doi:10.6041/j.issn.1000-1298.2024.09.038

基于区块链的远洋捕捞产品新鲜度评价与可信追溯模型研究

马文琪[1,2]　孙传恒[2,3]　罗　娜[2,3]　徐大明[2,3]　邢　斌[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研究中心,北京 100097)

摘要:针对远洋捕捞追溯流程缺少产品新鲜度定量分析,分析结果可信度差等问题,以三文鱼为例,详细分析远洋捕捞追溯流程,基于层次分析法建立了远洋捕捞产品新鲜度指标评价体系,提出新鲜度得分公式,实现了标准统一的产品新鲜度评价。结合 ECDSA 签名技术与智能合约实现了追溯责任的精准定位,通过引入信誉积分数据,建立了奖励、惩罚、补偿机制三位一体的企业双向信誉评价模型,保障了信誉评价主体的积极性及新鲜度得分数据的真实性,实现了产品新鲜度的可信追溯。安全性分析表明信誉积分的攻击难度等价于 ECDSA 私钥的破解难度,证明了信誉评价模型可信、安全及不可篡改的特性。性能测试结果显示,追溯数据读写吞吐量保持在 500 笔/s 与 150 笔/s 以上,读写成功率分别为 100% 与 98%,数据写入平均耗时为 0.416 s,数据查询平均耗时为 0.142 s,相比基于可靠企业信誉评估机制的区块链农产品可信追溯模型,存储与查询效率分别提升 55.8% 与 63.4%,基本满足产品实际追溯业务需求。

关键词:三文鱼;远洋捕捞产品;区块链;椭圆曲线数字签名算法;层次分析法

中图分类号:TP309.2　　**文献标识码**:A　　**文章编号**:1000-1298(2024)09-0428-14　　**OSID**:

Freshness Evaluation and Reliable Traceability Model of Pelagic Fishing Products Based on Blockchain

MA Wenqi[1,2]　SUN Chuanheng[2,3]　LUO Na[2,3]　XU Daming[2,3]　XING Bin[2,3]

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

Abstract: In light of lack of quantitative analysis in the traceability process of pelagic fishing and the limited credibility of the analysis results, the traceability process of pelagic fishing was examined in detail by using salmon as an example. A freshness index evaluation system for pelagic fishing products was established based on the analytic hierarchy process. By applying this method to the evaluation of freshness, a standardized and replicable process for assessing the quality of pelagic fishing products was created, a freshness scoring formula was proposed and standardized product freshness evaluation was achieved. By incorporating ECDSA signature technology and smart contracts, accurate identification of traceability responsibility was achieved. Furthermore, by introducing credit score data, a two-way enterprise reputation evaluation model with reward, punishment, and compensation mechanisms was established to ensure both enthusiasm from credit evaluation subjects and authenticity of freshness score data. This approach enabled trusted traceability of product freshness. The security of this credit evaluation model was of paramount importance, which was addressed by ensuring that the system was as secure as the underlying ECDSA private keys, thus confirming the credibility, security, and immutability characteristics of the credit evaluation model. Performance test results indicated that read and write throughput for traceability data remained above 500TPS and 150TPS, respectively; reading success rate

收稿日期:2024-01-29　修回日期:2024-03-24

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:马文琪(1999—),男,硕士生,主要从事区块链技术研究,E-mail:1179254745@qq.com

通信作者:孙传恒(1978—),男,研究员,博士,主要从事区块链技术、物联网和大数据追溯技术研究,E-mail:sunch@nercita.org.cn

reached 100% while writing success rate standed at 98%. The average time for data writing was 0.416 s while data querying tooks an average time of 0.142 s. Compared with blockchain-based agricultural products trusted traceability models relying on reliable enterprise reputation evaluation mechanisms, storage efficiency was increased by 55.8%, query efficiency was improved by 63.4%, effectively meeting actual product traceability business needs.

Key words: salmon; pelagic fishing products; blockchain; ECDSA; analytic hierarchy process

0　引言

远洋渔业是战略性产业，实现其绿色、健康、可持续发展对丰富国内优质水产品供应、促进多双边渔业合作、维护国家海洋权益等具有重要意义[1-2]。2022 年，农业农村部提出为全面实现远洋捕捞水产品追溯体系创造条件，开展公海渔船渔获物追溯试点。目前远洋捕捞产品溯源体系集中于捕捞环节，难以打通一条完整可信的溯源链，各个环节实际联系密切但溯源体系无法将彼此进行有效衔接，溯源责任难以进行精准定位。我国目前已进行了二维码追溯[3]的相关试点工作，但以上问题仍未得到有效解决。新鲜度作为评价远洋捕捞产品最重要的指标，是决定消费者购买力的首要因素[4-5]，产品一旦产生腐败变质会严重损害厂家商誉[6]，一旦发生食品安全等事故更是会对整个行业造成巨大打击[7]，全溯源流程的各个环节对于产品新鲜度的正确定量评价是决定产品适销性的关键因素。除此之外，远洋捕捞追溯过程中存在信息不对称、易发生安全和欺诈隐患等问题[8]，新鲜度的定量评价结果容易失真，此类现象会严重损害消费者的权益。因此，迫切需要保障产业链环节之间有效衔接，在建立环境信息自动化监测与标准统一的新鲜度定量评价方法的同时，保障追溯流程中产品新鲜度评价结果的可信度，精准定位溯源责任源头，真正实现远洋捕捞产品新鲜度的可信追溯。

区块链技术可追溯、不可篡改等特性及智能合约自动执行、执行结果不可篡改等特点成为打破溯源瓶颈的突破口[9]，分布式的共识使交易在互不信任的分布式系统中进行验证，无需受信任的第三方干预[10]，可为实现远洋捕捞产品新鲜度定量评价的可信追溯提供有力保障。以农业为例，区块链溯源给予每一个农产品一个确定的数字身份，通过数字化流通手段形成农产品从生产到销售全部信息的数据闭环[11]。近些年，区块链技术已广泛应用于农林渔牧行业可信追溯[12]，文献[13-15]将 MD5、SHA256 等哈希算法与溯源结合，链上存储散列值，链下存储追溯数据，以哈希校验的方式构建了可信追溯模型。文献[16]在水产品区块链溯源模型中引入 IPFS 系统，实现了追溯数据的隐私控制。文献[17]建立了面向追溯主体的区块链多链可信追溯架构，满足各追溯主体差异化的追溯需求。文献[18]提出一种基于区块链的水产品撮合交易模型，实现了水产品交易的去中心化可信、不可篡改性。然而，区块链节点存在发布数据失真的问题[19-20]，远洋捕捞场景下，各企业基于谋求利益的出发点，可能产生欺诈行为，造成信任危机。信誉评价机制可有效增强区块链数据可信度[21-23]，文献[24]设计了基于层次分析法的农产品企业信誉度评估机制，但信誉评价计算与存储完全置于链下，评价结果的校验依赖第三方监管机构，因此仍存在数据泄露、篡改的安全风险。

针对以上问题，本文以三文鱼为例，以层次分析法与温度追溯数据为基础构建新鲜度评分体系，提出新鲜度得分公式，实现远洋捕捞全流程产品新鲜度的定量分析。结合新鲜度得分与区块链，设计奖励、惩罚、补偿机制三位一体的企业信誉评价模型，基于椭圆曲线数字签名算法(ECDSA)实现智能合约方法调用的权限匹配算法，以实现追溯责任的精确定位，保障链上新鲜度得分结果的真实性，信誉评价结果的可靠性及信誉评价主体的积极性。在此基础上实现远洋捕捞产品新鲜度可信追溯系统，进行智能合约功能测试、读写性能测试及信誉评价模型安全性分析，以期为实际远洋捕捞可信追溯模型设计提供参考。

1　远洋捕捞产品新鲜度定量评价方法

层次分析法是一种简便、灵活而又实用的多准则决策方法[25]，能够将各风险因素层层分解，将复杂的过程简单清晰化。本章基于层次分析法提出产品新鲜度得分的概念，实现对于产品新鲜度的定量评价，提升消费者对于溯源流程的可信度。

1.1　指标体系构建

温度是影响鱼类产品新鲜度的最重要因素[26]，在捕捞、加工、仓储、销售等过程中，低温可以减缓微生物反应，降低三文鱼腐败、变质风险，本文以各环节温度合规性作为新鲜度评判标准，根据层次分析法的基本步骤，系统分析有关资料和信息，以三文鱼远洋捕捞追溯流程产品新鲜度评价作为目标层(A)，最终确定 3 个准则层，13 个指标层，如图 1 所

示,建立了远洋捕捞追溯产品新鲜度评价递接层次模型。GB/T 27304—2008《食品安全管理体系水产品加工企业要求》规定了捕捞、加工、仓储各环节的温度标准,以此为依据确定了指标层各指标的合规范围,如图 2 所示。

在层次分析评价过程中,通过指标两两重要性

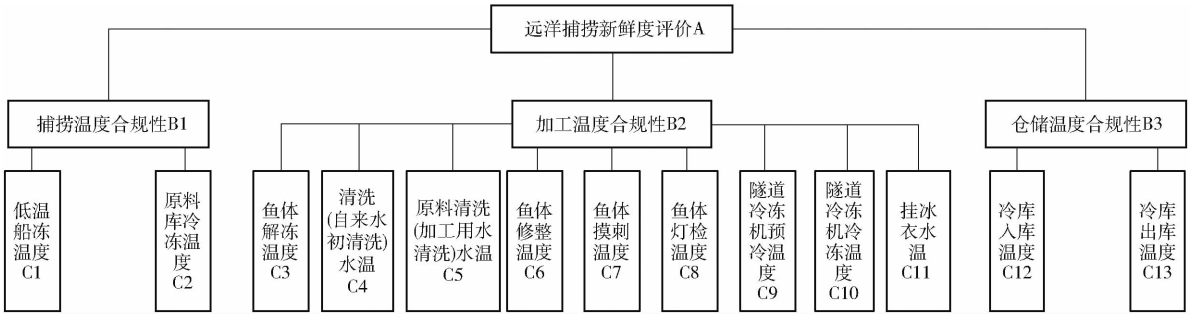

图 1 远洋捕捞溯源新鲜度评价指标体系

Fig. 1 Freshness evaluation system of pelagic fishing traceability model

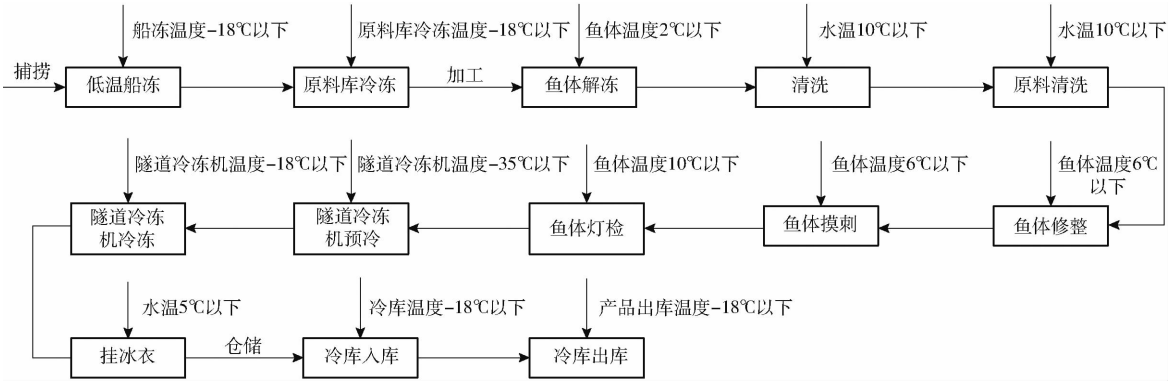

图 2 远洋捕捞溯源新鲜度评价指标合规范围

Fig. 2 Compliance range of freshness evaluation index of pelagic fishing traceability

比较,量化构建了层次单排序中的判断矩阵,采用相对尺度对同一层次因素进行两两比较,尽可能减小性质不同的诸因素相互比较的困难从而提高准确度。比较时遵循原则见表 1,一致性检验计算公式为

$$a_{ij} = 1/a_{ji} \tag{1}$$

式中 a_{ij}——因素 i 和因素 j 的比较结果

表 1 判断矩阵标准评价

Tab. 1 Judgment matrix standard evaluation result

标度	含义
1	两个因素相比,具有同样重要性
3	两个因素相比,一个因素比另一个因素稍微重要
5	两个因素相比,一个因素比另一个因素明显重要
7	两个因素相比,一个因素比另一个因素强烈重要
9	两个因素相比,一个因素比另一个因素极端重要
2,4,6,8	上述两相邻判断的中值
倒数	A 与 B 相比如果标度为 3,那么 B 与 A 相比就是 1/3

将所有专家形成的打分矩阵按位相乘,使用几何平均法得到唯一集成矩阵,计算集成矩阵的权重,为了检验每个层次各因素之间重要性的排序是否合理,需进行一致性检验,如果一致性比率小于 0.1,判断矩阵取得令人满意结果,否则重新进行要素赋值,计算公式为

$$C_R = C_I/R_I \tag{2}$$

其中

$$C_I = (\lambda_{\max} - k)/(k-1) \tag{3}$$

式中 C_R——一致性比率

C_I——一致性指标

R_I——随机一致性指标

$\lambda_{\max}$——最大特征值

k——判断矩阵阶数

$k=1$ 时,$R_I=0$;$k=2$ 时,$R_I=0$;$k=3$ 时,$R_I=0.58$;$k=4$ 时,$R_I=0.90$;$k=5$ 时,$R_I=1.12$;$k=6$ 时,$R_I=1.24$;$k=7$ 时,$R_I=1.36$;$k=8$ 时,$R_I=1.41$;$k=9$ 时,$R_I=1.46$。

本文基于专家以及现场加工人员共计 10 位的意见,按照评分刻度进行打分构造判断矩阵,目标层(A)→准则层(B)的集结判断矩阵及一致性检验见表 2;准则层(B)→指标层(C)的集结判断矩阵及一致性检验见表 3~5,根据计算结果可得判断矩阵一致性检验均成功通过。

1.2 评价体系确立及新鲜度得分公式构造

对以上指标及权重进行汇总,确定评价指标体系如表 6 所示。

层次总排序用来表示同一层次的所有元素对于

表 2　目标层对准则层的集结判断矩阵及一致性检验

Tab. 2　Judgment matrix of target layer and criterion layer and consistency test

	捕捞温度	加工温度	仓储温度	权重
捕捞温度	1	1	0.111	0.090 9
加工温度	1	1	0.111	0.090 9
仓储温度	9	9	1	0.818 2

表 3　捕捞温度合规性对指标层的集结判断矩阵及一致性检验

Tab. 3　Judgment matrix and consistency test of fishing temperature compliance on index layer

	低温船冻温度	原料库冷冻温度	权重
低温船冻温度	1	4.599	0.821 4
原料库冷冻温度	0.217	1	0.178 6
$C_I=0, C_R=0<0.1$，满足一致性检验			

表 4　加工温度合规性对指标层的集结判断矩阵及一致性检验

Tab. 4　Judgment matrix and consistency test of processing temperature compliance to index layer

	解冻温度	清洗水温	原料清洗水温	修整温度	摸刺温度	灯检温度	预冷温度	冷冻温度	挂冰衣水温	权重
解冻温度	1	0.5	1.314	0.917	0.189	0.152	0.166	0.182	0.128	0.026 3
清洗水温	2	1	1.822	1.240	0.224	0.165	0.195	0.217	0.135	0.035 3
原料清洗水温	0.760	0.548	1	0.480	0.206	0.166	0.152	0.156	0.138	0.023 2
修整温度	1.090	0.806	2.082	1	0.241	0.173	0.161	0.165	0.138	0.030 7
摸刺温度	5.266	4.453	4.853	4.141	1	0.408	0.596	0.661	0.217	0.104 1
灯检温度	6.554	6.058	6.023	5.775	2.449	1	0.685	0.729	0.273	0.150 7
预冷温度	6.023	5.121	6.554	6.218	1.676	1.458	1	0.749	0.517	0.167 4
冷冻温度	5.468	4.601	6.389	6.056	1.513	1.370	1.335	1	0.592	0.173 0
挂冰衣水温	7.752	7.357	7.195	7.241	4.589	3.660	1.933	1.689	1	0.289 2
$C_I=0.037, C_R=0.025\,63<0.1$，满足一致性检验										

表 5　仓储温度合规性对指标层的集结判断矩阵及一致性检验

Tab. 5　Judgment matrix and consistency test of storage temperature compliance on index layer

	入库冷藏温度	出库温度	权重
入库冷藏温度	1	3.028	0.751 7
出库温度	0.330	1	0.248 3
$C_I=0, C_R=0<0.1$，满足一致性检验			

表 6　远洋捕捞追溯产品新鲜度评价指标体系

Tab. 6　Evaluation index system of freshness of pelagic fishing traceability products

目标层	准则层	权重	指标层	权重
远洋捕捞追溯流程产品新鲜度评价	捕捞温度合规性	0.090 9	低温船冻温度	0.821 4
			原料库冷冻温度	0.178 6
	加工温度合规性	0.090 9	鱼体解冻温度	0.026 3
			清洗水温	0.035 3
			原料清洗水温	0.023 2
			鱼体修整温度	0.030 7
			鱼体摸刺温度	0.104 1
			鱼体灯检温度	0.150 7
			隧道冷冻机预冷温度	0.167 4
			隧道冷冻机冷冻温度	0.173 0
			挂冰衣水温	0.289 2
	仓储温度合规性	0.818 2	入库冷藏温度	0.751 7
			冷库出库温度	0.248 3

目标层的相对重要性，总排序权重是遍历顶层到底层权重进行的合成，所有影响远洋捕捞新鲜度评价的因素总排序见表 7。

表 7　层次总排序

Tab. 7　Hierarchical total sort result

权重类别	指标最终权重
低温船冻温度	0.074 665 26
原料库冷冻温度	0.016 234 74
解冻温度	0.002 390 67
清洗水温	0.003 208 77
原料清洗水温	0.002 108 88
修整温度	0.002 790 63
摸刺温度	0.009 462 69
灯检温度	0.013 698 63
加工预冷温度	0.015 216 66
冷冻温度	0.015 725 70
挂冰衣水温	0.026 288 28
入库冷藏温度	0.615 040 94
出库温度	0.203 159 06

在目标为三文鱼远洋捕捞追溯流程产品新鲜度评价时，令方案层包括捕捞温度合规性、加工温度合规性、仓储温度合规性，确定 13 个准则层指标的权重。产品新鲜度分数计算公式为

$$F=\sum_j W_jX_j+\sum_k W_kX_k+\sum_l W_lX_l \quad (4)$$

式中　F——产品新鲜度得分

W——各个环节指标权重，下标 j、k、l 分别表示捕捞、加工、仓储环节

X——各个环节指标得分，符合行业标准得分值为 100，否则为 0，下标 j、k、l 分别表示捕捞、加工、仓储环节

2 远洋捕捞追溯企业信誉评价模型

本文以区块链中的组织代表追溯环节,节点代表追溯企业,新鲜度可信追溯的实现需将新鲜度得分与 ECDSA、智能合约、信誉评价模型相结合。以捕捞企业 A 为例,A 根据层次分析法定义的新鲜度评价指标体系计算产品新鲜度得分,基于 ECDSA 实现的智能合约方法权限匹配算法,调用捕捞环节数据上传方法,以 SHA256(产品数据)为产品的链下唯一追溯键 key,将 key 与企业标识拼接,上传(标识 + key,"基本追溯数据哈希,温度追溯数据,新鲜度得分")键值对,下一环节的加工企业检验链上新鲜度得分计算正确性,基于信誉评价公式进行信誉评价。

2.1 信誉积分奖惩机制及信誉评价模型

为了保障新鲜度得分计算结果的正确性,避免数据失真,本研究针对链上新鲜度得分数据计算的准确性,通过奖励、偿还与惩罚机制进行信誉积分归属权的判定,实现对企业的信誉评价,评价结果分为失信和可信两种,失信企业被限制与区块链网络交互及调用智能合约。本研究将追溯节点划分为两类:涉及自身信誉积分加减的节点记为非中性节点,存在上传虚假数据和虚假校验的可能;未涉及自身信誉积分加减的情况记为中性节点,此类节点为诚信节点。奖励机制是某一企业检测到上一追溯环节的企业上传虚假数据。偿还机制是企业证实下一环节的企业未进行真实信誉评价或者被下一环节的企业证实诚信上传数据。惩罚机制亦具有两种行为:一是企业被下一环节的企业证实上传虚假数据,二是企业被上一环节的企业证实虚假信誉评价,核心准则是作恶行为一定要实现信誉积分的减少。每个企业的信誉积分初始值均记为 $Point_{initial}$,信誉积分转移值为 $Point_{transfer}$,产品作恶容忍度设为 $tolerance_{product}$,企业作恶容忍度设为 $tolerance_{enterprise}$,四者均由各企业确立一个统一值,后两者为百分比形式。如果某企业信誉积分值降低至初始积分的 $(1-tolerance_{enterprise})$,被智能合约剥夺参与追溯的权限,以加工环节企业检验捕捞环节企业为例,分别记为 B 与 A,A 向 B 转移一笔值为 $Point_{transfer}$ 的信誉积分。下一环节企业对上一环节企业进行信誉评价需要核算新鲜度得分 $Score_{bulao}$ 是否计算正确,具体算法定义为

$$Value = \sum_{i=1} Verify(t_i) + Calucate(score) \tag{5}$$

其中

$$Verify(t_i) = \begin{cases} 0 & (t_i < T_{\min} \text{或 } t_i > T_{\max}) \\ 1 & (t_i > T_{\min} \text{且 } t_i < T_{\max}) \end{cases} \tag{6}$$

$$Calucate(score) =$$

$$\begin{cases} 0 & \left(score_{blockchain} \neq AHP\left(\sum_{i=1}^{n} \lambda_i (T_{\min} < t_i < T_{\max} ? 1 : 0)\right)\right) \\ 1 & \left(score_{blockchain} = AHP\left(\sum_{i=1}^{n} \lambda_i (T_{\min} < t_i < T_{\max} ? 1 : 0)\right)\right) \end{cases} \tag{7}$$

式中 $Value$——信誉评价结果总分

$Verify$——温度数据合规性检验得分

$Calucate$——新鲜度得分真实性检验得分

t_i——上一环节企业写入链上的温度数据

$score$——当前环节企业基于层次分析法计算的新鲜度得分

$score_{blockchain}$——上一环节企业写入链上的新鲜度得分

AHP——链下扫码得到温度后,计算得到的新鲜度得分

λ_i——上一环节企业新鲜度指标层权重

$T_{\min}$——上一环节企业行规最低标准温度

$T_{\max}$——上一环节企业行规最高标准温度

如果两项检验均满分,该产品记录为诚信产品,否则记录为失信产品,企业可以此为依据拒绝接收失信产品。由于各环节企业上传的数据量差异较大,为保障公平以比值的形式决定信誉积分的归属。如果失信产品总数与产品总数的比值小于 $tolerance_{product}$,B 向 A 转回大小为 $Point_{transfer}$ 的信誉积分,否则将信誉积分扣押在自身账户中,具体过程如图 3 所示,图中存储各节点信誉积分账户数据的区块代表企业节点服务器,便于描述信誉评价流程。

针对评价结果,A 可质疑 B 有虚假信誉评价,骗取信誉积分的嫌疑,调用智能合约随机选举方法,选

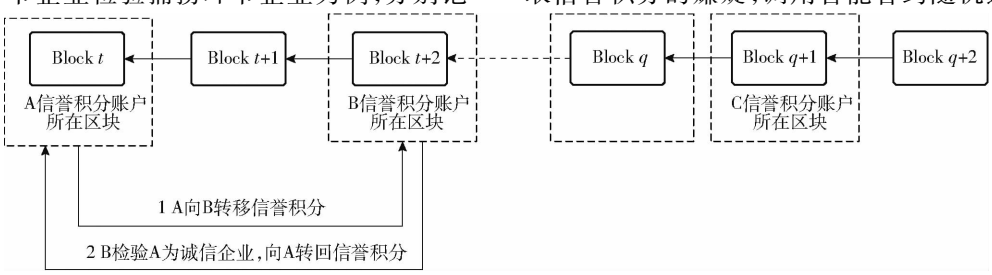

图 3 A 上传真实数据、B 诚实校验流程

Fig. 3 A uploaded real data and B verified it honestly

举除自身及 B 所在环节外的企业进行二次校验，假设仓储环节的企业，记为 C，由于 C 不涉及自身信誉积分的增减，本研究中认定为诚实校验节点。查询到自身为二次校验方后，C 向 B 请求失信产品数据，B 向 C 发送失信产品编号。C 进行校验后上传二次检验证明，如果二次检验的结果是 A 的失信产品与总产品数比值大于 $tolerance_{product}$，仍然判定 A 失信行为成立，A 需再向 B 转让大小为 $Point_{transfer}$ 的信誉积分，如图 4 所示。如果二次检验的结果是 A 失信产品与总产品数比值小于 $tolerance_{product}$，判定 B 虚假校验，B 向 A 转让大小为 $2Point_{transfer}$ 的信誉积分，如图 5 所示。

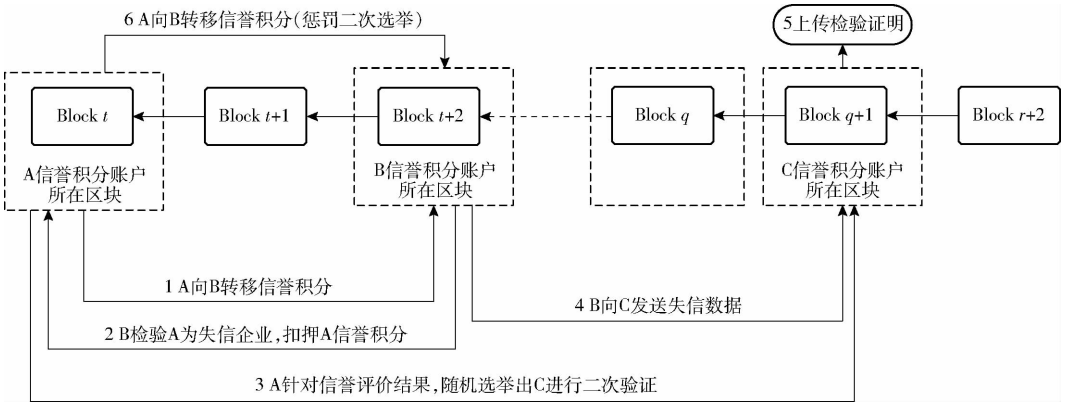

图 4　A 上传虚假数据、B 诚实校验流程

Fig. 4　A uploaded false data and B verified it honestly

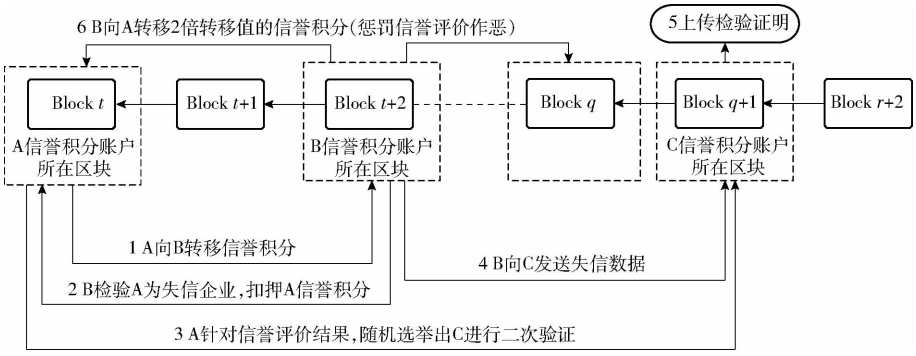

图 5　A 上传真实数据、B 虚假校验流程

Fig. 5　A uploaded real data and B verified false data

2.2　信誉评价真实性保障机制

为了保障高效的数据共享以及产业链的有效衔接，追溯模型采用单链的存储模式，相比多链的优点是全流程数据可验证，信誉积分转移高效便捷，缺点是丧失了多通道数据隔离的特性，同一智能合约中的方法对链上的所有组织、节点开放调用权限[27]，针对同一 key 键，Hyperledger Fabric 在世界状态数据库中仅维护键对应的最新值，后方环节企业在校验数据时如果恶意调用数据上传合约方法，修改 key 键对应的 value 值，篡改上一环节企业的世界状态数据，除非在区块链交易记录中遍历查询旧键值对，否则此类骗取信誉积分的作恶行为在二次校验中无法受到惩罚，而区块链遍历查询会引入较高的时间成本。椭圆曲线密码(Elliptic curve cryptography, ECC)的概念由文献[28]提出，椭圆曲线数字签名算法(ECDSA)是使用椭圆曲线密码(ECC)对数字签名算法(DSA)的模拟，于 2000 年成为 IEEE 和 NIST 标准，在一般群模型下已证明具备 EUF-CMA[29]安全性。本研究基于 ECDSA 签名算法保障了信誉评价的真实性，实现了精确到企业的追溯责任定位。在追溯数据上传、新鲜度得分更新的输入参数中输入当前企业 ECDSA 公钥、消息数据 message、对 message 的签名 r、对 message 的签名 s，其中 message 数据为 key 与 value 的拼接，智能合约方法被调用时需验证公钥是否能成功验证传入参数中私钥对不重复消息的签名，验证成功则为数据添加当前追溯环节的环节标识并上传数据，验证失败则证明调用方与合约方法不匹配，此机制严格锁定了合约方法的调用方。同时，本研究在信誉评价模型的智能合约中引入随机验证、信誉积分转让的方法。上一环节的企业如果质疑下一环节的企业存在骗取信誉积分的作恶行为，发起随机选举进行二次验证，下一环节企业的作恶行为可以被二次验证方成功验

证,保障了信誉积分数据的安全性与信誉评价的真实性,提升了信誉评价的积极性。

3 系统实现

3.1 远洋捕捞追溯环节及追溯数据

远洋捕捞各环节参与企业主体众多,全产业链涉及的关键环节主要有:捕捞、加工、仓储、销售 4 个环节,其中捕捞属于上游环节,加工与仓储属于中游环节,捕捞属于下游环节,本研究将追溯数据划分为两类,分别是基本追溯数据、温度追溯数据,引入了新鲜度得分与信誉积分数据,每个环节具体的追溯数据如表 8 所示。

表 8 远洋捕捞全流程追溯数据

Tab. 8 Whole process of pelagic fishing traceability data

追溯环节		基本追溯数据	温度追溯数据
捕捞	链上	MD5(捕捞环节基本追溯数据)	低温船冻温度、原料库冷冻温度、捕捞环节产品新鲜度得分
	链下	捕捞方式、捕捞海域、捕捞种类、捕捞尺寸、捕捞完整度、联系方式、捕捞日期、执照证明	低温船冻温度、原料库冷冻温度、捕捞环节产品新鲜度得分
加工	链上	MD5(加工环节基本追溯数据)	解冻温度、清洗水温、原料清洗水温、修整温度、摸刺温度、灯检温度、加工预冷温度、冷冻温度、挂冰衣水温、加工环节产品新鲜度得分
	链下	肉色、加工企业、加工数量、加工人信息、加工日期、检疫证明、消杀信息、产品保质期	解冻温度、清洗水温、原料清洗水温、修整温度、摸刺温度、灯检温度、加工预冷温度、冷冻温度、挂冰衣水温、加工环节产品新鲜度得分
仓储	链上	MD5(仓储环节基本追溯数据)	入库冷藏温度、出库温度、仓储环节产品新鲜度得分
	链下	保温库板、仓库人电话、检疫记录、存储数量、存储时长、保鲜方式	入库冷藏温度、出库温度、仓储环节产品新鲜度得分
销售	链上	MD5(销售环节基本追溯数据)	产品最终新鲜度得分
	链下	销售形式、进货价格、销售价格、保质期、生产日期	产品最终新鲜度得分

3.2 远洋捕捞产品追溯流程

远洋捕捞产品追溯流程如图 6 所示,智能合约首先初始化各环节企业的信誉积分账户、公共信誉积分账户。以捕捞企业 A 与加工企业 B 为例,A 将

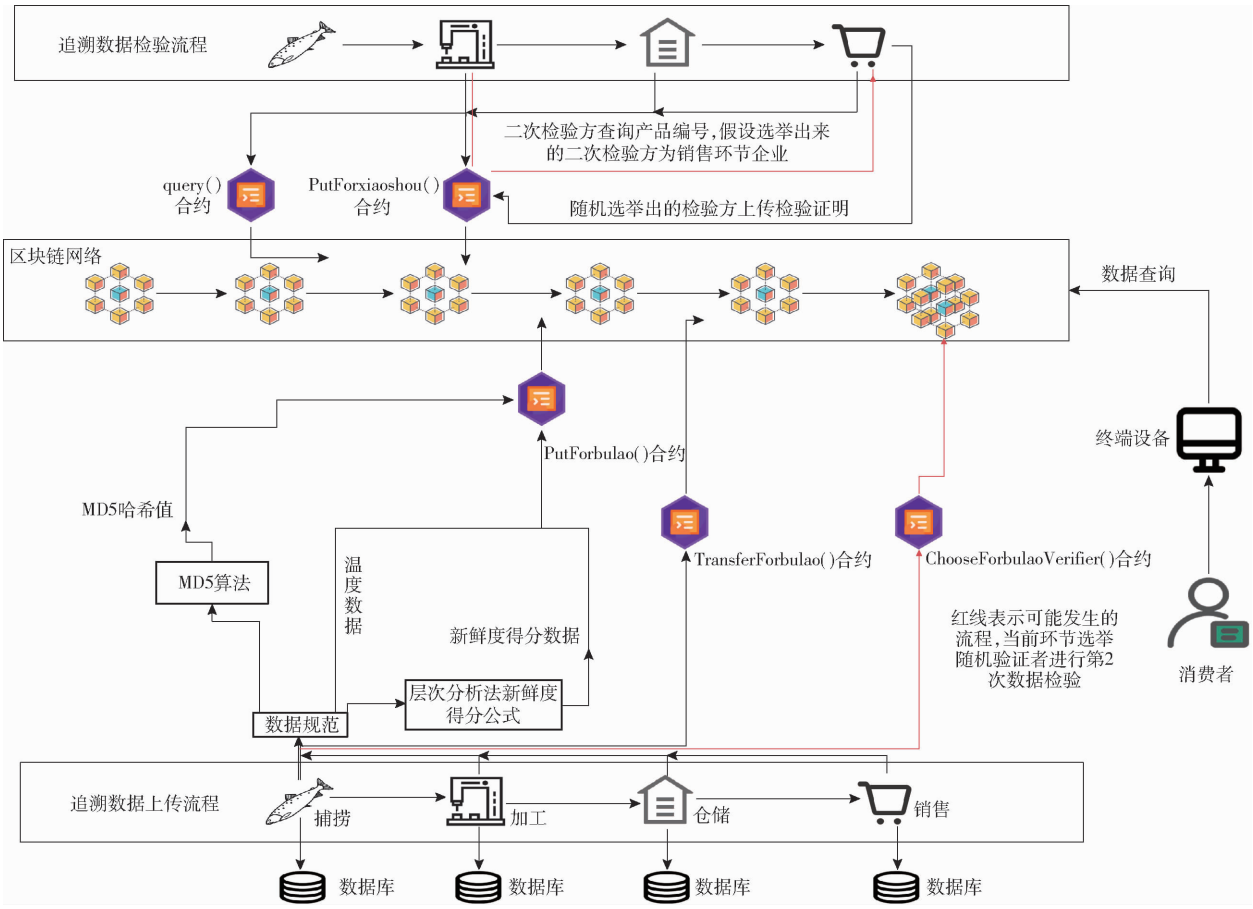

图 6 远洋捕捞新鲜度可信追溯流程

Fig. 6 Reliable traceability model for freshness of pelagic fishing

捕捞的三文鱼进行打码标记，记录基本溯源信息并对整鱼进行船冻处理。基于 MD5 算法处理基本溯源数据获得摘要值，使用传感器监测低温船冻温度、原料库冷冻温度等温度数据，基于层次分析法定义的新鲜度计算公式，计算新鲜度得分，调用捕捞企业数据上传方法将哈希值、温度数据、新鲜度得分上传至区块链网络，Hyperledger Fabric 通道的特性[30]保证了上链温度数据对于全追溯环节的可见性，实现了全流程的温度监督，后续流程的基本数据和温度数据处理方式与捕捞环节相同。成功上传数据后，A 调用捕捞企业信誉积分转移方法向 B 的信誉积分账户发起信誉积分转让交易，B 收到渔获物产品后，按照 2.2 节的信誉评价机制进行信誉评价，检验完成后上传评价结果。如果 A 认为 B 在数据校验时有作恶的可能，调用捕捞企业随机选举方法选择校验方进行信誉评价结果的二次校验，二次校验的企业向 B 请求检验失败的数据，上传二次校验结果，此轮结果同样触发信誉积分的奖惩机制。加工企业 B 在进行解冻、清洗、去头去脏、开片、修整、摸刺等操作后，向仓储环节的企业信誉积分账户、公共信誉积分账户发起信誉积分的转移交易，仓储企业负责三文鱼加工产品的保鲜贮藏，销售企业负责向消费者、企业等销售产品，后续两环节的数据处理、数据上传及信誉评价的过程与前两个环节相同。

本研究的智能合约分为数据上链、信誉积分、数据查询模块，具体定义如表 9 所示。

表 9　智能合约设计

Tab.9　Design of smart contract

合约模块	合约业务逻辑	合约方法	描述
数据上链	捕捞企业数据上链	PutForbulao( )	通过验签机制上传捕捞环节数据
	加工企业数据上链	PutForjiagong( )	通过验签机制上传加工环节数据
	仓储企业数据上链	PutForcangchu( )	通过验签机制上传仓储环节数据
	销售企业数据上链	PutForxiaoshou( )	通过验签机制上传销售环节数据
信誉积分	捕捞企业信誉积分转移	TransferForbulao( )	捕捞企业转让信誉积分
	加工企业信誉积分转移	TransferForjiagong( )	加工企业转让信誉积分
	仓储企业信誉积分转移	TransferForcangchu( )	仓储企业转让信誉积分
	销售企业信誉积分转移	TransferForxiaoshou( )	销售企业转让信誉积分
	捕捞企业随机选举	ChooseForbulaoVerifier( )	捕捞企业怀疑下一环节故意骗取信誉积分，随机选择自身及下一环节以外的企业进行验证
	加工企业随机选举	ChooseForjiagongVerifier( )	加工企业怀疑下一环节故意骗取信誉积分，随机选择自身及下一环节以外的企业进行验证
	仓储企业随机选举	ChooseForcangchuVerifier( )	仓储企业怀疑下一环节故意骗取信誉积分，随机选择自身及下一环节以外的企业进行验证
	销售企业随机选举	ChooseForxiaoshouVerifier( )	销售企业怀疑下一环节故意骗取信誉积分，随机选择自身及下一环节以外的企业进行验证
	选举方身份验证	CheckForVerifier( )	当前企业检验自身是否是二次验证者
数据查询	数据查询	query( )	根据链下追溯号查询对应的区块链数据

本文智能合约方法采用参数传入签名和方法内部验签的方式对合约方法的调用方进行调用权限匹配。调用方链下使用私钥对不重复消息签名，输入签名参数，由智能合约根据登记的组织公钥进行验签。验签通过权限匹配成功；否则匹配失败。权限匹配的算法（非单独合约方法）如下：

算法 1：合约方法调用权限匹配算法

Function ECDSA_check(public,msg,r,s)

Input：调用方公钥：public，签名消息：msg，签名 1：r，签名 2：s

Output：成功返回成功，失败返回失败原因

```
1  if public! = publickey then //公钥符合要求
2      key ← esdsa. Base64ToPublicKey ( public ) // base64 转化为可计算公钥
3      R←SetString(r, 10)  S←SetString(s, 10) //获取私钥的链下数字签名
4      flag←ecdsa. Verify(key, msg, R, S) //验证两个签名
5      if flag then //两个签名验证成功
6          return success // 签名验证成功证明具有调用合约方法权限
7      else return error  // 签名验证失败导致调用合约方法失败
8  else return error  //不允许使用已使用过的消息进行签名验证
9  else return error  //参数公钥不符合要求
```

3.3　数据上链模块

初始化方法上传各企业的企业公钥、信誉积分

账户、追溯环节号以及公共信誉积分账户,4 个企业及公共信誉积分账户名分别记为 bulao、jiagong、cangchu、xiaoshou、common,溯源组织名为 orgbulao、orgjiagong、orgcangchu、orgxiaoshou。

初始化数据后,4 个企业按照追溯流程顺序上传追溯数据。基于 ECDSA 实现的智能合约方法权限匹配机制,为每个溯源企业分别定义数据上传方法,在数据上链过程中为每个企业添加独特标识,定义 4 个标识分别为 one、two、three、four,以捕捞企业为例,执行流程如图 7 所示。

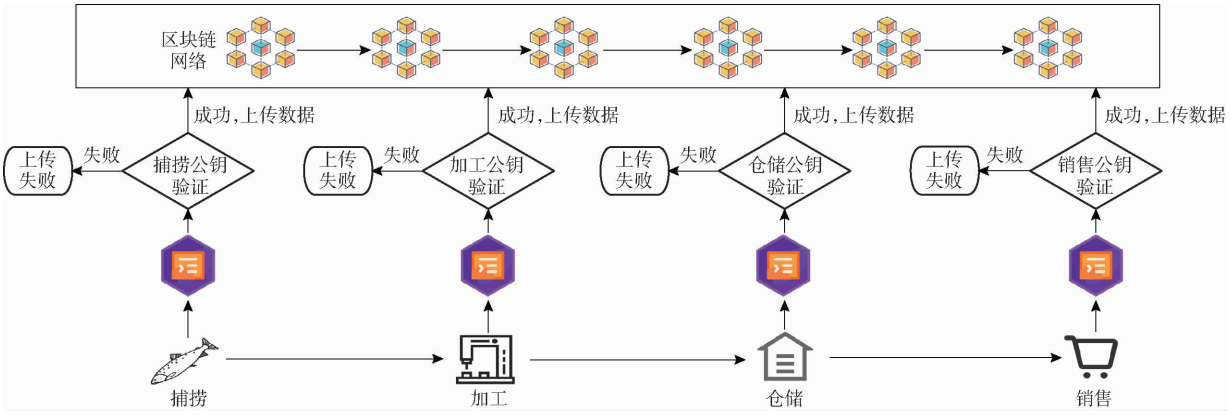

图 7 数据上传方法

Fig. 7 Data upload algorithm

追溯数据的上传算法如下:

算法 2:捕捞企业数据上传方法

Function PutForbulao (public1, msg, r, s, number, value)

Input:捕捞企业公钥:public1,签名消息:msg,签名 1:r,签名 2:s,链下追溯键:number,上链数据:value

Output:成功返回上传数据,失败返回失败原因

1 if msg = = key + value then // 避免了其余环节企业调用已使用过的签名修改世界状态键值对

2 if ECDSA_check (public1, msg, r, s) &&GetState ("bulao") > $tolerance_{enterprise}$ * $Point_{initial}$ then // 确保调用方信誉积分符合要求

3 key←"one" + number // 拼接环节标识与链下追溯键获取链上追溯键

4 PutState(key, [ ]byte(value)) // 上传追溯数据

5 return success // 追溯数据成功上传

6 return error // 未通过权限匹配算法

7 return error // 签名消息不正确

3.4 信誉积分转移及随机验证模块

3.4.1 信誉积分转移方法

每个企业在上传完成数据后,需向下一环节的企业和公共账户发起一笔信誉积分转移的交易,调用合约中的信誉积分转移方法。下一环节的企业基于定义的信誉评价模型进行评估,如果满足信誉积分偿还的条件,下一环节的企业发起一笔信誉积分偿还的交易,否则将积分保留在自己账户中,将检验结果写入链上。以捕捞企业为例,算法如下:

算法 3:捕捞企业信誉积分转移方法

Function TransferForbulao (public1, msg, r1, s1, account1, account2, value)

Input:捕捞企业公钥:public1,签名消息:msg,public1 签名 1:r1,public1 签名 2:s1,转出账户:account1,转入账户:account2,信誉积分转移值:value

Output:成功返回转移后的两账户余额,失败返回失败原因

1 if GetState (msg) = = null && account1 = = bulao then

2 flag←ECDSA_check (publici, msg, r, s) // 用算法 1 对签名进行验签

3 if flag&&GetState (account1) > $tolerance_{enterprise}$ * $Point_{initial}$ then

4 source←account1 target←account2 // 获取源账户及目标账户名称

5 sval←GetState (source) tval←GetState (target) //查询源账户及目标账户的积分余额

6 if sval > value&&value > 0 then // 判断当前余额是否足够及避免当前组织发起一笔负数转移

7 sval←sval-value tval←tval + value // 源账户与目标账户实现链上信誉积分转移

8 PutState (source, [ ]byte (sval)) // 修改后的源账户状态保存至账本

9 PutState (target, [ ]byte (tval)) // 修改后的目标账户状态保存至账本

10 PutState (message) // 保存已经使用过的 message 数据至账本

```
11        return success
12      return error   //当前账户不满足转移积分条件
13    return error //未通过权限匹配算法
14    return error   //签名消息与转出账户不正确
```

3.4.2 随机选举方法

在下一环节企业上传信誉评价结果后，当前企业可以接受，将信誉积分作为惩罚结果进行转让，也可以质疑，向下一环节企业请求签名，调用算法如下：

算法 4：捕捞企业随机选举方法

Function：ChooseForbulaoVerifier（key_for_public1，msg，r1，s1，key_for_public2，r2，s2，account，id_for_bulao）

Input：捕捞企业公钥存储键：key_for_public1，签名消息：msg，public1 签名 1：r1，public1 签名 2：s1，加工企业公钥存储键：key_for_public2，public2 签名 1：r2，public2 签名 2：s2，信誉积分账户：account，企业环节号：id_for_bulao

Output：成功返回上传数据，失败返回失败原因

```
1 if GetState（msg）= = null&&account = = bulao&&GetState（key _ for _ public1）= = public1&&GetState（key _ for _ public2）= = public2 then
2   for i = 1to 2 flagi←ECDSA_check（publici，msg，r，s）// 用算法 1 对所有签名进行验签
3       if flag1&&flag2&&GetState（account）> tolerance_enterprise * Point_initial then
4       id←GetState（id_for_bulao）// 获取发起选举企业的环节号，捕捞企业即为 1
5       time←tub. GetTxTimestamp（）// 为避免共识失败，获取交易时间戳
6       math_rand. Seed（time. Seconds）// 以交易时间戳作为伪随机数生成算法的种子
7       rand←math_rand. Intn（4）//尝试生成除了当前环节及下一环节的伪随机数
8       if rand ! = id% 4&&rand! = （id + 1）% 4 &&rand! =0 then // 选举成功的条件
9       choose：="捕捞企业的二次检验企业序号" PutState（choose，[]byte（rand））//如果选取到符合规定的随机数，选举成功，将选举出的企业序号写入链上
10      PutState（message）// 保存已经使用过的 message 数据至账本
11      return success
12  return error   //未选举出符合条件的随机数，需重新调用方法
13  return error   //签名未通过权限匹配算法
14  return error   //签名消息不正确
```

随机选取除当前企业及第 1 次检验的企业来对结果进行检验，第 2 次检验的企业将检验错误的数据发送给二次验证企业，二次验证企业进行二次检验并将结果写入链上。

4　系统分析及实验测试

本研究基于层次分析法构建了远洋捕捞产品新鲜度评价指标体系，实现了新鲜度定量分析，设计企业信誉评价机制保障了链上新鲜度数据的可信性，结合 ECDSA 与智能合约实现了追溯责任的精准定位，保障了信誉评价主体的积极性，构造了远洋捕捞产品新鲜度可信追溯模型。针对追溯模型进行测试与分析，智能合约使用 go 语言实现，测试环境为 Hyperledger Fabric 1.4，Ubuntu 20.04，Docker 20.10.21，系统包含 4 个组织，每个组织中包含 1 个节点，具体环境配置如表 10 所示。

表 10　区块链配置

Tab.10　Configuration of blockchain

设置	值	备注
共识机制	raft	允许网络不大于 1/2 的节点宕机，使用心跳机制触发 leader 选举
链数	1	单通道
组织数	4	捕捞组织、加工组织、仓储组织、销售组织
节点数	4	每个组织中包含一个节点
数据库	CouchDB	区块链使用 CouchDB 数据库存储链上数据
最大出块时间/s	2	最长打包生成区块间隔
区块最大交易数	100	区块能接受的最大交易数量
区块最大容量/MB	100	区块所能接受的最大容量

4.1　智能合约方法功能测试

本研究中的智能合约方法为权限匹配算法 + 功能方法的组合体，相比传统智能合约方法引入了权限匹配算法，保障了新鲜度数据的真实性与信誉评价的准确性，提升了信誉评价的积极性。本节以捕捞环节的企业为例，分别对合约中的数据写入方法、信誉积分转移方法、随机选举方法进行测试，所有方法输入参数均与第 3 节中相同，以 PutForbulao 方法为例展示输入参数。

捕捞企业获取产品，调用 PutForbulao 方法，上传产品追溯数据，测试输入如图 8 所示。

区块链浏览器执行结果如图 9 所示，在输入正确的公钥、消息、签名 r、签名 s 时，捕捞企业调用方法，在区块链与世界状态中成功写入（企业标识 + 追溯号，value）键值对，PutForbulao 方法测试成功。

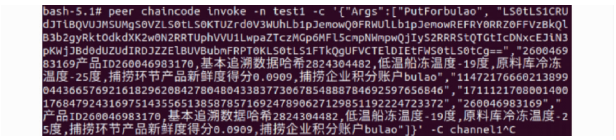

图 8 PutForbulao 方法输入参数

Fig. 8 PutForbulao method input parameters

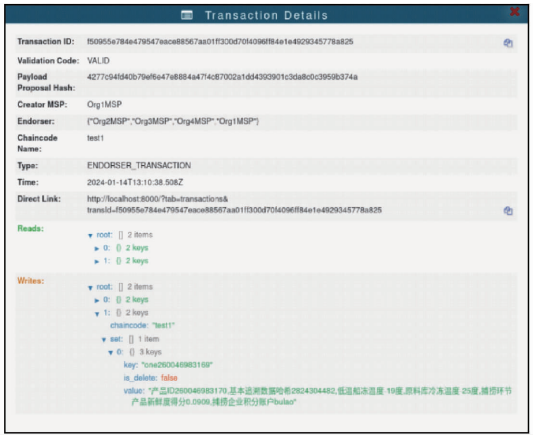

图 9 PutForbulao 方法执行结果

Fig. 9 PutForbulao method execution result

上传完成追溯数据后，捕捞企业调用 TransferForbulao 方法向加工企业转移信誉积分，信誉积分初始值与单次转移值由各企业确立统一值，本文假设初始值为 100，单次转移值为 20，执行结果如图 10 所示，捕捞企业成功向加工企业转移信誉积分，加工企业在收到产品后，按照 2.2 节中的机制对捕捞企业进行信誉评价。

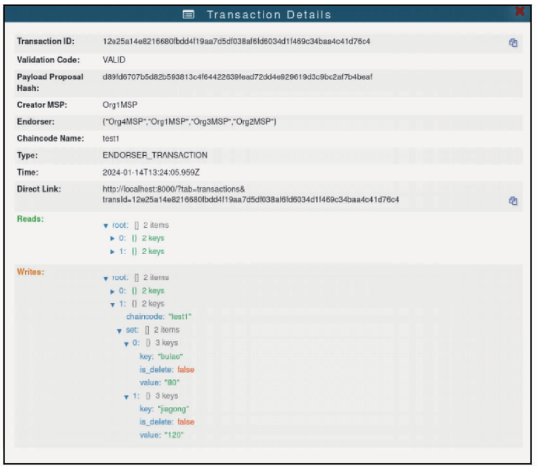

图 10 TransferForbulao 方法执行结果

Fig. 10 TransferForbulao method execution result

加工企业完成评价后，将检验结果写入链上，捕捞企业可以质疑检验结果，对加工企业进行反向信誉评价，捕捞企业准备用于签名的消息，向加工企业请求对该消息的签名，调用 ChooseForbulaoVerifier 方法随机选举二次检验企业，执行结果如图 11 所示，结果为选举出仓储企业，加工企业将失信产品数据发送给仓储企业，仓储企业进行二次校验。

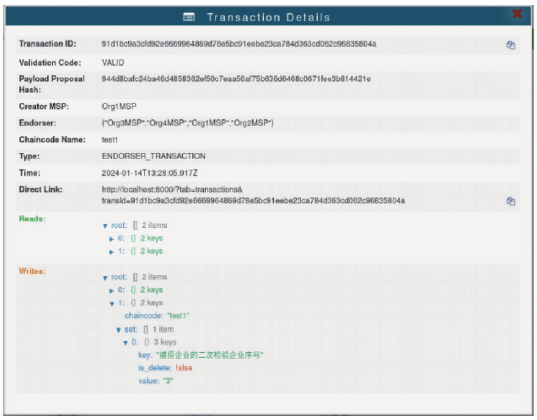

图 11 ChooseForbulaoVerifier 方法执行结果

Fig. 11 ChooseForbulaoVerifier method execution result

4.2 信誉评价模型安全性分析

本文构建了企业之间的信誉评价机制保障新鲜度数据的可信度，现对信誉评价模型进行安全性分析，以捕捞企业 A 为例，假设 A 上传数据 value，数据的链下追溯号为 key，message 消息为 key 数据与 value 数据的拼接，A 使用私钥 SK 对消息 message 进行签名，得到 R、S，签名计算如下：$[R, S = Sign(message, SK)]$。签名计算完成后，A 调用智能合约方法并使用方法传参中输入的公钥 PK 验证签名 R、S，验证成功则成功调用方法，验证方法如下：$[ECDSA.Verify(PK, message, R, S)]$。假设 A 企业上传的新鲜度数据计算存在错误，加工企业（记为 B）准确上传检验结果即可。假设计算正确，B 试图调用 A 的数据上传方法，篡改世界状态中的 value 为 value1，谎称计算结果错误来骗取信誉积分。此时 B 已知数据有 value、value1、PK、message、R、S。签名数据 R、S 只能实现 key 与 value 拼接数据的成功检验，相当于给予了 key 与 value 一个锁定关系，B 根据 PK、R、S 调用 A 的数据上传方法无法修改 key 对应的 value 值，需要获取 A 对于消息数据的签名，此时的数据篡改攻击转化为对私钥的攻击，攻击成功概率非常小，攻击者几乎不可能伪造有效签名，B 此时只能调用自身数据上传方法，环节标识的存在决定 B 无法修改 A 写入世界状态中的数据。

4.3 性能测试

基于 Hyperledger Caliper 框架进行性能测试，图 12、13 显示写、读吞吐量保持在 150、500 笔/s 以上。同样基于 Caliper 框架测试数据读写合约方法的执行成功率，图 14、15 显示写入方法的平均交易成功率保持在 98% 以上，查询方法的平均交易成功率稳定在 100%，可满足远洋捕捞追溯的效率要求。

基于 ECDSA 签名技术提出合约方法匹配算法，将追溯责任精确定位至企业节点，在此基础上设计了评价结果可靠、评价主体积极性高的信誉评价体

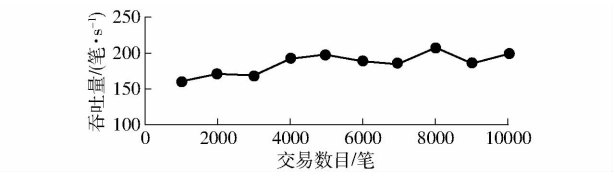

图 12　追溯数据写入性能测试

Fig. 12　Trace data write performance

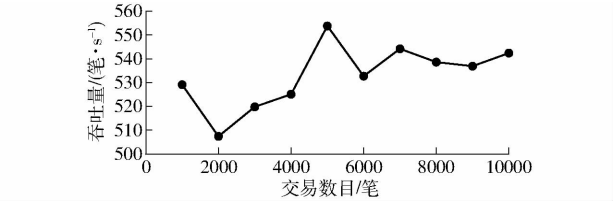

图 13　追溯数据查询性能测试

Fig. 13　Trace data query performance

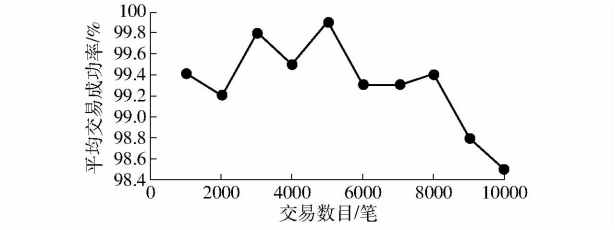

图 14　追溯数据写入成功率测试

Fig. 14　Trace data write success test

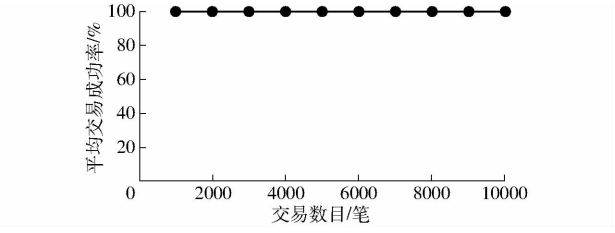

图 15　追溯数据查询成功率测试

Fig. 15　Trace data query success test

系，实现了区块链水产品可信追溯模型。文献[24]同样基于信誉评估机制鼓励节点上传真实数据，通过引入监管节点，结合星际文件系统与多链技术保障了评估结果的可信度。将文献[24]方案与本文方案分别记为方案 1 与方案 2，对两种方案的数据存储与数据查询性能进行对比，进行 1 000 次数据存储与数据查询测试，对比结果如图 16、17 所示。

结果显示，同为基于可靠企业信誉评估机制的区块链可信追溯模型，方案 1 数据平均写入时间为 0.941 s，数据平均查询时间为 0.388 s。本文方法在保证信誉评估结果可信度的同时，数据写入平均耗

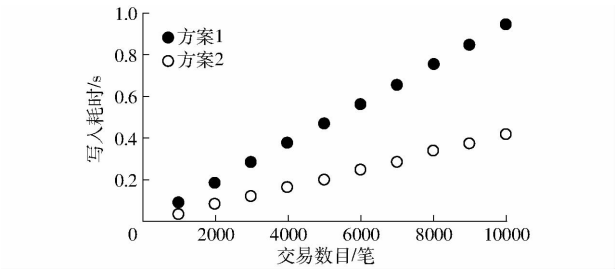

图 16　追溯数据写入效率对比

Fig. 16　Trace data write efficiency comparison

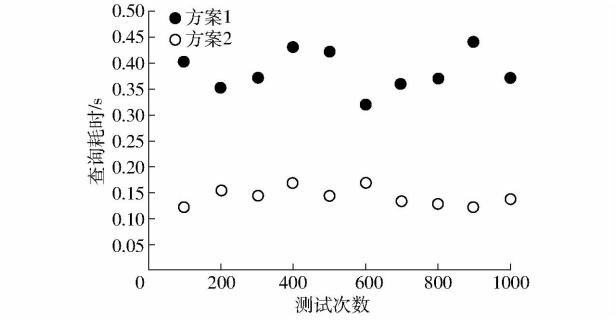

图 17　追溯数据查询效率对比

Fig. 17　Trace data query efficiency comparison

时为 0.416 s，数据查询平均耗时为 0.142 s，本文方案存储与查询效率分别提升 55.8% 与 63.4%，可较好满足追溯需求。

5　结论

(1)对远洋捕捞流程进行详细分析，划分追溯数据为基本追溯数据与温度追溯数据，基于层次分析法在温度追溯数据基础上建立了远洋捕捞新鲜度指标评价体系，提出新鲜度得分公式，实现了远洋捕捞产品新鲜度的定量分析。

(2)提出链上双向可转移信誉积分的概念，针对溯源流程中新鲜度得分数据真实性及数据校验行为构建了奖励、惩罚、补偿机制三位一体的信誉评价模型，结合 ECDSA 签名与智能合约，将追溯责任精确定位到具体企业，以交易时间戳为种子构造伪随机数生成器，实现了企业之间的双向信誉评价，保障了评价主体的积极性与信誉评价的真实性。性能测试结果显示，追溯数据读写吞吐量保持在 500 笔/s 与 150 笔/s 以上，读写成功率分别为 100% 与 98%，数据写入平均耗时为 0.416 s，数据查询平均耗时为 0.142 s，相比基于可靠企业信誉评估机制的区块链农产品可信追溯模型，存储与查询效率分别提升 55.8% 与 63.4%。可较好满足实际业务追溯需求。

参　考　文　献

[1]　乐家华，俞益坚. 世界远洋渔业发展现状、特点与趋势[J]. 上海海洋大学学报，2021，30(6)：1123－1131.
LE Jiahua，YU Yijian. The status quo，characteristics and trends of world pelagic fishery development[J]. Journal of Shanghai Ocean University，2021，30(6)：1123－1131.（in Chinese）

[2]　陈新军. 我国远洋渔业高质量发展的思考[J]. 上海海洋大学学报，2022，31(3)：605－611.

CHEN Xinjun. Reflections and suggestions on high-quality development of distant-water fisheries in China[J]. Journal of Shanghai Ocean University, 2022,31(3):605 - 611. (in Chinese)
[3] 卢昌彩. 我国渔获物可追溯绿色标签管理实践与探索[J]. 决策咨询,2019(3):48 - 50.
[4] RODRIGUEZ-SALVADOR B, DOPICO D C. Understanding the value of traceability of fishery products from a consumer perspective[J]. Food Control, 2020,112:107142.
[5] 殷泽生,戴振庭,周瑜,等. 基于鲜度指示剂的水产品新鲜度快速检测方法的研究进展[J]. 食品与发酵工业,2022,48(18):329 - 336.
YIN Zesheng, DAI Zhenting, ZHOU Yu, et al. Research progress of rapid freshness detection method of aquatic products based on freshness indicators[J]. Food and Fermentation Industries, 2022,48(18):329 - 336. (in Chinese)
[6] CUI H, KARIM N, JIANG F, et al. Assessment of quality deviation of pork and salmon due to temperature fluctuations during superchilling[J]. Journal of Zhejiang University—Science B(Biomedicine & Biotechnology),2022,23(7):578 - 603.
[7] ZHANG Y, TANG Y, ZHANG Y, et al. Impacts of the COVID - 19 pandemic on fish trade and the coping strategies: an initial assessment from China's perspective[J]. Marine Policy,2021,133:104748.
[8] FOX M, MITCHELL M, DEAN M, et al. The seafood supply chain from a fraudulent perspective[J]. Food Security,2018,10(4):939 - 963.
[9] DAI H N, ZHENG Z, ZHANG Y. Blockchain for internet of things: a survey[J]. IEEE Internet of Things Journal,2019,6(5): 8076 - 8094.
[10] 徐恪,凌思通,李琦,等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报,2021,44(1):55 - 83.
XU Ke, LING Sitong, LI Qi, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers,2021,44(1):55 - 83. (in Chinese)
[11] 曾诗钦,霍如,黄韬,等. 区块链技术研究综述:原理、进展与应用[J]. 通信学报,2020,41(1):134 - 151.
ZENG Shiqin, HUO Ru, HUANG Tao, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications,2020,41(1):134 - 151. (in Chinese)
[12] 李旭东,杨千河,姚竟发,等. 基于区块链的农产品溯源技术研究综述[J]. 江苏农业科学,2022,50(6):16 - 24.
LI Xudong, YANG Qianhe, YAO Jingfa, et al. Study on traceability technology of agricultural products based on blockchain[J]. Jiangsu Agricultural Sciences,2022,50(6):16 - 24. (in Chinese)
[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.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceabilty based on blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(1):1 - 13. (in Chinese)
[14] 刘双印,雷墨鸳兮,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, LEl Moyixi, XU Longqin, et al. Development of reliable traceabilty 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)
[15] 张斌,李大鹏,蒋锐,等. 面向区块链溯源的链下扩展存储方案[J]. 计算机与现代化,2022(10):106 - 112.
ZHANG Bin, LI Dapeng, JIANG Rui, et al. An off-chain extended storage scheme for blockchain traceability[J]. Computer and Modernization, 2022(10):106 - 112. (in Chinese)
[16] 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)
[17] 冯国富,胡俊辉,陈明. 基于区块链的水产品交易溯源系统研究与实现[J]. 渔业现代化,2022,49(1):44 - 51.
FENG Guofu, HU Junhui, CHEN Ming. Research and implementation of aquatic product transaction traceability system based on blockchain[J]. Fishery Modernization, 2022,49(1):44 - 51. (in Chinese)
[18] 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)
[19] 王文娟,张旭,陈明,等. 基于区块链的水产品撮合交易模型与系统实现[J]. 农业机械学报,2023,54(1):364 - 375.
WANG Wenjuan, ZHANG Xu, CHEN Ming, et al. Trading matching model and system implementation for aquatic products based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(1): 364 - 375. (in Chinese)
[20] MIRABELLI G, SOLINA V. Blockchain and agricultural supply chains traceability: research trends and future challenges[J]. Procedia Manufacturing, 2020, 42: 414 - 421.
[21] ATHANERE S, THAKUR R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing[J]. Journal of King Saud University—Computer and Information Sciences, 2022, 34(4): 1523 - 1534.
[22] HUANG C, WANG Z, CHEN H, et al. Repchain: a reputation-based secure, fast, and high incentive blockchain system via

sharding[J]. IEEE Internet of Things Journal, 2020,8(6):4291 – 4304.

[23] 玄世昌,汤浩,杨武.基于信誉积分的路况信息共享中共谋攻击节点检测方法[J].通信学报,2021,42(4): 158 – 168.
XUAN Shichang, TANG Hao, YANG Wu. Method for detecting collusion attack node in road condition information sharing based on reputation point[J]. Journal on Communications, 2021,42(4): 158 – 168. (in Chinese)

[24] 伍德伦,饶元,许磊,等.农产品区块链信息可信评估差异化共享模型设计与实现[J].农业工程学报,2022,38(11): 309 – 317.
WU Delun, RAO Yuan, XU Lei, et al. Design and implementation of the trusted evaluation and differentiated sharing model for agricultural block chain information[J]. Transactions of the CASE,2022,38(11):309 – 317. (in Chinese)

[25] 王红岩,刘钰洋,张晓伟,等.基于层次分析法的页岩气储层地质工程一体化甜点评价:以昭通页岩气示范区太阳页岩气田海坝地区 X 井区为例[J].地球科学,2023,48(1):92 – 109.
WANG Hongyan, LIU Yuyang, ZHANG Xiaowei, et al. Geology-engineering intergration shale gas sweetspot evaluation based on analyti hierarchy process:application to Zhaotong Shale Gas Demonstration Disrct,Tai Yang Shale Gas Field,Hai Ba Area,X wel region[J]. Earth Science, 2023,48(1):92 – 109. (in Chinese)

[26] YU Y J, YANG S P, LIN T, et al. Effect of cold chain logistic interruptions on lipid oxidation and volatile organic compounds of salmon (*Salmo salar*) and their correlations with water dynamics[J]. Frontiers in Nutrition, 2020, 7:155.

[27] 朱涛,姚翔,许玉壮,等.基于 Fabric 的跨境汇款追踪平台实现[J].信息安全学报,2018,3(3):50 – 61.
ZHU Tao, YAO Xiang, XU Yuzhuang, et al. Cross-broder remittance tracing platform based on Fabric[J]. Journal of Cyber Security, 2018,3(3):50 – 61. (in Chinese)

[28] 颜萌,马昌社.高效的两方 ECDSA 门限方案[J].华南师范大学学报(自然科学版),2022,54(4):121 – 128.
YAN Meng, MA Changshe. An efficient threshold scheme for two-party ECDSA[J]. Journal of South China Normal University (Natural Science Edition), 2022,54(4):121 – 128. (in Chinese)

[29] 严都力,禹勇,李艳楠,等.ECDSA 签名方案的颠覆攻击与改进[J].软件学报,2023,34(6):2892 – 2905.
YAN Duli, YU Yong, LI Yannan, et al. Subversion attack and improvement of ECDSA signature scheme[J]. Journal of Software,2023,34(6):2892 – 2905. (in Chinese)

[30] 孟吴同, 张大伟. Hyperledger Fabric 共识机制优化方案[J]. 自动化学报, 2021, 47(8): 1885 – 1898.
MENG Wutong, ZHANG Dawei, Optimization scheme for Hyperledger Fabric consensus mechanism[J]. Acta Automatica Sinica,2021, 47(8): 1885 – 1898. (in Chinese)

(上接第 390 页)

[29] HE Tiantian, YUN Fei, LIU Tian, et al. Differentiated mechanisms of biochar- and straw-induced greenhouse gas emissions in tobacco fields[J]. Applied Soil Ecology,2021,166:103996.

[30] HUANG Rong, WANG Yingyan, GAO Xuesong, et al. Nitrous oxide emission and the related denitrifier community: a short-term response to organic manure substituting chemical fertilizer[J]. Ecotoxicology and Environmental Safety, 2020, 192: 110291.

[31] DUAN Ran, LONG Xien, FENG Yue, et al. Effects of different fertilizer application methods on the community of nitrifiers and denitrifiers in a paddy soil[J]. Journal of Soils and Sediments,2018,18:24 – 38.

[32] 王梦洁,蒋文婷,徐有祥,等.长期生物炭添加对稻田土壤细菌和真菌反硝化 N_2O 排放的影响[J/OL].环境科学:1 – 13[2023 – 12 – 19]. https://doi.org/10.13227/j.hjkx.202309176.
WANG Mengjie, JIANG Wenting, XU Youxiang, et al. Effects of long-term biochar addition on N_2O emission from bacterial and fungal denitrification in paddy soil[J/OL]. Environmental Science:1 – 13[2023 – 12 – 19]. https://doi.org/10.13227/j.hjkx.202309176. (in Chinese)

[33] 秦子元,张忠学,孙迪,等.水氮耦合对黑土稻作产量与氮素吸收利用的影响[J].农业机械学报,2021,52(12):324 – 335,357.
QIN Ziyuan, ZHANG Zhongxue, SUN Di, et al. Effects of water and nitrogen coupling on rice yield and nitrogen absorption and utilization in black soil[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021,52(12):324 – 335, 357. (in Chinese)

[34] ZHANG M, LI B, XIONG Z Q. Effects of organic fertilizer on net global warming potential under an intensively managed vegetable field in southeastern China: a three-year field study[J]. Atmospheric Environment,2016,145:92 – 103.

[35] 魏甲彬,成小琳,周玲红,等.冬季施用鸡粪和生物炭对南方稻田土壤 CO_2 与 CH_4 排放的影响[J].中国生态农业学报(中英文),2017,25(12):1742 – 1751.
WEI Jiabin, CHENG Xiaolin, ZHOU Linghong, et al. Effects of chicken manure and biochar on CO_2 and CH_4 emission in paddy fields in South China[J]. Chinese Journal of Eco-Agriculture, 2017,25(12): 1742 – 1751. (in Chinese)