021,35(10):172 - 179.
ZHANG Xiaodie, HUANG Zhengzheng, ZHAO Jinhui, et al. Application of agricultural products supply chain traceability based on multi-blockchain[J]. Journal of Chongqing University of Technology (Natural Science), 2021,35(10): 172 - 179. (in Chinese)

[13] 姚前,张大伟. 区块链系统中身份管理技术研究综述[J]. 软件学报,2021,32(7):2260 - 2286.
YAO Qian, ZHANG Dawei. Survey on identity management in blockchain[J]. Journal of Software, 2021, 32(7): 2260 - 2286. (in Chinese)

[14] 蔡亮,端豪,鄢萌, 等. 基于双层协同的联盟区块链隐私数据保护方法[J]. 软件学报,2020,31(8):2557 - 2573.
CAI Liang, DUAN Hao, YAN Meng, et al. Private data protection scheme for consortium blockchain based on two-layer cooperation[J]. Journal of Software, 2021, 31(8): 2557 - 2573. (in Chinese)

[15] 孙知信,张鑫,相峰,等. 区块链存储可扩展性研究进展[J]. 软件学报,2021,32(1):1 - 20.
SUN Zhixin, ZHANG Xin, XIANG Feng, et al. Survey of storage scalability on blockchain[J]. Journal of Software, 2021, 32(1): 1 - 20. (in Chinese)

[16] SWATHI P, VENKATESAN M. Scalability improvement and analysis of permissioned-blockchain[J]. ICT Express, 2021, 7(3): 283 - 289.

[17] DU Mingxiao, MA Xiaofeng, ZHANG Zhe, et al. A review on consensus algorithm of blockchain[C]// 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, Canada, 2017: 2567 - 2572.

[18] 陈闻宇,李晓东,杨学,等. 一种基于区块链的 DNSSEC 公钥验证机制[J/OL]. 自动化学报,2021, DOI:10.16383/j.aas.c201082.
CHEN Wenyu, LI Xiaodong, YANG Xue, et al. A blockchain-based DNSSEC public key verification scheme[J/OL]. Acta Automatica Sinica, 2021, DOI: 10.16383/j.aas.c201082. (in Chinese)

[19] VERMA M. Smart contract model for trust based agriculture using blockchain technology[J]. International Journal of Research and Analytical Reviews, 2021, 8(2): 354 - 355.

[20] NAWGHARE P, RAMDASI C, SAMGLE S, et al. Supply chain management for aricultural products using blockchain technology[J]. Internatinal Journal of Engineerin Science, 2020, 5(4):174.

[21] 杨信廷,王杰伟,邢斌,等. 基于区块链的畜牧养殖资产监管身份认证研究[J]. 农业机械学报,2021,52(11):170 - 180.
YANG Xinting, WANG Jiewei, XING Bin, et al. Identification of animal husbandry assets supervision based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(11): 170 - 180. (in Chinese)