

基于长安链的特色农产品气候品质认证与溯源系统设计与实现

陈伏政, 刁仁宏

(成都信息工程大学 区块链产业学院, 四川 成都 610000)

摘要: 针对特色农产品溯源过程中的品质保证、数据泄露和数据监管等难题, 利用区块链的去中心化、不可篡改等特性进行处理。首先, 通过气候品质认证与 NFA 技术协同实现品质与防伪认证; 其次, 提出基于 NTRU 的线性秘密共享方案保障数据安全; 最后, 基于长安链构建监管溯源网络, 使用智能合约实现业务逻辑与数据安全共享, 搭建特色农产品气候品质认证与溯源系统。实验表明, 系统能同时支持 1~900 个并发线程数发送交易请求, 交易吞吐量平均值为 778 TPS, 最大交易时延平均值为 68 ms, 隐私溯源数据加解密平均耗时为 5.7 ms, 可满足溯源需求, 保障特色农产品品质, 实时监控数据, 有效避免数据泄露, 为特色农产品品质认证与溯源系统研究提供参考与借鉴。

关键词: 溯源; 长安链; 气候品质认证; NTRU; 线性秘密分享方案

DOI: 10.11907/rjdk.241902

中图分类号: TP309

文献标识码: A

文章编号: 1672-7800(2026)002-0144-10

扫描二维码阅读全文:



Design and Implementation of Climate Quality Certification and Traceability System for Specialty Agricultural Products Based on ChainMaker

CHEN Fuzheng, DIAO Renhong

(Blockchain Industry College, Chengdu University of Information Technology, Chengdu 610000, China)

Abstract: To address the challenges of quality assurance, data leakage, and data supervision in the traceability process of specialty agricultural products, the decentralized and tamper proof features of blockchain are utilized for processing. Firstly, through the collaboration of climate quality certification and NFA technology, quality and anti-counterfeiting certification can be achieved; Secondly, a linear secret sharing scheme based on NTRU is proposed to ensure data security; Finally, based on ChainMaker, a regulatory traceability network is constructed, and smart contracts are used to achieve business logic and data security sharing, building a climate quality certification and traceability system for characteristic agricultural products. Experiments have shown that the system can simultaneously support 1 to 900 concurrent threads to send transaction requests, with an average transaction throughput of 778 TPS, an average maximum transaction latency of 68 ms, and an average time consumption of 5.7 ms for encrypting and decrypting privacy traceability data. The system can meet traceability requirements, ensure the quality of specialty agricultural products, monitor data in real time, effectively avoid data leakage, and provide reference and inspiration for the research of specialty agricultural product quality certification and traceability systems.

Key Words: traceability; ChainMaker; climate quality certification; NTRU; linear secret sharing scheme

0 引言

2022年,为了全面提升农产品质量安全水平,农业农村部编制了《“十四五”全国农产品质量安全提升规划》,指

出我国面临着标准化水平有待提高、监管基础薄弱等问题,提出推动农产品品质评价体系建设与地理标志农产品发展,以实现标准化生产^[1]。此外,规划还强调在全链条监管中引入智慧监管与追溯管理手段,构建农产品的创新监管机制提升信息透明度,有效应对监管基础薄弱的

收稿日期:2024-12-03

基金项目:四川省国际科技创新合作/港澳台科技创新合作项目(2021YFH0076)

作者简介:陈伏政(1999-),男,CCF学生会员,成都信息工程大学区块链产业学院硕士研究生,研究方向为区块链应用系统设计;刁仁宏(1979-),男,硕士,成都信息工程大学区块链产业学院副教授、硕士生导师,研究方向为移动互联网应用、数据库技术等。

问题。

传统溯源系统通常依赖中心化数据库,存在信息化程度不高、数据丢失篡改、信息孤岛、缺少智慧监管手段等问题,无法实现溯源环节之间的信息流通和信息监管,难以改善监管基础薄弱的问题^[2,3]。目前,利用区块链技术构建特色农产品溯源系统,可有效改善上述问题,确保数据正确性与透明性,实现全过程智慧监管,提升监管效率。此外,在发生质量安全事件时,能有效追溯事件源头进行处理。

区块链技术在溯源系统中的应用广泛。弋伟国等^[4]针对果蔬溯源设计数据哈希值二次上链,改进“数据库+区块链”双存储设计以提升存储效率,但未解决敏感数据共享保护的问题。王莉等^[5]以大米为研究对象构建粮食防伪溯源系统,但未对溯源信息进行处理,系统采用的共识算法效率过低。李梦琪等^[6]针对水产品实际情况设计主从多链存储模型,通过并发分层存储溯源信息、降低存储压力,但系统查询时间过长。孙传恒等^[7]基于多个追溯主体构建多链区块链溯源系统,使用对称加密三重数据加密算法(Triple Data Encryption Algorithm, 3DES)与椭圆曲线加密算法(Elliptic Curve Cryptography, ECC)解决异构数据的存储保护和验证问题,但Raft共识算法不支持拜占庭问题^[8]。于合龙等^[9]设计区块链节点授权保护方法,以其为核心构建溯源系统,但加密共享使用的密钥为单一节点所持有,存在密钥泄露风险。Qi等^[10]结合IPFS文件系统(InterPlanetary File System)与区块链构建溯源系统,提出双重存储模式提升存储空间,但系统平台为以太坊Ethereum,存在性能过低、Gas消耗等问题。Yang等^[11]利用区块链+数据库方式实现果蔬等农产品的溯源系统。Wang等^[12]设计智能合约,基于属性加密与可搜索加密算法构建溯源系统来保护隐私数据。Zhang等^[13]利用密文策略属性基加密方法实现隐私数据的共享与保护。

然而,上述区块链溯源系统采用的区块链平台基本都为Fabric,吞吐量方面的表现不佳,实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)共识算法的效率过低。同时,在农产品溯源工作中缺少农产品品质评价,无法有效保障农产品品质,难以带动地理标志农产品发展,提升标准化水平。为此,本文采用效率更高的Tendermint拜占庭容错(Tendermint Byzantine Fault Tolerance, TBFT)共识算法,基于处理性能更好的单链交易、支持基于内存数据系统的长安链(ChainMaker)平台,构建特色农产品气候品质认证与溯源系统,主要贡献及创新点为:

(1)溯源环节中添加气候品质认证环节。权威认证机构通过该环节对特色农产品进行品质评价打分,生成品质等级证书,完成品质评价工作。同时,调用智能合约作为生产方生成证书的数字非同质化资产,实现特色农产品品质的链上链下协同保障,解决目前特色农产品溯源工作中缺乏品质评价与保障的问题。

(2)提出面向监管的溯源数据存储模型。引入了数论研究单位算法(Number Theory Research Units, NTRU)与线性秘密分享方案。首先,通过NTRU算法生成加密密钥;其次,利用线性秘密分享方案对解密私钥进行碎片化处理,将私钥碎片发送给参与方以避免单一节点保管私钥,防止私钥泄露;最后,针对隐私数据解密设置解密条件,解密方满足条件后方可查看隐私数据,以实现隐私数据安全分享,避免数据泄露。

1 相关技术

1.1 长安链

长安链是我国首个自主研发的区块链底层技术开源平台,具备自主可控、灵活装配、软硬一体、开源开放等特点。长安链的提出正式开启了我国自主创新区块链核心技术的道路,拥有高效并行的调度算法、高性能可信安全智能合约执行引擎、流水线共识算法等国际领先的区块链底层技术,具备高并发、低延时、大规模节点组网等技术优势,交易吞吐能力可达10万TPS,位居全球领先水平。

1.2 气候品质认证技术

气候品质认证技术源于全球范围内的多元化农产品认证标准,例如法国原产地保护标志、美国有机食品认证、澳洲新鲜农产品放心认证、日本有机农业标准、中国“三品一标”等^[14-19]。

该技术是信息时代中的创新性举措,主要分为气候品质评价指数法与气候品质认证评分法^[20]。气候品质认证技术可有效帮助消费者了解特色农产品的品质,增强其购买信心,提升特色农产品的价值、品牌效益与市场竞争力,促进现代农业健康发展^[21]。

1.3 TBFT

TBFT能在拜占庭节点数小于总数1/3的情况下,保证系统安全运行,每轮共识分为以下5个步骤^[22]:

步骤1:共识投票的准备阶段(NewRound),初始化共识相关状态。

步骤2:提案阶段(Proposal),通过leader节点打包区块并将其广播给follower节点。

步骤3:预投票阶段(Prevote),follower节点在收到proposal并验证合法后,广播自己的prevote投票。

步骤4:预提交阶段(Precommit),节点收到超过2/3的prevote投票后,广播自己的precommit投票到其他节点。

步骤5:提交阶段(Commit),节点收到超过2/3的precommit投票后,将proposal中的区块提交到账本。

此外,TBFT与PBFT的最大区别在于:①PBFT通过固定的leader节点打包交易,当leader节点发生故障时,通过view-change子协议更换leader,但在TBFT中leader是轮换的,每提交 n 个块后leader都会轮换成为下一个节点;②当一个交易具有随机性结果时,TBFT通过共识剔除该交易,

以保证链的稳定运行。

1.4 NTRU

Hoffstein 等^[23]基于格论与数论理论,提出一种基于格的公钥密码体制 NTRU。该算法的安全性基于格上的最短向量问题(Shortest Vector Problem, SVP),目前还没有算法能在有效多项式时间内解决该问题,因此算法在理论上具备抵抗量子计算机攻击的能力。

此外,相较于现有的公钥加密系统而言,NTRU 安全性更高,在保证相同安全性的情景下加解密速度更快、时间损耗更少。

1.5 线性秘密分享方案

线性秘密分享方案是一种密码学技术,分发者将秘密分成 n 个份额,使任意不少于 t 个参与者能正确重构出秘密 s ,小于门限值的参与者无法获得有关秘密的任何信息^[24]。

该方案的基本思路是利用二叉树结构对所有叶子节点进行取值,从而构建 $t \times n$ 的秘密共享矩阵,结合随机数掩盖秘密,将秘密掌管节点对应的秘密份额进行分享。在恢复秘密时,需要不少于 t 个秘密掌管节点合作,进行矩阵运算以恢复出秘密。此外,线性秘密分享方案安全性更高、难以破解,适用于多方协作加密、数据传输保密性等多方合作场景。

2 系统设计

2.1 气候品质认证工作

特色农产品的气候品质认证工作主要分为以下 3 个步骤:①选取气象要素指标;②确立与评定综合气象条件;③气候品质综合认证。其中,品质证书作为特色农产品的标识,能与其他产品进行区别,并通过该证书追溯到权威

机构,便于识别证书是否真实有效。

2.1.1 气象要素指标

气象要素指标首先需要收集该地区往年农产品的质量与其生长周期内的气候等数据;其次,整理、分析生长周期内不同阶段期间的生长情况,从中抽离、提炼出气象要素;最后,将其与敏感气象要素进行相关性分析得出气象要素指标。在确定气象要素指标后,根据农产品在气象要素指标下的不同生长情况,将指标区间划分为最适宜、适宜、次适宜和不适宜。

2.1.2 综合气象条件确立

最适宜:①所有区间全为最适宜;②选取的关键区间为最适宜和其余区间为适宜;③选取的关键区间半数以上为最适宜和其余区间为最适宜。

适宜:①所有区间全为适宜;②选取的关键区间为适宜和其余区间为次适宜及以上;③选取的关键区半数以上为适宜和其余区间为适宜及以上。

次适宜:①所有区间全为次适宜;②选取的关键区间半数以上为次适宜。

不适宜:不符合上述区间,自动划为不适宜。

2.1.3 气候品质综合认证

图 1 为农产品气候品质综合认证工作流程,综合得分由专家评分 $X_1 \in [0.05, 0.2]$ 和农产品的生长周期中不同阶段的评分 X_2, X_3 共同组成。首先,将农产品的生长周期 T 划分为关键生长周期 T_1 、普通生长周期 T_2 , $T = T_1 + T_2$;其次,设置关键生长周期 T_1 的权重占比为 $S_1 = 1/T + 0.4 \times T_1/(T \times T_2)$,普通生长周期权重占比 $S_2 = 0.6 \times (1/T)$;再次,根据生长周期内的综合气象条件评定区间对 K_i (第 i 天的综合气象条件区间)进行权重分配,当综合气象条件为最适宜区间、适宜区间、次适宜区间、不适宜区间时,权重

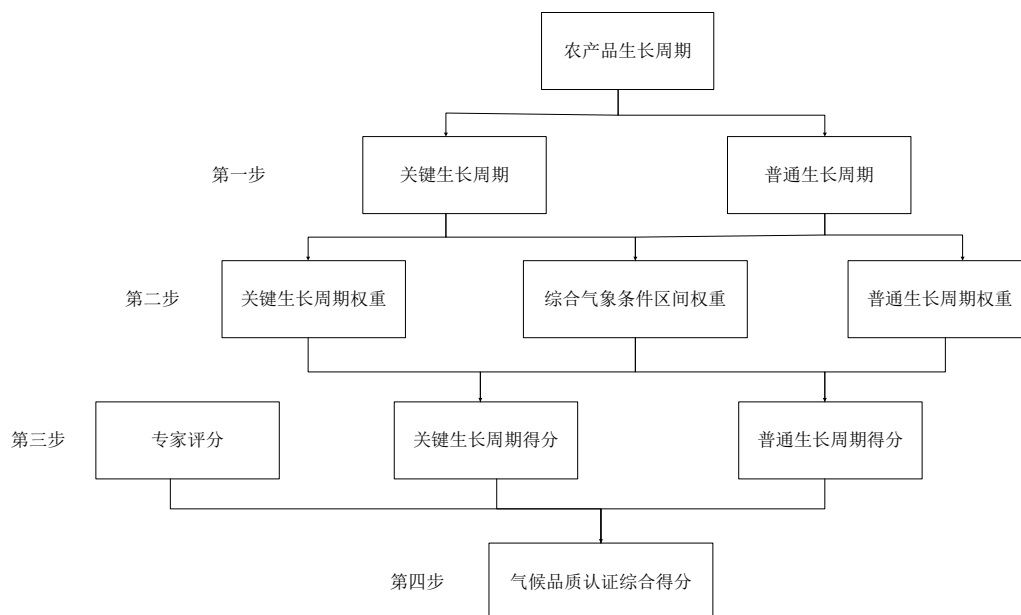


Fig. 1 Comprehensive score for climate quality certification

图 1 气候品质认证综合得分

K_i 分别为 1、0.7、0.4、0,从而计算关键生长周期得分 $X_2 = S_1 \times \sum_{i=1}^{T_1} K_i, i \in [1, T_1]$, 普通生长周期得分 $X_3 = S_2 \times \sum_{i=1}^{T_2} K_i, i \in [1, T_2]$;最后,计算农产品的气候品质认证综合得分 $Y = X_1 + X_2 + X_3$,当 $Y \geq 0.95$ 时产品认证等级为特优,当 $0.75 \leq Y < 0.95$ 时产品认证等级为优,当 $Y < 0.75$ 时产品认证等级为次优。

2.2 溯源数据处理

2.2.1 溯源数据分析

特色农产品供应链中涉及多个参与方(生产方、收购方、物流、仓储和销售商等),因此在追溯过程中数据信息存在来源广泛、规模庞大、种类繁多、具有异构性等问题,并非所有数据都适合共享溯源。例如,涉及特色农产品成本价格、数量等与质量安全无关的敏感数据不适宜完全透明公开,需要在区块链网络中进行脱敏化处理,防止数据泄露。

为此,本文对特色农产品的气候品质认证工作与供应链环节中的溯源信息进行整理、分析后,将其划分为公开数据和隐私数据,如表 1 所示。

2.2.2 隐私溯源数据保护流程

针对隐私溯源数据共享与解密私钥管理问题,提出基于 NTRU 的线性秘密分享方案的保护方案,如图 2 所示。具体流程步骤为:

步骤 1:系统初始化时,证书颁发机构(Certificate Authority, CA)调用 NTRU 算法生成公私钥。其中,公钥上链;私钥通过线性秘密分享方案进行处理,生成多个私钥份额,将其发送给供应链相关组织节点管理员。

步骤 2:监管机构查看隐私数据密文。

Table 1 Traceability data classification		
表 1 溯源数据分类		
供应链组织	公开数据	隐私数据
生产	产品名称、产品产地、生长周期	产品成本、产品数量、产品出售价格
品质认证	认证机构、认证产品、认证等级	气象数据哈希
收购	收购企业、收购时间、收购地点	收购成本、出货价格
物流	物流企业、物流路线、物流时间	物流成本、物流运输数量
仓储	仓储企业、仓储地点、仓储时间	仓储成本、仓储数量
销售	批发单位、进货时间、出货时间	进货价格、出售价格、进货数量

步骤 3:监管机构向供应链组织管理员节点发起解密数据申请。

步骤 4:对供应链组织管理员节点进行部分解密。

步骤 5:供应链组织管理员节点发送解密分片至监管机构。

步骤 6:监管机构收集所有解密分片。

步骤 7:对隐私数据进行解密,以查看数据。

密钥生成函数 $\text{KeyGen}()$ 的描述为:①依据参数集配置参数 $N=613, p=3, q=2\ 048$, 定义多项式环 $\mathcal{R} = \mathbb{Z}[x]/(X^N - 1)$;②任取多项式 $F, G \in \mathcal{R}$, 系数均属于 $\{-1, 0, 1\}$;③令 $f = 1 + pF$, 若 f 在 $\mathcal{R}_q = (\mathbb{Z}/q\mathbb{Z})[x]/(X^N - 1)$ 上不可逆, 则重新选择多项式;④令 $g = pG, h = f^{-1}g \bmod q$;⑤先构建线性秘密分享矩阵 Matrix , 初始化长度为 n 的向量 t , 令 $t[0] = f$;再依次重复步骤 2、步骤 3 生成 $f_1, f_2, \dots, f_{n-1}$, 令 $t[1] = f_1, t[2] = f_2, \dots, t[n-1] = f_{n-1}$;⑥令

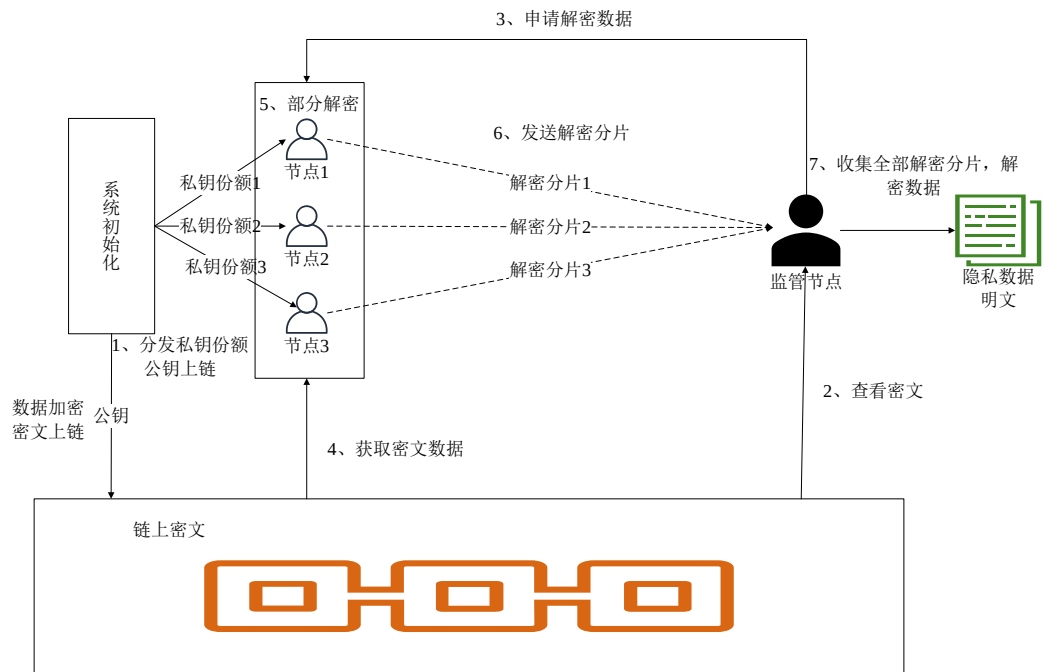


Fig. 2 Process of privacy data protection scheme

图 2 隐私数据保护方案流程

公钥为 h , 私钥份额 $keys = Matrix \cdot t$, 将公钥上链, 将私钥份额 $Keys$ 的各分量分发给各组织。

密文加密函数 $Encrypt()$ 的描述为: 任取多项式 $r \in \mathcal{R}$, 对于明文 m , 生成密文 $c = r \cdot h + m \pmod{q}$, 将密文上链。

密文解密分片函数 $Decrypt()$ 的描述为: 监管节点在得到供应链组织的授权后, 各组织节点利用自身持有的私钥份额对密文进行解密, 得到各自的解密分片 $s_i = f_i \cdot c \pmod{q}$, $i = 0, 1, \dots, n-1$, 并将 s_i 上链存储。

收集解密分片函数 $Collect()$ 的描述为: 监管节点在获取所有解密分片 $s = \sum_0^{n-1} s_i \pmod{q}$ 后, 解密得出隐私数据明文 $m = s \pmod{p}$ 。

2.2.3 溯源数据存储模型

本文在整理、分析供应链流程中溯源数据后, 提出了隐私溯源数据保护方案, 构建了面向监管的农产品溯源数据存储模型, 如图3所示。由此可知, 该模型的组织节点分别为品质认证、生产、收购、物流、仓储、销售和第三方监管等节点。

(1) 品质认证节点记录农产品的品质认证证书的相关数据, 通过非同质化资产 (Non Fungible Assets, NFA) 智能

合约发行品质证书 NFA, 并将其上传至区块链网络。证书 NFA 信息包括: 证书编号、证书种类和 Metadata 信息, Metadata 包括产品名称、产品产地、产品品质等级、产品描述、产品证书 URL、产品证书哈希等字段。

(2) 生产、收购、物流、仓储和销售等组织节点, 根据智能合约提供的格式, 将溯源数据分为公开溯源数据和隐私溯源数据。其中, 公开溯源数据直接上链存证; 隐私溯源数据先通过第三方监管节点上传至链中的公开 NTRU 公钥进行加密, 再将隐私溯源数据密文上链, 以保证隐私溯源数据的安全性与不可见性。

(3) 第三方监管节点有权在区块链网络中查看品质证书 NFA 的流通过程和解密查看隐私溯源数据, 实时监管区块链网络。

(4) 链上数据库 LevelDB 存储公开溯源数据、隐私溯源数据密文、品质证书 NFA、加密公钥等数据。

2.3 智能合约设计

本文针对特色农产品的数据存储模型, 设计品质证书 NFA 的发行与查询、数据上链、数据查询等智能合约, 节点通过调用合约接口自动实现业务逻辑。具体合约业务逻辑和设计如表2所示。

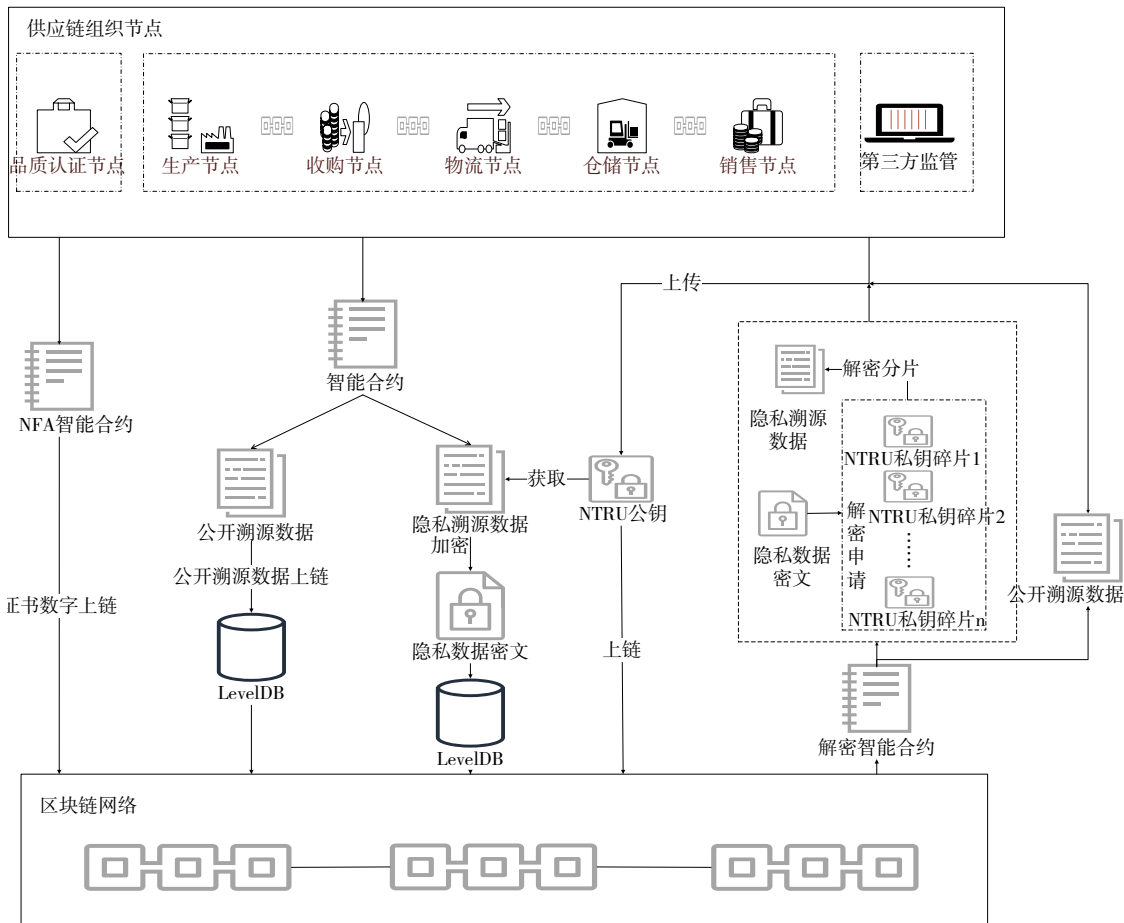


Fig. 3 Traceability data storage model for agricultural products

图3 农产品溯源数据存储模型

Table 2 Smart contract design
表 2 智能合约设计

合约功能	合约业务逻辑	合约方法	输入	输出
品质证书NFA发行与查询	品质认证中心发行NFA	Mint()	接收方地址、种类名,品质证书ID、证书详细信息	Success/Error
	NFA信息查询	getNFAInfo()	证书ID	证书详细信息
	公开数据上链	SavePublicInfo()	特色农产品ID,特色农产品公开数据	交易ID,区块高度
数据上链	隐私数据加密公钥上链	SavePublicKey()	加密公钥,加密公钥哈希	交易ID,区块高度
	隐私数据密文上链	SavePrivateCipher()	隐私数据密文,隐私数据密文哈希	交易ID,区块高度
	隐私数据密文哈希和解密分片上链	SaveShare()	隐私数据密文哈希、密文对应的多个解密分片	交易ID,区块高度
	公开溯源数据查询	getPublicInfo()	特色农产品ID	特色农产品公开数据
数据查询	隐私数据解密查询	getPrivateInfo()	隐私数据密文哈希	特色农产品隐私数据解密分片

3 系统实现

3.1 系统架构

图 4 为溯源系统架构,从上至下分别为应用服务层、合约层、网络层、数据存储层和数据收集层。

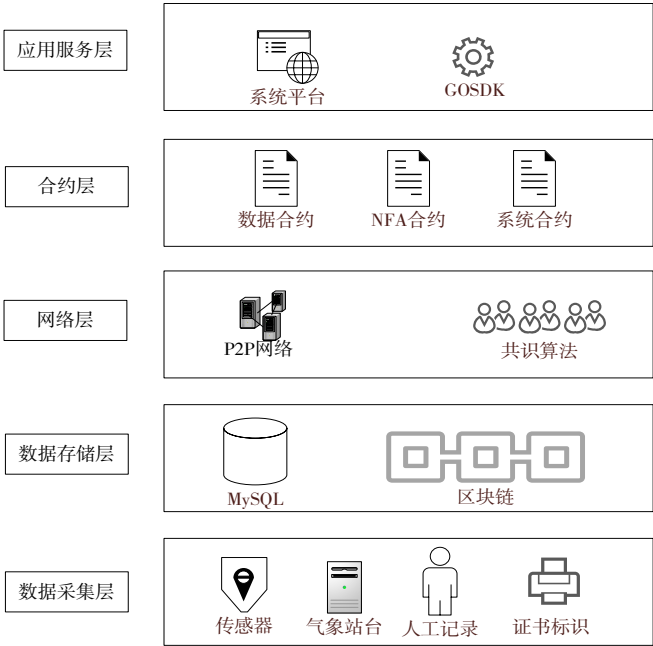


Fig. 4 System architecture
图 4 系统架构

- (1)数据收集层。通过供应链环节中物联网传感器、气象站台,实时收集特色农产品生长周期内的气象数据与溯源过程中的数据信息,辅以人工记录的方式补充和完善数据,确保溯源信息的完整性与准确性。证书标识粘贴在特色农产品的包装上便于识别。
- (2)数据存储层。通过区块链、本地 MySQL 数据库存储与管理数据,处理数据采集层收集到的数据。通过区块链技术保证数据的可追溯性和不可篡改性,且在本地 MySQL 数据库中存储数据副本及系统用户的相关信息。
- (3)网络层。在点对点(Peer-to-Peer, P2P)网络高效传播区块信息,并在共识算法下验证信息一致性,保证节

点数据的安全性及准确性。

(4)合约层。负责智能合约的编写与部署,提供数据合约、NFA 合约与系统合约。其中,数据合约主要将溯源数据存储在区块链;NFA 合约主要将特色农产品的品质证书转为 NFA,保障证书的唯一性与安全有效性;系统合约主要是各供应链环节组织管理员对组织内用户进行管理的操作,包括权限修改、添加、删除用户等。

(5)应用服务层。为供应链环节中的用户提供可视化的系统平台,用户注册登录后进入系统,通过 GOSDK 提供的智能合约接口操作农产品溯源数据,并将数据上传至区块链网络中或查询农产品信息,实时监控监管机构用户提供的数据。

3.2 系统功能

本文以四川省广元市苍溪县猕猴桃为例进行特色农产品的气候品质认证工作。首先,评定生长周期内的气象要素(见图 5);其次,对特色农产品进行综合认证赋分,生成品质证书(见图 6)。

生育期	时间范围	气象因子	最适范围	2014年气象条件	评级
发芽展叶期	3月初至3月下旬	气温	10~17℃	16.7℃	最适宜
		降水	50~100mm	80.4mm	最适宜
		积温	500~850℃	759.0℃	最适宜
开花期	4月初至4月下旬	气温	18~20℃	18.2℃	最适宜
		降水	10~25mm	2.0mm	不适宜
		日照时数	40~60h	57.9h	最适宜
果实膨大期	5月中旬至7月中旬	气温	20~26℃	25.2℃	最适宜
		降水	300~400mm	119.1mm	次适宜
		雨日数	<25d	36d	不适宜
		日照时数	300~400h	375.3h	最适宜
糖分转化期	7月下旬至8月中旬	气温	25~27℃	27.9℃	最适宜
		气温日较差	9~11℃	9.8℃	最适宜
		降水	130~230mm	96.9mm	适宜
		雨日数	<15d	11d	最适宜
		日照时数	130~230h	204.7h	最适宜

Fig. 5 Example of meteorological element evaluation for specialty agricultural products
图 5 特色农产品气象要素评定示例

图 7 展示的内容是特色农产品品质证书生成的 NFA,展示内容为证书编号、证书种类、证书 URI 及证书 Metadata 信息,由品质认证节点生成并发送给生产组织节点。其

中,证书Metadata信息为品质证书的具体信息。



Fig. 6 Specialty agricultural products quality certificate
图6 特色农产品品质证书



Fig. 7 Quality certificate NFA
图7 品质证书NFA

图8为监管机构在区块链网络中的监管界面。该界面包括网络中节点组织、链上合约、区块数量与交易信息等,便于监管机构实时查看链上信息。

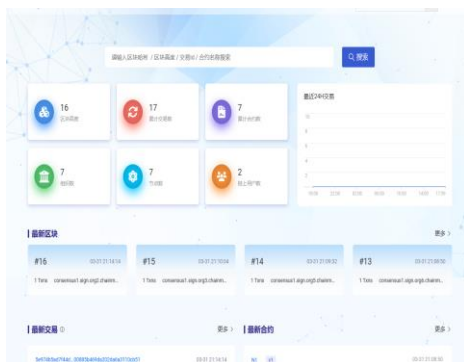


Fig. 8 Transaction data supervision interface
图8 交易数据监管界面

图9为系统提供给供应链中组织用户的溯源数据上传功能界面,用户可将不同溯源环节中的数据上传至系统。同时,系统还提供了增删改等功能,在确认信息无误后可调用相应的智能合约接口实现溯源数据上链操作、完成存储,保障数据安全性。

图10为系统提供给消费者的特色农产品信息查询界面。本文以苍溪县猕猴桃为例,消费者通过该界面输入苍

溪县猕猴桃的溯源码后,将展示猕猴桃的品质证书信息、溯源环节中的溯源信息。

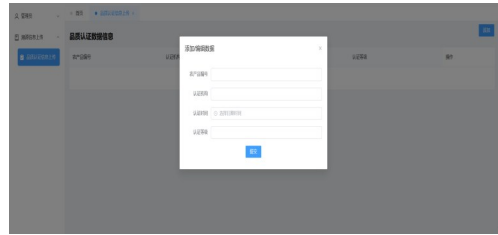


Fig. 9 Traceability data upload interface
图9 溯源数据上传界面



Fig. 10 Featured agricultural product traceability information interface
图10 特色农产品溯源信息界面

4 系统分析与测试

4.1 安全性分析

隐私数据保护方案的安全性取决于NTRU算法的安全性。该算法的安全性来源于一个搜索问题——最短向量问题(Shortest Vector Problem, SVP),可使用格基约简算法(Block Korkin Zolotarev reduction, BKZ)与量子Grover算法进行求解^[25,26]。

表3为格维度 $N=500/800/1\ 000$ 时两种算法的计算用时,单位为一台计算机以每秒一百万次操作的速度在一年内所执行的工作量,即MIPS Year(Million Instructions Per Second, MIPS)。由此可知,BKZ算法、量子Grover算法求解SVP问题的计算用时为指数关系,绝对时间很长,无法完全解决SVP问题。在一定条件下,SVP问题是NP完全问题,因此NTRU算法被认为是安全的,具有抗量子性。

Table 3 Comparison of calculation time

表3 计算用时比较

N	$T_{BKZ}(N)$	$T_G(N)$
1 000	5.23×10^{96}	1.23×10^{12}
800	6.59×10^{74}	2.25×10^9
500	9.33×10^{41}	1.76×10^5

Albrecht等^[27-29]提出,当 (f, g) 中模数 q 过小时存在子域攻击,此时NTRU的公钥能被分解到某个子域上,易于解决该子域格上的SVP问题,从而恢复私钥 (f, g) 。为此,

NTRU 算法的参数目前不在子域攻击的范围内。

4.2 性能测试

4.2.1 测试环境

通过虚拟机 Ubuntu-22.04.4-desktop Linux 系统,搭建基于长安链 ChainMaker V3.0.0 的农产品溯源网络,配置 8 核处理器,50 GB 存储容量,10 GB 运行内存进行实验。区块链采用 TBFT 共识算法,区块链数据库引擎为 LevelDB,利用键值查询提升数据查询效率,具体配置如表 4 所示。此外,本文使用 Go 语言编写智能合约,将 GOSDK 部署到 ChainMaker 网络。

Table 4 Blockchain configuration

表 4 区块链配置

配置项	值	描述
链数量	1	溯源链
共识节点	7	1 共识节点/组织
共识机制	TBFT	拜占庭容错共识算法
数据库	LevelDB	区块链配置的数据库引擎
区块生成时间/ms	200	区块生成的间隔
区块最大容量	1 000	区块中最大可以包含的交易数量

4.2.2 性能测试

针对本文设计的隐私溯源数据保护方案进行 20 轮测试,密钥生成及私钥处理平均耗时为 121 ms(见图 11),密文加解密平均耗时为 5.7 ms(见图 12)。由此可知,方案耗时主要为密钥生成、私钥处理部分,能满足系统在溯源场景中处理隐私数据的需求。

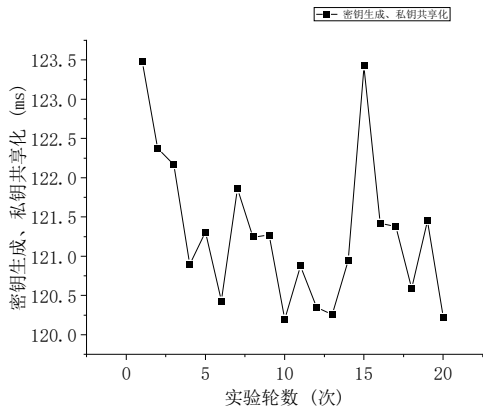


Fig. 11 Time consumption for key generation and private key sharing

图 11 密钥生成、私钥共享化耗时

在测试系统性能的过程中,区块链测试工具为 Cmc (ChainMaker Client, Cmc) 工具。本文使用交易吞吐量与交易时间延迟指标作为测试指标。其中,交易吞吐量指系统在单位时间内能处理的交易数量,以衡量系统处理能力;交易时间延迟指标指从一个交易发起到系统完成处理该交易的时间间隔,以反映系统负载与响应能力。

同时,通过设置并发线程数(系统能承载最大线程数量)的数量,在单个线程执行等量的查询交易次数下,对交易吞吐量、交易时间延迟进行测试,如图 13、图 14 所示。由此可见,当并发线程数在 100~900 区间内,系统吞吐量与交易时延会随着并发线程数增加而增加,表明系统在处

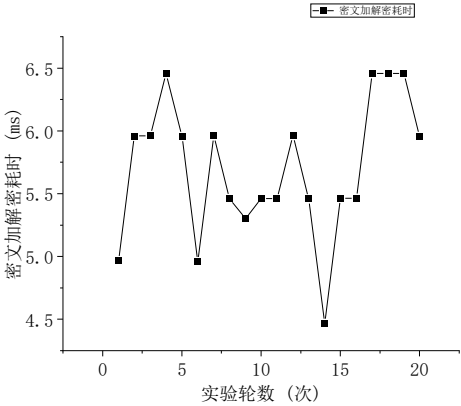


Fig. 12 Time Consumption of ciphertext encryption and decryption

图 12 密文加解密耗时

理大量并发的查询请求时逐渐接近资源极限,但能满足日常需求,承载能力良好。在 900~1 000 区间中,交易吞吐量与交易时延急速下降,出现交易失败情况,表明系统资源已饱和,接近或达到了最大承载压力,可判断系统并发线程数在 900 左右时达到极限。

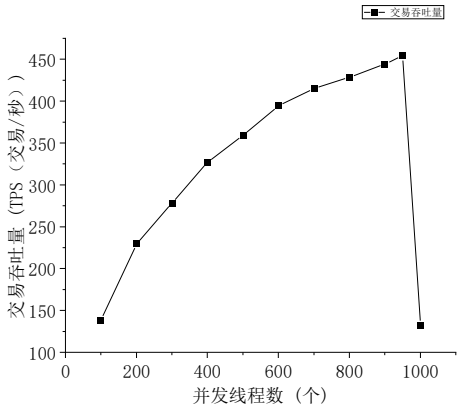


Fig. 13 Transaction throughput – number of concurrent threads

图 13 交易吞吐量—并发线程数

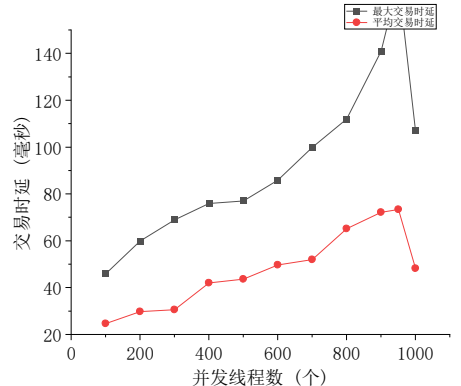


Fig. 14 Transaction latency – number of concurrent threads

图 14 交易时延—并发线程数

为此,本文设置并发线程数为 500,对不同交易数量进行交易吞吐量和交易时延测试,分别为 500、1 000、2 000、5 000、10 000、20 000、50 000,如图 15 所示。由此可见,交易吞吐量随着交易数量的增加逐步上升,在 980 TPS 处趋于稳定,平均值为 778 TPS。

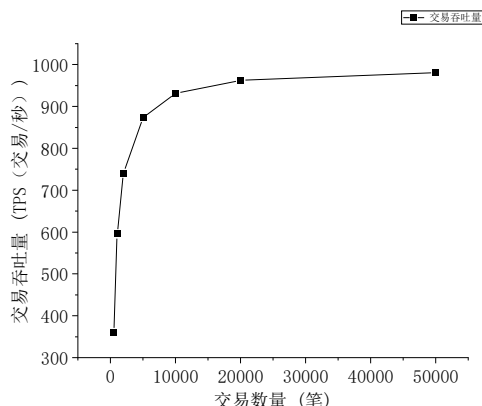


Fig. 15 Transaction throughput - number of transactions

图 15 交易吞吐量—交易数量

图 16 为交易时延。由此可见,最大交易时延随着交易数量增加而降低,在 60 ms 趋于稳定,平均交易延迟随着交易数量增加而降低,在 2 ms 附近趋于稳定,表明系统能处理大量并发请求,例如在溯源数据查询时可保障高吞吐量和低时延。

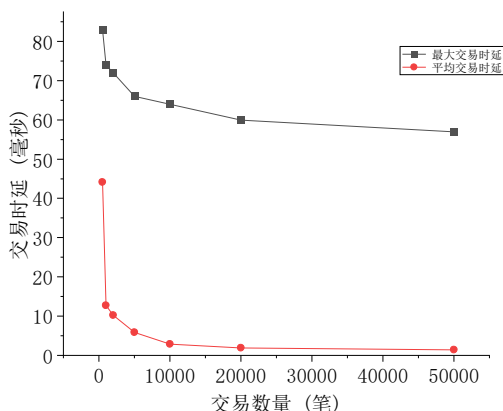


Fig. 16 Transaction latency - number of transactions

图 16 交易时延—交易数量

4.3 方案比较

本文方法与其他方案的比较结果如表 5 所示。由此可知,本文使用的系统平台为长安链 ChainMaker,能在单链模式下具备良好的交易性能与负载能力,支持大规模数据传输。采用 TBFT 共识算法能更高效地在节点网络中达成共识,提升系统吞吐量,使其满足溯源查询需求。

此外,本文所提方法利用气候品质认证技术对特色农产品品质进行认证保障,在隐私数据的保护方案中引入了 NTRU 算法与线性秘密分享方案,具备更好的加解密能力与抗量子性,可进行私钥管理,避免私钥泄露。

5 结语

本文实现了长安链在特色农产品溯源中的应用,在特色农产品溯源过程中融入了气候品质认证工作,提出了气候品质认证与溯源系统。首先,选取区块链平台与共识算法确保系统交易性能更优;其次,利用气候品质认证技术

Table 5 Scheme comparison

表 5 方案比较

项目	本文	文献[4]	文献[5]	文献[7]	文献[9]
平台	ChainMaker	Fabric	Fabric	Fabric	Fabric
共识算法	TBFT	PBFT	无	RAFT	PBFT
加密算法	NTRU	无	RSA	ECC+3DES	CBC+ECC
抗量子性	是	否	否	否	否
加解密效率	高	无	低	中	高
吞吐量/TPS	778	200	258	无	200
交易时延/ms	2.00	66.00	500.00	38.86	85.00
链架构	单链	单链	单链	多链	多链
气候品质认证	是	否	否	否	否

与 NFA 技术,对特色农产品品质进行认证双重保障,增强消费者的购买信心,推动农产品品质评价体系建设与地理标志农产品发展;再次,针对隐私数据设计保护方案,引入 NTRU 算法保证隐私数据安全共享,在安全性方面具备抗量子攻击的能力;最后,使用线性秘密分享方案实现密钥管理,通过多个节点共同管理密钥碎片,避免单一节点保管致使密钥泄露。

实验表明,系统能处理大量并发请求,满足溯源需求,具备加解密高效率、高吞吐量、低时延、高交易性能等特点,为我国首个自主研发的长安链平台的应用提供了参考与借鉴。然而,本文方案基于单链设计,存储空间有限,后续将基于多链架构进行设计,结合星际文件系统(InterPlanetary File System, IPFS)进行存储,以减轻区块链的负载压力。

参考文献:

- [1] Ministry of Agriculture and Rural Affairs. Notice on issuing the "14th Five Year Plan for national agricultural product quality and safety improvement" [EB/OL]. https://www.gov.cn/zhengce/zhengceku/2022-02/24/content_5675448.htm.
农业农村部.关于印发《“十四五”全国农产品质量安全提升规划》的通知 [EB/OL]. https://www.gov.cn/zhengce/zhengceku/2022-02/24/content_5675448.htm.
- [2] SUN C H, YU H J, XU D M, 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.
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.
- [3] ZHAO B. Research on the application practice of intelligent supervision in food safety supervision [J]. China Food Safety Magazine, 2024 (28): 17-19.
赵兵.智慧监管在食品安全监管中的应用实践研究[J].食品安全导刊, 2024(28): 17-19.
- [4] YI W G, HE J G, LIU G S, 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, 52(2): 309-315, 345.
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, 52(2): 309-315, 345.
- [5] WANG L, REN J R, WANG T, et al. Design and implementation of food security traceability system based on blockchain [J]. Science Technology

- and Engineering, 2023, 23(4): 1625–1634.
- 王莉,任健荣,王涛,等. 基于区块链的粮食防伪溯源系统的设计与实现[J]. 科学技术与工程, 2023, 23(4): 1625–1634.
- [6] LI M Q, YANG X T, XU D M, et al. Design and implementation of aquatic products blockchain traceability information management system based on master slave multi chain[J]. Fishery Modernization, 2021, 48(3): 80–89.
- 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.
- [7] SUN C H, WAN Y P, LUO N, et al. Research on 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.
- 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.
- [8] CAI Y, CAI T. Research on network information encryption based on 3DES-ECC algorithm[J]. Network Security Technology & Application, 2016(8): 32, 34.
- 蔡宇,蔡婷. 基于3DES-ECC算法的网络信息加密研究[J]. 网络安全技术与应用, 2016(8): 32, 34.
- [9] YU H L, CHEN B Y, XU D M, 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.
- 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.
- [10] QI Y, ZHANG H J. Improving agricultural product traceability using blockchain[J]. Sensors (Basel), 2022, 22(9): 3388.
- [11] 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: 36282–36293.
- [12] WANG Y Z, WANG H, ZHENG D, et al. A blockchain-based traceability system with efficient search and query[J]. Peer-to-peer Networking and Applications, 2022, 16: 675–689.
- [13] ZHANG L Y, ZHANG T S, WU Q, et al. Secure decentralized attribute-based sharing of personal health records with blockchain[J]. IEEE Internet of Things Journal, 2022, 9: 12482–12496.
- [14] ZHANG X, LIU C X, XU J P, et al. Construction and systematic implementation of multi-chain-based management model for fruits and vegetables in full-process and information scheme[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(6): 365–379.
- 张新,刘崇宣,许继平,等. 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[J]. 农业机械学报, 2024, 55(6): 365–379.
- [15] QU H H, LI S P. The experience of geographical indication protection in France and its enlightenment to China[J]. Yantai Fruits, 2023(3): 27–28, 56.
- 曲恒华,李淑平. 法国地理标志保护经验及对我国的启示[J]. 烟台果树, 2023(3): 27–28, 56.
- [16] MU J H, XU J D. The development of organic agriculture in America and its enlightenment to China[J]. Food and Nutrition in China, 2021, 27(3): 18–22.
- 穆建华,徐继东. 美国有机农业发展及对我国的启示[J]. 中国食物与营养, 2021, 27(3): 18–22.
- [17] JIN F Z, SONG Y, YUAN G Y, et al. Quality safety management and certification of agricultural products in Australia[J]. China Animal Industry, 2007(17): 82–86.
- 金发忠,宋烽,袁广义,等. 澳大利亚的农产品质量安全管理与认证[J]. 中国牧业通讯, 2007(17): 82–86.
- [18] LU Y N. The promotion and enlightenment of organic agriculture in Japan[J]. Journal of Shandong Agricultural University (Social Science Edition), 2015, 17(2): 63–67.
- 卢永妮. 日本有机农业的推进及启示[J]. 山东农业大学学报(社会科学版), 2015, 17(2): 63–67.
- [19] YANG Z Q, LIANG J. Evaluation of the microeconomic effects of China's agricultural product quality regulation policies: taking the quality certification of "three products and one standard" as an example[J]. Journal of Macro-quality Research, 2024, 12(1): 86–102.
- 杨芷晴,梁静. 我国农产品质量规制政策的微观经济效应评估:以“三品一标”质量认证为例[J]. 宏观质量研究, 2024, 12(1): 86–102.
- [20] BAI Z Z, LI L, WANG H L, et al. Climatic quality certification of agricultural products in China: experience, problems and countermeasures[J]. Dynamics of Social Sciences, 2021(5): 44–48.
- 柏振忠,李亮,王红玲,等. 我国农产品气候品质认证:经验、问题与对策[J]. 社会科学动态, 2021(5): 44–48.
- [21] XU Q Q, LI Y B, CAO W, et al. Research progress of climate quality certification technology of agricultural products[J]. Chinese Journal of Tropical Agricultural, 2022, 42(4): 132–135.
- 徐擎擎,李衍彪,曹伟,等. 农产品气候品质认证技术研究进展[J]. 热带农业科学, 2022, 42(4): 132–135.
- [22] ETHAN B. Tendermint: byzantine fault tolerance in the age of blockchains [EB/OL]. https://known-production.s3.amazonaws.com/uploads/attachment/file/1814/Buchman_Ethan_201606_Msater%2Bthesis.pdf.
- [23] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[EB/OL]. <https://www.ntru.org/t/hps98.pdf>.
- [24] ZHANG L, LIU B X. Review of blockchain technology[J]. Computer Engineering, 2022, 48(8): 1–11.
- 张亮,刘百祥. 区块链与秘密分享融合技术综述[J]. 计算机工程, 2022, 48(8): 1–11.
- [25] SCHNORR C P, EUCHNER M. Lattice basis reduction: improved practical algorithms and solving subset sum problems[J]. Mathematical Programming, 1994, 66(1–3): 181–199.
- [26] CHEN Y, NGUYEN P Q. BKZ 2.0: better lattice security estimates [C]// Seoul: International Conference on the Theory and Application of Cryptology and Information Security, 2011.
- [27] ALBRECHT M, BAI S, DUCAS L. A subfield lattice attack on over-stretched NTRU assumptions[C]// Berlin: Annual International Cryptology Conference, 2016.
- [28] CHEON J H, JEONG J, LEE C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero[EB/OL]. <https://eprint.iacr.org/2016/139.pdf>.
- [29] EIKE K, VADIM L. CHRISTIAN S. A concrete treatment of fiatshamir signatures in the quantum random-oracle model[EB/OL]. <https://eprint.iacr.org/2017/916.pdf>.

(责任编辑:刘嘉文)