doi:10.6041/j.issn.1000-1298.2024.06.038

基于多链的果蔬全程全息信息管理模型构建与系统化实现

张　新[1]　刘崇宣[1]　许继平[1]　王小艺[2]　于家斌[1]　赵峙尧[1]
(1.北京工商大学计算机与人工智能学院,北京 100048;2.中国音乐学院,北京 100101)

摘要:果蔬全供应链既具有业务环节繁杂、数据多源异构、利益角色众多等通用食品供应链特征,又具有风险演变趋势复杂、时效性要求强、存在突发新发风险等特性。为有效解决传统果蔬供应链监管方案存在的监管覆盖面不足、溯源效应周期长、各主体间协同效应差等问题,构建了基于区块链多链的果蔬全程全息信息管理模型,并进行了系统化验收。首先,在果蔬全程全息信息解析的基础上,构建基于多链的果蔬全程全息信息管理模型。然后,提出一种基于区块综合索引指数的果蔬信息快速检索方法,并设计了基于公证链的果蔬信息跨链安全交互机制。其次,基于长安链开源区块链平台设计并开发了果蔬全程全息信息管理原型系统。最后,进行了实验验证和系统案例应用分析。结果表明,本系统公开数据上链平均耗时为 589.03 ms,隐私数据上链平均耗时为 708.59 ms,公开数据查询平均耗时为 26.87 ms,隐私数据查询平均耗时为 30.67 ms。本文设计的基于多链的果蔬全程全息信息管理模型及系统在满足不同需求用户对于不同权限信息的上链和查询需求的同时,实现了对果蔬全程全息信息的穿透式监管,满足了企业对隐私数据的权限控制与安全共享需求,提高了果蔬信息检索效率,为果蔬全程全息信息管理模型开发提供参考与借鉴。

关键词:果蔬全程全息;多链;信息管理;区块综合索引指数;公证链;长安链
中图分类号:TP309.2;TS201.6　　**文献标识码**:A　　**文章编号**:1000-1298(2024)06-0365-15　　**OSID**:

Construction and Systematic Implementation of Multi-chain-based Management Model for Fruits and Vegetables in Full-process and Information Scheme

ZHANG Xin[1]　LIU Chongxuan[1]　XU Jiping[1]　WANG Xiaoyi[2]　YU Jiabin[1]　ZHAO Zhiyao[1]
(1. *School of Computer and Artificial Intelligence*, *Beijing Technology and Business University*, *Beijing* 100048, *China*
2. *China Conservatory of Music*, *Beijing* 100101, *China*)

Abstract: The full supply chain of fruits and vegetables not only has the characteristics of complex business processes, heterogeneous data sources, and numerous interest roles in the general food supply chain, but also has the characteristics of complex risk evolution trends, strong timeliness requirements, and the presence of sudden new risks. To effectively address the pain points of traditional fruit and vegetable supply chain supervision solutions, such as insufficient regulatory coverage, long traceability effect cycles, and poor collaborative effects among various entities, a blockchain based full-process and information management model for the entire process of fruits and vegetables was constructed, and a systematic acceptance was conducted. Firstly, based on the analysis of holographic information throughout full-process and information of fruits and vegetables, a multi-chain-based holographic information management model for fruits and vegetables was constructed. Then a fast retrieval method for fruit and vegetable information based on block comprehensive index was proposed, and a cross chain secure interaction mechanism for fruit and vegetable information based on notary chain was designed. Secondly, a prototype system for the full-process and information management of fruits and vegetables was designed and developed based on the open-source blockchain platform of chainMaker. Finally, experimental verification and system case application analysis were conducted. The results showed that the average time for public data uplink in this system was 589.03 ms, the average time for private data uplink was

收稿日期:2023-09-21　修回日期:2023-11-06
基金项目:国家重点研发计划项目(2022YFF1101103)
作者简介:张新(1989—),男,副教授,博士,主要从事区块链与人工智能融合应用研究,E-mail:zhangxin@btbu.edu.cn
通信作者:赵峙尧(1989—),男,副教授,博士,主要从事粮油食品供应链危害物风险评估与预警研究,E-mail:zhaozy@btbu.edu.cn

708.59 ms, the average time for public data queries was 26.87 ms, and the average time for private data queries was 30.67 ms. The multi-chain-based full-process and information management model and system designed not only met the needs of different users with different permission informations for uploading and querying, but also achieved penetrating supervision of full-process and information of fruits and vegetables, and met the needs of enterprises for permission control and secure sharing of private data, improved the efficiency of fruit and vegetable information retrieval, and provided reference for the development of full-process and information management model.

Key words: full-process and information of fruits and vegetables; multi-chain; information management; block comprehensive index; notary chain; chainMaker

0 引言

果蔬产业对世界农业经济影响深远[1-3]。保障果蔬质量安全不仅与消费者的健康息息相关,还关系到消费者对产品的信任度和消费意愿。果蔬质量安全问题的重点在于农药残留、微生物腐败和真菌毒素侵袭等方面[4-5]。因此,对果蔬进行危害物安全监测,尽早发现问题并进行记录和处理,防止食品安全问题事件的发生刻不容缓[6-7]。目前已经有许多采用物联网和神经网络等信息化技术保障农产品质量安全的方案,可以用于记录农产品生产中涉及的信息,提高追溯系统中数据的准确性,但基本都存在隐私数据与公开数据协调性差、数据中心化存储、透明度不足和易被篡改等问题,无法满足监管部门和消费者的监管溯源需求[8-9]。“十四五”规划重点强调了要加强食品风险监管,构建完善食品风险全程全息信息管理系统,实现智慧监管[10]。因此,构建去中心化、安全可信的果蔬全程全息信息管理体系是当今亟待解决的重要研究课题。

区块链是一种基于点对点传输、密码学、分布式数据存储、共识机制等技术的分布式账本技术,具有去中心化、难以篡改、隐私保护、可追溯、账本公开透明等特性[11-14]。基于区块链构建的农产品信息管理系统有助于提高农产品的质量与安全性,为消费者与监管部门提供真实有效的溯源信息,协助监管部门对农产品供应链进行精准监管,减轻消费者对食品安全问题日益增长的担忧[15-17]。但区块链本身特点可能会导致溯源过程中出现计算资源浪费、检索效率低等问题。目前,学者们针对基于区块链的农产品溯源监管模型构建进行了多角度研究。文献[18]设计了基于区块链技术和物联网(IOT)集成增强的可追溯性系统,实现了对整个食品供应链中食品的移动、加工和存储各类数据的跟踪。文献[19]设计了基于区块链和射频识别(RFID)技术的供应链可追溯系统框架,提高了食品供应链数据跟踪的效率。但单链架构无法满足果蔬全程全息信息管理对性能和容量的需求,存在负载问题。文献[20]设计了“区块链 + IPFS(星际文件系统)”的双存储模型,以减轻区块链的存储压力,提高了数据传输效率。而单链架构中缺乏数据隔离性,无法满足果蔬全程全息各环节企业间的隐私数据隔离。文献[21]设计了基于区块链多链的杂粮供应链追溯模型,将企业链与追溯主链结合,实现了数据隔离存储,提高了溯源系统的可扩展性。上述研究都在农产品溯源领域取得了显著的成果,但对于果蔬这种时效性要高的短保农产品,存在溯源监管效率研究上的不足。文献[22]提出了一种基于布隆过滤器的智能交通系统(ITS)数据多关键词搜索协议,通过携带存储空间利用率较高的布隆过滤器来储存信息,提高了数据查询性能和效率。文献[23]基于区块访问次数动态调整索引层级设计了一种优化的跳表检索结构,有效提高了溯源查询效率,但在果蔬全程全息信息管理背景下对区块检索顺序排序时,在关注区块访问次数的同时,不应忽略区块中包含风险信息数量的重要性。

本文通过对果蔬全程全息信息深入解析,构建基于区块链多链的果蔬全程全息信息管理模型,同时设计果蔬全程全息信息上链存储模式,并提出基于区块综合索引指数的果蔬信息快速检索方法和基于公证链的果蔬信息跨链安全交互机制,最后基于我国首个自主可控区块链软硬件技术体系长安链开源平台设计并开发果蔬全程全息信息管理系统,以期解决传统果蔬供应链信息管理方案存在的数据覆盖面小、溯源效应周期长、各主体间协同效应差等问题。

1 果蔬全程全息信息管理模型构建

1.1 果蔬全程全息信息流转特性分析

食品全程全息是指从食品起源到消费者餐桌的整个生命周期中,对涉及到食品安全风险的所有相关信息以及供应链管理相关信息的综合考虑。这些信息包括食品供应链各环节中与食品安全相关的直接信息和有潜在关联的间接信息,还包括业务信息等与企业供应链管理相关的信息。通过对食品全程

全息的考虑，在提高食品供应链的可信度和透明度的同时，可以全面评估食品供应链存在的食品安全风险，确保可以及时采取相应的措施来降低风险发生的概率，保障食品的质量安全。同时促进食品供应链不同参与方之间的紧密协作、相互支持，共同推动食品产业的高效运作与协同发展。本研究以果蔬全程全息作为研究对象，果蔬全程全息信息如表 1 所示。

表 1　果蔬全程全息信息

Tab.1　Full-process and information of fruits and vegetables

果蔬全程全息环节		多维数据分类			
		基本信息	危害物信息	环境监测信息	业务信息
种植		种植基地信息：名称、地址、联系方式、资质等；种植信息：质量控制体系、果蔬种类、种子来源、种苗质量、种植时间、收获时间等；人为操作信息：灌溉排水时间、疾病防治信息、肥料信息及使用记录、农药信息及使用记录、种植和收获方式等；种植土壤信息：土壤类型、土壤质量、土壤墒情、土壤盐度、土壤 pH 值等	真菌毒素：刀菌、木霉、单端孢等；重金属：铅、镉、汞等；农药残留：毒死蜱、啶虫脒、伏杀硫磷等；病虫害：霜霉病、枯萎病、灰霉病、炭疽病等；灌溉水源及地下水污染：氢氧化物、苯酚、动物粪便致病菌、可溶性固体物等	环境实时信息：温湿度、光照强度、气候类型、昼夜温差、降水量等；其他环境信息：视频图像信息；人为、自然灾害信息	交易记录、成本信息、人员信息、违规记录、坏果率、违规记录
收储	收购	收购记录、抽检记录、果蔬种类、企业信息、产品信息	真菌毒素：展青霉素产毒菌、赭曲霉毒素产毒菌等；害虫：烟粉虱、白粉虱、蓟马、叶螨、蚜虫、介壳虫、斑潜蝇等；其他危害物：保鲜剂残留等	环境实时信息：温湿度、挥发性有机化合物等；其他环境信息：视频图像信息；人为、自然灾害信息	交易记录、收购价格、成本信息、人员信息、腐损率、违规记录
	除杂	除杂方式、杂质种类、含杂量、除杂率			
	贮藏	收储企业信息：名称、地址、联系方式、资质等；入库及出库记录；保鲜方式；保鲜剂信息、使用记录和使用时间			
加工	预冷	预冷方法选择、预冷温度、预冷时间、预冷机器设备信息	真菌毒素：漆斑霉、轮枝孢、黑色葡萄状穗霉、展青霉素产毒菌等；重金属：铅、镉、汞等；食品接触材料污染物：纸和木制包装（防腐剂、溶剂、粘合剂、光引发剂等）；塑料包装（邻苯二甲酸酯类化合物等塑化剂、2,6-二叔丁基对苯醌等）；玻璃、陶瓷以及金属包装（重金属、甲醇、酚等）；其他危害物质：非法添加剂；保鲜剂残留；易致敏物质等	环境实时信息：温湿度、挥发性有机化合物等；其他环境信息：视频图像信息；人为、自然灾害信息	配料信息、食品添加剂使用记录、加工数量、交易记录、成本信息、人员信息、机密技术、加工价格、加工损失率、违规记录
	去皮	去皮方法选择、磨料信息、去皮试剂信息、去皮容器温度、设备信息			
	保鲜	保鲜方法选择；包装材料；保鲜剂信息；保鲜酶使用记录、时间；清洗剂使用记录			
	干燥	干燥方法选择、干燥卫生信息、干燥机器设备信息			
	包装	包装工艺及材料信息、包装时间、产品包装编号、产品批次号			
	其他	加工企业信息：名称、地址、联系方式、资质等；检测记录；灭菌工艺；清洁记录			
仓储		仓储企业信息：名称、地址、联系方式、资质等；库存编号；产品来源；产品数量；入库时间；质检编号；出库时间	真菌毒素：黄曲霉毒素、链格孢霉毒素、赭曲霉毒素、单端孢霉烯族毒素等	环境实时信息：温湿度、挥发性有机化合物等；其他环境信息：视频图像信息；人为、自然灾害信息	交易记录、成本信息、人员信息、腐损率、违规记录
运输		运输企业信息：名称、地址、联系方式、资质等；运输负责人信息；运输车辆信息；出发地及出发时间；途经城市与目的地；抵达时间；车辆内部的温度及卫生情况	运输过程中温湿度异变霉生成的真菌与毒素、其他真菌毒素、物理杂质	环境实时信息：温湿度、挥发性有机化合物等；其他环境信息：视频图像信息；人为、自然灾害信息	交易记录、成本信息、人员信息、腐损率、违规记录
销售		销售企业信息：名称、地址、联系方式、资质等；产品信息：名称；进货时间和编号；产品存储位置；生产日期和保质期；出货时间；抽检记录；保鲜储藏设备等	真菌毒素、保鲜剂残留、物理杂质、真菌毒素、卫生情况	环境实时信息：温湿度、挥发性有机化合物含量等；其他环境信息：视频图像信息；人为、自然灾害信息	交易记录、成本信息、人员信息、腐损率、违规记录

表 1 中包含了果蔬供应链从农田到消费者手中的 6 个重要环节，其中每个环节可能包含多个子环节，每个子环节也包含多个具体步骤，如加工环节包含预冷、去皮、保鲜、干燥、包装 5 个子环节，其中保鲜子环节包含清洗、使用保鲜剂等具体步骤。除人工录入外，部分环节的信息通过监控摄像头、温湿度传感器、RFID 射频识别设备、标签扫描设备等物联网设备进行自动化采集，有效提高数据准确性和时效性。果蔬全程全息信息不是都与共享、追溯和监管相关，所以需

要各环节主体企业根据需求将信息按敏感程度分类上传至系统进行验证并加密上链存储，系统根据不同用户分配不同的访问权限，保护企业敏感数据不被泄露。

1.2 基于多链的果蔬全程全息信息管理模型框架

在果蔬全程全息流转特性分析的基础上构建了基于多链的果蔬全程全息信息管理模型，如图 1 所示。将果蔬产品从种植到销售的 6 个环节，通过多链隔离技术构建 6 条独立的局部区块链，不同环节的企业可以在参与环节的局部链上记录和管理数据，各环节链可通过公证链进行信息安全交互。同时设立一条追溯链，各环节企业将公开数据上传至追溯链，消费者与监管部门可以在追溯链上进行防伪、追溯等操作。

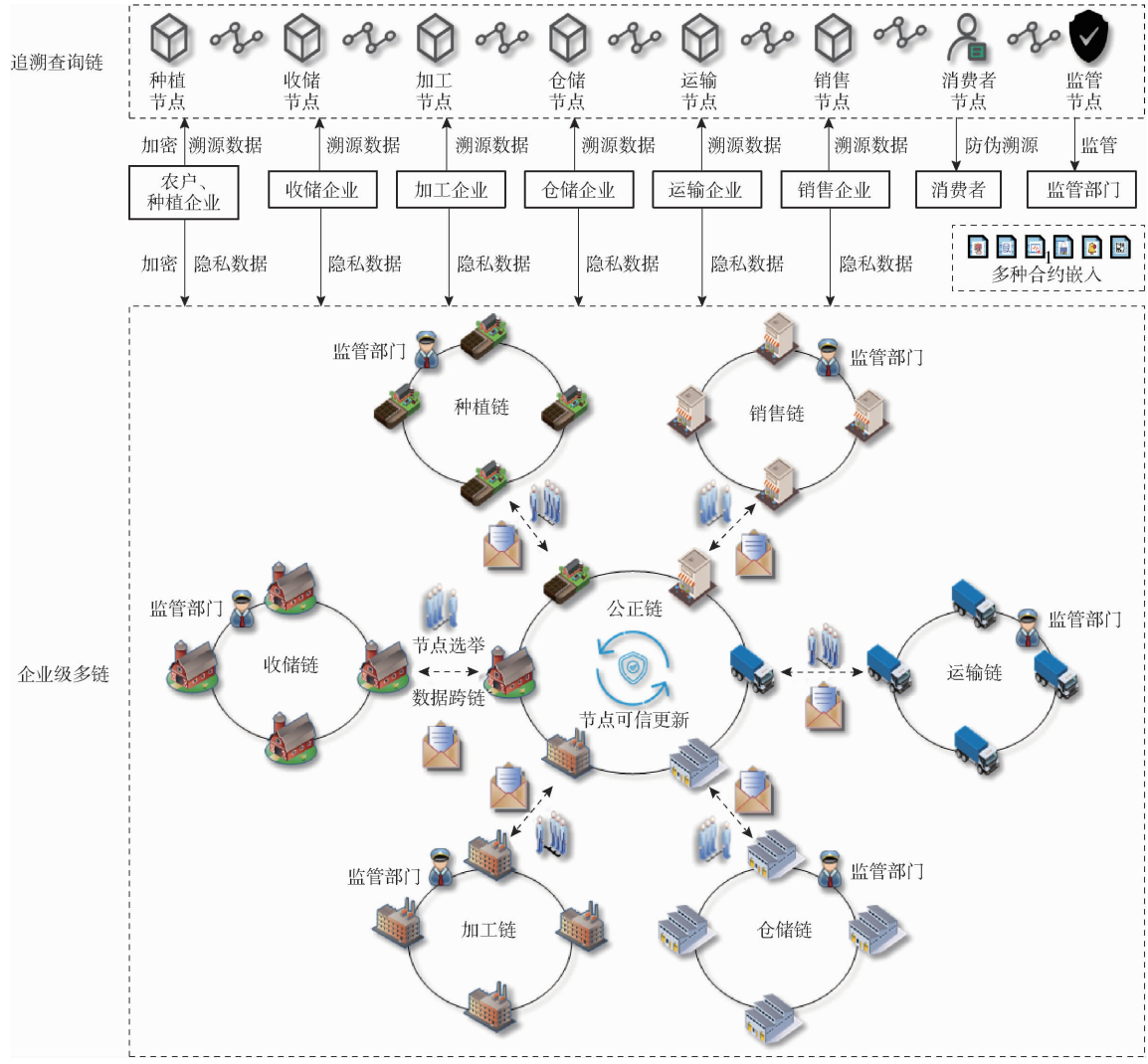

图 1 基于多链的果蔬全程全息信息管理模型

Fig. 1 Model of a multi-chain-based fruit and vegetable full-process and information management

企业可根据需求将信息分为公开数据和隐私数据，将两类数据通过不同的存证方式上链存储到两类局部链。追溯链存储公开数据，企业级多链存储隐私数据。公开数据是指果蔬产品从种植到销售各环节可公开数据，用于追溯产品的来源与流通路径，以确保产品的质量和安全，同时为监管部门提供证据支撑，协助监管部门对产品信息进行全流程多维度的精准追踪和高效监督。隐私数据是指在供应链各环节中，对企业具有重要价值和保密性的信息，有效地监管和保护这些敏感数据的安全，是保障企业利益和商业信誉的关键。在果蔬全程全息信息管理中，由于不同环节企业属于不同局部链，监管范围分散，难以构建高效的共同监管体系，多个链条之间的数据互相独立，导致监管部门难以快速获得突发质量安全事件相关的全部信息。为解决上述问题，本研究将监管部门加入企业级多链中的每条局部链，实现穿透式实时监管，从而加强监管决策的准确性和效率。

1.3 果蔬全程全息信息上链存储模式

为满足果蔬隐私数据的上链需求，本文采用分享隐私存证的隐私数据上链方式。首先使用 AES 算法对隐私数据进行对称加密，将果蔬隐私数据明

文 p_r 和通过用户提供的任意密码进行密钥扩展后得到的对称加密密钥 k_{AES} 作为加密函数的参数输入，通过 AES 加密函数 δ 输出密文 c_r，公式为

$$c_r = \delta(k_{AES}, p_r) \tag{1}$$

选取任意两个安全大素数 A、B，将 A 和 B 相乘得到 N，即

$$N = AB \tag{2}$$

T 是将 A 和 B 分别减 1 后差的积，即

$$T = (A-1)(B-1) \tag{3}$$

选择一个与 T 互质且小于 T 的整数 E 作为一个密钥，另一个密钥 D 计算公式为

$$DE \bmod T = 1 \tag{4}$$

求出 N、E、D 后，将 (N,E) 定义为公钥，(N,D) 定义为私钥，由此方法生成不同的非对称密钥发放给不同身份的用户。

使用公钥加密对称密钥 k_{AES} 得到密钥密文 c_{RSA}，即

$$c_{RSA} = k_{AES}^{E} \bmod N \tag{5}$$

当私钥持有者获取到密钥密文 c_{RSA} 后，通过私钥解密可以获得对称加密密钥 k_{AES}，解密过程为

$$k_{AES} = c_{RSA}^{D} \bmod N \tag{6}$$

得到对称加密密钥 k_{AES} 后，通过将密文 c_r 和密钥 k_{AES} 作为解密函数的参数输入，AES 解密函数 η 会输出果蔬隐私数据明文 p_r，解密过程为

$$p_r = \eta(k_{AES}, c_r) \tag{7}$$

经过此加密和解密过程，可以控制不同身份用户对隐私数据的访问权限。加密解密流程如图 2 所示。

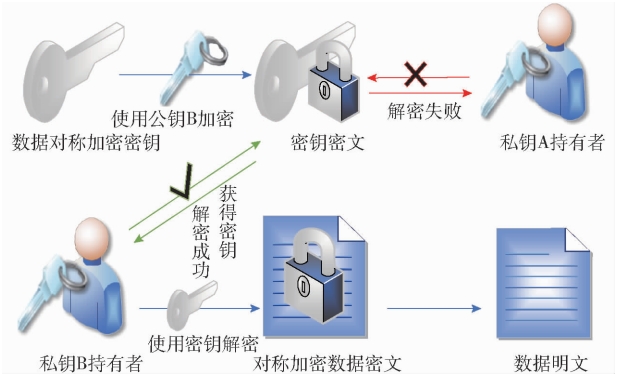

图 2　果蔬隐私数据加密解密流程

Fig. 2　Encryption and decryption process of fruit and vegetable privacy data

在上链存储模式中，分发非对称密钥是确保数据隐私安全的重要环节。通过证书颁发机构(CA)，生成和分发非对称密钥对，参与链上节点的用户可以通过申请证书来获取相应的非对称密钥对。根据具体的企业链需求进行调整和扩展，以确保隐私数据的安全和访问控制。

本模型中各企业通过追溯数据智能合约将通过追溯链节点共识的果蔬公开数据记录在追溯链账本，果蔬隐私数据通过各环节企业的隐私数据智能合约上传至企业链账本。相比于只使用关系型数据库的复杂模式，将果蔬全程全息中的各类数据储存在不同数据库中，可以更加高效地追溯果蔬全程全息中的大量文档、图像、视频等数据。本模型使用 LevelDB 和 TikvDB 存储区块数据，IPFS 存储追溯链账本和企业链账本中的图像、视频等大型文件，Mysql 存储元数据和部分索引标识等辅助数据。其中 TikvDB 数据库作为状态数据库，因其具有强大的富查询能力，通过视图查询和 Mango 查询，可以为监管部门提供灵活、高效、可扩展的查询方式，帮助监管部门实时获得追溯链数据和企业链数据，快速定位风险信息，进行精准高效的监管，存储和查询过程如图 3 所示。此外，本模型中不同的存储介质会协同工作，每种存储介质存储不同的数据，并且采用 Binlog 记录所有更新语句，同时存储介质之间也进行数据同步和数据共享，以确保不同节点上的数据一致性。

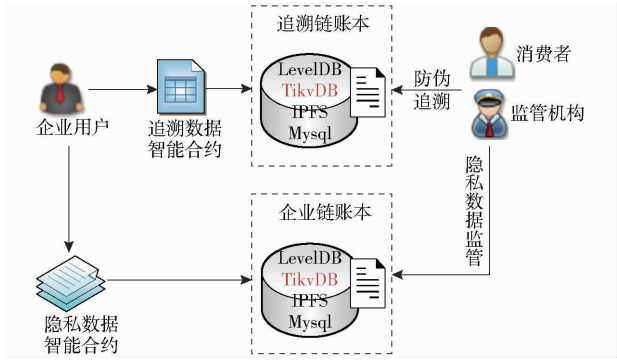

图 3　果蔬全程全息信息存储流程

Fig. 3　Full-process and information storage and query process of fruits and vegetables

1.4　基于区块综合索引指数的信息快速检索方法

新鲜果蔬保质期短且容易受到环境污染，易出现腐烂、变质等情况，因此新鲜果蔬的监管和溯源对时效性要求很高。若发现某批次产品存在质量问题，需要快速定位问题批次，及时采取措施，如召回、处理或改进，以减少质量问题的影响范围。消费者关注的重点之一就是果蔬产品的新鲜程度，高时效性的溯源系统可以为消费者提供及时的产品信息。而果蔬全程全息信息规模庞大，导致可能存在大量的数据冗余，传统区块链检索方法效率较低，数据溯源和监管需要遍历整个区块链上的全部交易，检索特定数据时会浪费大量的时间和计算资源。为满足新鲜果蔬数据的快速监管和溯源需求，本文在局部链中设计了基于布谷鸟过滤器的 CMerkle 树区块结

构,同时引入了基于区块综合索引指数的跳表检索结构,实现对果蔬全程全息信息的快速检索。

1.4.1 基于布谷鸟过滤器的 CMerkle 树区块结构

布谷鸟过滤器由一个二进制向量和一系列随机映射函数组成,当需要判断一个交易是否存在于区块中时,通过随机映射函数计算其在二进制向量中的位置,并检查对应位置的计数值是否大于零。如果计数值大于零,则可能存在该交易;如果等于零,则肯定不存在该交易。布谷鸟过滤器采用复杂的数据结构和替换策略,可以通过牺牲一定的空间消耗来降低误判率,提高了检索的准确率,相比于常用的传统布隆过滤器有更好的查询性能和更低的空间开销[24-25]。布谷鸟过滤器使用特定的哈希函数对一个键进行哈希,并用桶内位数 M 进行取模,计算得到第 1 个桶的索引,将第 1 个桶索引的指纹和哈希进行异或得到第 2 个候选桶的索引。在桶中迁走一个键时,可以直接用当前桶索引和桶中的指纹计算出备用桶。桶索引计算过程为

$$b_1 = \mathrm{Hash}(x) \bmod M \tag{8}$$

$$b_2 = (b_1 \oplus \mathrm{Hash}(\mathrm{Finger}(x))) \bmod M \tag{9}$$

式中 $\mathrm{Hash}(x)$——使用的哈希函数

$\mathrm{Finger}(x)$——数据 x 的数据项指纹

b_1、b_2——两个备用桶的索引

数据插入过滤器原理如图 4 所示,当 2 个哈希函数都被映射到了已存储条目的桶 6 和桶 2 时,桶 4 的条目被迁移到桶 3,桶 6 的条目被迁移到桶 4,项目 x 可插入桶 6 中。哈希函数和桶中座位数量可以动态调整,这样可以在提高时间效率的同时,提高空间效率。

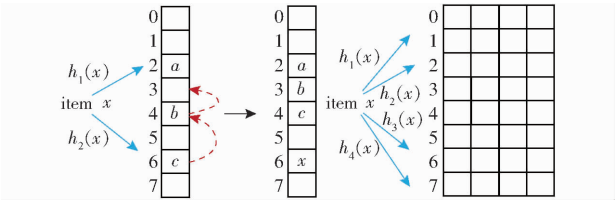

图 4 数据插入布谷鸟过滤器原理图

Fig. 4 Schematic of data insertion cuckoo filter

传统的 Merkle 树的查找元素效率相对较低,每个内部节点的哈希值都是根据其子节点的哈希值计算得出的,因此要验证一个子叶节点是否存在于 Merkle 树中,需要从根节点开始逐级向下验证哈希值,直到找到目标子叶节点或者验证失败为止。这个过程可能需要遍历多个层级的节点,对于果蔬全程全息背景下数据规模庞大的 Merkle 树来说,可能会产生较大的计算开销,从而影响到溯源查询效率。

为解决上述问题,本文提出了基于布谷鸟过滤器的 CMerkle 树区块结构,如图 5 所示。

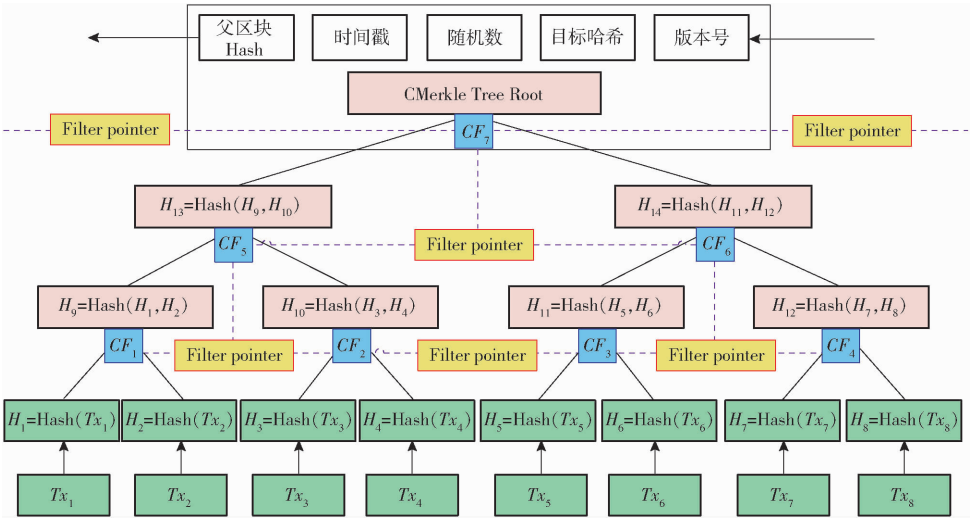

图 5 CMerkle 树区块结构

Fig. 5 CMerkle tree block structure

构建 CMerkle 树索引结构时,在原有的 Merkle 树的基础上将布谷鸟过滤器(Cuckoo filter,CF)加入每个非子叶节点。将果蔬数据分为固定大小的偶数个数据块,将每一个数据块进行 SHA-256 计算得到的 Hash 值记录到子叶节点,子树节点记录了其所有子叶节点记录的 Hash 值拼接后再次计算得到的 Hash 值。布谷鸟过滤器记录了所有子树的交易溯源码,树根部位的布谷鸟过滤器存储了整个果蔬区块的交易溯源信息。布谷鸟过滤器之间通过过滤器指针链接,实现过滤器间的快速跳转。查找区块时,若树根中没发现目标信息即可跳转到下一区块,避免在区块体中进行无效搜索,从而缩短检索耗时;若存在目标信息则利用布谷鸟过滤器对左右子树进行下一步判断,利用广度优先算法对子树进行顺序判断,存在即进入下一层,直至检索到目标数据。布谷鸟过滤器存储数据为交易信息的映射,Merkle 树结

构以及 SHA－256 加密算法可以防止信息被恶意篡改，同时根部的布谷鸟过滤器存储的 Hash 值保存在区块头中，以防交易信息被恶意用户出于个人利益非法修改，保证交易溯源信息的真实性。

1.4.2　基于区块综合索引指数的果蔬信息跳表检索

跳表是一种随机化的数据结构，通过并联链表实现快速插入、删除、查询，且复杂度低，通过“空间换取时间”的思想提高效率[26－27]。

随着果蔬信息的不断上链，区块链长度会逐渐增加，因此需要动态插入索引以保障时间复杂度维持在 $O(\lg N)$。本文引入区块综合索引指数 I_{rs} 对所有区块索引顺序进行排序。区块综合索引指数是由果蔬产品生产周期内某区块的被访问次数与该区块中包含风险信息的数量共同决定，即

$$I_{rs} = P\mathrm{lb}\,(n+2) \tag{10}$$

其中

$$P = \frac{V_i}{V_{all}} \tag{11}$$

式中　n——区块中包含的风险信息的数量

V——访问次数

P——搜索指数，是一个果蔬产品生产周期中区块 i 被访问次数在局部链中所有区块被访问总数中的占比

构建索引架构时根据每个区块的区块综合索引指数进行排序，区块综合索引指数越大，在跳表中的索引层级越高。果蔬区块的跳表索引以及区块标识通过键值对的形式存储在 LevelDB 中。检索时首先从最高级索引开始检索，这样可以减少区块综合索引指数较低区块对检索耗时的影响，从而提高对区块综合索引指数较高区块的搜索效率。跳表中最高索引层级根据当前区块高度估算得出，并会随着区块总量增加而逐渐增加，每一级区块均由低一级别区块中区块综合索引指数前 1/2 的区块中选出，索引层数越高区块数量越少，如图 6 所示。

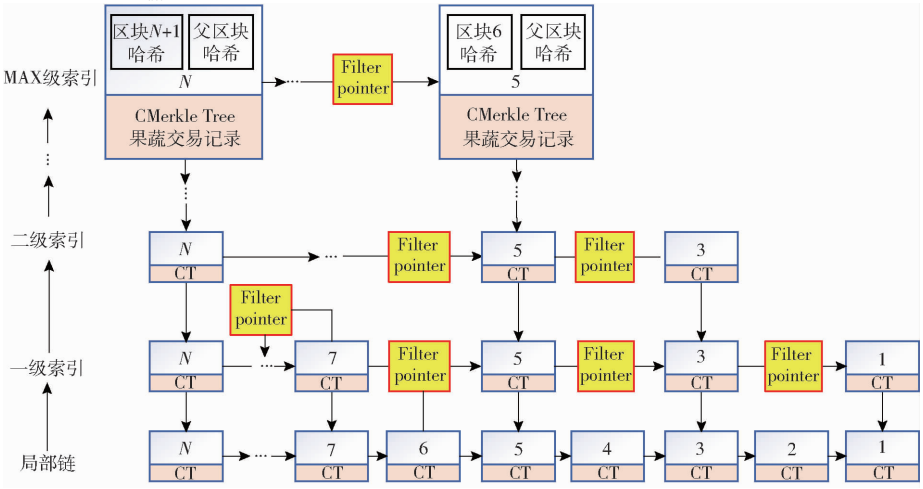

图 6　果蔬区块跳表检索结构图

Fig. 6　Search structure of fruit and vegetable block jump table

1.5　基于 TBFT 和公证链的跨链共识模式

果蔬全程全息中涉及到的各个节点大多是相互信任的，符合 PBFT 算法要求至少 2/3 节点被信任的前提条件，且相比于公链常用的 PoW、PoS 和 DPoS 等算法，PBFT 拥有更高的响应速度和数据吞吐量，更好地满足果蔬供应链信息监管系统的需求[28]。传统的 PBFT 算法在主节点失效时才会更换主节点，且更换主节点时视图切换协议复杂。本文采用长安链平台上的 TBFT 共识机制作为果蔬全程全息各环节局部链的链内共识机制。TBFT 是一种基于 Tendermint 算法的拜占庭容错共识算法，对传统 PBFT 复杂的视图切换协议进行了优化，将固定的视图切换流程分散到各个共识过程之中，每进行预先设定区块数量的提交后就会进行一次主节点的轮换，实现更好的公平性，以及减少了视图更换的时间浪费。同时，TBFT 可以通过共识投票将与读写集不一致的交易进行剔除，从而保证链的稳定性和正确性，与其他共识算法相比更适用于本文研究的果蔬全程全息信息的共识需求。

公证人机制能支持不同结构的区块链进行跨链交易，原理简单，无需进行复杂的工作量证明，相较于其他跨链机制有着更高的处理效率，更适用于具有高时效性要求的果蔬全程全息信息管理[29]。而传统的公证人机制存在“中心化”争议，违背了区块链“去中心化”的思想，过于依赖公证人节点的信誉，存在公证人节点作恶情况。针对以上问题，本文提出了一种基于公证链的跨链机制，将公证链作为信息传输的媒介，公证链中各节点由果蔬全程全息多链架构中不同局部链中的节点选举产生，并会周期性更新，舍弃受信第三方，解决了传统公证人机制

存在的中心化问题。当进行跨链操作时,数据拥有者会将信息从其局部链上传至公证链,再通过公证链传递给接收链进行读取,保证了局部链间的数据隔离。

本文所提出的公证链跨链机制以图 7 为例,具体步骤如下:

(1)用户发送跨链请求与用户非对称加密公钥 B 到种植链某一节点,请求要读取收储链中某个果蔬收储链的隐私数据。

(2)种植链的公证人节点会将跨链请求以及公钥 B 封装成跨链事务上传至公证链。

(3)收储链的公证人节点从公证链读取到跨链请求与公钥 B 并写入收储链。

(4)收储链通过公证人节点将使用公钥 B 加密后密钥密文以及跨链果蔬收储隐私数据的密文封装成跨链事务上传至公证链。

(5)种植链的公证人节点读取到跨链事务并将其写入种植链。

(6)用户通过种植链节点读取并解密获取目标数据。

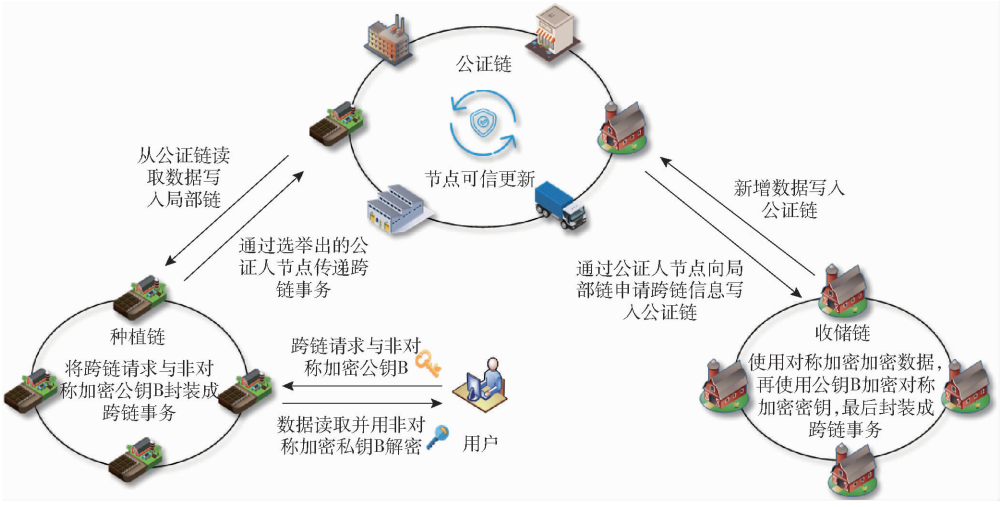

图 7 公证链机制跨链流程

Fig. 7 Cross-chain process of notary chain mechanism

2 基于长安链的果蔬全程全息信息管理系统设计与实现

本文设计的基于多链的果蔬全程全息信息管理系统围绕果蔬全程全息信息管理模型构建,对整个果蔬供应链进行全程多维度实时监管,为消费者提供溯源服务,全方面保障果蔬的食品安全。本系统可以帮助果蔬企业更好地管理供应链信息,促进各环节企业间信息交互,避免出现信息不对称和不透明等问题,同时保护企业隐私数据的安全。

2.1 系统架构设计

本文提出的基于多链的果蔬全程全息信息管理系统采用我国首个自主可控区块链软硬件技术体系长安链开源区块链平台开发[30]。结合果蔬全程全息各环节企业、用户、监管部门的不同需求,采用通道技术构建多链架构,保障公开数据的公开透明以及企业间隐私数据的安全交互,同时实现穿透式监管。本文设计的系统整体架构如图 8 所示,该系统架构共分为:物理层、数据层、协议层、合约层、业务层、应用层。

物理层通过生产设备、各类传感器、GPS 技术、射频识别、手持终端设备、视频监控等采集设备,实时获取果蔬全程全息各环节中的各项数据;定制统一的数据采集规范,实现采集数据的标准化,提高数据质量,减少数据处理成本,提升数据分析效率;数据处理包括对数据进行加工、计算、清洗、整理、筛选、转化、融合等操作。

数据层包括各类数据库和区块账本,将物理层采集并处理的关键数据、时间戳、Hash 值、数字签名等信息上链储存到长安链的区块链网络中,其中不同节点身份权限不同,所能访问的内容不同;本地数据库提供数据备份和恢复、离线处理等功能;TikvDB 数据库提供扩展查询功能,构建 key - value 键值索引,提高追溯数据的查询效率;产品各环节设备采集到的图像、音频、视频文件通过分布式数据库 IPFS 进行存储,并结合链上哈希的方式为监管部门提供完整、真实的风险信息。

协议层包括 TCP/IP 通讯协议、P2P 网络协议、TBFT 共识机制、基于公证链的跨链安全交互机制,在提高效率的同时,保障果蔬全程全息各环节数据不被篡改、真实可信和保障企业间隐私数据交互的安全可靠。

合约层包括用户智能合约、数据可信交互智能合约以及风险预警智能合约,同时将国家制订的多

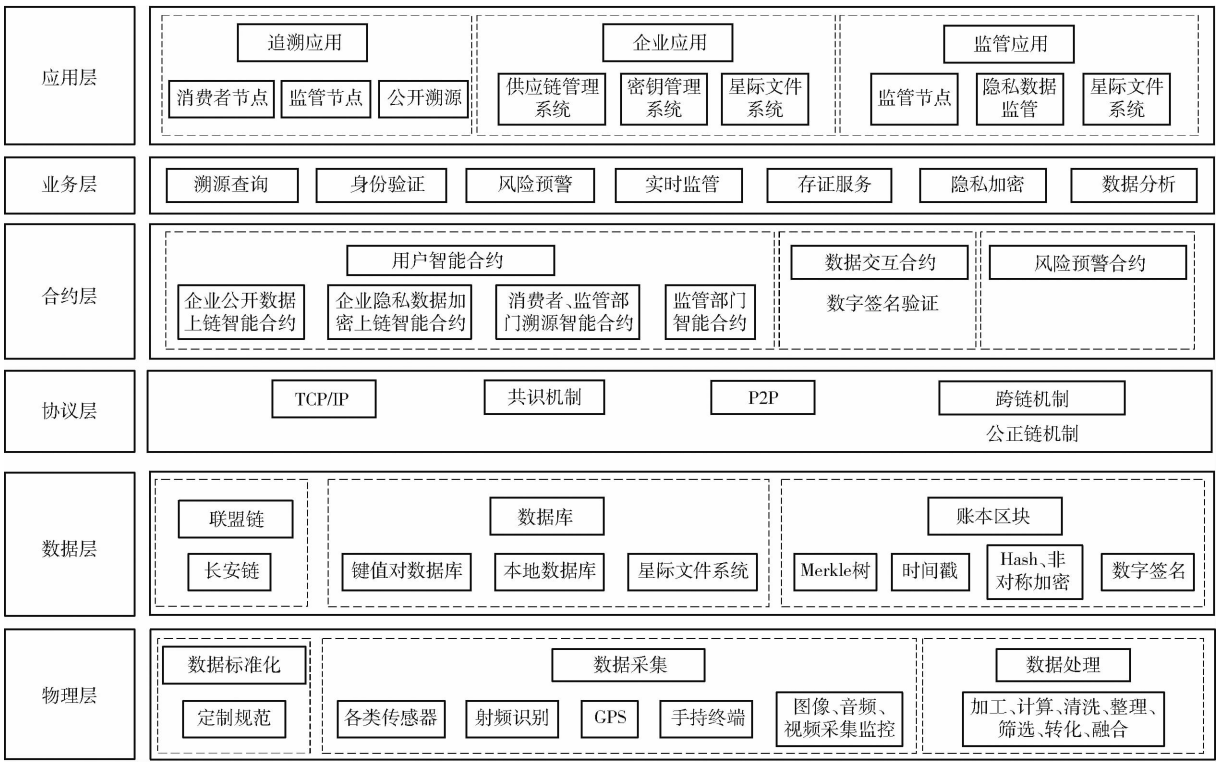

图 8　系统架构设计

Fig. 8　System architecture design

种监管条例和行动纲要嵌入其中，实现果蔬质量的规范化管理。用户智能合约针对不同用户需求采用定制化服务，具体包括企业数据上链智能合约、企业隐私数据加密智能合约、溯源智能合约、监管部门智能合约等。数据可信交互智能合约通过数字签名算法验证数据是否被篡改。风险预警智能合约通过预先设定好的风险预警规则，自动监控数据、交易和操作，对风险信息以及风险事件实时监管，协助企业和监管部门更好地管理和处理风险。

业务层作为果蔬全程全息信息管理系统的核心，涵盖整个系统的溯源查询、身份验证、风险预警、实时监管、存证服务、隐私加密、数据分析等业务。

应用层根据不同用户的不同需求将具体应用分为追溯应用、企业应用、监管应用 3 类。追溯应用为消费者和监管部门提供追溯服务；企业应用为企业提供供应链管理和密钥管理等服务；监管应用为监管部门提供隐私数据监管服务。

2.2　功能模块设计

完整的果蔬全程全息信息管理系统的功能需要满足监管部门、企业用户、消费者 3 类用户的不同需求，功能模块如图 9 所示。在果蔬全程全息监管系统中，监管部门拥有最高权限，负责审批企业用户注册、数据修改请求，并对违规行为进行处理。企业用户作为果蔬全程全息各环节的主体，需上传实时信息至区块链，并通过数据交互和加密模块保证信息的安全性和隐私性。消费者可以利用溯源防伪验证模块查询产品信息，并通过反馈和举报功能推动供应链各环节优化和改进，确保果蔬产品品质和安全性。

2.3　系统实现

本研究的测试环境基于长安链 v2.2.1 搭建，使用的虚拟机系统版本为 Ubuntu 20.04，硬件配置为：16 GB 内存、8 核 Intel i7 - 12700 2.30 GHz 处理器、

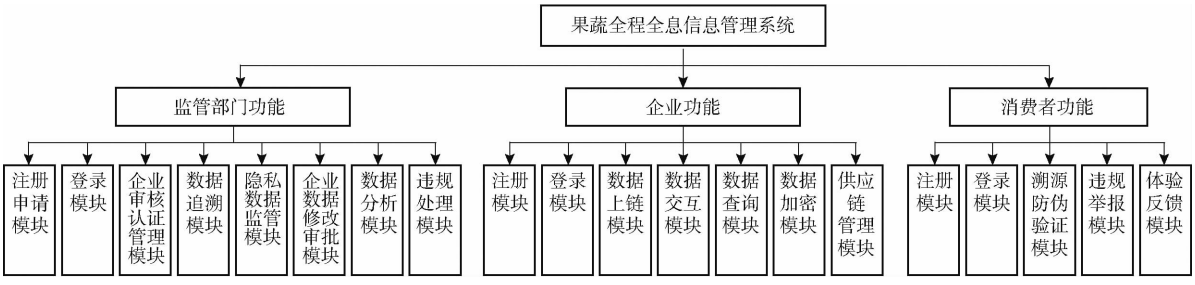

图 9　系统功能模块设计

Fig. 9　Design of system functional modules

150 GB 硬盘。为便于系统的维护和扩展,采用 B/S 服务器系统架构,基于 TCP/IP 协议,并以 Ubuntu 作为操作系统,Docker 作为应用容器引擎,Golang、JavaScript、Java 作为主要编程语言,使用 Vue、Gin 进行前、后端开发。

(1)数据库

数据库设计采用区块链与数据库技术相融合,使用云数据库、线下数据库、状态数据库、IPFS 星际文件系统 4 类数据库进行相关数据的存储。为了节点的快速同步,以及便于果蔬历史数据的快速查验,增加了读写集数据库,基于写集更新状态数据库,读写集的存储采用支持读写集的 LevelDB 数据库。果蔬全程全息信息管理平台调用智能合约产生的业务数据种类繁多,数据量大,需要多地部署并需要具备高可靠性,对于查询的需求较高,因此采用支持复杂查询和聚合操作等强大功能的 TikvDB 数据库,实现对果蔬产品状态的实时监管。为满足后续果蔬信息的溯源监管,以及查看产品状态的流转,建立了基于 LevelDB 的索引数据库,主要存储信息包括:基于区块综合索引指数的跳表索引、状态修改信息、账户交易历史、合约调用历史。对于公开数据和隐私数据的存储,本系统采用关系型数据库 Mysql 结合 IPFS 星际文件系统,建立果蔬全程全息风险数据库,对果蔬全程全息信息及区块链网络中的关键信息进行记录,提高数据的存储和传输效率,保障数据的可靠性与一致性。

为保证数据库数据的一致性,增加 Binlog 功能,首先将果蔬区块以文件形式写入磁盘进行缓存,再将磁盘上的数据写入各类数据库,预防数据库故障时出现数据丢失,同时提高数据库读取数据的效率。整体的数据库架构如图 10 所示。

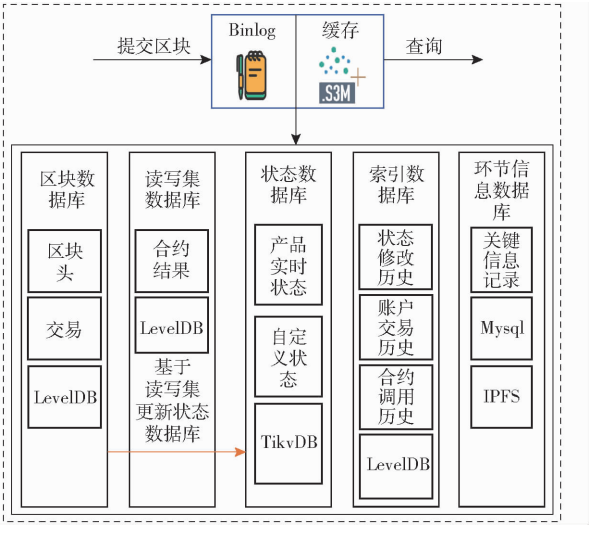

图 10 数据库架构设计

Fig. 10 Database architecture design

(2)服务器端

长安链网络的运行、测试和智能合约的部署都在 Ubuntu 系统中的 Docker 容器下完成。通过长安链的可视化界面对底链配置进行管理、浏览和资源监控。采用单机多节点部署,将果蔬全程全息上的 6 个环节分别建立 6 条企业局部链,每条局部链中包含多个企业以及监管部门,分别作为其中的不同组织,每个组织包含多个节点,实现各组织的背书、记账等功能。建立追溯链与每条局部链相连接,加入监管节点以及消费者节点,实现公开数据的追溯。长安链区块链网络中使用的证书类型有 4 大类:CA 证书、组织证书、节点证书、用户证书。CA 证书代表有签发能力的证书,可以签发下级证书。用户证书和节点证书不具备签发能力。CA 证书可通过 chainmaker cryptogen 或者自建的 CA 证书服务生成,也可通过向证书颁发机构申请获得,本组织的所有节点证书以及用户证书都是由此 CA 证书签发生成。本系统属于面向强权控制场景,采用长安链提供的 PermissionedWithCert 模式,使用数字证书的标识方法,每个接入的节点都需要得到 CA 颁发的数字证书,在证书字段中附加组织和角色信息,发出的每笔交易都需要附加数字签名。PermissionedWithCert 模式采用基于角色的权限控制模型,链上需进行权限管理操作,将用户绑定到某一组织,再将资源绑定到其组织,以此方式实现资源和用户的关联。系统后端多链配置信息如图 11 所示。

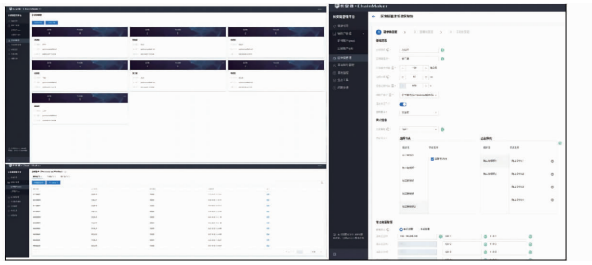

图 11 系统后端多链配置

Fig. 11 System backend multi-chain configuration

智能合约是运行在长安链上的一组“动态代码”,通过动态部署实现长安链上的具体业务和逻辑。作为一种计算机程序或交易协议,智能合约自动执行合约中规定的计算、交易、记录和其他操作,可以在没有中间人的情况下进行交易、资产转移以及其他合同义务,确保交易的透明、可靠、安全,同时也能明显提高交易效率以及降低成本。用户在区块链上发起的交易,会首先进入交易池,交易池会存放所有链上交易,经过共识驱动在合约虚拟机中执行交易。本系统智能合约采用 Golang 作为智能合约的主要编程语言,基于 Docker 类型的 Go 合约可以直接编译成平台机器码压缩再进行部署和调用。本

系统使用的部分智能合约如图 12 所示。

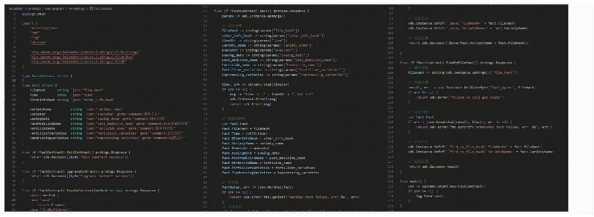

图 12　部分智能合约展示

Fig. 12　Partial smart contract display

3　实验验证与案例分析

3.1　检索效率分析

3.1.1　区块内数据检索效率

测试用到的区块和数据集来源于 xblock 平台，此平台提供了比特币、以太坊等区块链领域几大主流平台的数据集。首先进行了数据检索效率的测试，区块内数据的检索效率是影响果蔬全程全息信息溯源监管效率的关键因素。对本文提出的 CMerkle 树区块结构中的布谷鸟过滤器进行测试，在数据数量分别为 1 000、5 000、10 000、50 000、100 000 的 5 种规模下与传统布隆过滤器进行对比，两种过滤器在各数据量级都进行 60 轮测试并求均值，实验结果如图 13 所示。实验结果表明在数据数量为 10 000 及以下时，布隆过滤器和布谷鸟过滤器的检索效率差距并不大，布谷鸟过滤器略优于布隆过滤器。在数据数量为 100 000 时，布隆过滤器和布谷鸟过滤器的检索耗时差距明显，分别为 15.9 ms 和 7.13 ms。结果表明，布谷鸟过滤器相比布隆过滤拥有更高的检索效率，同时更加灵活，适用于数据量庞大的果蔬全程全息信息管理。

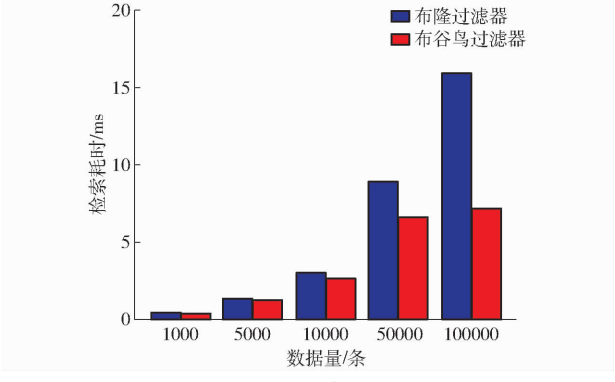

图 13　过滤器检索耗时对比图

Fig. 13　Comparison graph of filter retrieval time consumption

3.1.2　目标区块检索效率

分别选取了 10 000 个区块和 50 000 个区块作为测试数据集，对比了传统链表检索方式和本文提出的基于区块综合索引指数的跳表索引结构的检索效率。首先随机将测试集区块根据区块综合索引指数进行排序，在排序前 1/2 区块中随机选取 1 000 个目标区块进行 60 轮检索。如图 14a 所示，传统链表式搜索在总区块量为 10 000 和 50 000 下的平均检索耗时分别为 7.37 ms 和 38.07 ms。如图 14b 所示，基于本文提出的索引结构在总区块数为 10 000 和 50 000 下的平均检索耗时分别为 0.21 ms 和 0.31 ms。实验结果表明，本文提出的基于区块综合索引指数的跳表索引结构检索效率相较传统链表式搜索有明显提升。

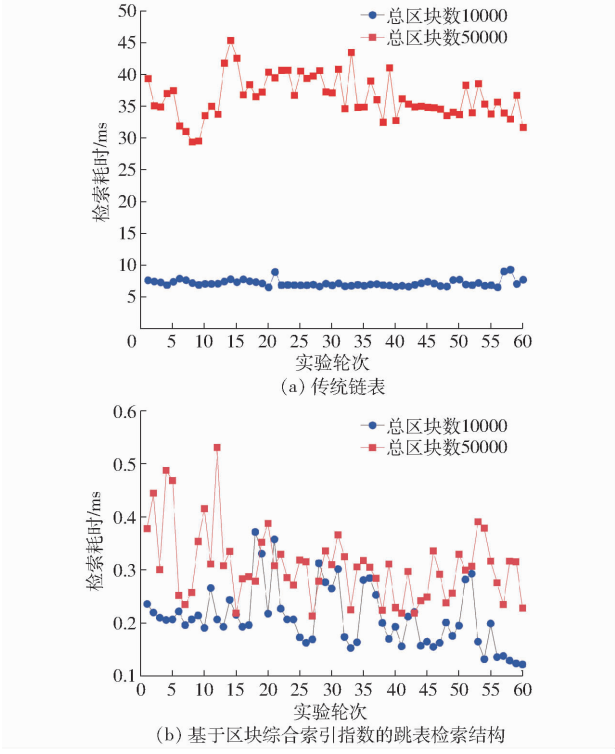

图 14　两种检索结构耗时对比

Fig. 14　Comparison of time consumption between two retrieval structures

在区块总量 3 000 ~ 50 000 每个数量级中区块综合索引指数排名前 1/2 区块中的随机 1 000 个进行检索效率测试，对本文提出的基于区块综合索引指数的跳表检索与传统链表检索的检索耗时变化趋势对比，如图 15 所示。结果表明，传统链表式检索耗时会随着区块总量增加呈现线性增长趋势，而本文提出的索引结构受区块总量影响较小，在区块量增大过程中对关键区块的索引耗时增幅小。

3.1.3　共识性能测试

使用长安链性能分析工具 time counter 2.3.1 对系统底链进行性能测试，选取区块高度 111 ~ 130 进行测试，分析了在 TBFT 共识机制下，一轮完整共识中关键阶段的耗时，实验结果如图 16 所示。总计测试 20 个区块，完成一轮共识的总耗时平均值为 75.7 ms。结果表明，共识效率满足果蔬全程全息场景下的高频交易量需求。

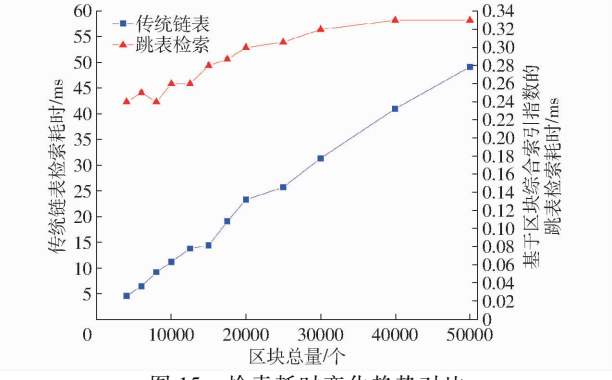

图 15 检索耗时变化趋势对比

Fig. 15 Comparison of search time consumption trends

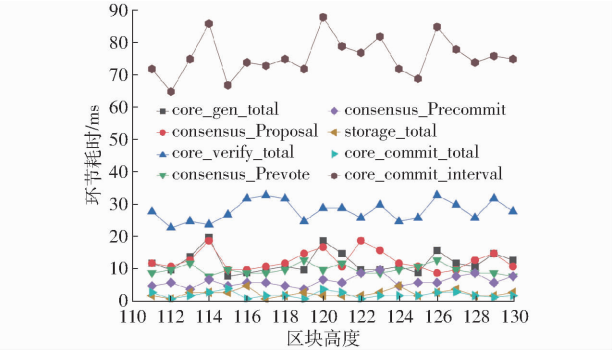

图 16 共识性能测试

Fig. 16 Consensus performance testing

首先对果蔬全程全息信息管理系统中不同权限的数据上链耗时进行了 30 轮测试，如图 17 所示。公开数据上链平均耗时为 589.03 ms，隐私数据上链平均耗时为 708.59 ms，隐私数据需要调用更多智能合约，通过分享隐私存证的加密方式进行加密，所以相比公开数据上链耗时较长。随后对公开数据和隐私数据两种数据的查询效率进行 30 轮测试，如图 18 所示。公开数据查询平均耗时为 26.87 ms，隐私数据查询过程更为复杂，查询平均耗时为 30.67 ms，可以满足不同需求用户对不同权限数据的上链和查询需求。

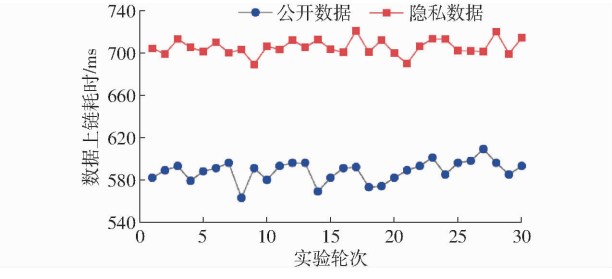

图 17 数据上链耗时

Fig. 17 Data upload blockchain time consumption

3.2 应用案例

通过对某果蔬供应链中的北京某果蔬企业进行实地调研，该企业参与的果蔬供应链环节包含收储、加工、仓储等环节，其余种植、运输、销售等环节隶属于其它企业，各企业之间的信息并不能

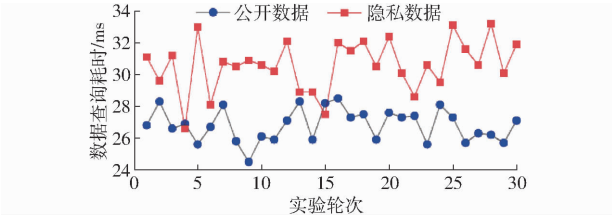

图 18 数据查询耗时

Fig. 18 Data query time consumption

很好地互联互通，无法形成一条完整的信息链，导致信息处理效率低，无法满足对果蔬全程全息信息的高效溯源监管需求，同时企业内部各环节的工厂间同样存在信息孤岛问题。经分析，采用本文设计的基于多链的果蔬全程全息信息管理系统对其信息管理模式进行优化。系统用户前端采用 TCP/IP 网络通讯协议，基于两种模型进行设计与实现。监管部门和企业用户通过 Web 端进行注册、登录、数据实时监管、数据实时管理等操作。消费者通过移动设备在 APP 上进行溯源、防伪等操作。APP 端相较使用 Web 端更加方便快捷，但 Web 端拥有的功能和权限更全面。Web 端登录时可选择监管者、企业两种身份，两者访问权限不同，可执行的操作权限不同。本系统满足监管部门多类监管需求，包括区块链管理、供应链管理、企业管理、交易管理、合约管理、产品管理、企业数据修改审批等。本系统还设计了举报中心模块，监管部门可以在举报中心查看消费者举报信息以便及时对违规企业进行处理。本系统对果蔬全程全息信息进行可视化处理，包括节点数、交易数、区块信息等，实现对果蔬全程全息的实时监控，监管部门还可以在首页通过溯源码进行快捷产品追溯。供应链管理模块可以对各环节所有用户节点的全部信息以及节点状态进行实时监控，同时可以批量或单独对用户节点进行查询、冻结、警告等操作。监管节点的权限可以访问系统中所有环节的全部数据。监管用户对节点隐私信息查询时会调用监管智能合约，系统会将指定密文解密成明文。企业用户相比监管用户增加了信息采集上传模块以及数据修改申请模块，虽然其权限方面受到限制，不能直接访问其他节点的隐私数据，但可以通过数据交互模块与其他企业进行数据的安全共享。企业用户想修改信息时需要将需要修改的信息通过分享隐私存证的方法广播至其局部链，局部链中的监管节点收到解密后进行审批，审批通过后将信息上链，同时删除其数据库中原始数据。面向监管用户与企业用户的系统 Web 端界面如图 19 所示。

系统移动端 APP 为消费者提供溯源功能，消费

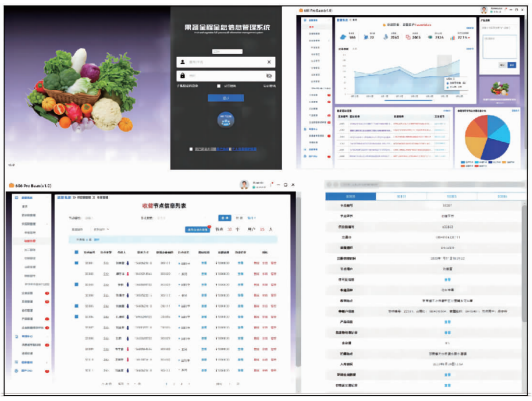

图 19　系统 Web 端界面

Fig. 19　Web interface of system

者可以在登录之后扫描果蔬溯源二维码或者输入溯源码，便可获取果蔬全程全息的全部公开溯源信息，包括产品信息、溯源信息、区块信息等。消费者也可以通过 APP 对违规信息和不合格产品进行举报，协助监管部门维护果蔬的质量安全。消费者还可以对产品进行反馈，反馈信息将发送到对应的企业用户，协助企业用户对产品进行改进与调整，面向消费者的系统 APP 端界面如图 20 所示。

图 20　系统 APP 端界面

Fig. 20　APP interface of system

3.3　对比分析

3.3.1　果蔬信息上链方式对比

果蔬全程全息信息通过传感器感知、手动录入、自动化技术等方式完成采集，常用的数据存证方式主要包括 5 种：内容存证、哈希存证、链接存证、隐私存证、分享隐私存证[28]。在果蔬全程全息信息管理背景下将 5 种数据上链方式进行比较，如表 2 所示。

内容存证和链接存证都满足公开透明和完整数据可验证的特点，对于需要上传至追溯链的公开数据，可以通过内容存证或者链接存证的方式直接上链存储。

对于需要上传至企业级多链的隐私数据，哈希存证仅可将数据内容的哈希值上链，虽然保障了数据无法被篡改，但无法满足监管者对于完整信息数据验证的需求。而隐私存证采用的是对称加密的算法对数据进行加密储存，存在密钥管理问题，无法做到链上隐私数据的安全共享。分享隐私存证首先采用对称加密对隐私数据进行加密，再使用非对称加密将对称加密使用的密钥进行加密。可以使用不同身份用户的公钥将对称加密密钥进行加密，进行不同身份用户的访问权限分配，实现隐私数据的安全共享。

表 2　果蔬信息上链方式对比

Tab. 2　Comparison of fruit and vegetable information upload blockchain methods

存证方式	果蔬信息存储需求			
	公开透明	隐私保护	完整数据验证	隐私安全共享
内容存证	√		√	
哈希存在		√		
链接存证	√		√	
隐私存证		√	√	
分享隐私存证		√	√	√

注：√表示满足该功能需求。下同。

3.3.2　系统对比

将本文提出的基于多链的果蔬全程全息信息管理系统与现有的农产品信息管理系统进行对比，结果如表 3 所示。

与其他系统相比本系统使用了去中心化的数据存储模式，构建了多链架构实现对果蔬全程全息信息穿透式监管，数据防篡改能力强，兼顾对隐私数据的分类、保护、跨链交互以及访问权限管理，采用 CMerkle 树以及 4 类数据库实现数据分类存储映射，链上使用 TBFT 算法实现高效共识。经测试，数据查询耗时小于 35 ms，相比其他系统，本系统拥有更高的溯源监管效率和企业数据管理能力。

4　结论

（1）对果蔬全程全息信息管理系统流转特性进行研究，对果蔬全程全息进行全面分析，抽象出了其中的重要环节，对各环节存在的信息进行多维度分类。

（2）构建了基于多链的果蔬全程全息信息管理模型，解决了果蔬全程全息信息监管难以及企业隐私数据保护性差等问题。根据不同功能需求将多链分为追溯链和企业级多链，将监管节点加入每一条局部链，实现了对果蔬供应链的穿透式监管。采用分享隐私存证的隐私数据上链方式，实现了对用户身份的权限管理。

（3）设计了 CMerkle 树区块结构和基于区块综合索引指数的跳表检索结构，实现了对数据的快速

表 3 农产品信息管理系统对比

Tab. 3 Comparison of agricultural product information management systems

方案	文献[29]	文献[31]	文献[32]	文献[33]	文献[34]	本系统
数据存储模式	中心化	去中心化	去中心化	去中心化	去中心化	去中心化
区块链架构	—	单链	多链	单链	多链	多链
隐私数据隔离	×	×	√	×	√	√
数据跨链安全交互	—	—	—	—	—	√
数据监管范围	部分信息	部分信息	部分信息	部分信息	关键信息	全程全息
数据防篡改能力	弱	强	强	强	强	强
数据隐私性分类	×	√	√	×	√	√
隐私数据保护	×	√	√	×	√	√
身份权限管理	√	√	√	×	√	√
数据存储	中心数据库	Merkle Tree、本地数据库	Merkle Tree、关系数据库	Merkle Tree、CouchDB、Webyog SQLyog	Merkle Tree、CouchDB、IPFS	CMerkle Tree、LevelDB、TikvDB、MysqL、IPFS
共识机制	—	PBFT	PoW、PoS	Kafka	Kafka	TBFT
监管溯源效率	低	中等	中等	中等	高	高
企业数据管理能力	中等	弱	中等	弱	中等	强

注:—表示文献中对该模块未做出具体描述,×表示不满足该功能需求。

检索。测试结果表明,CMerkle 树区块结构中用于检索数据的布谷鸟过滤器相较于传统布隆过滤器更适用于数据量不断增加的果蔬全程全息信息管理。基于区块综合索引指数的跳表检索结构相较于传统链表结构拥有更高的检索效率。

(4)设计了具有去中心化特点的公证链跨链交互机制,同时结合分享隐私存证的加密方式实现不同链间隐私数据安全交互。

(5)基于上述理论为基础结合长安链区块链平台,构建出了果蔬全程全息信息管理系统的整体架构,同时根据不同用户需求进行了功能模块设计。并提出了系统数据库端、服务器端的设计与实现方案。最后进行了系统实现。对系统的区块链性能以及数据的上链和查询耗时进行了测试,公开数据上链平均耗时为 589.03 ms,隐私数据上链平均耗时为 708.59 ms,公开数据的查询平均耗时为 26.87 ms,隐私数据查询平均耗时为 30.67 ms,可以满足不同需求用户对于不同权限数据的上链和查询需求。与其他现有果蔬信息管理系统相比,在保护隐私数据安全的同时有更高监管溯源的效率,为食品监管溯源、食品供应链信息管理提供借鉴。

参 考 文 献

[1] WALLACE T, BAILEY R, BLUMBERG J, et al. Fruits, vegetables, and health: a comprehensive narrative, umbrella review of the science and recommendations for enhanced public policy to improve intake[J]. Critical Reviews in Food Science and Nutrition, 2020, 60(13): 2174 - 2211.

[2] THAKURA N, RAIGOND P, SINGH Y, et al. Recent updates on bioaccessibility of phytonutrients[J]. Trends in Food Science & Technology, 2020, 97: 366 - 380.

[3] SAMTIYA M, ALUKO R, DHEWA T, et al. Potential health benefits of plant food-derived bioactive components: an overview[J]. Foods, 10(4): 839.

[4] 邵平, 刘黎明, 吴唯娜, 等. 传感器在果蔬智能包装中的研究与应用[J]. 食品科学, 2021, 42(11): 349 - 355.
SHAO Ping, LIU Liming, WU Weina, et al. Research and application of sensors in intelligent packaging of fruits and vegetables[J]. Food Science, 2021, 42(11): 349 - 355. (in Chinese)

[5] 徐霞红, 权浩然, 何开雨, 等. 农田环境中农药残留比例型荧光传感系统研究[J]. 农业机械学报, 2020, 51(11): 229 - 234.
XU Xiahong, QUAN Haoran, HE Kaiyu, et al. Proportional fluorescence sensing analysis of pesticide residues in agricultural environment[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(11): 229 - 234. (in Chinese)

[6] FOONG S Y, MA N L, LAM S S, et al. A recent global review of hazardous chlorpyrifos pesticide in fruit and vegetables: prevalence, remediation and actions needed[J]. Journal of Hazardous Materials, 2020, 400: 123006.

[7] LI C, ZHU H, LI C, et al. The present situation of pesticide residues in China and their removal and transformation during food processing[J]. Food Chemistry, 2021, 354: 129552.

[8] KONG J, YANG C, LIN S, et al. A graph-related high-order neural network architecture via feature aggregation enhancement for identification application of diseases and pests[J]. Computational Intelligence and Neuroscience, 2022, 2022: 4391491.

[9] BOUZEMBRAK Y, KLUCHE M, GAVAI A, et al. Internet of Things in food safety: literature review and a bibliometric analysis[J]. Trends in Food Science & Technology, 2019, 94: 54 - 64.

[10] 国家卫生健康委员会食品安全标准与监测评估司.《食品安全标准与监测评估"十四五"规划》解读[J]. 中国卫生资

源，2022，25(5)：662.
[11] 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)
[12] ZHANG B，XU J，WANG X，et al. Research on the construction of grain food multi-chain blockchain based on zero-knowledge proof[J]. Foods，2023，12(8)：1600.
[13] 董云峰，张新，许继平，等. 基于区块链的粮油食品全供应链可信追溯模型[J]. 食品科学，2020，41(9)：30－36.
DONG Yunfeng，ZHANG Xin，XU Jiping，et al. Blockchain-based traceability model for grains and oils whole supply chain[J]. Food Science，2020，41(9)：30－36.(in Chinese)
[14] 许继平，孙鹏程，张新，等. 基于区块链的粮油食品全供应链信息安全管理原型系统[J]. 农业机械学报，2020，51(2)：341－349.
XU Jiping，SUN Pengcheng，ZHANG Xin，et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery，2020，51(2)：341－349.(in Chinese)
[15] AGI M A N，JHA A K. Blockchain technology in the supply chain：an integrated theoretical perspective of organizational adoption[J]. International Journal of Production Economics，2022，247：108458.
[16] MISRA N N，DIXIT Y，AL-MALLAHI A，et al. IoT，big data，and artificial intelligence in agriculture and food industry[J]. IEEE Internet of things Journal，2020，9(9)：6305－6324.
[17] TREIBLMAIER H，GARAUS M. Using blockchain to signal quality in the food supply chain：the impact on consumer purchase intentions and the moderating effect of brand familiarity[J]. International Journal of Information Management，2023，68：102514.
[18] TAN A，GLIGOR D，NGAH A. Applying blockchain for halal food traceability[J]. International Journal of Logistics Research and Applications，2022，25(6)：947－964.
[19] WANG L，HE Y，WU Z. Design of a blockchain-enabled traceability system framework for food supply chains[J]. Foods，2022，11(5)：744.
[20] YAO Q，ZHANG H. Improving agricultural product traceability using blockchain[J]. Sensors，2022，22(9)：3388.
[21] 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 Jinghua，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)
[22] JIANG S，CAO J，WU H，et al. Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems[J]. Information Sciences，2023，635：72－85.
[23] 刘炜，王栋，佘维，等. 一种面向区块链溯源的高效查询方法[J]. 应用科学学报，2022，40(4)：623－638.
LIU Wei，WANG Dong，SHE Wei，et al. An efficient query method for blockchain traceability[J]. Journal of Applied Sciences，2022，40(4)：623－638.(in Chinese)
[24] ZHAO Y，DAI W，WANG S，et al. A review of cuckoo filters for privacy protection and their applications[J]. Electronics，2023，12(13)：2809.
[25] 汤永利，李静然，闫玺玺，等. 支持联合搜索的动态前向安全可搜索加密方案[J]. 计算机研究与发展，2022，59(8)：1853－1866.
TANG Yongli，LI Jingran，YAN Xixi，et al. A forward secure dynamic searchable encryption scheme supporting conjunctive search[J]. Journal of Computer Research and Development，2022，59(8)：1853－1866.(in Chinese)
[26] SINGH B C，YE Q，HU H，et al. Efficient and lightweight indexing approach for multi-dimensional historical data in blockchain[J]. Future Generation Computer Systems，2023，139：210－223.
[27] LI Z，JIAO B，HE S，et al. Phast：hierarchical concurrent log-free skip list for persistent memory[J]. IEEE Transactions on Parallel and Distributed Systems，2022，33(12)：3929－3941.
[28] LI Y，QIAO L，LV Z. An optimized byzantine fault tolerance algorithm for consortium blockchain[J]. Peer-to-Peer Networking and Applications，2021，14：2826－2839.
[29] DONG Y，FU Z，STANKOVSKI S，et al. Nutritional quality and safety traceability system for China's leafy vegetable supply chain based on fault tree analysis and QR code[J]. IEEE Access，2020，8：161261－161275.
[30] 北京市科委. 国内首个自主可控区块链软硬件技术体系“长安链”发布[EB/OL]. https://www.most.gov.cn/dfkj/bj/zxdt/202102/t20210205_172727.html，2021－02－05.
[31] YANG X，LI M，YU H，et al. A trusted blockchain-based traceability system for fruit and vegetable agricultural products[J]. IEEE Access，2021，9(5)：36282－36293.
[32] ZHANG X，SUN Y，SUN Y. Research on cold chain logistics traceability system of fresh agricultural products based on blockchain[J]. Computational Intelligence and Neuroscience，2022，2022：1957957.
[33] 弋伟国，何建国，刘贵珊，等. 区块链增强果蔬质量追溯可信度方法研究与系统实现[J]. 农业机械学报，2022，53(2)：309－315，345.
GE Weiguo，HE Jianguo，LIU Guishan，et al. Development and implementation of blockchain to enhance traceability and reliability of fruit and vegetable quality[J]. Transactions of the Chinese Society for Agricultural Machinery，2022，53(2)：309－315，345.(in Chinese)
[34] 孙传恒，于华竟，罗娜，等. 基于智能合约的果蔬区块链溯源数据存储方法研究[J]. 农业机械学报，2022，53(8)：361－370.
SUN Chuanheng，YU Jinghua，LUO Na，et al. Blockchain traceability data storage method of fruit and vegetable foods supply chain based on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery，2022，53(8)：361－370.(in Chinese)