doi:10.6041/j.issn.1000-1298.2023.04.044

面向追溯主体的果蔬全供应链区块链多链模型研究

孙传恒[1]　万宇平[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中心，北京 100097）

摘要：面向全供应链环节建立的农产品区块链溯源系统，追溯链中存储面向多个追溯主体的追溯数据，由于各主体追溯数据的差异化，跨供应链环节的数据难以实现共享和访问控制，敏感数据无法差异化保护和验证，风险数据不能针对性监管。因此，面向不同追溯主体的追溯数据并不适合由同一条区块链账本存储。通过分析果蔬全供应链各追溯主体的需求，建立了面向追溯主体的区块链多链追溯架构，利用溯源链实现消费者的溯源需求，通过共享链实现上下游企业间的数据流转，基于隐私链实现企业隐私数据的安全保护与授权共享，利用监管链实现监管部门对所有环节风险数据的管控。本文基于 Hyperledger Fabric 设计面向追溯主体的果蔬供应链区块链模型并实现了主体链果蔬溯源系统，测试结果表明，溯源链中追溯数据平均查询时间为 38.86 ms，获取共享链中已验证的共享数据平均耗时 806.80 ms，获取隐私链中已验证的隐私数据平均耗时 910.35 ms，获取监管链中已验证的监管数据平均耗时 675.90 ms。面向追溯主体建链的追溯系统在满足消费者需求的基础上，实现了供应链各环节追溯数据的数据共享与控制访问，解决了异构数据的存储保护和验证问题，满足了风险追溯数据针对性的监管需求，为果蔬区块链溯源模型设计提供了参考和借鉴。

关键词：果蔬追溯；追溯主体；多链；数据共享；数据监管；Hyperledger Fabric

中图分类号：TP309.2；TS201.6　　**文献标识码**：A　　**文章编号**：1000-1298(2023)04-0416-12　　**OSID**：

Blockchain Multi-chain Model of Fruit and Vegetable Supply Chain for Traceability Subjects

SUN Chuanheng[1]　WAN Yuping[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: In recent years, agricultural food safety problems have occurred frequently, which seriously infringe on people's health. Due to the traceability feature of blockchain technology, the agricultural food traceability system based on blockchain was introduced, aiming to better supervise all traceability data generated in the supply chain and ensure food safety. The multi-chain traceability system of agricultural food was established for the whole supply chain. It stored traceability data for multiple participating subjects in blockchain. Due to the difference of traceability demand data of each subject, it was difficult to realize data sharing and access control across supply chain links, it was also difficult to protect sensitive data in a differentiated way, and risk traceability data cannot be subjected to targeted supervision. Therefore, the traceability data for different subjects was not suitable to be stored in the same ledger. Based on this idea, a subject-oriented chain building method was proposed, in which the traceability data for different traceability participating subjects were stored in different blockchains. By analyzing the traceability subjects in the fruit and vegetable supply chain, a multi-chain traceability architecture was established based on the traceability participating subjects. The traceability demand of consumers were realized through the traceability chain, the data flow among enterprises was realized through the sharing chain, the security protection and authorization sharing of the enterprise's private data

收稿日期：2022-06-07　修回日期：2022-07-04

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

were realized based on the privacy chain, and the regulatory chain was used to realize the management and control of risk data in all links by the regulatory authorities. A subject-oriented multi-chain traceability system was designed and implemented based on Hyperledger Fabric. A suitable storage scheme was designed according to the characteristics of each blockchain. At the same time, in order to ensure the authenticity of the data obtained by each subject after data sharing, a collaborative verification method was proposed to achieve this purpose. The test results showed that the average query time of the traceability chain was 38.86 ms, the average time to obtain real shared data was about 806.80 ms, the average time to obtain real private data was about 910.35 ms, and the average time to obtain real regulatory data was about 675.90 ms. The subject-oriented chain building traceability system solved the problems existing in the previous blockchain multi chain system on the basis of realizing the traceability requirements of each subject, and provided reference significance for fruit and vegetable blockchain traceability system.

Key words: fruit and vegetable traceability; traceability subject; multi-chain; data sharing; data regulatory; Hyperledger Fabric

0　引言

区块链是一种以点对点传输、共识机制、哈希算法、密码学、智能合约等技术为核心的分布式账本[1]，具有去中心化、不可篡改、开放性、可追溯的特点[2]。区块链的技术特点使其具有普适性的底层技术框架[3]，数据可追溯和不可篡改的技术特性与农产品溯源领域极为契合[4-6]。相比于传统基于标签技术、无线传感器、射频识别(Radio frequency identification, RFID)等方式记录追溯数据，基于区块链技术构建的农产品溯源系统提高了溯源信息的透明度和安全性，打破了传统溯源系统数据存储中心化的局面[7]，同时增强了供应链各追溯主体之间的信息互通性[8]，对于保证数据的可追溯性和安全性、提升农产品品质、保障食品安全具有重要意义。

农产品区块链溯源系统中面向的消费者、上下游企业、本企业、监管部门等追溯主体存在差异化的追溯需求[9]。消费者作为供应链环节的终端用户，产品追溯信息的透明度和获取信息的便捷程度，是消费者关注的方面；上下游企业主要以交易关系为主，上下游企业存在信任缺失、信息不对称、资源利用率低等问题，使得各企业难以形成利益共同体，因此，实现信息的可信共享、交流互通是上下游企业的追溯需求；企业隐私和商业机密作为本企业最重要的资产之一，事关企业在行业内的话语权和竞争力，故隐私数据的安全存储和授权共享是本企业的迫切需求；监管部门聚焦于供应链安全标准化和监管体系系统化，对于风险追溯数据实现可信针对性监管是监管部门的追溯需求。由于不同追溯主体追溯需求的差异化，同时兼顾各追溯主体的追溯需求成为了农产品区块链溯源系统亟需解决的问题。

近年来国内外学者从不同角度解决农产品区块链溯源系统中追溯主体的需求。隐私数据作为供应链参与企业的关键敏感数据，如何安全地保护和共享隐私数据是追溯系统需要考虑的重点，一些学者对此进行了研究[10-11]：通过在追溯系统中引入对称加密和非对称加密等密码学技术，在区块链上对上下游企业的隐私数据进行加密及验证，在保护了隐私数据的同时，提高了追溯数据的查询效率。然而，供应链的可持续发展需要监管机构的介入，因此部分学者开始考虑追溯系统中数据监管的需求[12-13]：分析供应链的运作流程及参与方职责，构建智能合约追溯方法，同时引入监管方法，将数据监管范围扩大至供应链全生命周期。同时，有学者考虑到追溯关键数据的验证对追溯系统的安全性提出了很高的要求，而公有链相比联盟链能提供更为可信的追溯平台[14]，因此提出在以太坊公有链上建立追溯链，并在其上部署商业交易的智能合约方法，凭借开放透明的公有链平台，消除了供应链参与方之间的信任问题，实现了大豆交易追踪和信息追溯。然而，随着对区块链追溯的深入研究，单链区块链结构追溯系统存储压力大、难并发等弊端日益凸显[15]，多链区块链追溯架构应运而生[16-18]：通过在追溯系统中引入多链的架构，将传统单链区块链中的业务和数据按照一定规则划分至多链区块链系统之中，一方面降低了单链区块链系统下网络日益增长的节点对网络速率的影响，另一方面对共享信息、隐私保护、监管数据等进行针对性的优化与改进。多链技术的开发，也为链间的信息协调和跨链交流带来了新的挑战，如何分配和协同多链之间的功能成为了新的研究方向[19]：通过在联盟链平台设计多链追溯架构，利用跨链技术与智能合约实现多链追溯系统各链间的数据共享，克服了链间交互难度大、数据共享困难的问题。众多研究表明，利用区块链技术来增强食品和农业供应链中信息安全、共享信息透明度

和监管认证的趋势愈发明显[20]。

然而,现今的大多区块链多链追溯系统每条区块链的账本中混合存储了面向多个追溯主体的追溯数据。首先,数据共享仅存在于本环节企业间,实现跨环节的数据共享和对其它追溯主体的访问控制变得困难;其次,面向不同追溯主体的溯源数据在容量、隐私、安全性等方面均存在较大差异,数据的差异化存储保护和验证较为困难;最后,具有监管意义的追溯数据遍布于供应链各环节中,现今的追溯系统无法满足监管方对所有风险追溯数据的针对性监管需求。因此,该区块链存储结构下无法同时兼顾各追溯主体的溯源需求。

针对上述区块链追溯系统的不足,本文从果蔬供应链的追溯主体出发,设计果蔬区块链的主体链多链追溯架构。面向消费者、上下游企业、本企业、监管部门 4 个追溯主体设计溯源链、共享链、隐私链、监管链,以此满足各追溯主体差异化的追溯需求,实现追溯数据的可信追溯、授权共享、高效验证、隐私保护和针对性监管。

1 主体链多链追溯结构设计

本研究提出面向果蔬供应链追溯主体的主体链多链追溯结构,针对多链追溯系统跨环节企业无法实现数据共享和访问控制,数据分类存储与验证难度大,风险数据难以得到针对性监管等问题,参考果蔬实际应用环境,综合考虑各追溯主体的需求,构建了溯源链、共享链、监管链和隐私链 4 条主体链。由于各环节节点同时参与了 4 条链的账本维护,因此对于溯源链的追溯数据和监管链中的风险数据,上下游企业也可通过本地环节节点获取;对于消费者,消费者节点仅能通过溯源链中的消费者追溯节点访问溯源链的数据;对于监管者,监管者节点仅能对监管链中的风险数据进行监管,而不能对其它链中的数据进行访问,保证了上下游企业间内部数据的隐私性,也避免了企业内部商业信息被第三方机构泄露的风险。

多链追溯架构基于 Hyperledger Fabric[21] 联盟链开发,通过通道技术构建 4 条主体链子链,参与节点通过加入主体链子链,实现对该子链上区块链账本的维护。同时,由于链间通道隔离机制可实现不同主体链子链中的节点参与不同的链上共识记账,加入子链的节点才能够广播和接收该链上的账本数据。不同的节点可以加入一条或多条子链,同一条链中的所有节点通过共识算法[22]实现链中账本备份。本研究构建的多链区块链模型结构如图 1 所示。

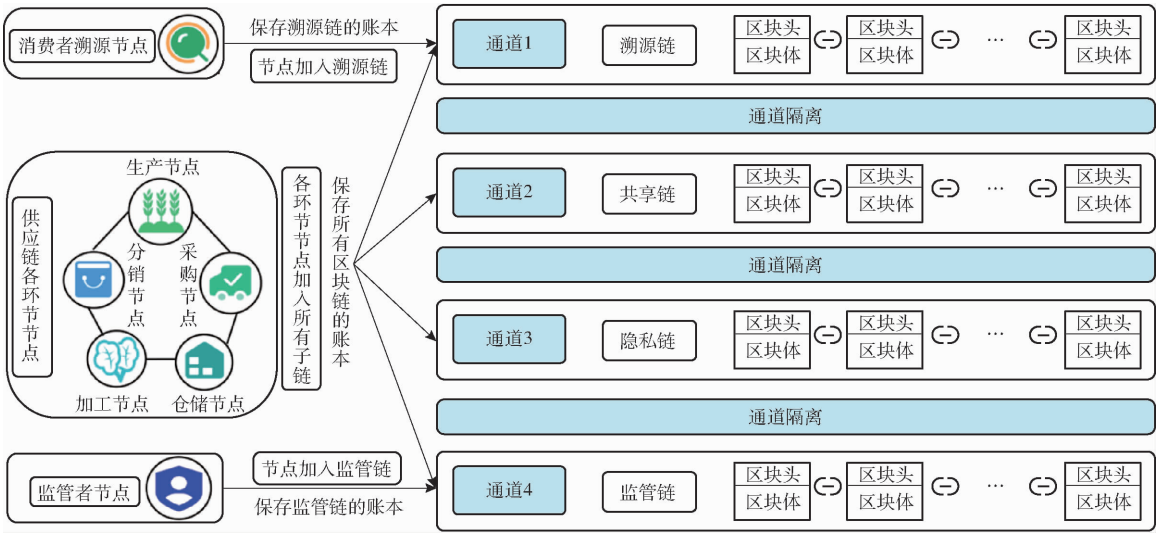

图 1 主体链区块链模型结构

Fig. 1 Model structure of subject-oriented blockchain

2 面向追溯主体的多链追溯模型设计

2.1 果蔬供应链追溯数据多链存储设计

果蔬供应链追溯过程包含生产、采购、仓储、加工、分销环节,数据由各类物联网设备采集并自动上传视频、图像、文本等操作信息,取代易导致源头数据可信度低的传统手动录入信息方法,保证了数据源头安全[23]。本研究从果蔬供应链中的追溯主体出发,建立面向消费者溯源的溯源链、面向企业数据共享的共享链、面向企业数据保护的隐私链和面向监管部门管控风险数据的监管链。通过分析对比各主体链数据特点,考量数据保护、存储成本和追溯效率,为各链设计存储方案,如表 1 所示。

溯源链中存储果蔬在全供应链环节可公开溯源的追溯数据,此类数据旨在帮助消费者获取购得产

表 1　果蔬追溯数据多链存储

Tab. 1　Traceability of multi-chain storage for fruit and vegetable

主体链	存储方案	生产	采购	仓储	加工	分销
溯源链	链上：明文	生产企业、产地、品种、收获日期、生产资质	采购企业、采购资质	仓储企业、存储时间	加工企业、加工日期、包装日期、产品认证标识、加工资质	销售企业、保质期限、销售资质
共享链	链上：明文哈希值 链下：数据库存储明文	生产环境信息、生长周期信息、种苗来源、培育日期、气候、培育数量、收获数量、出货数量、产品批次	采购清单、采购时间、采购数量、采购批次、承运企业、承运车辆	进仓时间、出仓时间、进仓数量、出仓数量、库存	加工数量、灭菌工艺、加工工艺、包装工艺	销售产品批次、销售日期、进货数量、销售数量
隐私链	链上：明文哈希值 链下：数据库存储密文	种植户信息、生产成本	采购人员信息、采购金额、采购单价、采购成本、采购合同、运输人员、运输成本	仓储人员信息、仓储成本、维护成本	加工人员信息、原料成本、加工成本	销售人员信息、进货价格、销售单价
监管链	链上：IPFS 哈希值 链下：IPFS 文件系统	农事信息、生产资质、检疫报告	采购物流信息、采购资质、采购审查、验收报告	仓储环境信息	加工信息、灭菌消毒、微生物检测、食品添加剂、加工资质	销售信息、销售资质

品的相关信息，打破消费者和产品企业信息不对称的壁垒；共享链存储供应链环节企业间用于交流和分析的共享数据，对供应链优化产业结构具有重要意义；隐私链中包含的数据为各供应链环节产生的隐私数据，隐私数据的泄露会对本企业的商业发展造成严重影响，同时，隐私数据也仅会共享给经过本企业授权的企业；监管链存储供应链各环节会对产品的品质与安全造成影响的风险数据，这部分数据亟需监管部门进行严格的监督与审查。果蔬追溯数据依据追溯主体需求分配至各链存储，同时由于面向不同追溯主体的溯源数据在数据类型、数据量、隐私性等方面均有差异，故通过主体链的建链方式，各链数据的性质趋同，因此对不同主体链的数据可采用不同的存储方案以满足链上数据的存储需求。

数据采集过程中，追溯数据包含了两种类型的采集数据，一种为追溯流程仅需上传一次的静态信息，如企业信息、人员信息、批次号信息等；另一种为各类传感器多次采集记录的动态信息，如温湿度信息、图像信息等，此类数据会在该批次果蔬生产过程，根据具体采集的数据类型设置采集频次累计存储，动态数据的采集和上链频次如表 2 所示。数据存储过程中，同一批次果蔬的静态数据是以环节为单位统一上传至区块链系统，即某一批次的果蔬在一环节完成后流入下一环节，完成环节的节点会将所有该批次号的静态数据上传至区块链系统；同时为减少区块链系统的网络负载，动态数据则会累计采集一定的时间后统一上传该段时间采集的信息至区块链。为了便于后续统一查找某一批次果蔬全流程的数据，每个环节在上传数据的时候都会上传本批次果蔬的批次号作为这批产品的唯一标识。

表 2　动态数据采集与上链频次

Tab. 2　Collection and storage frequency of dynamic data

采集数据类别	采集数据	采集间隔	上链间隔	供应链环节	上链
生产环境信息	空气温湿度、土壤温湿度、pH 值、电导率、气体（二氧化碳、氧气）浓度、光照强度	30 ~ 60 min	6 ~ 24 h	生产	共享链
生长周期信息	生长周期记录	1 ~ 7 d	1 d	生产	共享链
农事信息	灌溉、除草	1 ~ 7 d	1 d	生产	监管链
	施肥、病虫害防治	7 ~ 60 d	1 d	生产	监管链
采购物流信息	位置信息、仓储温湿度、气体（二氧化碳、氧气、乙烯）浓度	1 ~ 10 min	1 ~ 6 h	采购	监管链
仓储环境信息	仓储温湿度、气体（二氧化碳、氧气、乙烯）浓度	1 ~ 10 min	1 ~ 12 h	仓储	监管链
加工信息	清洗、选剔、包装等（根据具体果蔬类别和加工工艺而定）	10 ~ 60 min	6 ~ 24 h	加工	监管链
销售信息	交易信息（单号、时间、金额、人员等）	< 10 min	1 ~ 24 h	销售	监管链

本研究根据各参与追溯主体建链，通过数据授权能够实现数据的可控共享。其中，消费者的产品追溯数据为敏感层级最低的追溯数据，该追溯数据在追溯系统中所有参与企业均可访问；企业间的共享追溯数据仅供上下游企业访问；企业内部的隐私追溯数据敏感层级最高，对授权企业开放访问；涉及果蔬供应链质量安全风险的追溯数据，可供监管部门及各企业访问并通过 IPFS（星际文件系统）和监管链验证监管数据的真实性和原始性。本研究多链追溯数据存储架构模型如图 2 所示。

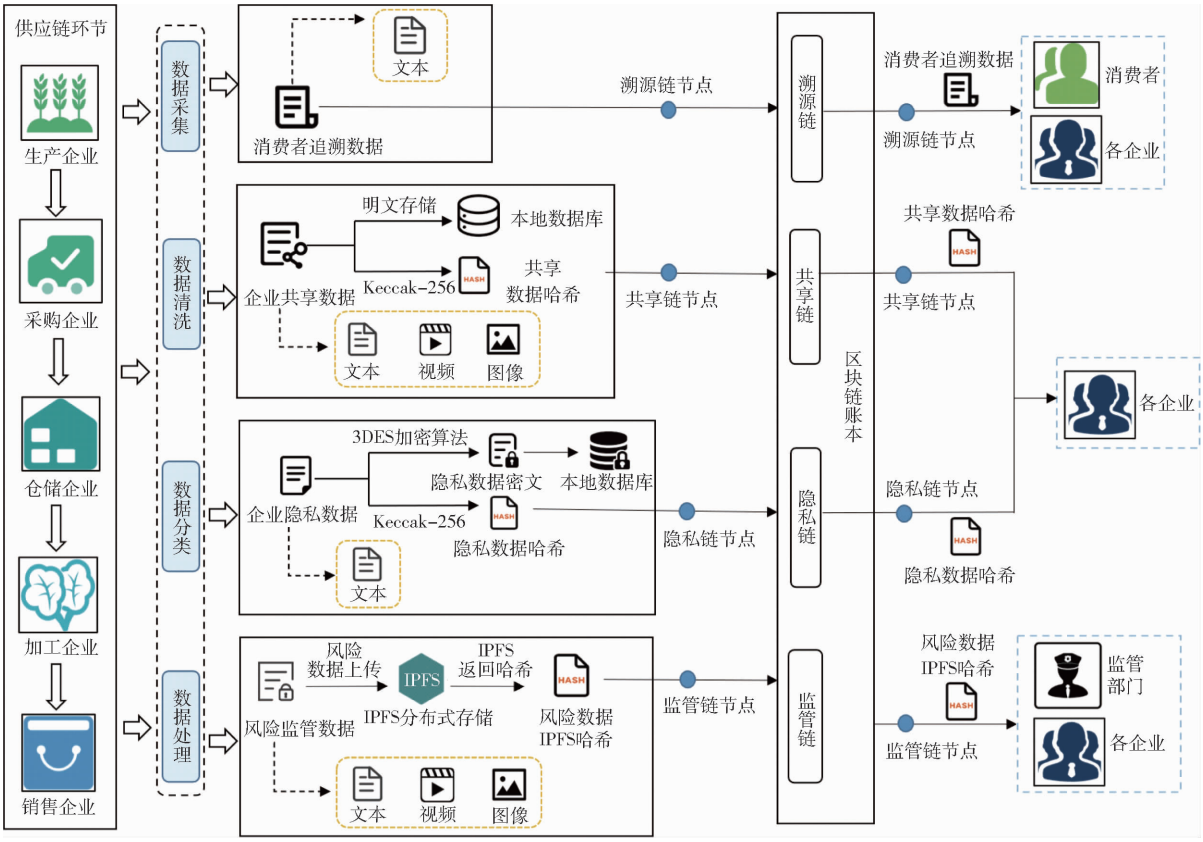

图 2 多链追溯数据存储架构模型

Fig. 2 Storage model of multi-chain traceability data

面向消费者的溯源链包含供应链环节的追溯数据，此类数据隐私敏感层级低、数据量较少，同时，消费者对追溯系统查询速度和透明性具有较高的需求。因此，溯源链数据均采用明文链上存储，消费者通过溯源节点直接查询明文数据，使得溯源链兼顾追溯效率和数据透明共享的特点。

面向企业的共享数据有一定的隐私性，数据种类繁杂，数据量大。因此共享链采用链上链下协同存储[24]共享追溯数据，链下企业数据库明文存储所有的共享数据，明文使用 Keccak－256 哈希算法散列，该散列方法可将任意文件类型、任意大小的输入单向压缩为 256 位的二进制字符串，散列后将哈希值上传至共享链存证。同时，果蔬追溯数据具备时效性，过期的共享追溯数据可以从链下数据库中删除，降低企业存储压力并节省成本。

风险数据的监管依赖数据的绝对真实性，此类数据需要有高度的可信技术支撑以保证数据的原始性和真实性，故本研究综合考量数据的类型、大小和安全性，采用 IPFS[25]和区块链相结合的方式存储。所有风险追溯数据被存储至 IPFS 平台，IPFS 平台的数据分布式存储有效保护原始数据，而 IPFS 返回的 256 位二进制数经过 Base－58 编码后返回 46 个字符组成的哈希值会被上传至监管链之中，监管链用来保证哈希值的安全。

隐私链主要存储企业供应链环节产生的隐私数据，此类数据敏感层级高、数据量小、数据价值高，同时企业的隐私数据能够通过加密算法实现可控共享。因此采用 Keccak－256 哈希算法将所有隐私数据明文散列后将哈希值存储至隐私链中，当已授权的上下游企业获取到隐私数据后，通过与隐私链中该隐私数据的哈希验证，保证接收到的隐私数据的原始性。

2.2 链上链下协同验证

本研究面向果蔬供应链追溯主体构建主体链多链模型，并设计各链的存储和验证方案，从而实现数据针对性存储及高效验证功能。各链数据的链上链下协同验证如图 3 所示。

由于溯源链中存储的数据为追溯数据明文，因

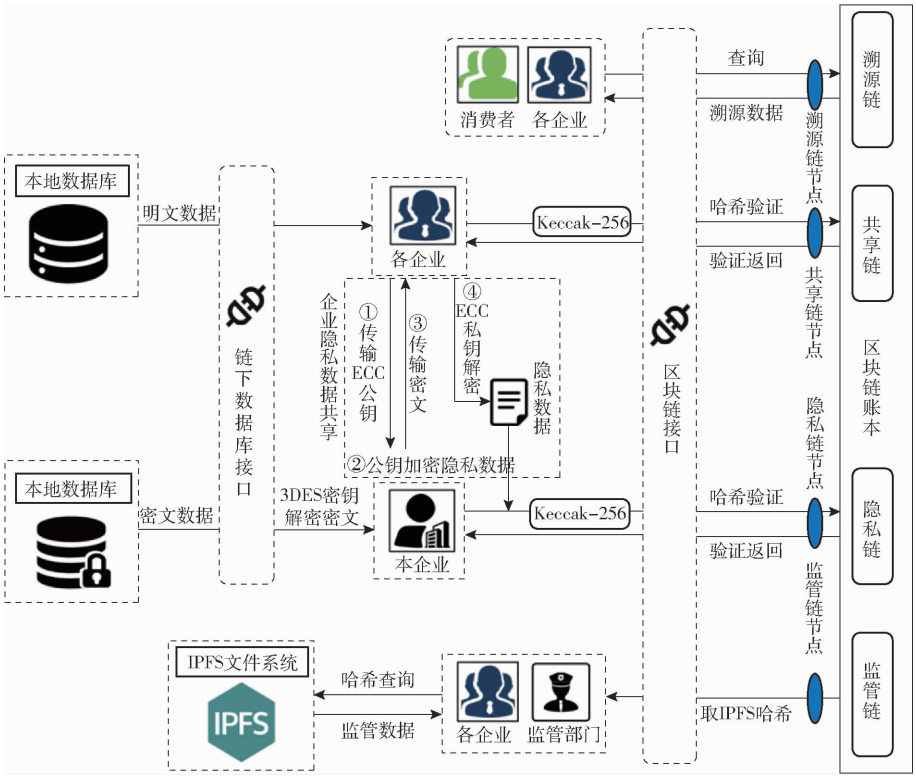

图 3　链上链下协同验证

Fig. 3　Collaborative verification of on-chain and off-chain

此存储至溯源链中的数据在被上传至链上后便不可篡改，因此对于可访问的主体无需进行额外的数据原始性验证。

共享链面向的追溯主体为各上下游企业，由于共享追溯数据量大，因此所有数据存储在链下企业数据库中，而共享链上存储共享数据经过 Keccak－256 哈希算法散列后的哈希值。当上下游企业之间需要共享追溯数据时，企业通过彼此开放的接口实现共享数据的传输，获取到其他企业共享的数据的企业通过 Keccak－256 哈希算法得到哈希值，并通过链上哈希校验智能合约与数据上传企业的哈希值进行比对，以此验证数据的原始性。

各企业将隐私数据进行 Keccak－256 哈希算法散列后的哈希值上传至隐私链，而隐私数据会经过对称加密三重数据加密算法（Triple data encryption algorithm，3DES）的密钥加密后，将得到的隐私密文存储至各企业本地的数据库中。当某一企业的隐私数据需要向被授权企业共享时，为防止隐私数据传输的泄露，授权企业会将非对称加密算法椭圆曲线加密（Elliptic curve cryptography，ECC）的公钥传输给该企业。该企业通过 ECC 公钥对隐私数据进行加密，并将密文传输给授权企业，授权企业通过 ECC 私钥解密密文从而得到隐私数据。同时，为验证隐私数据的原始性，将隐私数据经过 Keccak－256 哈希算法散列后，通过隐私链链上哈希校验智能合约进行校验，以此验证隐私数据的原始性。

监管部门通过从监管链上获取哈希值，并根据获取的哈希值从 IPFS 网络中获取原始监管数据，以此保证监管数据的原始性和真实性，实现监管部门对风险追溯数据的针对性监管。

2.3　智能合约设计

智能合约是一种无需第三方即可实现自我验证、自动执行合约条款的交易协议[26]。智能合约通过事件触发的机制而执行，其赋予对象以数字的特征并将其部署至区块链上[27]。本研究针对果蔬多链追溯模型设计哈希校验、数据上链、数据查询的智能合约方法，在链中的各追溯节点发起链上交易时，即可自动触发业务逻辑，实现链上交易逻辑的自动执行。哈希校验链上智能合约的触发会以交易的形式记录在区块链之中，全网节点均可查看，以此来监督失败的验证交易，从而保证全产业链追溯环节所有数据的可溯、可信、可靠。针对供应链主体的追溯需求，本研究设计相关合约功能，智能合约设计细节如表 3 所示。

3　面向追溯主体的果蔬追溯模型架构

3.1　模型架构

本研究基于联盟链多链技术构建面向供应链追溯主体的果蔬追溯模型，通过多通道技术实现节点

表 3 智能合约设计细节

Tab. 3 Details of smart contract design

合约功能	合约方法	描述	输入	输出
哈希校验	isShareData( )	共享数据链下接口传输,上传共享数据哈希与链上哈希校验	交易 ID 共享数据哈希	True/False
	isPrivacyData( )	隐私数据链下接口传输,上传隐私数据哈希与链上哈希校验	交易 ID 隐私数据哈希	True/False
数据上链	wriTraceChain( )	将面向消费者的追溯数据写入溯源链	明文数据	交易 ID
	wriShareChain( )	将面向企业间的追溯数据写入共享链	共享数据哈希	交易 ID
	wriPravicyChain( )	将面向本企业的追溯数据写入隐私链	隐私数据哈希	交易 ID
	wriSupervisionChain( )	将面向监管部门的追溯数据写入监管链	监管数据哈希	交易 ID
数据查询	quTraceData( )	查询溯源链账本中的公开数据	交易 ID/批次号/区块高度	溯源数据
	quShareData( )	查询共享链账本中的共享数据哈希	交易 ID/批次号/区块高度	共享数据哈希
	quPrivacyData( )	查询隐私链账本中的隐私数据哈希	交易 ID/批次号/区块高度	隐私数据哈希
	quSupervisonData( )	查询监管链账本中的监管数据哈希	交易 ID/批次号/区块高度	监管数据 IPFS 哈希

的账本管控和维护,以此实现上下游数据的高效共享;通过主体链式结构,针对各主体特点实现各主体追溯需求;设计多链存储方案,保证各链数据的存储安全及可靠验证。本研究提出的追溯模型架构如图 4 所示,由上至下共分为应用层、接口层、服务层、存储层、物理层 5 个层次。

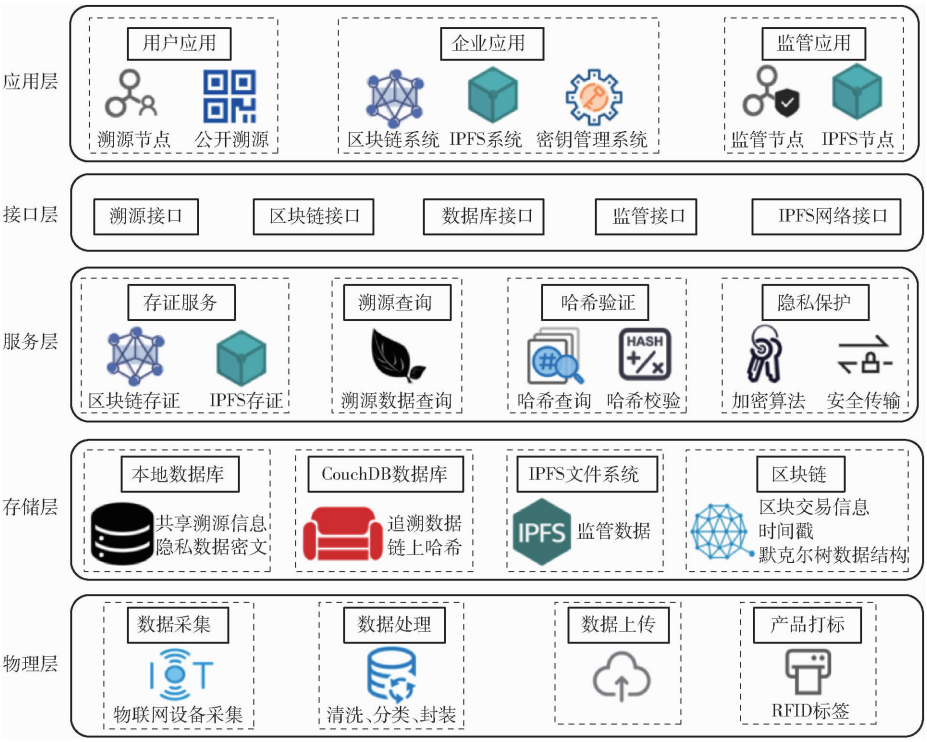

图 4 追溯模型架构

Fig. 4 Architecture of traceability model

应用层面向消费者、各企业、监管机构等追溯主体,根据不同主体不同的追溯需求,为不同主体提供不同的功能。

接口层封装了区块链账本数据操作接口、IPFS 网络接口和链下数据库接口。为消费者、企业、监管部门实现数据查询、数据上传、数据共享、数据验证等功能提供支持。

服务层为供应链追溯主体提供包含存证服务、溯源查询、哈希验证、隐私保护等关键服务,各类数据主要依靠接口层进行传递。

存储层中本地数据库主要存储共享溯源数据以减轻区块链网络负载,本企业经过加密的隐私数据密文也存储于此;IPFS 文件系统与链上哈希相结合的方法保证监管者获取的风险数据原始性和真实性;利用区块链系统防篡改特点,保护上链数据和哈希的原始性。为减少溯源数据的查询时间,溯源数据通过状态数据库 CouchDB 存储,数据通过 Key - value 键值索引查询。

物理层通过相关物联网设备采集链下追溯数据以保证源头数据的真实可信；数据处理技术实现追溯数据的分类上链；RFID 等标签技术为产品生成唯一电子标签。

3.2　测试环境

本研究的测试环境基于 Hyperledger Fabric 1.4.4 搭建，使用的虚拟机系统版本为 Ubuntu 14.04 LTS，硬件配置为：16 GB 内存、8 核 Intel i7－9700T 处理器、100 GB 硬盘。溯源链和监管链通过 11 个节点存储追溯数据，共享链和隐私链通过 10 个节点存储追溯数据。其中，4 条链均包含生产节点、采购节点、仓储节点、加工节点、销售节点各 2 个，即各环节节点均加入主体链中的各子链，均参与 4 条链中的账本维护。溯源链额外加入一个提供给消费者溯源的溯源节点，监管链额外加入一个满足供监管部门管控需求的监管节点。溯源区块链中的所有节点均采用状态数据库 CouchDB，通过索引检索状态数据库查询数据，测试环境具体的配置如表 4 所示。

表 4　多链配置信息

Tab. 4　Configuration information of multi-chain

区块链配置	数值/形式	描述
链数	4	溯源链、隐私链、共享链、监管链
组织数量	6	生产组织、采购组织、仓储组织、加工组织、销售组织、外部组织
节点数量	12	每个组织各两个节点，外部组织包含一个消费者溯源节点和一个监管者监管节点
数据库	CouchDB	各节点采用 CouchDB 状态数据库存储数据
共识机制	Raft	使网络中所有节点同步账本的一致性算法
出块时间/ms	500	排序节点根据出块时间打包交易发布区块
区块最大交易数量	100	一个区块中可以包含的最大交易数量
区块最大容量/MB	50	一个区块中最多存储数据的容量

4　性能分析

4.1　追溯模型性能分析

本研究通过外部接口将合约封装上链，测试工具为 Postman（Version 8.0.6），通过数据上链和数据查询脚本文件获取相关时间信息，各链通过接口进行 50 轮次的测试。各链上链数据类型示例如表 5 所示，溯源链将面向消费者的生产环节数据上链，其余链条将哈希值上链。

由于共享链、隐私链、监管链使用相同的智能合约、共识算法和区块生成机制，上链信息均为存储差异较小的哈希值，经过测试，3 条链的写入与查询时间差异较小，故本节仅列出溯源链和监管链的性能测试。溯源链的性能测试如图 5a 所示，追溯数据的平均写入时间为 593.10 ms，平均查询时间为38.86 ms，能够满足消费者快速获取追溯数据信息的需求；监管链的性能测试如图 5b 所示，数据的平均写入时间为 586.30 ms，平均查询时间为 37.04 ms，监管方也可在较短时间内查询到监管数据的哈希值。同时，测试过程中使用苹果与

表 5　溯源数据上链

Tab. 5　Upload traceability data to blockchain

主体链	上链数据	值
溯源链	溯源数据明文	产品名称：ZHNY 富士苹果|产品批次：HN2021090115O7c|生产企业：山东慧农果业公司|采收日期：2021－09－27|销售产品编号：7519622E－7DB8－4AE3－8590－89791DAC32BE|追溯码：HN2021091200100002
共享链	共享数据哈希	ff4d2a2a7a994ea742d8a3bbcc742c63e99775bef9e4d761987a05aeeff47e0c
隐私链	隐私数据哈希	2d9a1c071f4d65213ee5628944b61664ea94473cb534088559ed8e7b4a0adb67
监管链	监管数据 IPFS 哈希	QmRzFKZ7nkn1p7bSPrPNs2FTCPLmCWCeez2KMcNT2FtKAb

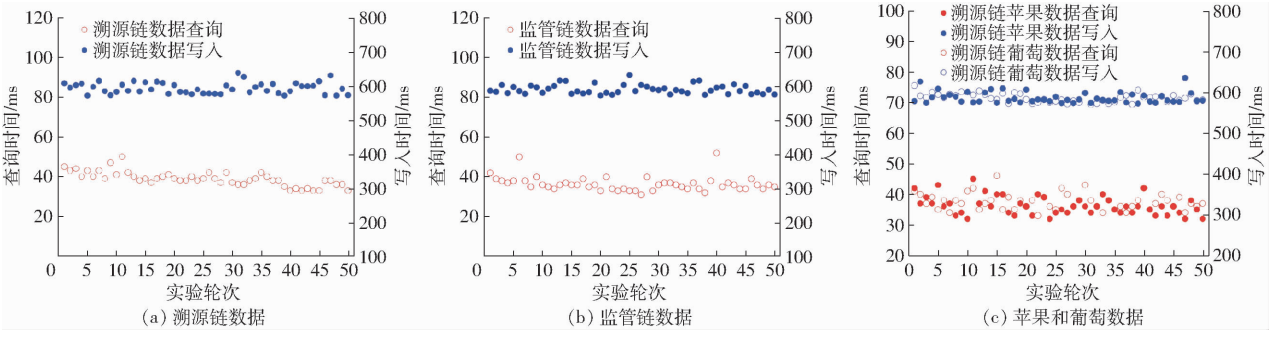

图 5　多链追溯数据写入与查询时间

Fig. 5　Time of upload and query traceability data of multi-chain

葡萄的果蔬供应链数据作为对比，如图 5c 所示，溯源链中的两类果蔬的查询和写入的时间差异较小，其它链的对比结果也与溯源链的结果一致，不同的果蔬供应链信息的差异对本文的模型效率影响很小。这是因为不同果蔬供应链数据的差异主要体现在动态数据上，由于本文将追溯各环节的动态数据均以哈希值的形式上链，使得不同的果蔬在上链存储时数据的类型和大小差异变得很小，因此在追溯系统的查询和写入结果基本一致。从测试结果可以看出，面向追溯主体建立的多链追溯区块链具有较好的数据写入及数据查询效率，能够满足果蔬溯源系统数据上链与查询需求。

4.2 链上链下协同验证分析

本节测试共享链、隐私链、监管链的链上链下验证耗时，每条链均进行 20 轮测试。本文的查询和验证总耗时包含了在链下数据库通过接口读取数据的时间。图 6a 显示了获取真实的共享数据、隐私数据、监管数据的总耗时，其中获取已验证的共享数据平均耗时 806.80 ms，获取已验证的隐私数据平均耗时 910.35 ms，获取已验证的监管数据平均耗时 675.90 ms；图 6b 显示了共享链和隐私链中采用哈希校验智能合约中链上验证的耗时，共享数据链上验证耗时 464.40 ms，隐私数据链上验证耗时 464.25 ms；图 6c 显示共享数据和隐私数据链上验证时间占数据查询验证总耗时的比例，共享数据链上验证占总耗时的 57.57%，隐私数据链上验证时间占总耗时的 51.02%，从上述测试结果可以看出，链上链下验证数据真实性的总耗时在可接受范围内，链上哈希验证智能合约也有着较好的性能。

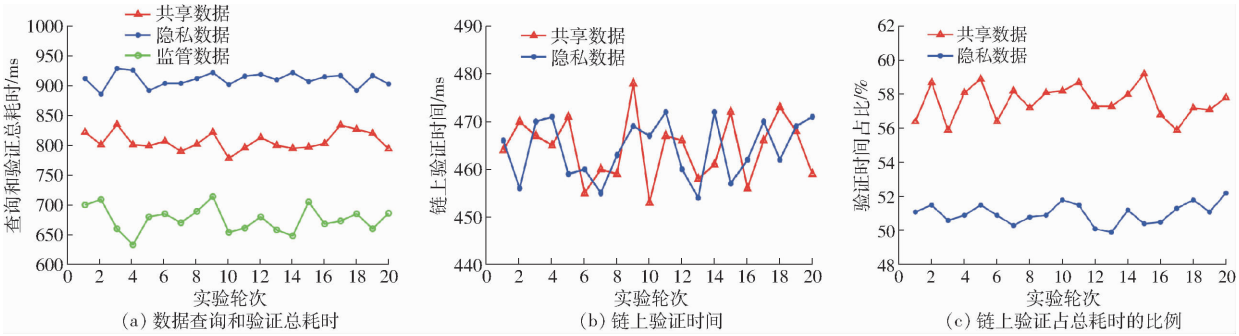

图 6 链上链下验证耗时分析

Fig. 6 Time consumption analysis of on-chain and off-chain validation

4.3 动态数据存取性能分析

以农事动态数据为例，测试存储至 IPFS 中动态数据的增长对存取效率的影响，测试的数据为监管链中的农事相关信息，数据包含文本、图像和视频信息。所有测试结果均重复实验 30 次，最终结果取所有结果的平均数以保证所有测试结果的真实性及可靠性。如图 7a 所示，选择测试 5 ~ 50 KB 的文本文件数据作为小容量数据上传与下载进行测试，随着上传的文本文件容量以每次 5 KB 的增幅增长时，上传时间和下载时间分别约在 56.40 ms 和 31.60 ms 上下波动，上传时间和下载时间并未呈现增长的态势，原因是当文件过小时，文件的绝对上传与下载时间相对于 IPFS 网络的初始化以及网络连接的时间占比过小，此时以网络的初始化以及网络连接的时间占据主导因素，因此文件容量的增长并未对文件的上传与下载速度产生明显影响；如图 7b 所示，当测试文件选择为 5 ~ 50 MB 的图像文件时，随着图像文件的容量以每次 5 MB 的增幅增长时，上传时间和下载时间都有较为明显的增长，此时文件的绝对上传与下载速度开始占据主导；如图 7c 所示，当测试文件选择 50 ~ 500 MB 的视频文件时，随着视频文件的容量以每次 50 MB 的增幅增长时，上传时间和

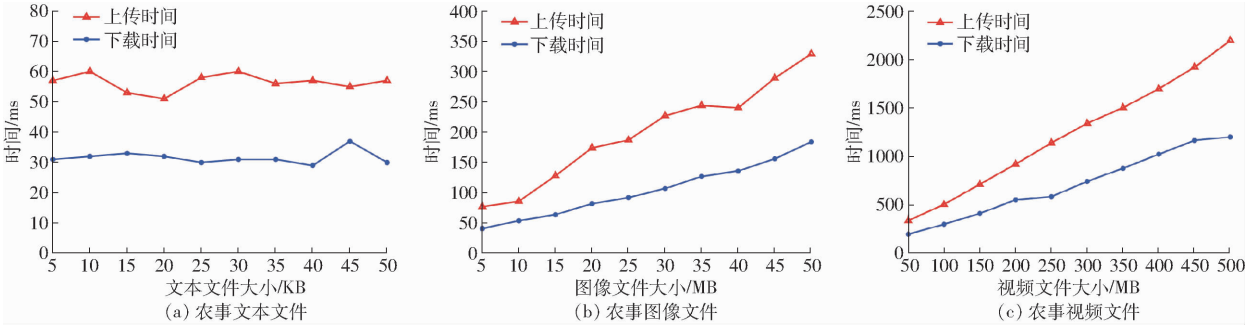

图 7 农事动态数据存取耗时分析

Fig. 7 Time consuming analysis of agriculture dynamic data

下载时间呈现显著增长的趋势，此时文件的绝对上传与下载速度为绝对主导因素，网络的初始化以及网络连接的时间对文件的上传与下载速度影响较小。从对 IPFS 网络不同类型和不同大小农事文件的测试可以看出，监管链的存储方案有着良好的写入和读取效率，能够满足监管机构高效获取可靠监管数据的需求。

5　系统实现

5.1　原型系统实现

本研究根据主体链追溯模型实现果蔬供应链溯源系统。如图 8a 所示，面向追溯主体建立的区块链溯源系统，其中面向消费者的溯源链共计生成 86 992 个区块，已完成的交易数量 112 902 笔。供应链各环节节点通过智能合约在溯源系统实现数据的上传以及查询功能，系统中的节点共同参与全网的共识记账。图 8b 显示了根据批次号查询的溯源数据的结果，由于该批次的数据录入数据由不同的节点上传，因此同批次下的供应链各环节数据上传存在时间差，使得各环节数据并未存储在相同区块之中，因此通过该批次号查询的数据来自几个不同的区块之中。图 8c 显示了共享链中哈希验证界面的结果，企业通过将获取到的共享数据和交易 ID 上传至共享链，通过哈希校验智能合约，即可在链上校验获取的数据的原始性。同时，校验的结果会在区块链中产生一条新的交易，该交易会将一条包含交易节点信息、交易 ID 编号和校验结果的数据作为一条新的数据记录到区块链中，该交易全网节点均可查看，用来监督企业间共享原始数据的行为。

(a) 主体链区块链溯源系统　　(b) 溯源链数据查询界面　　(c) 共享链哈希验证界面

图 8　主体链追溯系统浏览器界面

Fig. 8　Subject-oriented multi-chain traceability system browser

同时，为满足消费者追溯需求，本研究设计的主体链溯源系统为消费者提供扫码溯源的功能，消费者可根据所购得的产品中的二维码获取产品的溯源数据。如图 9 所示，经过查询后，消费者可获取产品介绍信息、溯源信息和相关企业信息。该批次产品的溯源信息存证会被展示给消费者，其中的静态溯源信息来自区块链，动态溯源信息来自企业的数据库。同时区块链追溯系统中的区块链地址、追溯哈希值和区块高度也可被消费者查看。

5.2　追溯方案对比

表 6 将传统溯源方案、单链区块链追溯方案、主从链区块链追溯方案、环节链追溯方案与本研究提出的主体链追溯方案在存储模式、网络负担、共享数据范围、数据透明度、数据存储效率、数据容错性、数据共享验证、隐私数据安全、监管数据范围和查询时间共 10 方面进行了对比。对比建立在相同的实验环境下，仅比较区块链链式结构改变而对追溯系统产生的影响。数据容错性表示

图 9　消费者扫码溯源界面

Fig. 9　Consumer traceability interface

溯源系统中部分节点崩溃时,区块链系统还能保证追溯数据是安全可信的,由于本文区块链系统使用 Raft 共识机制,因此可容忍全网不超过 1/2 的节点崩溃。本研究设计的主体链区块链追溯模型,在保证原有区块链溯源方案的多中心化、数据真实性、隐私数据高安全性的基础上,相比其它结构建立的区块链多链追溯方案,实现了全供应链环节数据的自由共享及访问控制,并通过可信验证保证供应链环节所有数据共享的真实性,强化了风险数据的针对性监管。

表 6 农产品追溯方案对比

Tab. 6 Comparison of agricultural product traceability solutions

项目	传统追溯方案(文献[28])	单链追溯方案(文献[12])	主从链追溯方案(文献[29])	环节链追溯方案(文献[30])	主体链追溯方案(本方案)
存储模式	中心化	多中心化	多中心化	多中心化	多中心化
网络负担		高	中	低	低
共享数据范围	环节内部	各环节	环节内部	环节内部	各环节
数据透明度	低	中	中	中	高
数据存储效率	高	中	低	低	低
数据容错性		1/2	1/2	1/2	1/2
数据共享验证		部分	部分	部分	全部
隐私数据安全	低	中	高	高	高
监管数据范围		所有数据	所有数据	所有数据	风险数据
查询时间/ms	<20	<50	<80	<50	<50

6 结论

(1)提出了一种适用于果蔬供应链的主体链多链追溯模型,建立了溯源链、共享链、隐私链、监管链的主体链追溯区块链系统。通过将追溯主体的需求数据存储至各主体链,结合主体需求和数据特点,设计了与各链相适应的存储和验证方案。主体链的追溯模型解决了各追溯主体的差异化追溯需求,满足了消费者的可信追溯需求,实现了各企业之间数据的授权共享与可信验证,加强了监管部门对风险追溯数据的针对性监管。

(2)提出的面向追溯主体的果蔬区块链模型,具备良好的性能。测试结果表明,溯源链数据的平均查询时间 38.86 ms;通过链上哈希校验智能合约,共享链上获取验证后的共享数据的平均耗时 806.80 ms、隐私链上验证后的隐私数据平均耗时 910.35 ms;通过“IPFS + 监管链”,获取验证后的监管数据平均耗时 675.90 ms。共享链链上智能合约耗时占验证总耗时的 57.57%,隐私链链上智能合约耗时占验证总耗时的 51.02%,链上哈希校验智能合约也有较为理想的性能。

(3)以农事动态数据为例,测试了动态数据的增长对链下 IPFS 系统的存取性能的影响,存储方案有着良好的存取效率。同时,将动态数据哈希值存储于链上的方案,使得本文的追溯模型能够适应不同的果蔬品种,追溯系统能够满足不同果蔬供应链追溯主体的查询与验证需求。

参 考 文 献

[1] 朱昱锦,姚建国,管海兵. 区块链即服务:下一个云服务前沿[J]. 软件学报, 2020, 31(1): 1 - 19.
ZHU Yujin, YAO Jianguo, GUAN Haibing. Blockchain as a service: next generation of cloud services[J]. Journal of Software, 2020, 31(1): 1 - 19. (in Chinese)

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. https://botcoin.org/bitcoin.pdf.

[3] 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)

[4] FENG H H, WANG X, DUAN Y Q, et al. Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges[J]. Journal of Cleaner Production, 2020, 260(3): 121031.

[5] MIRABELLI G, SOLINA V. Blockchain and agricultural supply chains traceability: research trends and future challenges[J]. Procedia Manufacturing, 2020, 42: 414 - 421.

[6] 于丽娜,张国锋,贾敬敦,等. 基于区块链技术的现代农产品供应链[J]. 农业机械学报, 2017, 48(增刊): 387 - 393.
YU Li'na, ZHANG Guofeng, JIA Jingdun, et al. Modern agricultural product supply chain based on block chain technology[J]. Transactions of the Chinese Society for Agricultural Machinery, 2017, 48(Supp.): 387 - 393. (in Chinese)

[7] 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)
[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 Machinery, 2021, 52(1):1 - 13. (in Chinese)
[9] HASTIG G M, SODHI M M S. Blockchain for supply chain traceability: business requirements and critical success factors[J]. Production and Operations Management, 2020, 29(4): 935 - 954.
[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] 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)
[12] WANG L, XU L Q, ZHENG Z Y, et al. Smart contract-based agricultural food supply chain traceability[J]. IEEE Access, 2021, 9: 9296 - 9307.
[13] ZHANG X, SUN P C, XU J P, et al. Blockchain-based safety management system for the grain supply chain[J]. IEEE Access, 2020, 8: 36398 - 36410.
[14] SALAH K, NIZAMUDDIN N, JAYARAMAN R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. IEEE Access, 2019, 7: 73295 - 73305.
[15] 张文芳,孙海锋,张晏端,等. 基于树形结构构造的联盟链主从多链共识算法[J]. 电子学报, 2022, 50(2): 257 - 266.
ZHANG Wenfang, SUN Haifeng, ZHANG Yanduan, et al. A consensus algorithm for consortium chain with tree based master-slave multi-chain architecture[J]. Acta Electronica Sinica, 2022, 50(2): 257 - 266. (in Chinese)
[16] LENG K J, BI Y, JING L B, et al. Research on agricultural supply chain system with double chain architecture based on blockchain technology[J]. Future Generation Computer Systems, 2018, 86: 641 - 649.
[17] DING Q Y, GAO S, ZHU J M, et al. Permissioned blockchain-based double-layer framework for product traceability system [J]. IEEE Access, 2019, 8: 6209 - 6225.
[18] PENG X Z, ZHANG X, WANG X Y, et al. Multi-chain collaboration-based information management and control for the rice supply chain[J]. Agriculture, 2022, 12(5): 689.
[19] WANG Y, CHENG T, XI J S. SCT - CC: a supply chain traceability system based on cross-chain technology of blockchain [C]// BenchCouncil International Federated Intelligent Computing and Block Chain Conferences. Springer, Singapore, 2021: 281 - 293.
[20] MUKHERJEE A A, SINGH R K, MISHRA R, et al. Application of blockchain technology for sustainability development in agricultural supply chain: justification framework[J]. Operations Management Research, 2021, 6: 19 - 31.
[21] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains[C]// Proceedings of the Thirteenth EuroSys Conference, 2018: 1 - 15.
[22] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11):2011 - 2022.
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms:the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11):2011 - 2022. (in Chinese)
[23] KUMAR N M, MALLICK P K. Blockchain technology for security issues and challenges in IoT[J]. Procedia Computer Science, 2018, 132: 1815 - 1823.
[24] 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)
[25] BENET J. IPFS-content addressed, versioned, P2P file system[J]. arXiv preprint arXiv:1407.3561, 2014.
[26] 欧阳丽炜,王帅,袁勇,等. 智能合约:架构及进展[J]. 自动化学报, 2019, 45(3): 445 - 457.
OUYANG Liwei, WANG Shuai, YUAN Yong, et al. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica, 2019, 45(3): 445 - 457. (in Chinese)
[27] 贺海武,延安,陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452 - 2466.
HE Haiwu, YAN An, CHEN Zehua. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(11): 2452 - 2466. (in Chinese)
[28] 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(增刊): 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(Supp.): 385 - 392. (in Chinese)
[29] 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)
[30] 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)