

基于区块链和边缘计算的水稻原产地溯源方法研究

孙传恒^{1,2} 袁 晟^{1,2} 罗 娜^{2,3} 徐大明^{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: 地理位置与环境因素的不同导致水稻品质存在差异, 优质原产地的稻米质优味美, 对消费者更有吸引力, 因此研究水稻原产地溯源, 建立水稻原产地可信溯源系统具有重要意义。传统物联网区块链溯源系统将溯源数据上传至中心化的服务器, 再由服务器上传至区块链; 这无法很好地利用边缘节点中的资源, 还使其易受数据伪造或数据丢失等安全风险的影响。设计了一套基于区块链和边缘计算的水稻原产地溯源模型, 依托嵌入式设备的边缘计算能力, 对传感器数据实时数据融合并在嵌入式设备上部署区块链。此外, 设计边缘计算场景下区块链网络的存储扩展方法和边缘计算工作流程。最后, 经过测试分析, 查询公开溯源数据的平均时间为 45.84 ms, 查询隐私溯源数据的平均时间为 50.92 ms, 边缘节点加密上链的平均时间为 1.27 s, 边缘多链存储容量消耗为传统单链的 18%, 能够满足水稻原产地溯源实际的应用需求。

关键词: 水稻原产地; 溯源; 区块链; 多链; 边缘计算

中图分类号: TP309.2; TS201.6 文献标识码: A 文章编号: 1000-1298 (2023) 05-0359-10 OSID:



Traceability Method of Rice Origin Based on Blockchain and Edge Computing

SUN Chuanheng^{1,2} YUAN Sheng^{1,2} LUO Na^{2,3} XU Daming^{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: Differences in geographic location and environmental factors lead to differences in rice quality. Rice of high quality origin has excellent quality and taste and is more attractive to consumers, so it is important to study the origin traceability of rice and establish a credible traceability system of rice origin. The traditional IoT blockchain traceability system uploads traceability data to a centralized server, which in turn uploads it to the blockchain; this does not make good use of the resources in the edge nodes and also makes it vulnerable to security risks such as data forgery or data loss. A set of rice origin traceability model was designed based on blockchain and edge computing. The edge layer of this model divided the local blockchain network according to the origin latitude and longitude, each origin region chain contained multiple edge nodes and one core node, and relied on the edge computing capability of embedded devices for real-time data fusion of sensor data and deployment of blockchain on embedded devices. Edge computing ensured the authenticity of the data source, and the blockchain ensured that the on-chain data cannot be tampered, and the combination of the two realized the trusted storage of traceability system data. In addition, the storage scaling method of the blockchain network under the edge computing scenario and edge computing workflow were designed. Finally, after testing and analysis, the average time for querying public traceability data was 45.84 ms, the average time for querying private traceability data was 50.92 ms, the average time for encrypting on-chain of edge nodes was 1.27 s, and the storage capacity consumption of edge multi-chain was 18% of that of traditional single-chain, which can meet the practical application requirements of rice origin traceability.

Key words: rice origin; traceability; blockchain; multi-chain; edge computing

收稿日期: 2022-08-22 修回日期: 2022-10-10

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

0 引言

我国是世界最大稻米生产国,60% 以上的居民以稻米为主食,水稻生产事关国家口粮安全^[1]。地理位置以及环境因素的差异导致了水稻品种和类型的多样性,同时其质量品质也存在显著差异^[2]。生活水平的不断提高使得人们更加注重稻米风味及营养品质,优质原产地的稻米产品质优味美,对消费者更有吸引力^[3]。因此,研究水稻原产地溯源,建立水稻原产地可信追溯系统,可以提高水稻信息对消费者的透明度、消费者对水稻原产地品牌的认可度,从而维护消费者权益并加强企业竞争力。

农产品供应链追溯具有链条长、生产分散、信息多源异构等特点,传统的追溯研究集中于利用射频识别(Radio frequency identification,RFID)、二维码、无线传感网络等物联网技术记录追溯数据,难以解决供应链追溯数据被篡改、上下游间信任成本较高等问题。区块链综合运用了分布式数据存储、对等网络、共识机制、加密算法等多种计算机技术^[4-5],具有去中心化、数据不可篡改、可追溯等特点^[6],旨在不可信的开放网络中,维护一个安全可信、不可篡改的公共账本^[7],能够有效解决供应链上下游数据在传递过程中的信任问题^[7-8],从而构建符合追溯需求的可信交易环境^[9]。将区块链技术与农产品追溯相结合,能做到分散资源集中管理、集中资源分散服务,为解决目前传统追溯体系存在的问题提供了技术支撑^[10]。在区块链农产品追溯系统中使用物联网技术对追溯各环节信息按照某种格式发送到数据中心进行“一物一码”标识,并将重要信息上传至区块链存证,利用区块链技术来保证数据的不可篡改^[11]。

近年来,国内外学者从不同角度探究区块链和物联网技术在追溯中的应用^[12-18],这些研究深入探索了区块链以及物联网技术在追溯方面的价值,但大多通过 RFID、传感器等收集水稻信息直接或通过网关上传到云端,再由云端进行溯源信息上链处理。这类方法存在以下问题:尽管区块链是去中心化的,但云端是中心化的,在云端上链前存在数据篡改风险;同时现有的物联网终端设备数量呈指数级增长,将这些物联网设备产生的海量数据全部传输到云端会对其计算存储资源造成很大压力^[19-20]。边缘计算是一种地理上分布式部署、在靠近数据源头处执行计算存储任务的技术^[21],它能够有效利用物联网设备中的计算与存储资源^[22],降低通信延迟和带宽消耗,减轻云端的计算存储负荷^[23-24]。同时,与区块链技术相结合,能够为追溯系统提供安全、高效的

数据共享模式,解决水稻原产地溯源存在的源头数据篡改、云端资源消耗大等问题。区块链与边缘计算结合还会面临物联网设备生成大量数据、数据繁杂异构、区块链存储空间占用过大等问题。

为了解决这些问题,本文提出水稻原产地溯源边缘区块链模型,该模型的边缘层根据产地经纬度划分局部区块链网络,每个产地区域链包含多个边缘节点和一个核心节点;边缘节点仅存储对应产区账本,核心节点存储全部产区账本。利用嵌入式设备的边缘计算能力,对物联网数据实时融合得到所需的水稻追溯信息;边缘节点作为区块链节点,将水稻追溯信息中的公开溯源数据和加密商业隐私数据写入边缘区块链账本。边缘区块链账本备份到核心节点再由其上传至核心链,边缘节点通过核心节点在核心链发布交易以注册身份加入到产地区域链。在该模型的基础上,设计嵌入式设备边缘计算的工作流程并实现原型。

1 水稻供应链关键信息

水稻供应链包括种植、加工、仓储、运输、销售等多环节^[25],由土壤温湿度传感器、称重传感器、GPS 定位装置等终端设备实时采集温湿度、生产数量、位置等溯源信息,保证高品质稻米产品源头数据真实性。在水稻产品追溯中,数据种类繁多,并非所有数据都可公开,涉及产量、价格等与产品质量安全无关的商业隐私信息需要进行加密处理。本文提取水稻供应链各环节关键追溯数据并将其划分为公开数据与商业隐私数据,具体如表 1 所示。由于水稻原产地溯源主要涉及产品信息、地理位置和生产数量,故本文主要对产品基本信息、温湿度信息、GPS 信息和产品重量信息等进行追溯,其中产品重量信息、产品成本、产品价格等为商业隐私数据。

2 基于区块链和边缘计算的水稻原产地溯源模型

2.1 水稻原产地溯源边缘区块链模型

在深入分析水稻供应链特点的基础上,本文设计基于区块链和边缘计算的水稻原产地溯源模型,主要由感知层、边缘层和应用层构成,如图 1 所示。感知层包括称重传感器、GPS 传感器、摄像头等;传感器收集到的数据通过无线传感网络传输到边缘层。边缘层的嵌入式设备作为边缘节点的同时还作为区块链节点维护相应账本,边缘层完成数据过滤、数据融合处理以及水稻产地溯源隐私数据加密后,边缘节点作为联盟链背书节点提交追溯信息上链;边缘区块链部分设计如下:根据产地经纬度划分为

表 1 水稻供应链关键信息

Tab.1 Key information of supply-chain

供应链环节	数据来源	公开数据	隐私数据
种植	温湿度传感器、GPS、称重传感器	土壤类型、土壤温湿度、地理位置以及生产企业、采收日期	种植成本、采收数量
仓储	摄像头、温湿度传感器、RFID、GPS、称重传感器	产品仓储地点、温湿度、进仓时间以及出仓时间	进仓数量、出仓数量、仓储存量、仓储成本、仓储管理人员信息
加工	GPS、称重传感器	稻谷清理与稻谷分级、稻谷抛光以及加工企业、日期、产品批次、地理位置	原料成本、进货数量、加工成本、加工数量、出货数量、负责人信息
运输	车载温湿度传感器、GPS	运输路线、运输过程产品温度、湿度、时间以及承运企业	运输成本、订单信息、运输产品批次及数量、承运车辆信息、运输人员信息
销售	RFID、称重传感器	产品批次、产品 ID、销售企业	进货价格、销售单价、进货数量、销售数量、销售员信息

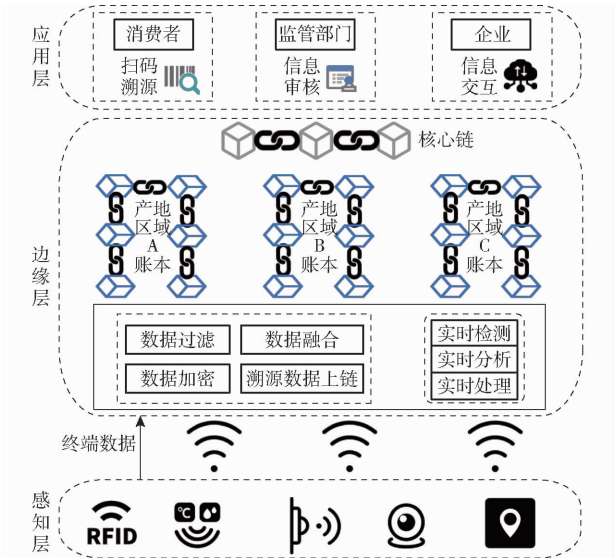


图 1 水稻原产地溯源模型

Fig.1 Rice origin traceability model

多个产地区域,每个产地区域里的边缘节点维护一个产地区域账本,产地区域账本备份到各产区对应的核心节点,全部核心节点维护一条核心链,边缘区块链节点注册和备份数据都上传至核心链。应用层负责消费者、监管部门以及企业的各种信息交互需求。

2.2 边缘区块链存储扩展设计

区块链融合边缘计算时,面临参与节点存储资源限制方面的挑战。在边缘计算节点部署区块链时,区块链全冗余存储机制和共识过程会消耗节点大量的存储和计算资源。由于作为边缘节点的嵌入式设备的存储容量限制,无法像原先的联盟链节点那样支持扩容;并且联盟链网络中存在大量的边缘侧节点,如果所有的节点都验证网络中的每笔交易,会大大限制联盟链的吞吐量。为了降低边缘节点需要存储的账本数据以及处理的交易量,本文设计基于原产地溯源的边缘区块链。边缘计算场景下,数据具有地域性、时效性等特点^[26]。由于边缘节点部

署在水稻产地,本文中根据产地经纬度将区块链网络划分为多个局部区块链网络。

水稻产地区域划分方式如下:

(1)划分区域。考虑水稻主要产地并非均匀分布,并结合文献[27]中的产地区域划分方法,将经度划分为2个带、将纬度划分为3个带,这样整个中国水稻产地地图被划分为6个区域,如图2所示,其中水稻产地地图的数据来源于2021年全国各省市统计年鉴。



图 2 水稻产地区域划分示意图

Fig.2 Diagram of regional division of rice production areas

(2)确定区域。在划分出6个区域的基础上,需要确定某边缘节点的坐标属于哪个区域,参考表2的原则确定水稻原产地区域,再构建边缘区块链多链网络。

边缘计算场景下联盟链多链示意图如图3所示,联盟链中的一个组织作为一个水稻供应链企业,一个通道内有多个组织,每个组织有多个边缘区块链节点。相同产地区域内的节点加入相同通道,绝大部分数据交换发生在相同产地区域的联盟链网络,处于不同产地区域的节点本身不需要进行频繁的数据交互。并且在每个产地区域都设置一个核心节点,核心节点加入各自产区的通道从而备份产区

表 2 水稻产地位置对应区域

产地经纬度范围	对应产地 区域
东经 135°02'30"至东经 108°00'00" 且北纬 53°33'00"至北纬 40°00'00"	A
东经 135°02'30"至东经 108°00'00" 且北纬 40°00'00"至北纬 28°00'00"	B
东经 135°02'30"至东经 108°00'00" 且北纬 28°00'00"至北纬 3°52'00"	C
东经 108°00'00"至东经 73°40'00" 且北纬 53°33'00"至北纬 40°00'00"	D
东经 108°00'00"至东经 73°40'00" 且北纬 40°00'00"至北纬 28°00'00"	E
东经 108°00'00"至东经 73°40'00" 且北纬 28°00'00"至北纬 3°52'00"	F

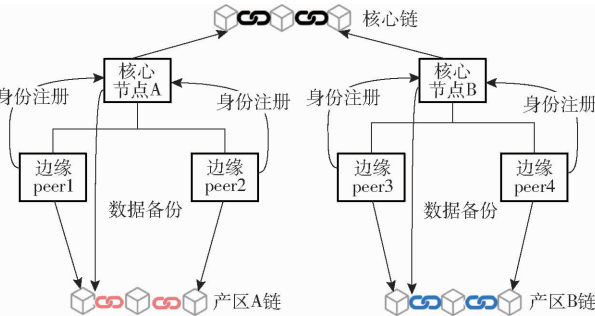


图 3 边缘计算场景下的联盟链多链示意图
Fig.3 Federation chain multi-channel in edge scenario

账本,同时所有核心节点维护一个核心链,核心节点再将各产区账本上传至核心链,通过核心节点完成不同产地区域网络溯源数据查询的需求。边缘节点加入边缘区块链需要通过核心节点注册身份,身份注册视为一个交易发布到核心区块链中。不同产地区域的边缘区块链节点处于不同的通道中,以通道的天然隔离实现溯源数据的隔离存储;同一个通道内的大量边缘节点是属于不同企业的,因此也不会造成中心化风险。由于本文水稻产地追溯链中的产区数量为 6,故每笔追溯数据上链需要达成共识的节点数量近似为原先的 1/6。这种边缘区块链设计减少了边缘区块链节点需要存储的追溯数据量,缓解了边缘区块链节点的存储压力。

2.3 水稻原产地溯源中的边缘计算

借助嵌入式设备的边缘计算能力,实现以下两个模块:对传感器数据实时融合得到所需的水稻追溯信息;将自身作为区块链节点,将水稻追溯信息中的公开溯源数据和加密商业隐私数据写入边缘区块链账本。

(1)数据融合

在水稻产地溯源中通过 GPS、称重传感器、RFID、温湿度传感器等实时采集水稻的 GPS、重量

等数据。感知层终端设备计算存储能力较弱,难以对传感器数据进行及时处理。边缘节点拥有较高的计算资源和存储空间,通过对传感器数据的分析,可以实现对异常数据进行过滤,将过滤处理后的各种传感器数据提取关键信息进行数据融合得到所需的水稻产地溯源数据。这保证了存储在区块链中的数据是可靠的,消除了传感器精度上的潜在误差或检测到的异常数据^[28]。

本文使用卡尔曼滤波算法对水稻产地溯源各环节传感器实时动态数据进行数据融合,其通过逐层递归的方式进行线性滤波,利用前一个采样周期的估计值加上当前测量值对当前状态进行准确的估计^[29]。这种方法存储计算消耗较少,具有良好的实时性和抗干扰能力,采用这种方法进行水稻产地溯源的数据级融合。

线性动态系统的卡尔曼滤波模型由状态方程、节点观测方程、状态一步预测值以及更新方程组成,根据文献[29]可以不断地迭代下去,在水稻原产地溯源环境存在干扰较多的情况下,通过卡尔曼滤波算法能够有效消除传感器数据中系统噪声和测量噪声的影响,更加准确地得到实际环境测量数据的真实值。表 3 为水稻产地溯源中的测量数据以及经过卡尔曼滤波后的数据,其中原始车载 GPS 经纬度经过经纬度和加速度数据融合后得到卡尔曼滤波 GPS 经纬度。

生产环节数据融合后最终得到溯源数据示例如下:产品批次:320911199734981328|产品名称:五常大米|上链节点 Id:320911|节点名称:peer0. org1. example. com|土壤类型:黑土|土壤温湿度:3. 04℃, 14. 44%|生产企业:五常市北大仓米业有限公司|产地经纬度:4 492. 927 6, N, 12 715. 428 3, E|采收日期:2022/07/05|种植成本:1. 25 元/kg|采收量:3 000. 0 kg。

(2)溯源数据上链

水稻原产地溯源通过称重传感器、GPS 定位设备、温湿度传感器等实时采集产品生物信息和空间信息数据。其中,并非所有数据可公开溯源,涉及商品价格、产量等不影响产品质量的商业隐私数据,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。本文将水稻追溯数据,划分为可公开溯源数据与商业隐私数据。嵌入式设备不仅是边缘节点,还将自身作为区块链上链节点,对公开溯源直接上链,商业隐私数据加密后再上链。溯源数据上链的详细流程如图 4 所示,边缘节点先将获取的传感器数据经卡尔曼滤波算法数据融合得到水稻溯源数据,再对溯源数据分类,将商业隐私数据通过 SM2

表 3 测量数据与卡尔曼滤波数据

Tab.3 Measured data and Kalman filtered data

序号	土壤温湿度传感器		车载温湿度传感器		车载 GPS	
	测量值	卡尔曼滤波值	测量值	卡尔曼滤波值	测量值	卡尔曼滤波值
1	3.20℃ ,14.7%	3.16℃ ,14.64%	25.40℃ ,53.5%	25.43℃ ,53.47%	3 018.195 2,N, 12 013.312 5,E	3 018.195 2,N, 12 013.312 5,E
2	3.10℃ ,14.5%	3.14℃ ,14.57%	25.50℃ , 53.4%	25.46℃ ,53.44%	3 018.195 0,N, 12 013.311 8,E	3 018.195 0,N, 12 013.312 5,E
3	3.20℃ ,14.8%	3.16℃ ,14.68%	25.30℃ , 53.6%	25.40℃ , 53.50%	3 018.195 0,N, 12 013.311 8,E	3 018.195 0,N, 12 013.312 5,E
4	3.10℃ ,14.4%	3.14℃ ,14.55%	25.50℃ , 53.5%	25.44℃ , 53.50%	3 018.194 4,N, 12 013.311 8,E	3 018.194 6,N, 12 013.312 5,E
5	3.00℃ ,14.3%	3.04℃ ,14.44%	25.60℃ , 53.4%	25.50℃ , 53.47%	3 018.194 4,N, 12 013.311 8,E	3 018.194 4,N, 12 013.312 5,E

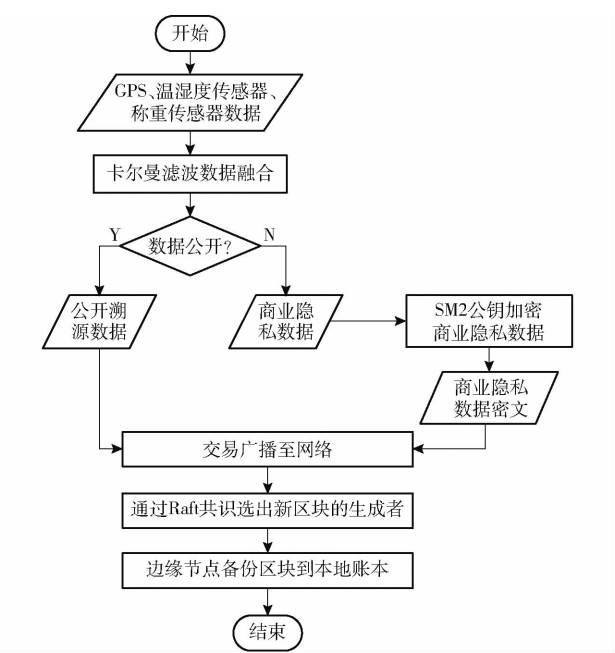


图 4 边缘节点上链流程

Fig.4 Edge node on-chain process

公钥加密后的隐私数据密文及公开溯源数据打包成交易提案广播至边缘侧区块链网络,网络通过 Raft 共识算法选出新区块的生成者,其余边缘节点再将新区块备份到本地账本中。

针对公开溯源数据消费者溯源需求、商业隐私数据授权共享需求,本文设计数据上链合约、获取公开数据合约、通过 SM2 椭圆曲线公钥密码算法^[30]私钥解密查询隐私溯源数据合约,具体的算法逻辑如表 4 所示。

表 4 算法逻辑设计

Tab.4 Design of smart contract function

算法功能	业务逻辑	方法	描述
数据上链	公开溯源数据上链	traceTrans()	上链数据包括数据键值、公开溯源数据、隐私数据数据密文
	隐私溯源数据密文上链		
数据查询	公开溯源数据查询	getPubdata(id)	通过水稻溯源码查询水稻公开溯源数据
	隐私溯源数据查询	getPridata(id ,key)	通过水稻溯源码和 SM2 私钥查询隐私溯源数据

本文对隐私溯源数据混合加密后上链、链上节点基于 SM2 私钥访问隐私数据、链上共享公开溯源数据,数据上链算法 1 如下:

算法 1:数据上链算法

输入:节点 peer,合约名称 cc,通道名称 channel,键值 id,公开数据 pubData,隐私数据密文 priData
输出:交易哈希 txID,区块高度 blockNum

```
if id 验证有效 then
    // 自动化生成 SM2 密钥对
    prk←getKey( ) // 溯源节点 SM2 私钥
    publicKey←&prk.PublicKey // 溯源节点 SM2 公钥
    // 通过溯源节点 SM2 公钥加密隐私数据 priData
    SM2EncryPri←SM2Encrypt( priData, publicKey)
    // 封装上链数据结构体
    traceObj←&traceObj{ id, pubData, SM2EncryPri }
    // 执行上链操作, marbleJSONasBytes 为 traceObj 的 json 编码
    err←PutState( id,marbleJSONasBytes)
    if err 非空 then
        return Error
    else
        return txID,blockNum
else
    return dataError
```

通过数据上链算法,边缘侧区块链节点调用数据上链智能合约发起交易提案,排序节点接收交易并排序后创建新区块广播到通道内各组织的主节点,主节点背书并同步广播到组织内其他节点。本文建立的追溯网络采用 Raft 共识机制,边缘区块链追溯系统的每秒处理事务数(Transaction per second,TPS) 约为 150。Raft 由全部追溯节点选取主节点进行记账、验证、广播,通过心跳机制选举主节点,主节点负责管理链内 Raft 集群中所有节点的复制,确保跟随节点和主节点的日志一致,核心共识过程是日志记录和数据提交。Raft 算法的通信复杂度为 $O(N)$,其中 N 为一个集群中节点的数量,通信复杂度是理论上衡量共识算法效率性的一个指标,因此共识效率较高,具有良好的拓展性;同时仅需 $2n+1$ (其中 n 为集群中最多允许的节点故障数)个节点参与排序即可,降低了部署成本。

溯源信息查询分为公开数据透明访问、隐私数据授权查询,隐私数据查询需要 SM2 私钥解密。隐私数据查询算法 2 如下:

算法 2:隐私溯源数据查询算法
输入:节点 peer,合约名称 cc,通道名称 channel,溯源数据溯源码 code, SM2 私钥 key
输出: 成功则返回隐私数据

```
if code = True and key = True then    //判断溯源码以及 SM2 私钥是否有效
    //获取隐私溯源数据密文
    traceinfo←GetState( code)
    priEncrydata←string( traceinfo. EncryTraceData)
    //通过 SM2 密钥解密隐私溯源数据密文
    pridata←SM2Decrypt ( priEncrydata,key)
else
    return error
return success
```

边缘节点以 Key-value 键值对的形式提交溯源数据,key 为产品 ID,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边缘节点构造交易背书提案,经过 Raft 集群共识排序,返回当前上链请求的交易哈希,生成新的区块与区块高度,详细信息如表 5 所示。

表 5 上链数据

Tab. 5 Key-value traceability data of blockchain

公开溯源数据	商业隐私溯源数据密文	交易哈希	区块高度
产品批次:320911199734981328 产品名称:五常大米 产品 ID: 5519222E - 7DB8 - 4AE3 - 8590 - 89781DAC32BE 上链节点 ID: 320911 节点名称: peer0. org1. example. com 厂家:五常市北大仓米业有限公司 土壤温湿度:3. 12℃, 14. 60% 产地经纬度: 4492. 9276, N, 12715. 4283, E	BKSmcqmL1a7sv1xlqO2is73ECtymuXFg4ZI qHlZlb9r5ThGsAZLcbbQxhxFO8/z24jloreiiuH bBJe32pFlb4KdXG0Bu6T + NTAI2IjAlwyxq UmKpQNfQC1EcHkcXFnBxVhejQdWihS1V JoF9uPulv3b8rlI4ouqTikeyLgEg4iDpFPmQV V8APZEBDhjXV + 7w	c360234ded55 292c773e13fe 7cbff0754c2fa 2eff8e6fed20a b5b61ec74b4a a9	10 482

本文的水稻产地溯源工作流程如图 5 所示。区块链中将存储两种类型的交易数据:一种是 GPS 数据、土壤温湿度等公开数据,另一种是数量、价格等隐私数据。终端数据经过解析、过滤以及数

据融合等处理后,将通过边缘节点作为背书节点提交上链,经验证后达成共识,存储到区块链中。终端提供交易数据给边缘节点,边缘节点处理数据、数据融合后再将追溯数据打包上传至边缘侧

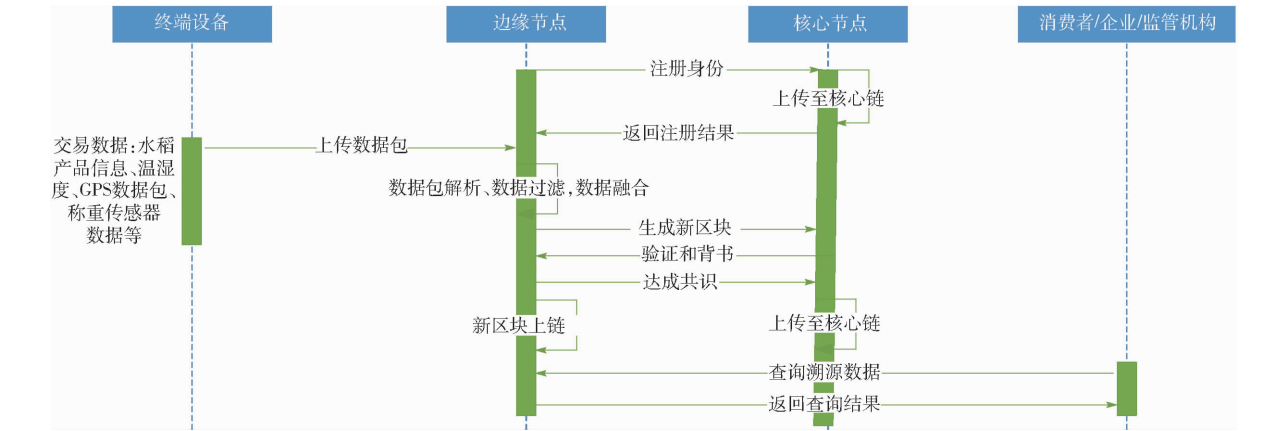


图 5 水稻产地溯源工作流程

Fig. 5 Rice origin traceability workflow

区块链,核心节点为边缘节点提供注册身份和备份溯源数据服务。

消费者、企业和监管机构可以使用计算机或手机查询追溯数据,在获得 SM2 私钥后可查询商业隐私数据。例如,一个人从超市买了一袋五常大米,可以使用智能手机扫描二维码查询与之相关的公开追溯数据,包括产品批次、产品 ID、产品名称、上链节点 ID、土壤温湿度、产地经纬度等。水稻企业或监管部门若要获取隐私数据,包括水稻的产量、价格和负责人等,需要获得数据提交节点的私钥,通过私钥解密查询商业隐私数据。

3 水稻原产地溯源系统实现

3.1 系统架构

基于区块链和边缘计算的水稻原产地溯源系统,通过区块链实现上链信息的不可篡改,保证水稻原产地溯源链上信息的真实可信。通过边缘计算不仅对感知层数据过滤融合,还将处理后的追溯信息上传至边缘侧区块链,实现公开数据明文与商业隐私数据加密上链。这保证了上链前信息来源可靠,同时通过差异化加密的方式保证了隐私安全和溯源数据的透明性,实现了区块链和物联网的有机结合。具体的系统架构共分为 5 层:感知层、边缘层、存储层、接口层、应用层。

物理层使用温湿度传感器、GPS、称重传感器、RFID 等终端设备,对水稻产地溯源过程中的物联网信息进行自动化获取,为边缘层的实时数据提取过滤和数据融合提供数据来源。

边缘层使用嵌入式设备对物联网数据进行实时数据处理和存储,如对 GPS 数据解析,对异常数据进行数据过滤,对温湿度传感器数据、GPS 数据进行数据融合,以减少数据冗余度,提高物理层采集数据的准确度。将溯源数据划分为公开溯源数据和商业隐私数据,并对公开溯源数据直接上链、商业隐私数据通过 SM2 加密后上链等都由边缘层来执行。边缘层既为存储层提供追溯信息,又是存储层联盟链的节点。

存储层中区块链数据账本由文件系统存储的区块结构和数据库维护的世界状态组成,通过 Go 语言编写的智能合约执行交易更新区块链账本。文件系统以 Merkle 树结构存储上链数据,通过链式区块结构实现数据正向记录和逆向追溯。世界状态以键值对的方式保存账本数据状态的最新值,通过智能合约执行交易时,可通过世界状态索引查询键值的最新状态,无需遍历整个事务日志,提高数据查询效率。

接口层封装了区块链账本数据写入和查询接口,为消费者、企业、监管部门实现数据查询、数据上传等应用层功能提供支持。

应用层链接存储层中的水稻产地追溯数据,可为消费者和溯源企业、监管机构提供个性化服务。比如消费者扫码获取原产地溯源信息,企业获取公开溯源数据,监管机构通过私钥解密查询商业隐私数据。

3.2 原型实现

为实现基于区块链和边缘计算的水稻产地溯源原型,采用 Rockchip RK3399 双核 Cortex - A72 + 四核 Cortex - A53 芯片系统(SoC),采用迅为开发板在嵌入式硬件上开发,利用这种硬件可以实现边缘计算。感知设备如 GPS、称重传感器、摄像头等通过无线传感网络传输数据到嵌入式设备。

在 RK3399 芯片上根据 Ubuntu 16.04 定制操作系统并部署 Fabric 1.4.4,由于 RK3399 的 CPU 核心是 arm64,而 Hyperledger Fabric 官方没有 arm64 版本的 docker 镜像,也没有发布相应的二进制文件(peer、orderer、configtxgen 等),因此需要编译 Fabric 源码获取。通过 Qt Creator 开发嵌入式程序并交叉编译后将程序移植到 RK3399 芯片上运行,如图 6 所示,该程序用于物联网数据获取并处理,包括物联网数据收集、数据过滤、数据融合等,最终将其中的关键数据打包为追溯信息上传到区块链。如图 7 所示,水稻产地溯源存储在区块链账本,追溯系统展示区块链数据存储信息,包括区块高度、交易 Hash 等,用户可查询水稻原产地溯源信息。本文实现的原型利用区块链技术和嵌入式硬件的边缘计算能力,在水稻产地获取源头数据经数据过滤、数据融合后直接将水稻追溯信息上传至边缘区块链,再由核心节点将边缘区块链账本上传至核心链。边缘计算保证数据来源真实性,区块链保证上链数据不可篡改,两者结合实现了追溯系统数据的可信存储。

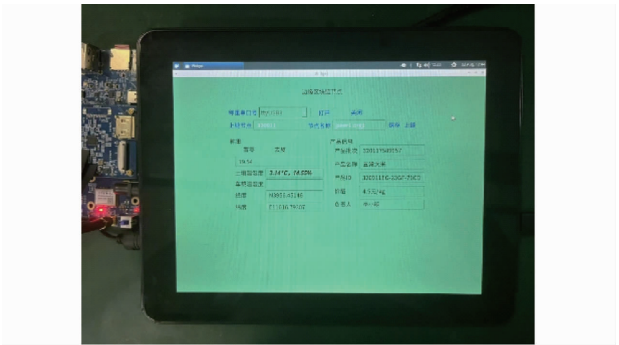


图 6 边缘区块链节点程序界面

Fig. 6 Edge node program interface diagram

同时,为满足消费者追溯需求,本研究设计的水

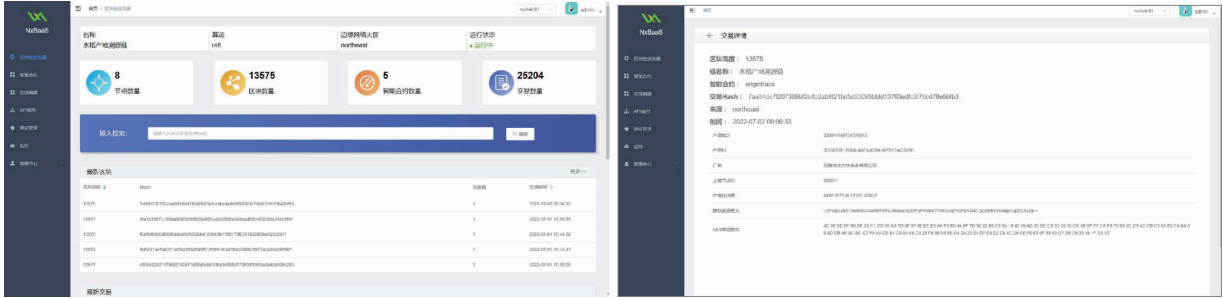


图 7 水稻产地追溯系统界面

Fig.7 Blockchain traceability system interface

稻产地溯源系统为消费者提供扫码溯源的功能,消费者可扫描产品上的二维码获取产品的溯源数据。如图 8 所示,经过查询后,消费者可获得产品介绍信息、溯源信息和区块信息。消费者可获得该批次产品的公开溯源信息,同时展示区块链追溯系统中的区块链地址、追溯 Hash 值和区块高度,确保数据不被篡改。



图 8 消费者扫码溯源界面

Fig.8 Consumer traceability interface

4 测试与分析

4.1 测试环境

通过 Ubuntu 16.04 Linux 系统,基于 Hyperledger Fabric v1.4.4 建立水稻产地溯源网络,RK3399 芯片存储容量 16 GB,运行内存 4 GB。区块链采用 Raft 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,测试工具为 Postman 和 Hyperledger Caliper,具体配置如表 6 所示。

4.2 上链与查询性能

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节点为 peer1.org1.example.com,通过接口每轮次测试 50 次,数据上链平均时延如图 9a 所示。在数据查询接口中,通过接口每轮次测试 50 次,公开溯源数据、隐私溯源数据解密查

表 6 区块链配置

Tab.6 Configuration of blockchain

设置	值	描述
共识机制	Raft	允许网络不大于 1/2 的节点宕机
通道数	7	产地溯源链划分为 6 个地理大区,1 个核心链
节点数	38	6 个大区,每个大区 1 个核心节点
数据库	CouchDB	5 个边缘节点,包括消费者节点、监管节点
区块生成时间/s	1	通过链外状态数据库提供富查询
区块容量/MB	20	链上区块生成时间间隔
区块交易数	100	每个区块容纳的最大容量
		每个区块接受的最大交易数

询所需的平均时延如图 9b 所示。根据图 9 所示,溯源数据加密上链的平均时间为 1.27 s,公开溯源数据平均查询时间为 45.84 ms,隐私溯源数据平均查询时间为 50.92 ms,能够满足水稻原产地溯源系统数据上链与查询需求。

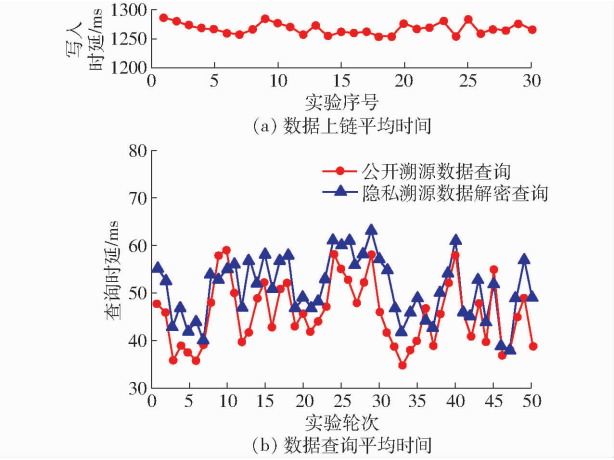


图 9 追溯数据上链与查询时间

Fig.9 Upload and query time of traceability data

4.3 存储性能

本文的边缘区块链模型利用产地区域划分区块链多链提升水稻区块链原产地溯源网络存储能力,根据产地经纬度划分产地区域,将我国水稻产地划分为 6 个水稻产区,每个产地区域单独维护一条链,每条链独立存储该产地区域内各追溯节点的溯源数

据,边缘区块链多链结构与传统单链结构存储容量对比如图 10 所示,相同区块数量下,边缘多链的存储容量消耗仅为传统单链的 18% 左右。

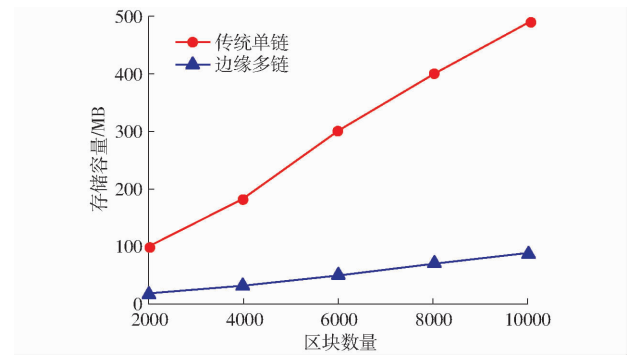


图 10 存储性能对比

Fig. 10 Storage performance comparison chart

通过产地区域划分水稻溯源,各产区边缘节点分布式独立存储溯源数据,缓解数据单链存储压力。追溯数据通过物联网设备采集,经边缘区块链节点处理后上传至所在区域的区块链网络,其中,单条溯源数据为 0.43 kB,由边缘区块链节点背书,经过智能合约上链生成新的区块。水稻原产地溯源场景下,由于边缘设备的性能限制,单链式溯源网络在满足联盟链架构基础上难以负载千万级数据存储需

求,多链存储网络通过通道隔离数据,能够满足水稻各产地区域海量溯源数据的存储需求。

5 结论

(1)提出了基于区块链和边缘计算的水稻原产地溯源模型,边缘节点将自身作为区块链节点,将水稻原产地溯源信息数据融合处理后上传至边缘侧区块链;通过产地经纬度划分产地区域构建边缘区块链网络,核心节点组建核心链负责各产地区域链的节点注册和账本备份。该研究解决了传统物联网区块链追溯系统数据来源中心化、通信延迟高以及云端资源消耗大等问题。

(2)在水稻原产地溯源模型中,通过区块链和边缘计算的部署,可以降低或防范一些潜在的安全风险。并成功地实现了原型,验证了本模型的可行性。测试结果表明,数据加密上链、公开数据查询、商业隐私数据解密查询的平均时延分别为 1.27 s、45.84 ms、50.92 ms,存储容量消耗为传统单链的 18%,系统具备良好的性能,能够满足水稻原产地溯源的需求,为边缘计算场景下区块链溯源系统的架构设计和存储容量扩展提供一定的借鉴与参考。

参 考 文 献

[1] 方福平,程式华. 水稻科技与产业发展[J]. 农学学报, 2018, 8(1): 100.
FANG Fuping, CHENG Shihua. The development of rice science, technology and industry in China[J]. Journal of Agriculture, 2018, 8(1): 100. (in Chinese)

[2] 冯玉超,杨宏志,安宇,等. 不同产地稻花香水稻代谢产物差异分析[J]. 食品工业科技, 2022, 43(1): 10-20.
FENG Yuchao, YANG Hongzhi, AN Yu, et al. Analysis on the difference of Daohuaxiang rice metabolites in different producing areas[J]. Science and Technology of Food Industry, 2022, 43(1): 10-20. (in Chinese)

[3] 马腾,孙传恒,李文勇,等. 基于 NB-IoT 的农产品原产地可信溯源系统设计与实现[J]. 中国农业科技导报, 2019, 21(12): 58-67.
MA Teng, SUN Chuanheng, LI Wenyong, et al. Design and implementation of trusted traceability system for agricultural products origin based on NB-IoT[J]. Journal of Agricultural Science and Technology, 2019, 21(12): 58-67. (in Chinese)

[4] 蔡晓晴,邓尧,张亮,等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI Xiaoqing, DENG Yao, ZHANG Liang, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131. (in Chinese)

[5] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)

[6] 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)

[7] 张奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020, 31(5): 1406-1434.
ZHANG Ao, BAI Xiaoying. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020, 31(5): 1406-1434. (in Chinese)

[8] 于华竟,徐大明,罗娜,等. 杂粮供应链区块链多链追溯监管模型设计[J]. 农业工程学报, 2021, 37(20): 323-332.
YU Huajing, XU Daming, LUO Na, et al. Design of the blockchain multi-chain traceability supervision model for coarse cereal supply chain[J]. Transactions of the CSAE, 2021, 37(20): 323-332. (in Chinese)

[9] 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)
- [10] 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)
- [11] FENG L, ZHANG H, LOU L, et al. A blockchain-based collocation storage architecture for data security process platform of WSN[C]//2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE, 2018: 75–80.
- [12] TIAN F. An agri-food supply chain traceability system for China based on RFID & blockchain technology[C]//2016 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016: 1–6.
- [13] 刘耀宗, 刘云恒. 基于区块链的 RFID 大数据安全溯源模型[J]. 计算机科学, 2018, 45(增刊 2): 367–368, 381.
- LIU Yaorong, LIU Yunheng. Security provenance model for RFID big data based on blockchain[J]. Computer Science, 2018, 45(Supp. 2): 367–368, 381. (in Chinese)
- [14] BORDEL B, LEBIGOT P, ALCARRIA R, et al. Digital food product traceability: using blockchain in the international commerce[C]//The 2018 International Conference on Digital Science. Springer, Cham, 2018: 224–231.
- [15] CARO M P, ALI M S, VECCHIO M, et al. Blockchain-based traceability in agri-food supply chain management: a practical implementation[C]//2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany). IEEE, 2018: 1–4.
- [16] LIN J, SHEN Z, ZHANG A, et al. Blockchain and IoT based food traceability for smart agriculture[C]//Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018: 1–6.
- [17] COCCO L, MANNARO K, TONELLI R, et al. A blockchain-based traceability system in agri-food SME: case study of a traditional bakery[J]. IEEE Access, 2021, 9: 62899–62915.
- [18] PINCHEIRA M, VECCHIO M, GIAFFREDA R. Benchmarking constrained IoT devices in blockchain-based agri-food traceability applications[C]//International Congress on Blockchain and Applications. Springer, Cham, 2021: 212–221.
- [19] HOU L, ZHENG K, LIU Z, et al. Design and prototype implementation of a blockchain-enabled LoRa system with edge computing[J]. IEEE Internet of Things Journal, 2020, 8(4): 2419–2430.
- [20] KONG W, LI X, HOU L, et al. A reliable and efficient task offloading strategy based on multi-feedback trust mechanism for IoT edge computing[J]. IEEE Internet of Things Journal, 2022, 9(15): 13927–13941.
- [21] 佟兴, 张召, 金澈清, 等. 面向端边云协同架构的区块链技术综述[J]. 计算机学报, 2021, 44(12): 2345–2366.
- TONG Xing, ZHANG Zhao, JIN Cheqing, et al. Blockchain for end-edge-cloud architecture: a survey[J]. Chinese Journal of Computers, 2021, 44(12): 2345–2366. (in Chinese)
- [22] SHI W, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637–646.
- [23] CHEN S, LI Q, ZHOU M, et al. Recent advances in collaborative scheduling of computing tasks in an edge computing paradigm[J]. Sensors, 2021, 21(3): 779.
- [24] MEHMOOD M Y, OAD A, ABRAR M, et al. Edge computing for IoT-enabled smart grid[J]. Security and Communication Networks, 2021, 2021: 1–16.
- [25] 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)
- [26] 殷昱煜, 叶炳跃, 梁婷婷, 等. 边缘计算场景下的多层区块链网络模型研究[J]. 计算机学报, 2022, 45(1): 115–134.
- YIN Yuyu, YE Bingyue, LIANG Tingting, et al. Research on multi-layer blockchain network model in edge computing[J]. Chinese Journal of Computers, 2022, 45(1): 115–134. (in Chinese)
- [27] 杨信廷, 钱建平, 张正, 等. 基于地理坐标和多重加密的农产品追溯编码设计[J]. 农业工程学报, 2009, 25(7): 131–135.
- YANG Xinting, QIAN Jianping, ZHANG Zheng, et al. Design of agricultural product trace coding based on geography coordinate and multi-encrypt[J]. Transactions of the CSAE, 2009, 25(7): 131–135. (in Chinese)
- [28] CASADO-VARA R, DE LA PRIETA F, PRIETO J, et al. Blockchain framework for IoT data quality via edge computing[C]//Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, 2018: 19–24.
- [29] 段杰, 姜岩, 唐勇伟, 等. 基于卡尔曼滤波算法的农业大棚数据融合处理技术研究[J]. 中国农机化学报, 2018, 39(5): 60–63.
- DUAN Jie, JIANG Yan, TANG Yongwei, et al. Research on data fusion processing technology of agricultural greenhouse based on Kalman filtering algorithm[J]. Journal of Chinese Agricultural Mechanization, 2018, 39(5): 60–63. (in Chinese)
- [30] 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 Jiwei, XING Bin, et al. Research of 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)