doi:10.6041/j.issn.1000-1298.2025.06.004

基于内容提取签名的果蔬区块链追溯数据保护与共享方法

孙传恒[1,2]　刘庆博[1,2]　陈　枫[2,3]　邢　斌[2,3]　罗　娜[2,3]

(1. 上海海洋大学信息学院, 上海 201306; 2. 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;
3. 国家农业信息化工程技术研究中心, 北京 100097)

摘要: 区块链追溯在保障农产品安全、协调各环节生产等方面发挥着关键作用。针对果蔬区块链追溯中隐私数据共享和安全保护需求,提出了一种基于内容提取签名的隐私数据可信共享方法。首先,分析果蔬供应链各环节数据设计溯源数据分类方式。其次,将内容提取签名(CES)与基于密文策略属性加密(CP-ABE)技术相结合,利用 CES 技术隐藏追溯信息中的敏感数据,实现追溯数据灵活、安全的共享,通过 CP-ABE 技术对不同角色实施不同的访问控制策略实现对数据的加密和隐私保护。基于以太坊搭建区块链进行仿真实验,系统测试结果显示,在扩散性测试中密文平均变化率为 90.2%,相关性实验中密文平均变化率达到 75.7%,显示出良好的安全性能。当明文子消息数量分别为 10、20 条时,平均验证时间为 0.102、0.159 ms,相较于传统方案提升 80.1%、84.3%。验证时间不随子消息数量的增加而线性增长。在存储效率方面,子消息数量为 5、10 条时所需存储空间分别减少 70.6%、85.3%。本方法在保障果蔬供应链数据隐私的同时,实现了高效可信的数据共享机制,为提升农产品安全监管水平提供了有益的技术参考与实践基础。

关键词: 区块链; 溯源; 数据共享; 属性基加密; 内容提取签名

中图分类号: TP311.11　　**文献标识码**: A　　**文章编号**: 1000-1298(2025)06-0047-09　　**OSID**:

Content Extraction Signature-based Sharing and Protection Method for Fruit and Vegetable Blockchain Traceability Data

SUN Chuanheng[1,2]　LIU Qingbo[1,2]　CHEN Feng[2,3]　XING Bin[2,3]　LUO Na[2,3]

(1. *College of Information Technology, Shanghai Ocean University, Shanghai* 201306, *China*
2. *National Engineering Research Center of Traceability Technology and Application of Agricultural Product Quality and Safety, Beijing* 100097, *China*
3. *National Agricultural Information Engineering Technology Research Center, Beijing* 100097, *China*)

Abstract: Blockchain traceability plays a crucial role in ensuring the safety of agricultural products and coordinating production in each link. In response to the privacy data sharing and security protection requirements in the blockchain traceability of fruits and vegetables, a privacy data trusted sharing method based on content extraction signature was proposed. Firstly, the data of each link in the fruit and vegetable supply chain was analyzed to design the classification method of traceability data. Secondly, the content extraction signature (CES) technology was combined with the ciphertext-policy attribute-based encryption (CP-ABE) technology. The CES technology was used to hide the sensitive data in the traceability information, achieving flexible and secure sharing of traceability data. The CP-ABE technology was used to implement different access control policies for different roles to achieve data encryption and privacy protection. A blockchain based on Ethereum was built for simulation experiments. The system test results showed that in the diffusion test, the average change rate of ciphertext was 90.2%, and in the correlation test, the average change rate of ciphertext reached 75.7%, demonstrating excellent security performance. When the number of plaintext sub-messages was 10 and 20 respectively, the average verification time was 0.102 ms and 0.159 ms, which was 80.1% and 84.3% faster than that

收稿日期: 2025-03-10　修回日期: 2025-04-25

基金项目: 国家重点研发计划项目(2023YFD2001304)和江苏省科技计划(重点研发计划现代农业)项目(BE2023315)

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: 罗娜(1983—),女,助理研究员,博士,主要从事农产品追溯技术研究,E-mail: luon@nercita.org.cn

of the traditional scheme. The verification time did not increase linearly with the increase in the number of sub-messages. In terms of storage efficiency, the required storage space was reduced by 70.6% and 85.3% when the number of sub-messages was 5 and 10 respectively. This method not only ensured the privacy of data in the fruit and vegetable supply chain but also realized an efficient and trusted data sharing mechanism, providing a beneficial technical reference and practical basis for improving the level of agricultural product safety supervision.

Key words: blockchain; traceability; data sharing; attribute-based encryption; content extraction signature

0 引言

食品安全问题作为关乎民众福祉和社会稳定的关键议题,始终是政府、企业和公众关注的焦点[1]。多起食品安全事件曾引发公众恐慌与信任危机,使得相关监管部门不得不加大对食品安全问题的重视力度,从而推动食品质量监控体系与追溯体系的不断完善和升级[2-4]。农产品质量追溯系统可以实现从田间生产到餐桌消费全流程的信息记录与监控,为各环节的质量管理提供依据[5-6]。通过建立完整的追溯体系,不仅能够在出现质量问题时快速锁定问题源头,及时采取应对措施,降低食品安全事件的损失,还能提升消费者对食品质量的信心,推动整个产业链的规范化与信息化管理[7]。

传统的农产品质量追溯方式主要依赖于纸质记录、人工登记以及中心化的信息管理系统,存在诸多不足[8]。首先,中心化系统容易受到人为操作失误和信息篡改的影响,确保数据的真实性与完整性面临诸多挑战。其次,各参与主体之间的信息孤岛问题严重,使得整体追溯链条无法形成一个统一、透明的管理体系。此外,由于追溯信息存储在单一服务器或数据库中,一旦遭遇系统故障或遭到网络攻击,极易造成大规模的数据丢失或泄露,从而给食品安全监管带来巨大风险[9]。区块链技术以其去中心化、不可篡改和全链条溯源的特点,为农产品质量追溯提供了一种全新的解决方案[10]。区块链通过分布式账本将各环节的数据信息记录在多个节点上,确保数据在存储、传输和共享过程中的安全性和透明度[11]。智能合约使得追溯信息可以自动按照预设规则执行和验证,降低了人为干预的可能性和操作风险[12]。因此,以区块链为载体的新兴追溯手段能够更好地解决传统溯源方式中数据中心化和信息易被伪造等问题,为食品安全监管提供坚实的数据保障和技术支撑[13-18]。

然而,尽管区块链技术在农产品质量追溯中展现出优势,但当前实际应用过程中仍面临诸多挑战[19]。首先,供应链追溯流程不仅只上传农产品从种植到销售的信息,还涉及相关参与者的价格、生产方式、加工工艺等隐私数据。若不对敏感数据进行隐私保护,可能会损害企业利益[20]。其次,溯源过程中的供应链各参与方处于一种博弈关系[21],企业在进行信息共享时由于担心核心数据泄露或自身利益受损,往往不愿意完全开放信息,这进一步削弱了追溯系统的整体可信度[22-23]。最后,如果追溯数据的采集与录入环节存在漏洞,则区块链系统所存储的数据依然难以代表真实情况[24]。因此,如何在保证数据安全的同时,实现各参与方之间的信息共享,仍然是当前亟待解决的问题。

针对上述问题,结合分析农产品质量追溯全链条流程,本文提出一种基于区块链的农产品质量追溯数据可信共享方法。该方法将内容提取签名(Content extraction signature, CES)与基于密文策略属性加密(Ciphertext-policy attribute-based encryption, CP-ABE)技术相结合,利用 CES 技术隐藏追溯信息中的敏感数据,实现追溯数据灵活、安全的共享,通过 CP-ABE 技术对不同角色实施不同的访问控制策略实现对数据的加密和隐私保护。这两项技术的有机结合在保障农产品供应链中敏感数据隐私的同时,实现数据在不同环节之间的高效可信共享。最后在区块链平台上搭建实验原型,并通过实验验证对系统安全性、效率性等进行综合评估。

1 果蔬农产品供应链关键信息分析

1.1 果蔬农产品供应链溯源数据分类

在现代果蔬农产品供应链中,各环节通过区块链技术进行数据记录和信息共享,为全程监管提供了可靠依据[25]。供应链主要包括种植、加工、仓储、运输和销售五大环节,每一环节在信息采集和传输过程中均产生大量数据[26]。这些数据中既包含有助于消费者、监管部门以及各合作方进行实时监控和数据共享的公开信息,也包含涉及商业机密、生产工艺、内部成本等敏感内容的隐私信息[27]。本文在对各环节进行深入分析的基础上,将上传至区块链的数据按公开信息和隐私信息进行分类。表 1 对供应链各环节上传至区块链的信息进行归纳整理,明确区分了公开信息与隐私信息的内容范畴。

表 1　农产品供应链各环节关键溯源数据

Tab. 1　Key traceability data of each link in agricultural product supply chain

环节	公开信息	隐私信息
种植环节	种植日期、农场地理位置、果蔬品种、环境监测数据（如温湿度、土壤信息）	种植技术细节、农药和化肥使用比例、成本投入、种植管理流程数据
加工环节	加工企业名称、生产批次编号、加工工艺概述、质量检测报告	加工配方、关键工艺参数、原材料来源信息、内部质量控制数据
仓储环节	仓储地点、温湿度监控记录、入库/出库时间、库存状态	仓储管理系统数据、精确库存数量、仓储成本、仓储调度和分配策略
运输环节	运输路线、发货与到达时间、物流服务商名称、运输状态信息	车辆实时定位、运输成本、司机身份信息、运输方式与具体操作流程
销售环节	销售渠道、销售时间、产品批次、市场销售价格、合规与认证信息	销售合同、议价与定价记录、客户信息、利润分配与营销策略数据

在区块链溯源中，对公开信息的记录和查询可以实现信息透明化、追溯可查；而对隐私信息则需结合加密技术和权限管理手段，确保只有具备相应权限的参与者才能访问。这种分类管理不仅保障了供应链各环节的信息公开透明，还在很大程度上防范了数据泄露和商业机密暴露的风险。基于此分类构建的农产品供应链追溯模型，可以实现全流程、全参与方可信的数据管理。

1.2　关键技术

传统的数字签名技术在互联网领域中主要用于身份验证，但在某些具体应用中其功能可能存在一定的局限性[28]。例如在电子政务等场景中，签名使用者可能需要根据实际需求对原始数据进行适当裁剪和删除，以实现敏感隐私信息的隐藏或减少数据的传输量[29]。CES 可以满足上述需求，签名拥有者能够在无需原始签名者参与的情况下，从已签署的数据中删减部分子数据，进而生成多个版本的截取信息及其对应的可验证签名。即便数据被裁剪，验证方仍能确认所接收信息的真实性与签名的有效性[30]。考虑到追溯信息中包含大量敏感的商业隐私数据，这类信息必须受到合法保护。CES 技术能够通过对其中敏感内容的隐藏，有效保障企业隐私。农产品质量追溯中引入 CES 等相关技术为构建基于区块链的农产品隐私数据共享模型奠定理论基础。CES 算法描述为：

(1) $\mathrm{KeyGen}(1^{\lambda})\rightarrow(\mathrm{sk},\ \mathrm{pk})$：根据安全参数 λ，签名者获取自身的公私钥对 $(\mathrm{sk},\ \mathrm{pk})$。

(2) $\mathrm{Sign}(\mathrm{M},\ \mathrm{sk},\ \mathrm{CEAS})\rightarrow\delta_{\mathrm{full}}$：签名者根据原始数据 M、私钥 sk 以及内容截取访问结构 CEAS，生成 M 的原始签名 δ_{full}。

(3) $\mathrm{Ext}(\mathrm{M},\mathrm{CEAS},\ \mathrm{X},\ \mathrm{pk},\ \delta_{\mathrm{full}})\rightarrow\delta_{\mathrm{ext}}$：截取者根据 M、原始签名 δ_{full}、原始签名者公钥 pk，以及截取子集 X，生成截取签名 δ_{ext}。

(4) $\mathrm{Verif}(\mathrm{M}',\mathrm{CEAS},\ \mathrm{X},\ \mathrm{pk},\ \delta_{\mathrm{ext}})\rightarrow(\mathrm{True\ or\ False})$：验证者输入截取消息 M′、内容截取访问结构 CEAS、截取子集 X、签名者公钥 pk，以及截取签名 δ_{ext}。若验证该截取签名有效，则输出 True，否则输出 False。

2　农产品供应链追溯隐私数据保护与共享

2.1　农产品隐私数据保护与共享模型

传统的基于中心化数据库存储的农产品溯源数据存储共享系统在隐私安全和互操作性等方面存在诸多漏洞，而且各环节企业无法真正控制和管理自己的数据记录。因此提出一种基于区块链的农产品隐私数据安全存储共享方案，星际文件系统（Interplanetary file system，IPFS）存储农产品加密后的原始数据，而区块链上只保存加密数据的索引。并且采用 CP－ABE 和 CES 实现溯源隐私数据的安全共享。基于区块链的农产品隐私数据共享模型如图 1 所示。系统各部分的流程和角色介绍如下：签名持有者（加工商）在对本环节生产的农产品进行质量检测申请时，会将农产品公开数据传递给签名者（质量检测机构），由质量检测机构负责为其完成质量检测、创建专属质检报告并生成全局签名，随后将完整数据加密后发送给加工商；当加工商收到信息后负责验证数据完整性和安全性，并通过 CES 技术隐藏隐私数据生成新的签名。

加工商将加密后的原始报告和提取签名上传至 IPFS 服务器，IPFS 采用分布式存储的方式，将上传的数据分散存储在网络上的多个节点上并使用内容寻址来标识数据，每个数据块都有唯一的 CID 地址。当用户需要访问特定的数据时，其可以使用 CID 地址来查询数据。区块链网络存储 IPFS 地址和质检报告的数据摘要，区块链网络中加工商根据自己意愿提前设置智能合约，一旦访问用户满足智能合约的条件，触发合约自动执行，确保只有通过授权的用户才可以得到 IPFS 地址，访问农产品的质量检测数据。

消费者、监管者、上下游环节等角色作为数据访问者，根据自身需要请求访问区块链中上传的相应数据。并基于角色的属性可对同一份数据进行不同程度的解密和验证。不同的验证者可以根据其权限查看相应信息。对于查询数据的各方来说，即使只收到部分数据，其仍能通过生成的内容提取签名验

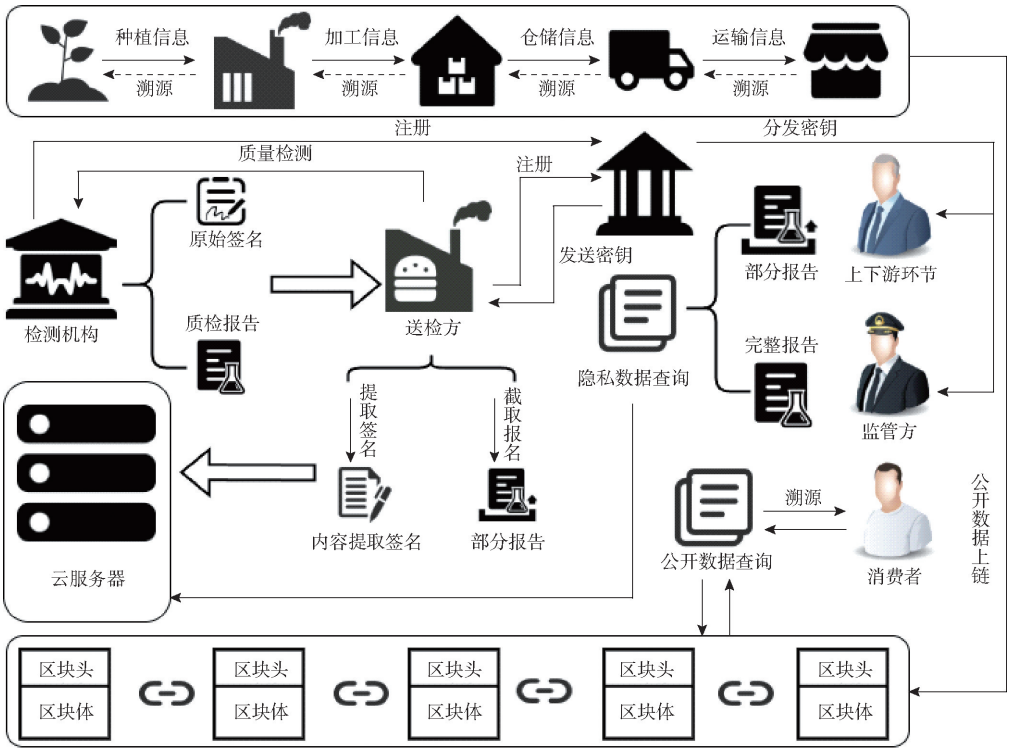


图 1 基于区块链的果蔬农产品隐私数据共享模型

Fig. 1 Agricultural product privacy data sharing model based on blockchain

证该数据的真实性和完整性。这确保了数据在保持隐私的同时仍能得到可信验证。

2.2 果蔬农产品隐私数据共享方法

2.2.1 密钥生成

首先,检测机构运行密钥生成算法 KeyGen 均匀随机地选择两个素数 p 和 q 并计算 $N=pq$。其次,随机选取一个与欧拉函数 $\varphi(n)=(p-1)(q-1)$ 互素的公共素数 e。计算 e 的逆元 $d=e^{-1}\bmod(p-1)(q-1)$。最后根据上述的计算,得到公钥 $PK=(N,e)$,私钥 $SK=(N,d)$,输出检测机构的内容提取签名公私钥对(SK,PK)。

2.2.2 签名生成

检测机构在完成农产品质量检测后会根据其溯源码生成专属的质量检测报告 M,报告详细记载了送检农产品的基本信息和检测结果。为了保证加工商的隐私信息在数据共享过程中不被泄露,本方案将使用内容提取签名技术,检测机构可对报告进行全局签名,加工商在收到检测机构的全局签名和完整的检测报告后,可以根据个人需求删除部分敏感信息,并获取有效的提取签名。将报告细分为 n 个子消息,即 $M=\{m_1,m_2,\cdots,m_n\}$,为了防止报告在共享过程中被送检方恶意违规截取造成消费者或其他环节节点误解,根据相关国家法律法规要求,检测机构需预先定义提取访问结构 CEAS,规定截取内容中必须包含子消息段的编号和顺序,即对任意的提取子集 $CI(M')$,都有 $CEAS\subset CI(M')$。例如 $M=\{m_1,m_2,m_3,m_4,m_5\}$,$CEAS=\{1,2,4\}$,则提取子集 $CI(M')=\{1,2,4,5\}$ 为合法截取。$CI(M')=\{1,2,5\}$ 因缺少必选子消息 m_4 为非法截取,由于提取子集中子消息的顺序与提取访问结构不同,$CI(M')=\{2,4,1\}$ 同样为非法提取。

本方案采用基于 RSA 的内容提取签名,签名的生成过程如下。对于消息 M 中的每个子消息 m_i,计算其哈希值 h_i,并进一步求得每个子消息的签名 σ_i。基于聚合签名 σ 输出 M 的全局签名 σ_{full}。签名完成后,检测机构使用自己的对称密钥 K_d 加密原始报告 M、原始报告的哈希值 h_M、全局签名 σ_{full}、提取访问结构 CEAS 和 CEAS 的标记 T,然后使用加工节点的公钥 PK_p 加密 K_d,最后将两个加密信息打包后发送给加工节点。

2.2.3 消息提取

在加工节点接收到检测机构发送的加密信息 Info 后,首先用自己的私钥 SK_p 解密得到检测机构的对称密钥 K_d,并进一步解密得到原始报告 M、原始报告的哈希值 h_M、全局签名 σ_{full}、提取访问结构 CEAS 和 CEAS 的标记 T,然后对其正确性和完整性进行验证。对于原始报告 M,加工节点计算哈希值 h'_M,验证计算得出的结果 h'_M 是否与解密得到的哈希值 h_M 相等,如果相等则证明原始报告没有被篡改并进入下一步验证。加工节点使用检测机构的公钥 PK_d 依次验证每一个子消息的签名 σ_i 的正确性,如果验证通过则认为 σ_i 为有效签名。如果上述两

个步骤的验证中有任意一个验证结果失败，则表明加工节点未能正确地接收到检测机构发送的检测报告并将停止信息的共享。如果两次验证全部通过，则可证明原始报告 M 和签名 σ_{full} 真实准确可靠，加工节点可根据自身隐私信息保护意愿和数据共享的需要对原始文档进行内容提取并生成新的提取签名 σ_{ext}，签名提取算法具体如下。首先加工节点基于提取访问结构 CEAS 生成需要共享的提取子集 $CI(M')$，并从原始文档 M 中提取出子消息集 $M'=\{m_i\}$，其中 $i\in CI(M')$。然后，解析全局签名 σ_{full} 并从中提取出可公开共享的子消息 m_i 的子签名 σ_i，计算子签名的集合 σ_f，并输出内容提取签名 σ_{ext}。内容提取签名的流程如图 2 所示。

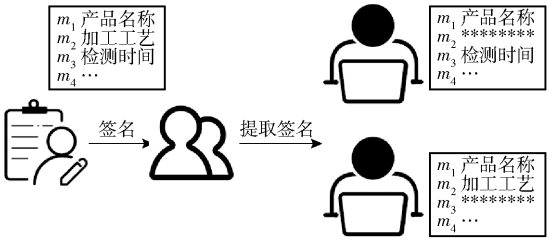


图 2　内容提取签名流程

Fig. 2　Process of CES

2.2.4　数据加密

在加工节点完成子消息签名提取后，为实现对不同环节角色灵活的数据共享，将采用对称加密技术和 CP－ABE 技术相结合的方式来进行数据的访问控制。对于每个被提取的子消息 m_i 及其哈希值 $h_i, i\in CI(M')$ 加工节点使用对称加密密钥 k_p 进行加密，而剩余未被截取的子消息集和其哈希值使用对称加密密钥 k_s 来加密。基于对不同角色的共享需求制定不同的访问控制策略结构树，执行数据加密算法 Encrypt 根据加工节点的属性基加密主公钥 PK，待加密的密钥 k_i，访问控制策略 A 得到加密后的对称密钥 c_{k_i}，将加密后的密文 C_{m_i}、C_{k_i} 以及全局签名 σ_{full}、内容提取签名 σ_{ext} 信息上传至 IPFS，IPFS 会返回对应的存储地址哈希值 Hash。并将报告 M 的摘要、完整报告 M 的哈希值 h_M 和 IPFS 存储地址 Hash 通过数据上传智能合约上传到联盟区块链中。

2.2.5　数据共享

当供应链上的其他环节节点想要访问加工节点上传的农产品质量检测报告 M 时，需要向区块链发起一个数据访问请求，区块链收到请求后，区块链节点需验证请求用户的身份，首先查询用户身份是否符合加工节点预先设置的访问控制列表的访问条件，若不符合，则代表访问请求用户不是加工节点的已授权用户，智能合约不执行任何操作并返回失败；否则智能合约将自动触发，向用户返回存储在区块链上的报告摘要、完整报告 M 各个子消息 m_i 的哈希值和 IPFS 存储地址 Hash。算法流程为：

输入：服务器地址 urls

输出：用户私钥 SK，数据 Data

```
function retrieveData(string memory urls, PrivateKey SK) public returns (Data memory) {
    bytes memory E_Data = downloadEncryptedData(urls);
    bytes memory E_K = downloadEncryptedKey(urls);  //检查用户属性是否满足访问策略
    if (! isPolicySatisfied(SK.attributes, E_K.policy)) {
        revert("访问被拒绝:属性集合不满足访问策略");}  // 若不满足,终止操作
    bytes memory K = CPABE.decrypt(SK, E_K);
                //得到对称密钥 K
    Data memory decryptedData = Symmetric.decrypt(K, E_Data); //得到明文数据对象
    return decrypted_Data;}        //返回解密后的数据
```

2.2.6　数据解密

用户得到 IPFS 存储地址 Hash 后将其提交给 IPFS 服务器，由于存储在 IPFS 上的数据与其生成的哈希地址一一对应，用户可根据哈希地址从 IPFS 中获取各个子消息和对应哈希值的密文 C_{m_i}、C_{k_i} 以及全局签名 σ_{full} 和内容提取签名 σ_{ext}。运行 CP－ABE 的解密算法 Decrypt，使用自己的属性基加密私钥 SK 解密对称密钥密文 c_{k_i} 得到对称密钥 k_i。根据用户属性不同，解密结果有两种情况，供应链上的其他环节节点只拥有原始报告隐藏敏感信息后的提取部分 M' 的访问权限，因此其解密结果为 k_p。而对于监管节点来说，其被允许访问原始报告 M 的完整部分，因此其可以解密得到所有的对称密钥 k_p、k_s。完成解密后，继续使用对称密钥 k_i 解密得到子消息 m_i。隐私数据共享如图 3 所示。

2.2.7　数据验证

数据验证包含数据完整性验证和签名有效性验证两部分。首先根据解密得到子消息 m_i 还原原始文档 M 计算其哈希值，并验证是否与从区块链智能合约中得到的哈希值相同，数据完整性验证完成后用户可通过以下步骤验证提取签名 σ_{ext} 的正确性。首先判断 $CEAS\subset CI(M')$ 是否正确，若不正确则表示提取文档 M' 为非法提取则拒绝接收此数据，否则将继续执行下面的操作；对于普通用户，解析提取签

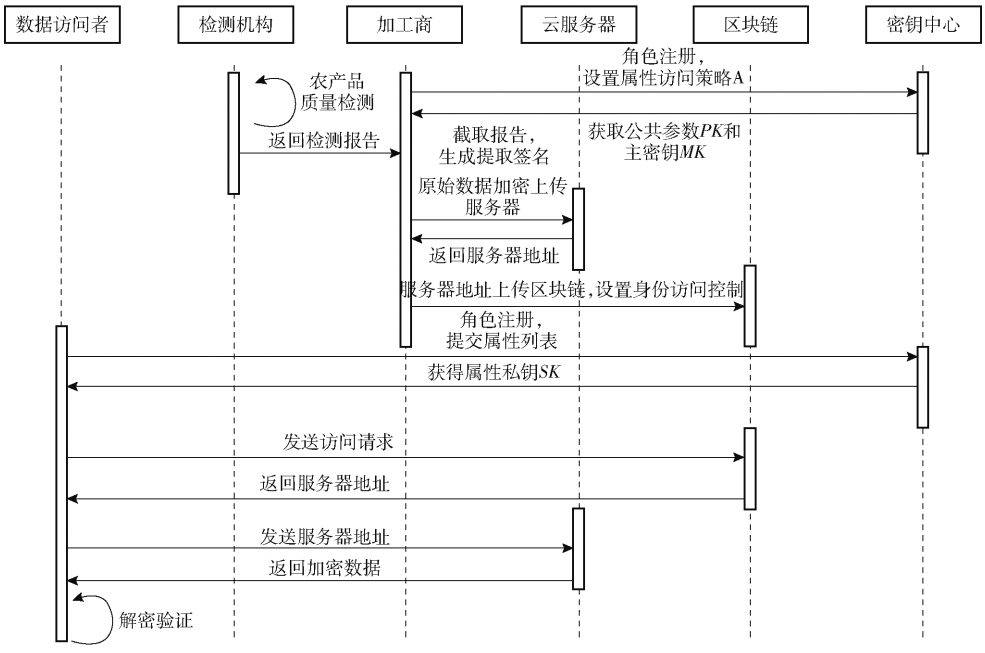


图 3 隐私数据共享流程图

Fig. 3 Privacy data sharing process structure

名 $\sigma_{ext} = T \| CEAS \| \sigma_f$、提取文档 $M' = \{m_i\}$，对于每个 $i \in CI(M')$，计算哈希值 h_i 和子签名 σ_i；使用公钥 PK 验证等式是否成立，若成立则证明截取签名有效；否则签名无效。

通过上述方案的实施，加工节点能够实现对其自身数据的有效管理。属性基加密技术确保了在数据共享过程中，不同身份的请求者能够访问不同层级数据。具体来说，监管节点具备访问全部原始数据的权限，而其他环节的节点则只能读取部分已截取数据。此种数据共享机制，能够在保障数据安全性的同时，提供灵活的数据访问策略。此外，结合内容提取签名技术，能够为每个环节传输的数据附加数字签名，从而有效地对接收到的数据进行验证。这一措施大大减少了数据上传阶段人为干预的可能性，增强了数据的真实性与可信度。通过数字签名，确保了数据在传输过程中未被篡改，有助于提升供应链中各参与方对彼此之间的信任。该方案不仅满足了数据拥有者对隐私保护的需求，同时也实现了数据公开部分的可信共享，有效促进了供应链各方的协同合作。各参与实体能够在更加透明和可信的环境中共享数据，从而提升了供应链的整体效率。

2.3 智能合约设计

利用区块链开发应用平台以太坊基于 Solidity 语言设计相关智能合约以及对应触发规则。智能合约的业务逻辑设计如表 2 所示。

表 2 智能合约设计

Tab. 2 Smart contract design

合约名称	合约方法	输入	输出	功能
公开数据上传合约	AddPublicData( )	农产品追溯公开数据	True/False	上传农产品追溯公开数据
隐私数据上传合约	AddPrivateData( )	农产品隐私数据摘要、数据哈希值、IPFS 地址	True/False	上传农产品追溯隐私数据
公开数据查询合约	GetPublicData( )	农产品批次号	农产品追溯公开数据	查询农产品追溯公开数据
隐私数据查询合约	GetPrivateData( )	农产品批次号	农产品隐私数据摘要、数据哈希值、IPFS 地址	查询农产品追溯隐私数据

将农产品供应链各个环节的溯源信息写入区块链和读取的操作均由智能合约实现。以隐私数据存储为例，在上述合约中，定义了一个数据存储的方法，其中包含：一个 Data 结构体，用于接收并存储信息（批次号 batchId、农产品隐私数据摘要 dataSummary、数据哈希值 dataHash、IPFS 地址 ipfsAddress）这些数据将被存储在合约的状态变量中，供后续查询使用。一个映射，将批次号映射到 Data 结构体；一个 storeData 函数，用于存储数据。隐私数据存储智能合约具体算法为：

输入：农产品 dataId、摘要 dataSummary、哈希值 dataHash 输出：True/False

```
function storeData ( uint256 dataId, string memory
dataSummary, string memory dataHash) public {
    //检查是否已有数据,防止覆盖
    require(dataRecords[dataId].timestamp == 0,
    "Data already exists");
        //创建新的数据对象
    DataItem memory newItem = DataItem({
            Id: dataId,
            Summary: dataSummary,
            Hash: dataHash,
            timestamp: block.timestamp });
        //保存到映射中
    dataRecords[dataId] = newItem;
        //触发事件,通知存储成功
    emit DataStored(dataId);}
    Return true;
```

3　实验测试与分析

系统的开发平台为一台 CPU 为 Core i7 -8750H CPU@2.2 GHz 12 核、16 GB RAM 的 Windows 主机，开发环境选择 VMware workstation 16 pro 作为虚拟化平台，搭建 Ubuntu 22.04.1 64 位操作系统，虚拟机的配置为 8 个处理器核心，4 GB 的运行内存并分配 50 GB 的硬盘空间。本文基于以太坊的 go 语言客户端 geth -1.9.25 作为底层区块链网络平台，采用工作量证明(Proof of work，poW)机制构建了一个基于区块链的农产品隐私数据共享模型，运用 Solidity 编程语言编写智能合约，使用 Remix IDE 对智能合约进行编码与部署。通过仿真实验对各阶段进行测试，根据实验结果对性能效率进行评估。使用 Python 3.13 实现内容提取签名算法模拟测试数据验证时间，以确保系统性能和响应速度满足实际需求。

3.1　安全性测试

为验证所提出农产品质量追溯模型在安全性方面的有效性，本文对模型所采用的加密算法进行了扩散性测试。在保持访问控制策略不变的前提下，结合对称加密与基于属性的加密机制，对明文数据 M 进行加密处理。通过对明文中任意一位数据进行扰动，观察加密后密文整体变化情况。由图 4a 可知，该扰动所引起的密文平均变化率达到 90.2%，在保持明文数据不变的前提下，通过改变访问控制树的策略，观察加密后密钥整体变化情况，如图 4b 所示，属性私钥变化率平均为 75.7%。表明密文对明文具有良好的敏感性，能够有效抵抗已知明文攻击，满足实际生产环境中对数据安全性的需求。

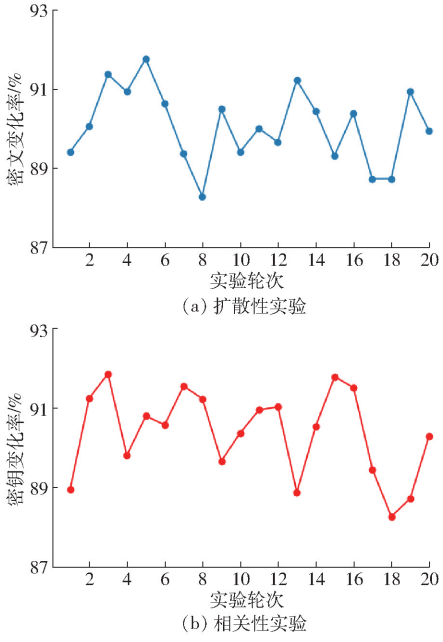


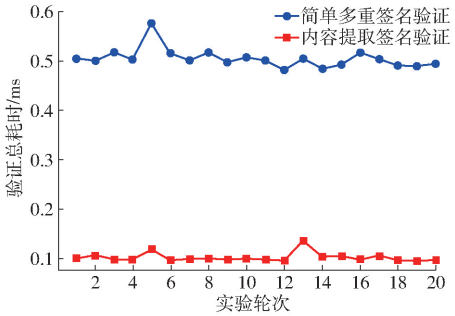
图 4　加密算法安全性测试结果

Fig. 4　Security testing of encryption algorithms

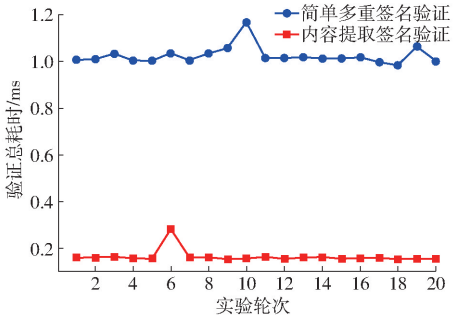
3.2　性能测试

目前，农产品质量追溯领域主要通过使用数字签名技术确保数据真实性。通过私钥签名、公钥验证的方式防止数据被篡改。本文对基于 RSA 的数字签名验证方案进行了性能测试，重点比较了传统的简单多重签名验证方案与提出的内容提取签名验证方案在不同子消息规模下的效率差异。分别在 10、20 条子消息数量下进行对比，并取算法运行 20 次的平均值作为实验结果。当子消息数量为 10 条时，简单多重签名的验证平均耗时为 0.515 ms，内容提取签名的验证平均耗时为 0.102 ms，效率提升 80.1%。而当子消息数量增加为 20 条时，简单多重签名的验证平均耗时增加至 1.010 ms，内容提取签名的验证平均耗时增加至 0.159 ms，效率提升 84.3%。当子消息数量由 10 条增加为 20 条时，内容提取签名的验证耗时增长 55.9%，而简单多重签名验证耗时增长 96.1%。如图 5 所示，内容提取签名验证方案在验证效率上具有显著优势。这是因为内容提取签名的验证基于 RSA 的同态性，这允许以仅一次 RSA 验证加上 $m-1$ 次的模 N 乘法运算为代价来验证 m 个签名。相较于简单多重签名验证，通过将模幂运算次数从 m 次降为 1 次，显著降低了计算开销。

尽管从签名生成者到签名持有者的 CES 完整签名长度仍是单个 RSA 签名长度的 n 倍，但一旦用户截取了文档并生成内容提取签名，则签名只有一个 RSA 模数的长度加上 CEAS 编码和 CEAS 标记的小开销。分别在 1、2、5、10 条子消息数量下设计实验对比 CES 签名和 RSA 签名的存储空间消耗，实验结果



(a) 10条子消息



(b) 20条子消息

图 5 不同签名方案验证时间对比

Fig. 5 Comparison of verification times for different signature schemes

如图 6 所示,当子消息数量为 1 时,由于 CES 签名 tag 的存在,其所需存储空间较标准 RSA 签名多 23.5%,但随着子消息数量增长,CES 签名的存储空间不变,多重 RSA 签名所消耗的空间随子消息数量的增多而线性增加。当子消息数量为 5、10 条时,CES 签名相比多重 RSA 签名在存储空间方面分别减少 70.6%、85.3%,显示出其在存储效率上的显著优势。

4 结束语

针对当前区块链溯源系统在数据可信共享过程

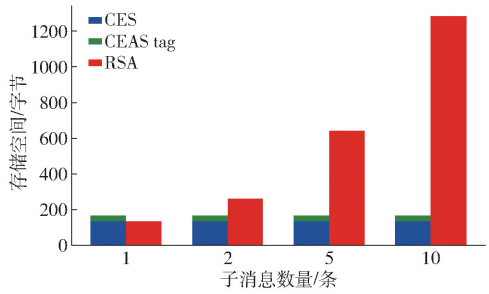


图 6 不同签名方案存储空间对比

Fig. 6 Comparison of storage space for different signature schemes

中存在的隐私保护不足问题,提出了一种基于区块链的果蔬农产品隐私数据保护与共享模型。该模型引入内容提取签名技术,在保证数据可验证性的前提下,有效隐藏溯源信息中的敏感内容,实现数据共享与隐私保护的平衡。同时,结合基于密文策略的属性加密(CP-ABE)方法,根据数据的公开性设计访问控制策略,实现细粒度的访问权限管理,进一步提升了系统的数据安全性与访问灵活性。在扩散性测试中,密文平均变化率达到 90.2%,在相关性测试中密文平均变化率为 75.7%,展示出较强的数据安全性。与传统数字签名方案对比分析发现,本文所提模型验证效率具有显著优势:当子消息数量为 10、20 条时,验证时间分别减少 80.1% 和 84.3%;在存储效率方面,子消息数量为 5、10 条时所需存储空间分别减少 70.6% 和 85.3%。总体而言,所提模型在保障果蔬供应链中数据共享的同时,兼顾了安全性与系统效率,构建了一种高效、可信、可控的数据共享机制,为果蔬供应链溯源研究提供了有力的技术支撑与实践参考。

参 考 文 献

[1] 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)

[2] 赵雅雯,李绍稳. 农产品质量安全可信追溯体系构建与建议[J]. 中国农业科技导报(中英文),2025,27(1):17-24.
ZHAO Yawen, LI Shaowen. Construction and recommendations for a credible traceability system for agricultural product quality and safety[J]. Journal of Agricultural Science and Technology, 2025, 27(1):17-24. (in Chinese)

[3] SANTHIYA K. Agriculture basedfood supply chain traceability using blockchain[C]//2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE, 2023: 1-6.

[4] GUAN S, WANG Z, CAO Y. A novel blockchain-based model for agricultural product traceability system[J]. IEEE Communications Magazine, 2023, 61(8): 124-129.

[5] 陈榆城,谢瑜,姚嘉艺,等. 区块链技术解决农产品信任危机探索——以临安山核桃为例[J]. 智慧农业导刊,2024,4(6):5-10.

[6] 陈丹丹,张立杰,蒋双丰,等. 基于区块链和星际文件系统的种植业农产品溯源模型[J]. 智慧农业(中英文),2023,5(4):68-78.
CHEN Dandan, ZHANG Lijie, JIANG Shuangfeng, et al. Traceability model of plantation agricultural products based on blockchain and interplanetary file system[J]. Smart Agriculture, 2023, 5(4): 68-78. (in Chinese)

[7] BARALLA G, PINNA A, CORRIAS G. Ensure traceability in European food supply chain by using a blockchain system[C]//

2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE, 2019: 40 - 47.

[8] IFTEKHAR A, CUI X, HASSAN M, et al. Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety[J]. Journal of Food Quality, 2020, 2020(1): 5385207.

[9] 谢江涛. 基于区块链的农产品供应链追溯系统[D]. 西安：西安电子科技大学, 2019.
XIE Jiangtao. Agricultural products supply chain traceability system based on blockchain[D]. Xi'an: Xidian University, 2019. (in Chinese)

[10] 陈邦越. 基于区块链的水稻全供应链溯源系统设计与实现[D]. 长春：吉林农业大学, 2021.
CHEN Bangyue. Design and implementation of a whole supply chain traceability system for rice based on blockchain[D]. Changchun: Jilin Agricultural University, 2021. (in Chinese)

[11] DEMESTICHAS K, PEPPES N, ALEXAKIS T, et al. Blockchain in agriculture traceability systems: a review[J]. Applied Sciences, 2020, 10(12): 4113.

[12] 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 Huajing, 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)

[13] 孙传恒,万宇平,罗娜,等. 面向追溯主体的果蔬全供应链区块链多链模型研究[J]. 农业机械学报, 2023, 54(4): 416 - 427.
SUN Chuanheng, WAN Yuping, LUO Na, et al. Blockchain multi-chain model of fruit and vegetable supply chain for traceability subjects[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4): 416 - 427. (in Chinese)

[14] 李修华,罗潜,杨信廷,等. 面向小麦区块链追溯系统的分级监管模型设计与实现[J]. 农业机械学报, 2023, 54(3): 363 - 371.
LI Xiuhua, LUO Qian, YANG Xinting, et al. Design and implementation of blockchain hierarchical supervision model for wheat supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(3): 363 - 371. (in Chinese)

[15] 刘晓辉,罗娜,邢斌,等. 基于属性可搜索加密的农产品区块链追溯隐私数据访问控制方法[J]. 农业机械学报, 2024, 55(10): 433 - 443.
LIU Xiaohui, LUO Na, XING Bin, et al. Attribute-based searchable encrypted agricultural blockchain traceability private data access control method[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(10): 433 - 443. (in Chinese)

[16] 李佳潞. 基于区块链的粮食供应链溯源方案的研究[D]. 北京：北京邮电大学, 2019.
LI Jialu. Research on traceability scheme of grain supply chain based on blockchain[D]. Beijing: Beijing University of Posts and Telecommunications, 2019. (in Chinese)

[17] 张德俊,饶元. 农产品区块链多监管差分隐私共享模型设计[J]. 江苏农业学报, 2024, 40(4): 740 - 752.
ZHANG Dejun, RAO Yuan. Design of multi-regulation differential privacy sharing model for agricultural product blockchain[J]. Jiangsu Journal of Agricultural Sciences, 2024, 40(4): 740 - 752. (in Chinese)

[18] 杨信廷,李金辉,罗娜,等. 基于属性访问控制模型的果蔬跨链追溯系统设计与实现[J]. 农业机械学报, 2023, 54(12): 376 - 388.
YANG Xinting, LI Jinhui, LUO Na, et al. Fruit and vegetable cross-chain traceability system based on attribute access control models[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(12): 376 - 388. (in Chinese)

[19] 杨信廷,李瑞,李金辉,等. 基于区块链技术的农业食品溯源研究进展[J]. 食品科学, 2024, 45(20): 299 - 310.
YANG Xinting, LI Rui, LI Jinhui, et al. Research progress on agricultural food traceability based on blockchain technology[J]. Food Science, 2024, 45(20): 299 - 310. (in Chinese)

[20] 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)

[21] 薛冰,孙传恒,刘双印,等. 区块链背景下农产品零售市场价格博弈模型与竞争策略[J]. 智慧农业(中英文), 2024, 6(4): 160 - 173.
XUE Bing, SUN Chuanheng, LIU Shuangyin, et al. Price game model and competitive strategy of agricultural products retail market in the context of blockchain[J]. Smart Agriculture, 2024, 6(4): 160 - 173. (in Chinese)

[22] 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.
YI Weiguo, HE Jianguo, LIU Guishan, et al. Development and implementation of blockchain to enhance traceability and reliability of fruit and vegetable supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(2): 309 - 315, 345. (in Chinese)

[23] 陈明, 孙浩, 邹一波, 等. 基于区块链的河豚供应链可信溯源优化研究[J]. 农业机械学报, 2022, 53(9): 295 - 304.
CHEN Ming, SUN Hao, ZOU Yibo, et al. Trusted traceability optimization of pufferfish supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(9): 295 - 304. (in Chinese)

(下转第 77 页)

Chinese)
[27] 孙霞，曾守桢. 群体综合评价中兼顾权威与共识的专家权重方法研究[J]. 数学的实践与认识，2014，44(8)：42－47.
SUN Xia，ZENG Shouzhen. A method based on authority and consistency for determining experts's weights in group comprehensive evaluation[J]. Mathematics in Practice and Theory，2014，44(8)：42－47.（in Chinese）
[28] 刘翠玲，戴月，赵琦. 农产品质量安全风险评估方法探索[J]. 食品科学技术学报，2016，34(6)：79－84.
LIU Cuiling，DAI Yue，ZHAO Qi. Study on risk assessment method of agricultural product quality and safety[J]. Journal of Food Science and Technology，2016，34(6)：79－84.（in Chinese）
[29] MA B，HAN Y，CUI S，et al. Risk early warning and control of food safety based on an improved analytic hierarchy process integrating quality control analysis method[J]. Food Control，2020，108：106824.
[30] 徐选华，陈晓红，王红伟. 一种面向效用值偏好信息的大群体决策方法[J]. 控制与决策，2009，24(3)：440－445，450.
XU Xuanhua，CHEN Xiaohong，WANG Hongwei. A kind of large group decision-making method oriented utility valued preference information[J]. Control and Decision，2009，24(3)：440－445，450.（in Chinese）
[31] GENG Z，DUAN X，LI J，et al. Risk prediction model for food safety based on improved random forest integrating virtual sample[J]. Engineering Applications of Artificial Intelligence，2022，116：105352.
[32] ANSARI M S，BARTOS V，LEE B. GRU-based deep learning approach for network intrusion alert prediction[J]. Future Generation Computer Systems，2022，128：235－247.
[33] 李鑫鑫，郑丹，杨建喜，等. 基于 GA－BP 神经网络的施工区域水质预测及预警模型研究[J]. 重庆交通大学学报(自然科学版)，2020，39(12)：106－110.
LI Xinxin，ZHENG Dan，YANG Jianxi，et al. Water quality prediction and early warning model of construction area based on GA－BP neural network[J]. Journal of Chongqing Jiaotong University(Natural Science)，2020，39(12)：106－110.（in Chinese）
[34] GENG Z，ZHAO S，TAO G，et al. Early warning modeling and analysis based on analytic hierarchy process integrated extreme learning machine (AHP－ELM)：application to food safety[J]. Food Control，2017，78：33－42.
[35] GENG Z，LIANG L，HAN Y，et al. Risk early warning of food safety using novel long short-term memory neural network integrating sum product based analytic hierarchy process[J]. British Food Journal，2022，124(3)：898－914.
[36] GENG Z，SHANG D，HAN Y，et al. Early warning modeling and analysis based on a deep radial basis function neural network integrating an analytic hierarchy process：a case study for food safety[J]. Food Control，2019，96：329－342.
[37] ZHANG W，PENG X，GUO J，et al. Pyrolysis kinetic analysis and model constructions of different ranks of coal and validation by GA－BP neural networks[J]. Journal of Analytical and Applied Pyrolysis，2024，182：106659
[38] 石庆兰，束金阳，李道亮，等. 基于 BiLSTM－GRU 融合网络的稻虾养殖溶解氧含量预测[J]. 农业机械学报，2023，54(10)：364－370.
SHI Qinglan，SHU Jinyang，LI Daoliang，et al. Dissolved oxygen prediction in rice and shrimp culture based on BiLSTM－GRU fusion neural networks[J]. Transactions of the Chinese Society for Agricultural Machinery，2023，54(10)：364－370.（in Chinese）
[39] 李道亮，刘畅. 人工智能在水产养殖中研究应用分析与未来展望[J]. 智慧农业(中英文)，2020，2(3)：1－20.
LI Daoliang，LIU Chang. Recent advances and future outlook for artificial intelligence in aquaculture[J]. Smart Agriculture，2020，2(3)：1－20.（in Chinese）

(上接第 55 页)

[24] 孙传恒，袁晟，罗娜，等. 基于区块链和边缘计算的水稻原产地溯源方法研究[J]. 农业机械学报，2023，54(5)：359－368.
SUN Chuanheng，YUAN Sheng，LUO Na，et al. Traceability method of rice origin based on blockchain and edge computing[J]. Transactions of the Chinese Society for Agricultural Machinery，2023，54(5)：359－368.（in Chinese）
[25] 陈锦雯，罗得寸，唐呈俊，等. 基于区块链的农业物联网可信溯源体系[J]. 信息安全学报，2022，7(2)：139－149.
CHEN Jinwen，LUO Decun，TANG Chengjun，et al. The trusted traceability system of agricultural internet of things based on blockchain[J]. Journal of Cyber Security，2022，7(2)：139－149.（in Chinese）
[26] YANG X，YANG X，YI X，et al. Blockchain-based secure and lightweight authentication for Internet of Things[J]. IEEE Internet of Things Journal，2021，9(5)：3321－3332.
[27] 王少华，孙传恒，罗娜，等. 面向预制食品溯源的隐私数据加密共享方法研究[J]. 农业机械学报，2024，55(5)：405－418.
WANG Shaohua，SUN Chuanheng，LUO Na，et al. Privacy data encryption sharing method for prepared food traceability[J]. Transactions of the Chinese Society for Agricultural Machinery，2024，55(5)：405－418.（in Chinese）
[28] 孙传恒，魏玉冉，邢斌，等. 基于智能合约和数字签名的马铃薯种薯防窜溯源研究[J]. 农业机械学报，2023，54(7)：392－403.
SUN Chuanheng，WEI Yuran，XING Bin，el al. Anti-channeling traceability of seed potatoes based on smart contracts and digital signatures[J]. Transactions of the Chinese Society for Agricultural Machinery，2023，54(7)：392－403.（in Chinese）
[29] 李永峰. 基于区块链与内容提取签名的数据共享技术研究[D]. 包头：内蒙古科技大学，2023.
LI Yongfeng. Research on data sharing technology based on blockchain and extracted signatures[D]. Baotou：Inner Mongolia University of Science & Technology，2023.（in Chinese）
[30] ZHANG L，PENG M，WANG W，et al. Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing[J]. Transactions on Emerging Telecommunications Technologies，2021，32(10)：e4315.