doi:10.6041/j.issn.1000-1298.2023.03.037

面向小麦区块链追溯系统的分级监管模型设计与实现

李修华[1]　罗　潜[1,2]　杨信廷[2,3]　罗　娜[2,3]　徐大明[2,3]　孙传恒[2,3]

(1.广西大学电气工程学院,南宁 530004;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研究中心,北京 100097)

摘要:针对现有的农产品溯源系统中数据监管存在的监管单一、权限集中,以及监管过程中隐私泄露等问题,通过研究小麦制粉行业全业务流程特性,设计并构建了面向小麦区块链追溯系统的分级监管模型。该模型以联盟链 Hyperledger Fabric 为基础构建多链架构,提出了基于密文策略属性加密(CP-ABE)技术的加密隐私密钥传输方法,通过一对多的加密属性设计多个数据监管部门,并在密文中嵌入访问结构实现权限管控。通过理论分析,所提出的分级监管模型能够在满足消费者追溯需求的基础上,实现企业隐私保护、分级授权管控、全流程穿透式实时监管的功能。在安全方面,该模型在控制策略保持不变的情况下,改变需加密密钥的任意一位,生成密文平均变化率为 95.5%;在保持密钥不变的前提下,通过改变企业授权访问策略,引起解密私钥平均变化率为 75.5%,具有较高的混淆性和安全性。在效率方面,所设计的分级监管模型公开溯源数据平均查询时延为 6.67 ms,隐私数据平均解密查询时延为 34.45 ms,数据监管平均查询时延为 37.78 ms。

关键词:小麦产品;溯源;权限管控;分级监管;区块链;多链

中图分类号:TP309.2;TS201.6　**文献标识码**:A　**文章编号**:1000-1298(2023)03-0363-09　**OSID**:

Design and Implementation of Blockchain Hierarchical Supervision Model for Wheat Supply Chain

LI Xiuhua[1]　LUO Qian[1,2]　YANG Xinting[2,3]　LUO Na[2,3]　XU Daming[2,3]　SUN Chuanheng[2,3]

(1. *School of Electrical Engineering*, *Guangxi University*, *Nanning* 530004, *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: Aiming at the problems of single supervision, centralized rights, and privacy leakage in the supervision process of the existing agricultural product traceability system, a blockchain hierarchical supervision model for wheat supply chain was designed and implemented after in-depth research on the characteristics of the whole business process of the wheat milling industry. In traditional traceability system of agricultural products, once there were problems such as product quality and privacy disclosure, it was difficult to precisely locate the responsibility, timely recall the products and prevent the information disclosure in time. Thus regulation was an indispensable part of the supply chain to ensure the integrity and legality of data. The above problems would be addressed to examine the application case of the Inner Mongolia's Zhaofeng Hetao Noodle Industry. Based on the multi-chain architecture of blockchain, the hierarchical supervision model of wheat authority control was designed and realized through Hyperledger Fabric of the alliance chain. The enterprise traceability data was open and transparent, and the privacy data was encrypted then uploaded to the blockchain. Privacy keys were encrypted and transmitted through the Ciphertext-Policy Attribute-Based Encryptionto achieve privacy protection and fine-grained control of data for enterprises. The traceability code was used as the traceability key value, which was stored in the blockchain together with the regulatory results. After proliferation test, the average change rate of the cipher text was 95.5% by changing any bit of the key to be encrypted while the control policy remained unchanged and the average change rate of the private key was 75.5% by changing the access policy while

收稿日期:2022-06-02　修回日期:2022-07-15

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:李修华(1983—),女,副教授,博士,主要从事作物检测和农业物联网研究,E-mail:lixh@gxu.edu.cn

通信作者: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

keeping the key unchanged, which possessed high security and confusion. After performance testing, the average query latency of the hierarchical supervision model designed was 6.67 ms for public traceability data, 34.45 ms for privacy data decryption, and 37.78 ms for data supervision, which can meet the actual application requirements of wheat. Theoretical analysis and experiments showed that the hierarchical supervision model proposed can achieve privacy protection, hierarchical authorized supervision, and real-time supervision of the whole process. On the premise of ensuring the independent operation of each module, it can strengthen information interconnection which had strong practicality.

Key words: wheat products; traceability; authority-control; hierarchical supervision; blockchain; multi-chain

0 引言

近年来食品添加剂滥用、重金属、农药、土壤污染等形式的污染引起的小麦及其制品安全问题受到了广泛关注[1-3]。可追溯性系统是解决食品安全问题的一个重要工具[4]。通过追踪和回溯生产、加工、仓储、配送及销售等多个环节中的食品信息，可追溯性系统能够有效监控食品的整个生产经营活动[5-6]。区块链是基于密码学的多方维护的链式存储结构，具有数据安全性强、信息开放度高、正向一致存储、逆向可追溯性等特点[7-8]。将区块链技术嵌入农产品供需网中可实现小麦“从农田到餐桌”全方位、多维度、高透明的高效追溯方式，具有区块链的底层技术优势和供应链的组织结构优势[9-10]。然而，区块链技术的去中心化与高度自治的特性使得上链数据的合法性难以得到监管，制约了农产品追溯行业的可持续性发展[11]。

传统追溯模型中存在的监管不规范性[12]、单一监管权限过度集中[13]、监管数据恶意泄露[14]、单方违约的安全风险[15]等都会引起隐私保护危机，因此基于区块链的分级监管追溯模型设计研究是有必要的。近年来，监管追溯模型的研究致力于解决隐私数据保护以及监管的问题：文献[16]采用区块链双层架构，使监管部门通过参与追溯过程的方式实现对整个供应链的监管；文献[17]提出了基于多链架构的网络准入机制，监管部门可以通过审核建链资质的方式来管控企业操作账本权限从而实现上链监管；文献[18]提出了将隐私数据进行混合加密的方式，通过节点间的差异化来兼顾监管与企业隐私保护两方面的需要。文献[19]提出了编码方案探讨未取得厂商注册码的中小企业及个体户身份识别方法，建立高效的信息关联媒介，解决信息传递的问题；文献[20]通过区块链构建稻米供应链信息监管模型，通过隐私数据分级加密和定制化监管合约解决稻米供应链数据的隐私加密、安全存储以及管理权限等问题；文献[21]提出了一种基于区块链的个人数据安全共享方案，该方案以用户为中心通过分发密钥的方式实现了数据所有者对数据的细粒度访问控制；文献[22]提出了农产品质量安全的可信溯源系统，通过制定多主体共识和智能合约规则集保证溯源信息的真实可靠和节点间的数据安全；文献[23]针对数据存证、数据源头设备等的不可信，提出了畜牧资产认证方案，通过对密文数据和签名打包后进行签名聚合操作实现资产监管的身份认证；文献[24]通过分布式多密钥生成协议和一些密码原语，构建了一个非交互式可验证多秘密共享方案，实现了具有监管功能的可追溯性方案。这些方案部分解决了隐私数据隐私保护以及监管的问题，却很少有考虑到由于单一监管所带来的权限集中和密钥泄露以及单方面违约所带来的安全风险，此外，企业隐私数据的密钥传输和数据所有权的管控以及信息的互通互联等问题还需要进一步研究。

针对上述问题，本文通过深入分析小麦制粉行业全流程供应链的生命周期，提出基于区块链的小麦分级监管模型。企业将隐私数据加密上链，密钥通过基于密文策略属性加密算法加密传输并在加密过程中嵌入访问结构来实现数据细粒度管控，确保仅当监管的属性满足密钥密文访问结构时才能解密密钥进而监管隐私数据，监管结果与溯源编码 Key 值上链存证；各阶段溯源编码以全球统一标识系统中的全球贸易项目代码为基础并进行扩展，相关信息写入射频识别标签中，随小麦产品一起在供应链中流通；设置多级监管解决权限集中以及单点故障等问题，实现全供应链上数据的互通互联、权限管控与有效监管。

1 小麦供应链关键信息分析和多链模型架构

1.1 小麦追溯关键环节及数据分析

在集成化的小麦产品销售过程中，涉及企业的进货成本、加工配料等数据属于商业机密[25]。为了保证上下游企业数据真实性以及企业的隐私安全，将企业数据划分为共享数据和一、二级隐私数据（表 1），共享数据公开透明，隐私数据分级监管。

表 1　供应链各环节关键信息

Tab. 1　Key information of supply-chain

生产信息	数据采集设备	共享数据	一级隐私数据	二级隐私数据
种植	摄像头、传感器、GPS 等	种子来源、小麦种类、环境信息、防疫信息、产品检验信息(农药残留、产品品质等)等	种子价格等	种植农户个人信息、联系方式、许可信息等
收储	摄像头、传感器、GPS、检验设备等	收储前后含水率、收储来源、收储温湿度、环境信息、收储时间、质检编号等	工人工资、收储成本等	仓储位置、仓库管理人员信息、仓库管理等
加工	摄像头、加工仪器、传感器、GPS、检验设备等	润麦加水率、碾磨方式、平筛孔径、清粉次数、配粉含量、包装信息等	原材料价格、加工成本等	加工配比、加工负责人信息等
运输	摄像头、温湿度传感器、GPS、标签扫描设备等	运输路线、通风情况、运输车辆类型、运输时间、病菌生成情况等	运输成本等	驾驶员信息、车牌号、订单信息、运输数量
销售	摄像头等	货物来源、保存情况、营业执照等	进货成本等	数量、销售人员信息

1.2　小麦多链模型构建

我国小麦溯源链拥有多环节、多主体、多数据的特点。然而，现有的溯源系统往往是“单链溯源”，企业将“农田到餐桌”的所有产品信息都上传到区块链，不仅加重了区块链的数据存储压力，造成容量问题，也容易导致企业隐私数据泄露等问题。本文提出基于联盟链通道技术构造的区块链多链架构(图 1)，解决单链溯源所存在的问题。主要的特点包括：为小麦制粉过程中的生产、加工、仓储、物流以及分销等环节设置一条企业隐私链，用于存储企业隐私信息；将企业追溯节点、监管节点和消费者节点联合共同建立联盟追溯链，用于存储链上公开溯源信息；监管节点设置监管链，用于监管信息索引存证。

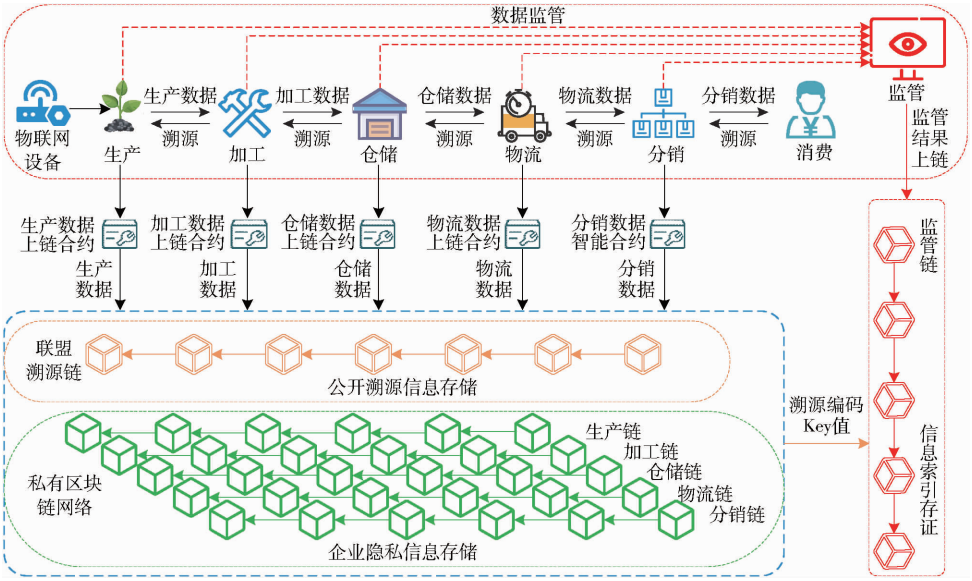


图 1　小麦供应链多链追溯架构

Fig. 1　Blockchain multi-chain architecture for supply chain traceability of wheat

为确保追溯网络的安全、稳定、可持续性发展，供应环节内某一企业追溯节点获得建链资质并搭建企业隐私链，组成私有区块链网络。每个环节内一或多个企业作为节点发起上链请求，同类多家企业共同备份隐私信息密文，通过通道的天然隔离性来实现数据的隔离存储，保证数据隐私安全；用于追溯的联盟溯源链内，存储可公开溯源信息，提供链间交易的安全环境，实现链间交易留痕管控和数据交互共享；在监管链中，溯源编码作为各阶段链上“键值对”的追溯 Key 值，由各个节点以“键值对”的形式更新状态数据库，并与监管信息一同写入监管链中索引存证，为数据穿透式全程监管提供有力支撑。

2　小麦分级监管模型设计

2.1　编码设计

GS1 全球统一标识系统(Global standards 1，GS1)也称 EAN. UCC 标识系统[26]，本文以该系统中全球贸易项目代码(Global trade item number，GTIN)为基础进行扩展，实现“一环一码”的编码方式，并结合射频识别技术(Radio frequency identification，RFID)[27-28]，将其应用到小麦溯源系统中。以生产阶段编码为例(表 2)，如第 003 区域 0006 田 2022 年 1 月 5 日播种，3 月 22 日收获，负责人为 056，则生产阶段编码(共 36 字符)为(01)9 6932306

表 2 生产阶段编码

Tab. 2 Production code

AI	指示符	厂商识别码	项目代码	校验位	AI	田间区域	田间编号	种植日期 + 采收日期	AI	负责人
01	N1	N2 N3 N4 N5 N6 N7 N8	N9 N10 N11 N12 N13	N14	10	A1 A2 A3	A4 A5 A6 A7	A8 A9 A10 A11 A12 A13 A14 A15 A16 A17 A18 A19	91	A20 A21 A22

123456 9 (10)003 0006 220105 220322 (91)056。

“产加储运销”5 个环节所对应的编码与最终形成的二维码类似树形结构,各个阶段编码为树权,最终二维码为树根,本阶段溯源编码作为链上“键值对”的追溯 Key 值(表 3),将产品数据以“键值对”的形式添加至世界状态数据库,将返回的交易哈希、区块高度存入对应的状态索引数据库,利用索引查询提升查询效率。将该编码方案应用到各个环节中,解决“一码到底”导致的信息丢失,实现数据自动化识别,有效提高系统的运行效率,为穿透式全程监管提供基础。

表 3 链上追溯数据 Key 值

Tab. 3 Key-value traceability data of blockchain

追溯数据键 Key 值	Key 值	交易哈希	区块高度
产品 ID:(01)9 6932306 123456 9 (10)003 0006 220105 220322 (91)	(01) 9 6932306 123456	4a7bbed769d5a7290e3f6b	
056|生产企业:内蒙古兆丰河套面业|生产批次:prod_batch_123456|	9 (10)003 0006 220105	282b1c40cf2fe19f74be17b	5 782
种子来源:采购|生产数据:生产环节追溯数据|农药用量:1 kg	220322 (91)056	3157cbebff4f94a258c	

2.2 分级监管模型设计

为解决单一监管所存在的单点故障、隐私泄露、权限管控等问题,在监管过程中设置多级监管(图 2)。追溯节点由某一环节内同类型的多家企业选举产生;监管节点由监控中心、最高监管部门等具有公信力、权威力的机构担任,作为一级监管机构(监管价格信息等),掌握主私钥。二级监管主要由监管者(监管交易记录、用户数据等)、中间方(监管抽检记录、质量信息等)、委托方(监管危害信息、许可信息等)等担任,通过一级监管机构下发获得从私钥,进而监管符合其属性的隐私数据并将结果上链存证。

基于属性加密算法是在文献[29]提出的基于身份加密算法的基础上发展起来的,本文借鉴基于密文策略的属性加密(Ciphertext-policy attribute-based encryption, CP-ABE)技术[30],并结合实际情况设置不同的访问策略。各企业在获得一级监管机构建链资质的前提下搭建私链,将企业隐私数据密文上传至该链中实现隐私保护,并通过监管中心广播的公钥对隐私数据密钥进行 CP-ABE 加密并在加密过程中设置访问策略实现权限管控,其访问策略中需包含一级监管机构,只有满足企业准入授权的监管机构才有相关权限对数据进行监管。一级监管机构建立沟通渠道,按一定规则将解密私钥分发给满足要求的二级监管者,监管者在获得私钥与企业授权监管的情况下对隐私数据解密并监管,同时将监管信息与溯源 Key 值上传至监管链中索引存证,保证监管的有效性。

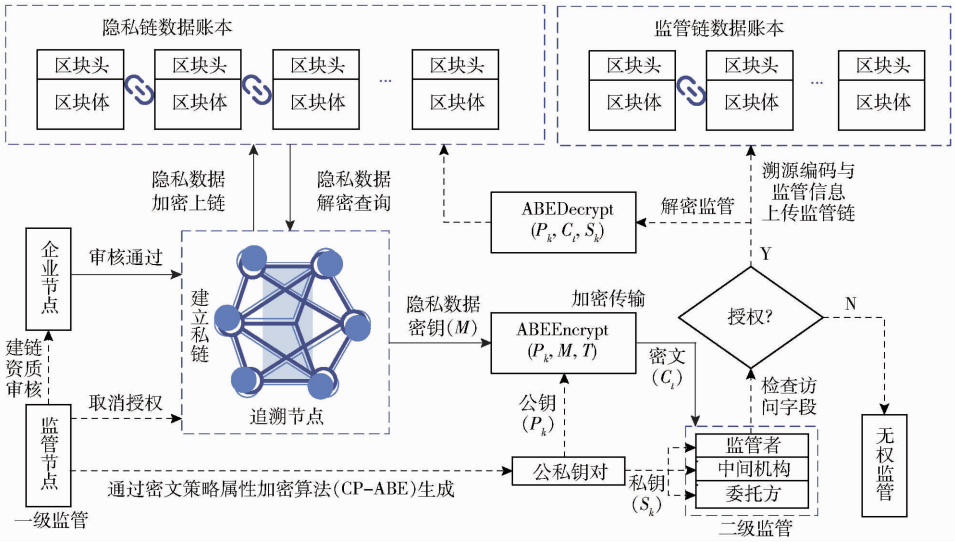


图 2 基于访问策略的分级监管模型

Fig. 2 Hierarchical supervision model based on access policy

CP－ABE 是一种公钥加密算法，与对称加密算法（Advanced encryption standard，AES）和椭圆曲线加密算法（Elliptic curve cryptography，ECC）不同的是，它是一种一对多的加密方案，还具有一定的容错能力[31]，在该加密算法中，访问策略嵌入在密文中，用户的属性嵌入解密私钥中，为实现数据的细粒度访问控制提供了基础。

CP－ABE 包含了 4 个基本算法：*Setup*，*Encrypt*，*KeyGen*，*Decrypt*，表示为

$$A=(Setup,Encrypt,KeyGen,Decrypt) \tag{1}$$

监管机构将安全参数 d 作为输入，系统设置算法输出加密公钥 P_k 和主私钥 M_k，记为

$$Setup(d)\rightarrow(P_k,M_k) \tag{2}$$

各企业获取由一级监管机构广播的公钥 P_k，将隐私数据密钥作为明文信息 M，通过访问结构 T 来制定密文访问策略，加密后输出的密文 C_t 发送给各个监管者，只有满足访问策略的监管者或中间机构才能解密密文，记为

$$Encrypt(P_k,M,T)\rightarrow C_t \tag{3}$$

一级监管机构根据主私钥 M_k 和属性集合 S，输出解密私钥 S_k，私钥中包含访问策略的用户属性，并按一定规格通过监管通道发送给二级监管机构，记为

$$KeyGen(M_k,S)\rightarrow S_k \tag{4}$$

二级监管机构收到企业发送的包含访问结构 T 的密文 C_t 以及通过监管通道获得的解密私钥 S_k 之后，判断是否被企业授权监管隐私数据，若未授权则返回失败，若已经授权则可对隐私数据进行解密获得隐私数据 *Info* 并监管，同时将溯源编码和监管信息上传至监管链中，记为

$$Decrypt(P_k,C_t,S_k)\rightarrow M\rightarrow Info \tag{5}$$

2.3　智能合约设计

智能合约作为一种计算机协议，在满足触发条件的情况下具有自动校验、执行合约逻辑并且不可逆等功能[7]。此次工作具体合约业务逻辑如表 4 所示。

表 4　智能合约设计

Tab.4　Design of smart contract

合约功能	合约业务逻辑	合约方法	描述
数据上链	公开数据上链	AddPubData( )	审查数据内容、格式是否符合上链要求
	隐私数据上链	AddPriData( )	以溯源编码作为上链 Key 值，通过混合加密方式上传隐私信息密文
控制策略	企业授权访问	EncryptPriKeyPolicy( )	各个企业通过不同的属性来规定密文访问结构，更改策略可以回收访问权限
	监管者权限解密	DecryptPriKeyPolicy( )	监管者在其属性符合密文中的访问结构时能解密密文从而获得隐私数据监管权限
数据查询	溯源数据查询	TracePubData( )	消费者扫描最终二维码，通过消费者节点查询全生命周期内的公开溯源数据
	隐私数据查询	TracePriData( )	监管机构在获得隐私数据监管权限条件下，解密查询实现对隐私数据监管

本文主要通过 CP－ABE 算法加密隐私密钥实现数据的权限管控、分级监管。为保证链上密文的安全性，通过对称加密和椭圆曲线混合加密的方式[18]，在隐私数据上链之前，采用对称加密算法 AES 对其进行加密，并通过智能合约自动生成的 ECC 公钥加密 AES 密钥后实现密文上链，用于解密的隐私密钥 M 利用 CP－ABE 公钥加密传输。控制策略算法和解密监管算法如下：

算法 1：控制策略算法

输入：隐私数据密钥 M，访问结构 T，随机数 d，属性集合 S，隐私数据 *Info*

输出：成功返回密文，失败则返回失败原因

1. 各环节内企业申请建立私链资质，监管机构按一定的规则进行审核，审核通过授予建链资格 Qualify 和用来加密的公钥 P_k

2. If(Qualify是否有效 & 是否建链 & 溯源编码 ProduceId 是否符合标准)

3. if (! getState(Info.id)) // 隐私密文是否已经上链

4. AESEncrypt(Info,key)→AesKey; // 获得 AES 密钥值

5. ECCEncrypt(AesKey,publicKey)→EncryPriData; // ECC 公钥加密获得隐私密文

6. stub.PutState(id, EncryPriData);隐私密文上链

7. Setup(d)→P_k,M_k; // 获得 ABE 算法公钥 P_k 和主私钥 M_k

8. KeyGeneration(M_k,S)→S_k; // 通过主私钥 M_k 和属性集合 S 生成解密从私钥

9. ABEEncrypt(P_k, M,T)→C_t; // 获得密钥加密后密文 C_t

10. else

11. return error; // Qualify 验证不成功

12. return success;

控制策略算法中第 1～2 步对上链请求合法性进行验证，第 3～6 步实现隐私数据密文上链，第 7～12 步面向企业返回隐私密钥加密后密文，面向监管返回隐私密钥解密私钥，失败返回失败原因。

算法 2:解密监管算法

输入:建链成功标志 SuccBuild,监管属性集合 S,密钥加密后密文 C_t,私钥 S_k,隐私密文 EncryPriData

输出:成功返回隐私数据,失败则返回失败原因

1. 监管节点 peer 发起隐私数据监管请求
2. if(S 在授权集合中 &SuccBuild 验证成功)
3. if (function == TracePriData&! getState (TraceCode) //验证编码的准确性
4. 根据监管的等级判断访问合法性
5. if(! isEmpty(C_t)&&! getState(id))
6. ABEDecry(P_k,C_t,S_k)→M;//获得隐私数据密钥
7. decryptPridata(EncryPriData,M)→Info; //隐私数据获取
8. else
9. return error;
10. else
11. return error; //失败返回
12. return success;

解密监管算法中第 1 ~ 3 步对数据监管请求合法性进行验证,第 4 ~ 5 步对监管等级进行验证,第 8 ~ 12 步成功返回隐私数据,失败返回失败原因。

3 性能与安全性分析

3.1 测试环境

通过虚拟机 VMware12 搭建 Ubuntu 16.04 Linux 系统,并搭建联盟链 Hyperledger Fabric v1.4.4 测试环境。虚拟机的配置为:8 核处理器、60 GB 存储容量、4 GB 内存。测试数据来源于内蒙古兆丰河套面业追溯平台,测试结果均通过区块链基准测试工具 Hyperledger Caliper 生成。本系统共包含 7 个组织,每个组织中包含 4 个节点,联盟追溯链中除各企业节点外还包含消费者节点,所有节点数据账本采用外部状态数据库 CouchDB,通过“键值对”的方式查询账本;建立的分级监管追溯模型采用 Raft 共识机制实现共识,每一条链运行 Raft 协议的单独实例,通过使用心跳机制选取主导节点并由主导节点进行广播、记账和验证,当主导节点断开连接时,由链内排序节点重新选取,并对此期间的操作进行回滚撤销,提高系统容错能力。测试环境具体的配置如表 5 所示。

3.2 安全性分析

为验证所提出的分级监管模型的安全性,经扩散性测试,在控制策略保持不变的情况下,通过改变隐私数据解密密钥(即明文 M)的任意一位,引起的 CP-ABE 加密后密文变化率如图 3a 所示,解密密钥的改变引起的密文平均变化率达到 95.5%;经相关性测试,在保持隐私数据密钥不变的前提下,通过改变企业授权访问策略(即访问结构 T),引起解密私钥变化率如图 3b 所示,其不相关性平均为 75.5%。测试结果得出所用的加密算法具备较高的混淆性以及安全性。

表 5 区块链配置

Tab.5 Configuration of blockchain

设置	值	备注
共识机制	raft	允许网络不大于 1/2 的节点宕机,使用心跳机制来触发 leader 选举
链数	7	监管链、生产链、加工链、仓储链、物流链、分销链、溯源链
节点数	28	每个组织中包含 4 个节点
数据库	28	各企业节点、消费者节点以及监管节点均配置 CouchDB 状态数据库
出块时间/ms	500	生成区块时间,排序节点通过出块时间间隔检测缓存数据
区块最大交易数	100	区块能接受的最大交易数量
区块容量/MB	100	区块所能接受的最大容量

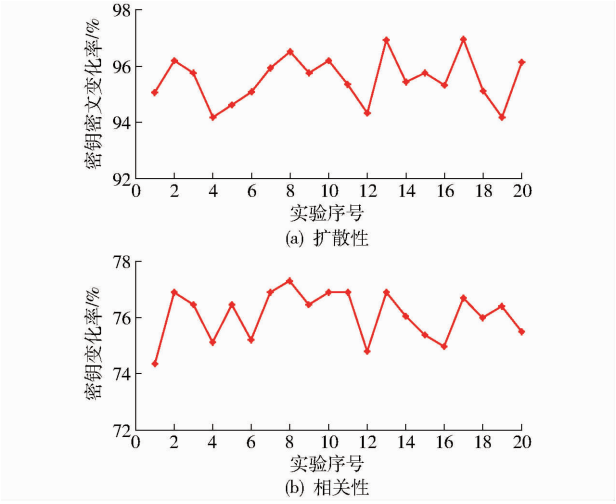


图 3 权限管控授权算法安全性测试

Fig.3 Authority-control security of authorization algorithm

3.3 效率分析

为查看所提出的分级监管模型的系统效率,本文主要以消费者溯源数据查询时延、企业隐私数据查询查询时延以及监管数据的监管查询时延进行测试。为排除数据的随机性与不真实性,对 600 个不同的数据进行了 20 轮测试并取其平均值,结果如图 4 所示。对于消费者节点,图 4a 中传统的迭代查询方法平均查询时延为 33.33 ms,本文所用的通过 5 个编码进行查询的方法平均查询时延为 6.67 ms;图 4b 中,各环节内企业对于本企业内的隐私数据的查询时延平均为 34.45 ms,监管部门通过解密隐私数据密钥对数据监管的时延平均为 37.78 ms。测试结果得出本文缩短了公开数据查询时延约 26.66 ms,增加的监管平均时延为 3.33 ms,能够满足实际应用需求。

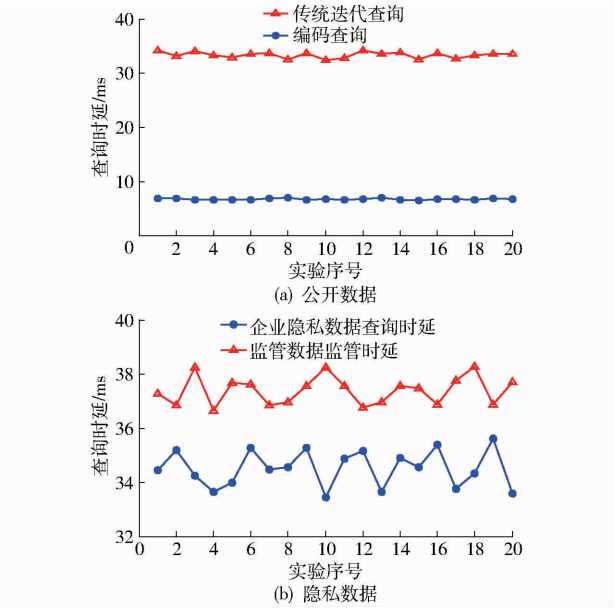


图 4　数据查询性能测试

Fig. 4　Latency of querying data from blockchain

由理论分析和测试结果可以得出，本文在保证各个环节独立运行的条件下，实现编码、溯源、监管的良性互动。安全性方面，通过链前监管合约保证上链编码 Key 值的规范性，监管信息以及 Key 值上链存证保证溯源数据的安全可靠，以密文上链的方式确保隐私数据的安全隐私性，解密密钥通过 CP－ABE 加密传输，提高了隐私密钥的传输安全性。效率方面，与传统的迭代查询相比，通过扫码获得 5 个编码的方式可以大大提高公开数据的查询效率；通过在密文中嵌入访问结构保证数据访问的权限控制，增加了企业对于监管部门的访问策略，实现了企业对隐私数据的细粒度管控，同时具有较好的查询效率。

4　应用案例分析

通过对小麦制粉产品的实地调研，开发了面向小麦全过程正向跟踪、逆向溯源的区块链追溯平台。以内蒙古兆丰河套小麦为例，消费者通过手机设备扫描追溯二维码（图 5a）获得 5 个阶段追溯编码，通过追溯编码调用追溯合约查询联盟溯源链账本，获取公开溯源数据。图 5b 展示了高筋小麦粉的基本介绍，通过扫码次数以及追溯码确保小麦产品“一物一码”以及溯源码的不可复用性；图 5c 展示了“产、加、储、运、销”全流程溯源信息，通过视频监控、传感器采集、定位追踪、智能化识别等多种物联网设备实时采集小麦全生命周期的视频图像、地理位置、农药化肥等产品操作信息和温湿度、风速光照、呼吸水分等产品生产信息，保证高品质小麦源头的信而有证；图 5d 展示了区块链上数据的溯源防伪信息，主要包括区块高度、追溯 Hash 以及访问地址，确保数据不被篡改。

目前该追溯平台共处理了 235 201 笔交易，生成了 154 655 个区块，监管机构通过链上数据交互记录不可篡改的特性管控上下游交易行为（图 6a）。监管机构满足企业隐私数据的授权策略时通过交易地址或者区块高度解密查询，从而实现数据监管，链上存证信息如图 6b 所示。通过应用该追溯平台，保证了小麦产品质量，提高了产品销量，增强了市场竞争力。

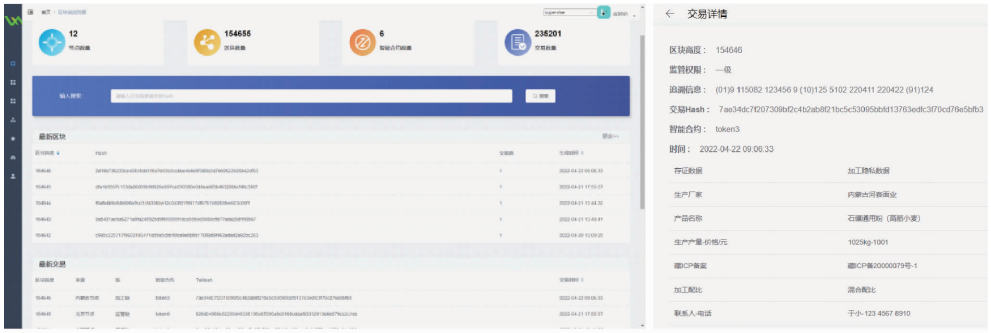
5　结束语

通过多链并行操作来实现不同数据的差异化存储，增加存储容量，提升系统运行效率。隐私数据密文上链，隐私密钥加密传输，提升传输安全性的同时通过访问权限实现隐私数据细粒度管控。一级监管授权企业建链资质，审计上链资格、内容与格式，二级监管通过属性集合满足访问策略来获取监管权限，从而实现隐私数据差异化的监管

(a) 小麦溯源二维码　(b) 产品介绍　(c) 溯源信息　(d) 防伪信息

图 5　手机溯源界面

Fig. 5　Tracing source of wheat products by mobile phone



(a) 区块链数据交互监管界面 (b) 隐私数据监管详情

图 6 小麦区块链溯源系统界面

Fig. 6 Blockchain traceability system for wheat products

与访问，监管结果上链存证，确保各个模块独立运行，实现编码、上链、溯源与监管模块之间的良性互动。所提出的分级监管方案，扩散性测试中平均密文变化率为 95.5%，相关性测试中私钥平均变化率为 75.5%，消费者追溯公开数据的平均时延为 6.67 ms，企业获取企业内隐私数据的平均时延为 34.45 ms，监管企业隐私数据的平均时延为 37.78 ms。所构建的小麦分级监管模型，面向监管能够解决监管难度大，监管过程中隐私泄露以及单一监管过度集中等问题；面向企业能够解决企业间隐私数据保护、需监管数据细粒度管控等问题。

参 考 文 献

[1] 尚艳娥. 小麦及其制品质量安全风险及控制[J]. 食品科学技术学报, 2016, 34(4): 7 – 11.
SHANG Yan'e. Safety risk and its control of wheat and wheat products[J]. Journal of Food Science and Technology, 2016, 34(4): 7 – 11. (in Chinese)

[2] AHMAD M N, ZIA A, VANDEN B L, et al. Effects of soil fluoride pollution on wheat growth and biomass production, leaf injury index, powdery mildew infestation and trace metal uptake[J]. Environmental Pollution, 2022, 298(1): 118820.

[3] 史雪岩, 李红宝, 王海光, 等. 我国小麦病虫草害防治农药减施增效技术研究进展[J]. 中国农业大学学报, 2022, 27(3): 53 – 62.
SHI Xueyan, LI Hongbao, WANG Haiguang, et al. Progress of pesticide reduction techniques in wheat production and the synetgistic effects on the prevention and control of wheat pests[J]. Journal of China Agricultural University, 2022, 27(3): 53 – 62. (in Chinese)

[4] STANISLAWEK M, MIARKA D, KOWALSKA H, et al. Traceability to ensure food safety and consumer protection as typified by case studies of three meat processing plants[J]. South African Journal of Animal Science, 2021, 51(2): 241 – 249.

[5] GALLO M, FERRARA L, CALOGERO A, et al. Relationships between food and diseases: what to know to ensure food safety [J]. Food Research International, 2020, 137(3): 109414.

[6] SUN S, WANG X. Promoting traceability for food supply chain with certification[J]. Journal of Cleaner Production, 2019, 217(6): 658 – 665.

[7] 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)

[8] 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 Mathinery, 2021, 52(1): 1 – 13. (in Chinese)

[9] 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)

[10] 何静, 胡鑫月. 区块链赋能食品供需网创新追溯模式[J]. 中国农业大学学报, 2021, 26(9): 257 – 265.
HE Jing, HU Xinyue. Innovative traceability model of the food supply and demand network enabled by blockchain[J]. Journal of China Agricultural University, 2021, 26(9): 257 – 265. (in Chinese)

[11] WEN B, WANG Y, DING Y, et al. A privacy-preserving blockchain supervision framework in the multiparty setting[J]. Wireless Communications and Mobile Computing, 2021,2021: 5236579.

[12] HONG W, MAO J, WU L, et al. Public cognition of the application of blockchain in food safety management—data from China's Zhihu platform[J]. Journal of Cleaner Production, 2021, 303(14): 127044.

[13] SHAN S, DUAN X, ZHANG Y, et al. Research on collaborative governance of smart government based on blockchain technology: an evolutionary approach[J]. Discrete Dynamics in Nature and Society, 2021,2021: 6634386.

[14] YANG H, XIONG S, FRIMPONG S A, et al. A consortium blockchain-based agricultural machinery scheduling system[J]. Sensors, 2020, 20(9): 2643.

[15] XUE Z, WANG M, ZHANG Q, et al. A regulatable blockchain transaction model with privacy protection[J]. International Journal of Computational Intelligence Systems, 2021, 14(1): 1642 - 1652.

[16] DING Q, GAO S, ZHU J, et al. Permissioned blockchain-based double-layer framework for product traceability system[J]. IEEE Access, 2019, 8: 6209 - 6225.

[17] 霍红,詹帅. 集成供应链视角下农产品质量安全全过程监管体系构建[J]. 中国科技论坛,2019(8):105 - 113.
HUO Hong, ZHAN Shuai. Construction of a whole-process supervision system for the quality and safety of agrifood from the perspective of integrated supply chain[J]. Forum on Science and Technology in China, 2019(8): 105 - 113. (in Chinese)

[18] 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 block chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(8): 328 - 335. (in Chinese)

[19] 郑立华, 冀荣华, 王敏娟, 等. 农产品追溯统一编码方案设计与应用[J]. 农业机械学报, 2019, 50(1): 385 - 392.
ZHENG Lihua, JI Ronghua, WANG Minjuan, et al. Design and application of traceable unified coding scheme for agricultural products[J]. Transactions of the Chinese Society for Agricultural Machinery, 2019, 50(1): 385 - 392. (in Chinese)

[20] 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.
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. (in Chinese)

[21] GAO H, MA Z, LUO S, et al. BSSPD: a blockchain-based security sharing scheme for personal data with fine-grained access control[J]. Wireless Communications and Mobile Computing, 2021,2021: 6658920.

[22] 刘双印, 雷墨鹭兮, 徐龙琴, 等. 基于区块链的农产品质量安全可信溯源系统研究[J]. 农业机械学报, 2022, 53(6): 327 - 337.
LIU Shuangyin, LEI Moyixi, XU Longqin, et al. Development of reliable traceability system for agricultural products quality and safety based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(6): 327 - 337. (in Chinese)

[23] 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. 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)

[24] MA T, XU H, LI P. A blockchain traceable scheme with oversight function[C]// International Conference on Information and Communications Security. Springer, Cham, 2020: 164 - 182.

[25] 李旭东, 杨千河, 姚竟发, 等. 基于区块链的农产品溯源技术研究综述[J]. 江苏农业科学,2022, 50(6): 16 - 24.
LI Xudong, YANG Qianhe, YAO Jingfa, et al. Study on traceability technology of agricultural products based on blockchain: a review[J]. Jiangsu Agricultural Science, 2022, 50(6): 16 - 24. (in Chinese)

[26] DENG M L, FENG P. Research on a traceability scheme for a grain supply chain[J]. Journal of Sensors, 2021,2021: 8860487.

[27] ZHENG M, ZHANG S, ZHANG Y, et al. Construct food safety traceability system for people's health under the internet of things and big data[J]. IEEE Access, 2021, 9: 70571 - 70583.

[28] WANG L, HE Y, WU Z. Design of a blockchain-enabled traceability system framework for food supply chains[J]. Foods, 2022, 11(5): 744.

[29] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]// Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008: 417 - 426.

[30] YAN B, DONG A, CHAI B, et al. Blockchain-assisted collaborative service recommendation scheme with data sharing[J]. IEEE Access, 2021, 9: 40871 - 40883.

[31] BUTERIN V. A next-generation smart contract and decentralized application platform[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper.