doi:10.6041/j.issn.1000-1298.2024.01.034

基于区块链的三文鱼冷链多链协同监管模型研究

孙传恒[1,2]　杨晓虎[1,2]　罗　娜[2,3]　陈　枫[2,3]　徐大明[2,3]　邢　斌[2,3]

(1. 天津农学院计算机与信息工程学院, 天津 300384; 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: 在冷链行业集群式发展的背景下,为解决在三文鱼冷链多链协同过程中由于监管数据持续性与碎片化所带来的跨链签名数据传输且真实性验证效率缓慢的问题,设计了基于区块链的三文鱼冷链多链协同监管模型,该模型包括基于聚合签名算法的数据验证与冷链模式监管的方法,该方法在提升跨链监管数据真实性验证效率的同时保证了三文鱼冷链监管的细粒度与完整性。最后,基于以太坊平台实现了三文鱼冷链多链协同监管模型的原型系统。经系统性能测试,在监管性能方面,多链架构监管性能相较于单链架构平均提高 17.98%,且随着区块链交易增多,多链架构监管性能优势将更加明显;在真实性验证效率方面,根据验证时间曲线的趋势线斜率分析,传统验证算法的斜率为 57.448,而聚合签名算法的斜率为 0.553。这表明随着签名数量的增加,聚合签名算法在验证效率方面具有明显的优势;在通信消耗方面,传统签名算法所需要的签名通信量在理论极限值下最多可达到 4 875 B,而聚合签名算法所需的签名通信量即使在未压缩的情况下也一直保持在 96 B。测试结果表明,在三文鱼冷链场景中,聚合签名与验证的方法在数据批量传输批量验证的条件下具有良好的效率优势,为可信冷链监管、集群式冷链发展提供借鉴与参考。

关键词: 三文鱼冷链; 冷链监管; 多链; 跨链; 聚合签名

中图分类号: TP309.2; TS201.6　　**文献标识码**: A　　**文章编号**: 1000-1298(2024)01-0360-11　　**OSID**:

Blockchain Based Salmon Cold Chain Multi-chain Collaborative Supervision Model

SUN Chuanheng[1,2]　YANG Xiaohu[1,2]　LUO Na[2,3]　CHEN Feng[2,3]　XU Daming[2,3]　XING Bin[2,3]

(1. *College of Computer and Information Engineering, Tianjin Agricultural University, Tianjin* 300384, *China*
2. *National Engineering Research Center for Information Technology in Agriculture, Beijing* 100097, *China*
3. *National Engineering Laboratory for Agri-product Quality Traceability, Beijing* 100097, *China*)

Abstract: In the context of the cluster development in the cold chain industry, the challenge of cross-chain signature data transmission and slow verification efficiency caused by the continuity and fragmentation of regulatory data in the collaborative process of salmon cold chain management was addressed. To tackle this issue, a blockchain-based multi-chain collaborative regulatory model for salmon cold chain management was proposed. The model incorporated a data verification and cold chain pattern monitoring method based on the aggregate signature algorithm, which ensured both the authenticity and integrity of salmon cold chain management while enhancing the efficiency of cross-chain regulatory data verification. Furthermore, a prototype system of the multi-chain collaborative regulatory model for salmon cold chain management on the Ethereum platform was implemented. Performance testing of the system revealed that the multi-chain architecture showed an average improvement of 17.98% in regulatory performance compared with the single-chain architecture, with the advantage becoming more pronounced as the number of blockchain transactions were increased. In terms of verification efficiency, the slope analysis of the verification time curve indicated that the aggregate signature algorithm had a significant advantage with a slope of 0.553, as opposed to the traditional verification algorithm with a slope of 57.448. This demonstrated that the aggregate signature algorithm exhibited remarkable efficiency

收稿日期: 2023-06-27　修回日期: 2023-08-07

基金项目: 国家重点研发计划项目(2022YFD2001804-2)和江苏省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: 邢斌(1983—),男,副研究员,主要从事农业信息化技术研究,E-mail: xingb@nercita.org.cn

advantages as the number of signatures were increased. Regarding communication overhead, the traditional signature algorithm required a maximum signature communication of up to 4 875 B under theoretical limits, while the aggregate signature algorithm consistently maintained a signature communication of 96 B, even without compression. The test results showed that the aggregate signature and verification method exhibited significant efficiency advantages in the batch data transmission and verification of the salmon cold chain scenario, providing valuable insights and references for trustworthy cold chain management and the development of cluster-based cold chains.

Key words: salmon cold chain; cold chain supervision; multi-chain; cross-chain; aggregate signature

0　引言

随着大众消费水平的提高以及饮食结构的优化,三文鱼由于含有丰富的营养物质而受到消费者的青睐,需求也在逐年上升[1-2]。但由于三文鱼本身的生理特性以及缺乏对三文鱼冷链物流环境有效的监管,市场上三文鱼质量参差不齐,严重影响企业以及消费者的利益[3-4]。根据 2019 年上海市生食三文鱼微生物抽检结果显示,抽样的 159 份样本中菌落总数与大肠菌群合格率均为 74.8%[5],冷链温湿度环境监管的缺乏是造成微生物繁殖的主要原因。因此,如何通过技术手段保证三文鱼冷链全流程的感知信息实时监控和产品信息可靠监管是目前三文鱼冷链亟待解决的问题[6]。

传统的三文鱼冷链信息化监管主要采取企业内部中心化的存储策略,该策略会导致冷链企业节点之间数据分散、中心化程度高、数据不透明以及可追溯性差等问题[7-8]。利用区块链技术去中心化、不可篡改、链式存储的特性[9-10],可以实现冷链实时性、全过程、透明化的数据监管[11-12],为实现三文鱼冷链物流以及环境信息可靠追溯提供良好的技术支持。因此,国内外学者从不同的角度探究区块链技术在冷链环境监控领域的应用。文献[13-16]采用了单链架构来构建追溯模型,但由于区块链数据永久保存且不可删除的特性,导致单链存储体量随着时间的推移逐渐增大,从而使得系统的查询性能变差,影响用户体验[17]。由此可见,单链模式只适用于节点数量较少、上链数据数量有限的应用场景,难以适用于冷链行业企业数量繁多、关联广泛的集群式供应链[18]。在实现集群式供应链区块链追溯时,多链式的区块链架构因其在扩展性、隔离性、高性能方面的良好表现而得到研究以及应用。文献[19-20]提出的主从多链架构将供应链各环节按链划分,保证了各环节节点之间数据的隐私性,并在一定程度通过多链技术来缓解存储性能的问题[21-23]。但是,区块链间的隔离机制使得节点需要对多链的共有的基础数据进行链下单独上传,由于缺乏链间的协同性,上传的信息会被篡改或者上传了错误的信息,从而导致跨链协同难、追溯信息易断链的问题[24-25]。

因此,将跨链技术应用到多链架构是解决链间协同的关键。同时,如何保证跨链传输过程中数据的真实性是跨链技术发展的难点之一[26]。文献[27]提出的集群式农产品供应链追溯模型通过中继技术连接各个环节的子链,并通过中继链对区块背书进行检验,以此来保证数据的真实性与有效性;文献[28-29]提出的跨链模型中,通过验证由跨链路由组成的跨链网络进行传输的区块签名信息,以此来跨链验证区块数据的真实性。上述方案中,利用的跨链数据真实性验证技术往往需要对区块背书或交易签名进行逐一验证之后才可证明数据的真实性。其次,在真实的冷链环境监测当中,数据的产生具有一定的持续性与碎片性[30],并且每一次上传的数据都将由负责上传的节点进行签名,如果利用上述基于背书或者签名验证的策略进行应用,往往会导致跨链传输过程中签名数据体积过大、且大量的签名数据验证过程缓慢的问题。

针对以上问题,本文提出基于区块链的三文鱼冷链多链协同监管模型。通过多链架构缓解区块链在冷链行业应用过程中产生海量数据所带来的存储性能问题与隐私数据隔离问题。并将 BLS(Boneh-Lynn-Shacham)聚合签名算法应用于多链协同中数据的真实性验证,在保证跨链数据安全性与完整性的前提下,提高跨链效率。

1　模型构建

1.1　三文鱼冷链多链协同监管模型

1.1.1　三文鱼冷链多链协同架构

在当前市场规模庞大、流通广泛的背景下,三文鱼冷链供应链呈现集群化发展。为了实现有效管理,可以将冷链环节划分为养殖链、运输链、仓储链和销售链 4 个类别的从链。每个类别的从链由不同企业的私链组成,私链用于存储各企业的监管信息和其他内部数据。主链作为监管链,负责存储从链通过跨链传输而接收的监管数据。企业的从链可以通过向监管链注册获得上传监管数据的权

限,从而融入到大规模流通背景下的冷链全流程监管中。

因此,本文提出了一种主从多链协同模型,旨在实现 4 条不同环节的企业从链与 1 条主链之间的高效通信(如图 1 所示)。该模型的架构包括主链、从链、锚定节点、感知节点和通信服务 5 个组件。主链可部署云端并作为监管链存储三文鱼的冷链监管信息。政府监管机构和消费者可以通过扫描包装二维码,并根据用户权限(政府监管权限或消费者监管权限)查询相应的三文鱼冷链监管信息。从链是企业链,存储企业内部数据,并通过锚定节点与主链进行通信。企业可通过向主链注册锚定节点来获取通信权限。锚定节点是从链与主链相互锚定的节点,承担信息的提取、BLS 签名的聚合、消息的传递以及 BLS 聚合签名的验证等功能。感知节点与从链绑定,负责将数据上传至从链。通信服务由远程过程调用(Remote procedure call,RPC)服务、非对称加密算法、通用跨链传输格式(Cross-chain information format,CTF)和网络通信服务组成,实现数据的提取、加密和传输功能。CTF 如表 1 所示。

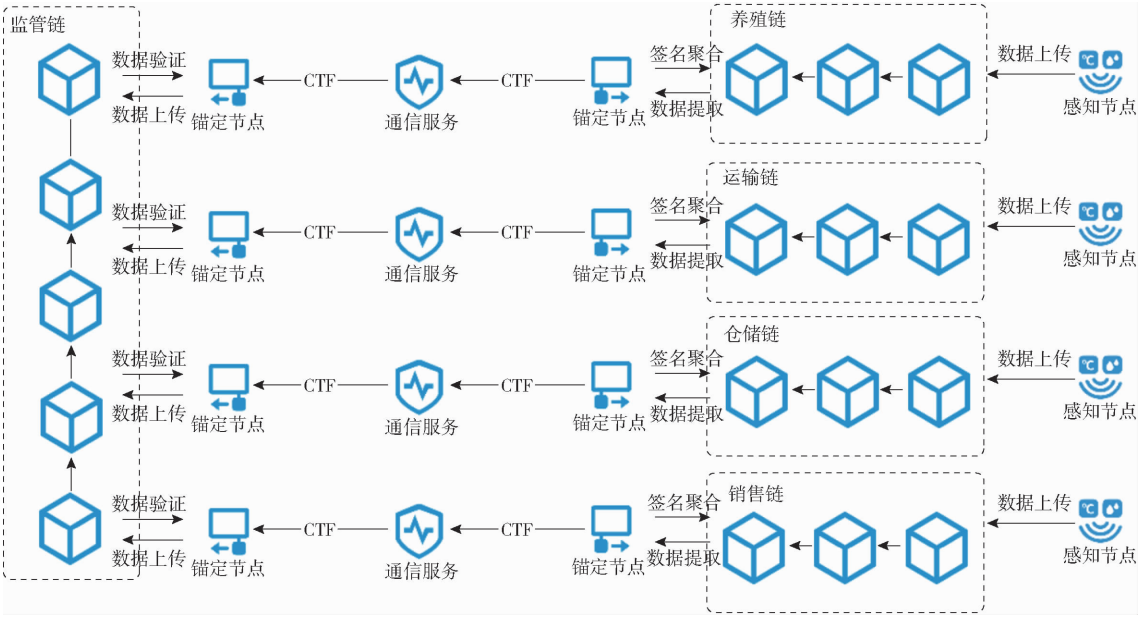

图 1 三文鱼冷链多链协同监管模型

Fig. 1 Multi-chain collaborative supervision model for salmon cold chain

表 1 跨链传输格式

Tab. 1 Cross-chain information format

消息字段		字段说明
From		发送链 ID
To		接收链 ID
Message	SCaddress	合约地址
	TraceNum	监管编号
	PubKey	节点公钥
	MulSign	聚合签名
	Proof	默克尔证明
	CargoName	货物名称
	Data	监管数据
Extra		其他信息

多链协同架构利用了区块链链间数据隔离的特性,使企业间的数据相互隔离,在保证了企业内部数据隐私性的同时,缓解了传统单链存储所带来的存储性能上的问题。最后,通过跨链 BLS 聚合签名验证技术,保证主从链之间监管信息的真实性与一致性。

1.1.2 三文鱼冷链监管模型

在实际的三文鱼冷链物流过程中,经常会遇到冷链企业产品监管标准缺乏和产品标签不统一,从而导致监管缺失和数据断链的发生。因此,本文设计了一种三文鱼数据绑定与模式监管的方法。如图 2 所示,以运输企业为例,企业工作人员首先在链上创建订单并录入基本信息,例如订单号、批次号、数量和运输车辆编号等。然后,企业物流人员通过扫描三文鱼包装上的二维码获取监管编号,并与链上企业订单和车辆感知设备相互绑定。一旦绑定完成,该批次三文鱼将根据订单需求自动匹配对应的合约监管模式,并在运输过程中按照相应的监管规则进行监管预警。所产生的监管数据将根据绑定信息在企业私链进行上链,进而由锚定节点自动上传至监管链。最后,当消费者或政府监管机构想要对该产品进行监管时,可通过监管链内置的访问控制合约进行权限认证,并根据权限读取相应的监管数据。监管权限表如表 2 所示。通过该方法,可以进一步提高监管的精细化程度,从而提升冷链监管的可信度和监管效果。

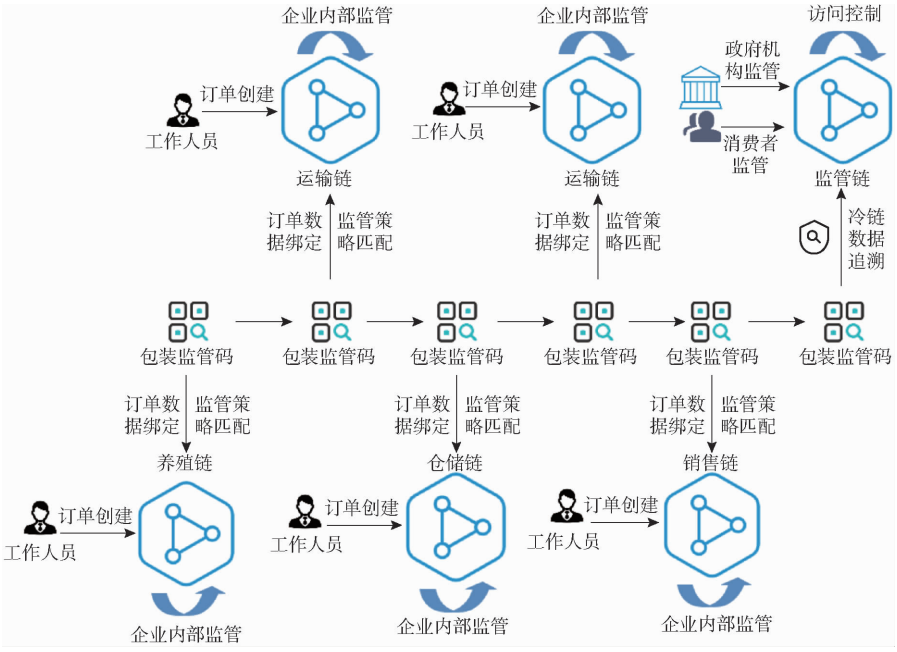

图 2　数据绑定与模式监管方法

Fig. 2　Method of data binding and pattern supervision

表 2　监管权限

Tab. 2　Regulatory authority

权限等级	可访问数据
政府监管机构权限	企业资质信息、运输许可信息、卫生合格证明、三文鱼检疫信息、微生物检测信息、重金属检测信息、溯源编号、批次号、温湿度数据、定位数据、产地信息、捕捞时间、运输时长、物流信息、销售时间、出库时间、入库时间、存储时长
消费者权限	溯源编号、批次号、物流信息、温湿度信息、产地信息、捕捞时间、检测状态

1.2　三文鱼冷链多链协同流程

本文以监管链与运输链之间跨链流程为例。在运输链的某运输订单中，感知节点会对每一次上传的数据进行签名，以此来保证数据上链的真实性。当运输链保存感知数据的区块上链之后，会自动触发的跨链传输机制，向监管链进行监管数据同步。在数据的完整性方面，本文通过提取区块交易树并生成 Merkle 证明来保证。整个跨链的流程总共分为 6 个阶段：注册阶段、感知阶段、存证阶段、传输阶段、验证阶段、链上存储阶段。跨链流程图如图 3 所示。

1.2.1　注册阶段

为了实现跨链传输的可控性与安全性，企业的通信服务在接入监管链之前都要进行通信身份信息的注册，只有经过监管链通信信息认证的节点才会获取监管数据上传的权限，注册信息如表 3 所示。通信信息由注册节点进行密码学加密，在跨链传输过程中进行解密并进行验证，因此只能由认证过的企业节点进行访问，且一旦进入通信控制列表之后便不能再进行更改。

1.2.2　感知阶段

区块链技术可以上传并永久存储可信和防篡改的感知信息。三文鱼运输从链除了锚定节点之外还包括负责数据实时上传的感知节点，感知节点收集的感知数据包括 RFID（Radio frequency identification）数据、二维码数据等基础服务数据与温湿度传感数据、北斗定位数据等监管数据。在监管数据上传之前，物流人员会通过链下扫描二维码获取基础信息（例如：批次号、产品编号、传感器编号等），并利用这些信息进行链上三文鱼运输订单绑定，绑定之后，感知节点将自动采集感知数据并进行下一步操作。

监管数据在上链之前需要在内存池满足一定的数量条件之后才可打包成块进行上链。因此，本文把区块监管数据记为集合

$$A_m \in \{m_1, m_2, \cdots, m_n, \cdots, m_N\}$$

其中，$1 \leqslant n \leqslant N$，$N$ 为单区块监管数据上传数量上限值。

在上链过程中，感知节点需要对数据进行 3 个阶段的处理，分别为初始化、预处理与签名。

（1）初始化：根据 BLS 聚合签名算法初始化一个质数阶双线性群，其中，双线性映射规则 $e: G_1 \times G_2 \rightarrow G_T$（$G_1$、$G_2$、$G_T$ 是阶为大素数 p 的乘法循环群）。并输出与曲线参数相关的密钥对 (P, p_k)，其中私钥 p_k 为曲线上的一个大整数，公钥

$$P = p_k g \tag{1}$$

其中，g 为 G_2 一个生成元。

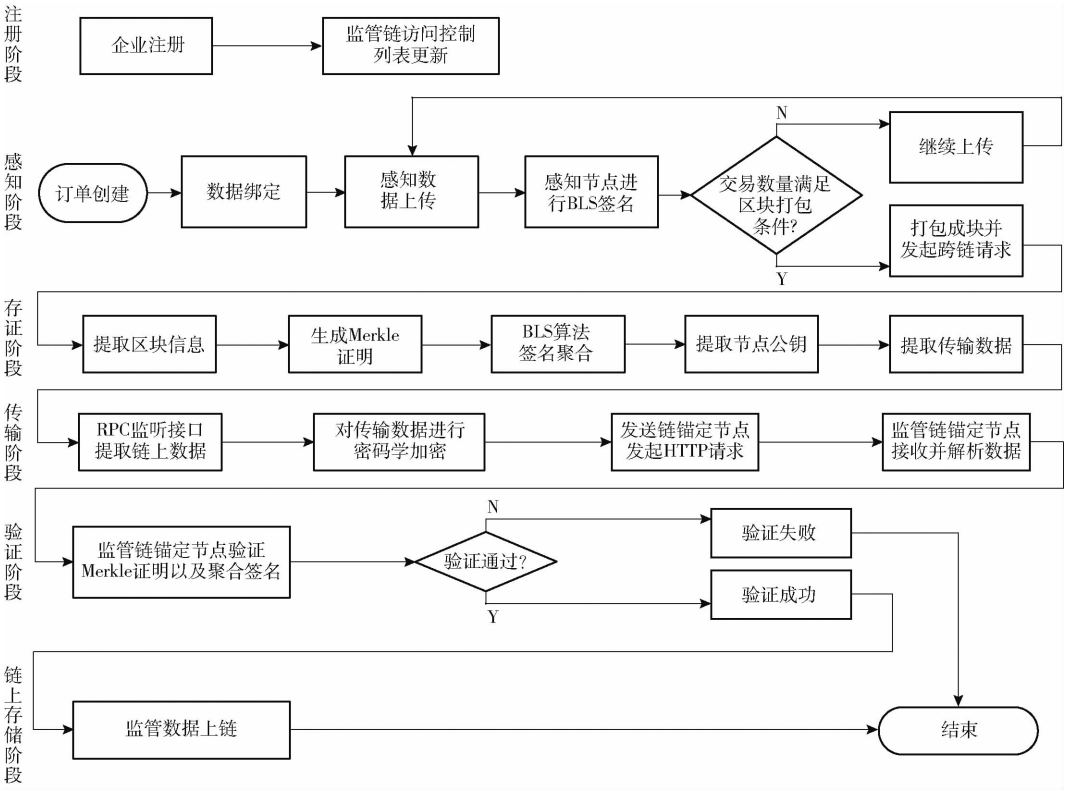

图 3 主从多链架构跨链流程图

Fig. 3 Cross chain flowchart of master-slave multi-chain model

表 3 通信控制列表

Tab. 3 Access information list

字段名称	字段说明
ChainType	链类型
ChainID	链 ID
IP	IP 地址
Port	端口号
MainAnchPeer	主链锚定节点地址
SubAnchAddress	从链锚定节点地址
Pk	通信服务公钥
Extra	其他

(2)预处理:选择曲线哈希算法 $H(m)$,该算法可将消息 m 映射为 G_1 上的点。然后根据该算法计算 n 条监管数据 m 的曲线哈希集合

$$A_H \in \{H(m_1), H(m_2), \cdots, H(m_n)\}$$

(3)签名:根据计算的哈希和私钥生成监管数据对应曲线哈希的签名,即

$$S_n = p_k H(m_n) \quad (S_n \in G_1) \tag{2}$$

根据上述运算生成签名集:$A_s \in \{S_1, S_2, \cdots, S_n\}$。

最后将签名集 A_s、监管数据集 A_m 以及其他区块基础数据打包成块并进行上链。

1.2.3 存证阶段

当监管数据区块上链成功,运输链锚定节点将自动触发跨链传输机制主动向监管链同步监管信息。存证阶段主要由运输从链发起,在运输从链跨链事件被触发之后发起。首先,节点提取区块中与感知数据相关的交易并根据哈希值生成 Merkle Proof,然后提取交易签名 S_r 并利用聚合签名算法对签名进行聚合,即

$$S = \sum_{r=1}^{n} S_r \tag{3}$$

其中,S 为聚合后的签名。若聚合成功,跨链合约将自动生成跨链存证并加入存证索引列表。验证索引列表如表 4 所示。

表 4 存证索引列表

Tab. 4 Inventory index list

消息字段	字段说明
SCAddress	订单合约地址
Index	跨链事件索引
BlockID	跨链区块号集
Mulsign	聚合签名
MerkleProof	默克尔证明

1.2.4 传输阶段

传输阶段主要由通信服务发起。通信服务首先通过 RPC 端口建立与区块链端口的连接,然后在链上访问控制列表合约中获取读取权限,紧接着跨链合约将生成的 CTF 信息通过 RPC 服务传送至超文本传输协议(Hyper text transfer protocol, HTTP)服务。运输链锚定节点的 HTTP Client 会将附带 CTF 信息的请求 Q_m 进行密码学加密与签名。最后,根据

预先设定好的路由信息进行通信传输。监管链锚定节点的 HTTP Server 接收 Q_m 之后，首先使用私钥进行解密，然后对消息签名进行密码学验证，保证数据在传输过程中的真实性与完整性。传输流程完毕之后，对 Q_m 进行解析并进入下一阶段。

1.2.5　验证阶段

监管链锚定节点在接收到 Q_m 中的 CTF 信息之后，首先监管链锚定节点提取感知数据，对所有数据进行 Keccak256 哈希计算并按规定路径进行排序，从而计算接收数据的 Merkle 树根哈希 $H(R)$，并与 CTF 中的证明字段 Proof 中的根哈希 $H(P)$ 进行对比，如果等式结果为 true，那么数据的完整性得到验证。

然后，提取 CTF 信息中的聚合签名 S 与节点公钥 P，利用聚合签名算法验证等式

$$e(g,S)=e(P,H(m_1))e(P,H(m_2))\cdots e(P,H(m_n)) \tag{4}$$

若等式结果为 true，那么数据的真实性就得到验证。

1.2.6　链上存储阶段

监管数据的真实性与完整性在得到验证之后，监管链智能合约将提取 CTF 中监管编号并在监管链中进行查询，如果存在该监管编号，则将 CTF 中的感知信息上传至该监管编号下，如果不存在该监管编号，则将自动创建该监管编号的索引信息并将 CTF 中的感知信息上载至该监管编号下。

2　多链协同监管模型智能合约

智能合约作为区块链核心技术之一，是在区块链中存储并经过多方认可的程序合约，合约函数可在满足其规定的条件下自动执行。本文设计的冷链多链协同模型中，智能合约分为主链合约与从链合约，合约逻辑公开透明且不可篡改。从链合约可以实现从链感知数据自动上传、跨链传输数据的处理与发送；主链合约实现了节点的注册与审核、跨链数据的接收与验证以及监管查询等功能。如表 5 所示。

表 5　智能合约设计

Tab. 5　Smart contract function design

区块链类型	合约算法	合约函数	描述
主链	感知数据验证合约算法	idExamine( )	数据上链身份审查
		dataReceive( )	跨链数据接收
		aggreSignVerify( )	跨链数据签名验证
		genMainEvidence( )	生成主链跨链存证
从链	三文鱼数据绑定与模式监管合约算法	bindOrder( )	三文鱼数据绑定
		format( )	感知数据预处理
		signBLS( )	交易数据签名
		packBlock( )	区块打包
	跨链数据处理合约算法	dataDraw( )	提取跨链数据
		genSignAggregation( )	将提取的签名进行聚合
		formatSend( )	格式化数据并发送
		genSubEvidence( )	生成从链跨链存证

2.1　主链感知数据验证合约算法

主链数据验证算法在主链锚定节点接收跨链数据之后进行。该算法在接收到数据之后首先验证数据发送方证书的合法性，然后提取接收数据的数据项，最后利用数据项中的参数分别验证感知数据项的聚合签名与数据哈希。具体算法为

输入：接收数据 receiveData、主链节点证书 cerMainAnchorPeer、从链节点身份证书 cerAnchorPeer

输出：验证成功 verifySuccess

```
if( idExamine( cerMainAnchorPeer) )     //接收链锚定节点身份认证
  if( idExamine( cerSubAnchorPeer) )    //发送链锚定节点身份认证
    receiveData = dataReceive( );   //锚定节点接收包
    {signAggre, P, dataHash, perDataArray, extra} = receiveData. draw( )     //提取数据项
    if( Merkle( perDataArray) = = MerkleRootHash)  //MerkleProof 验证
      if( aggreSignVerify( signAggre, P)  //聚合签名验证
        crossChainEvidence = genEvidence (signAggre, P, dataHash, extra);     //生成跨链存证
        return verifySuccess;
      else
        return sign verify false;
    else
      return hash verify false;
  else
```

```
    return subchain peer identity false;
else
  return mainchain peer identity false;
```

2.2 三文鱼数据绑定与模式监管合约算法

在实际的三文鱼冷链物流过程中,经常会遇到冷链企业产品监管标准缺乏和产品标签不统一,从而导致监管缺乏和数据断链的发生。因此,本文设计了一种三文鱼数据绑定与模式监管的方法,企业首先通过扫描全冷链认可的三文鱼包装二维码获取监管编号并与链上企业订单和车辆感知设备相互绑定,然后根据三文鱼的货架期需求[31],匹配不同的监管模式。最后,在运输或者存储过程中根据监管模式所规定的监管阈值对监测的参数进行监管预警,如果任一参数超过规定阈值,则预警次数就会加 1,并将预警信息永久上链。该算法保证了三文鱼在冷链物流过程中细粒度与完整性的监管。具体算法为

输入:感知节点身份证书 cerPerPeer、上传合约地址 uploadAddress、感知数据 data、订单号 orderNum

输出:交易哈希 transaHash、交易区块号 blockNum、签名 sign

```
if( idExamine( cerPerPeer) )    //感知节点身份认证
  if( isSenserID)          //感知设备编号是否绑定
    if( uploadAddress)          //上传合约地址验证
      if( isBindOrder( orderNum) )                    //订单编号是否绑定
        formatData  = format( data) ;          //格式化监管数据
        if( isLegal( formatdata) ) ;          //判断数据是否合法
          sign  =  signBLS( formatdata) ;    //感知节点对数据进行 BLS 签名
          upload( fomatdata, sign) ;          //数据上传内存池
          if( isAmout( dataNum) ) ;          //判断数据量是否满足打包成块的条件
            packBlock( ) ;          //打包成块
            return sign, transactionHash, blockNum;
          else
            return continue upload;    //继续上传
        else
          returnenvironmental warning; //监管预警
      else
      return ordernumber false;
    else
      return address false;
    else
     return senserID false;
  else
    return identity false;
```

2.3 从链跨链数据处理合约算法

从链跨链数据处理算法是在跨链事件触发后发起的,该算法可将跨链数据签名利用 BLS 签名聚合函数进行聚合,然后将聚合后的签名、感知节点公钥、感知数据、主链节点网络信息等跨链传输信息进行格式化。最后触发跨链传输事件传输格式化后的信息。具体算法为

输入:从链锚定节点身份证书 cerAnchorPeer、合约地址 SCAddress

输出:传输数据包 packageSend、跨链存证 crossChainEvidence

```
if( idExamine( cerAnchorPeer) )    //锚定节点身份认证
  if( SCAddress)          //上传合约地址验证
    if( orderNum)          //所属订单验证
      { perDataArray, signArray, extra}  =  dataDraw ( orderNum) ; //提取感知数据与签名集
      dataHash  =  Merkle( perDataArray) ;
        //生成 MerkleProof
      signAggre  =  genSignAggregation( signArray) ;
        //签名聚合
      P = selfPublicKey( ) ;      //感知节点公钥提取
        packageSend  =  formatSend ( perDataArray, signAggre, P, dataHash,  extra) ; //格式化传输数据
      targetAnchorPeerInfo  =  drawTargetInfo( ) ;
        //提取监管链锚定节点网络信息
          emit  crossChainEvent  ( packageSend, targetAnchorPeerInfo) ;      //触发跨链传输事件
      crossChainEvidence  =  genEvidence( signAggre, P, dataHash,  extra) ;      //生成跨链存证
      return packageSend, crossChainEvidence;
    else
      return order number false;
  else
    return smart contract address false;
else
  return identity false;
```

3 系统实现与测试

原型系统使用 Solidity 和 NodeJS 语言进行开发,Remix IDE 和 VSCode 为集成开发环境。硬件系统运行处理器为 Intel(R) Core(TM) i7 - 9700 CPU,硬盘存储容量 100 GB,运行内存 8 GB,符合实

验运行需求。

3.1　系统设计与实现

3.1.1　系统架构

本文实现了基于区块链主从多链协同的冷链监管系统。通过主从多链的架构分别存储主链公开的监管数据以及从链企业的隐私数据，真正做到了数据的隔离；通过聚合签名验证的方式提高主从链之间传输数据的验证效率从而提高系统整体的效率；实现了三文鱼冷链的物流与环境监管，防止在冷链过程中恶意断冷、断湿、路线偏离与溯源断链的发生，保证了消费者以及企业的权益。三文鱼冷链监管模型架构如图 4 所示，共分为 4 层，由下到上分别为区块链层、服务层、接口层和应用层。

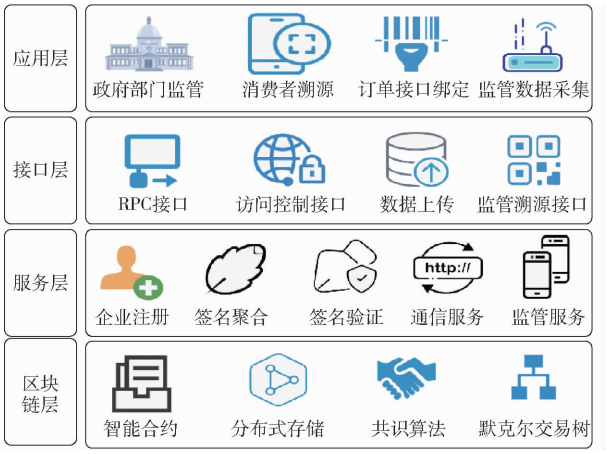

图 4　三文鱼冷链多链协同系统架构

Fig. 4　Architecture of salmon cold chain multi-chain collaborative system

区块链层内置不可篡改以及共同维护的智能合约，同时，利用区块链分布式存储的优势，保证了存储数据的可靠性与安全性；服务层企业注册服务为冷链企业提供了监管链的数据上传身份，同时企业节点利用授权身份所上传的数据需经过聚合签名的验证。同时，在通信过程中，利用 HTTP2 服务套件对信息进行加密传输；接口层封装节点与区块链交互的 RPC 接口、节点的访问控制接口、监管溯源接口以及主链与从链的感知数据上传接口。这 4 类接口内部都封装有特定的端口信息与数据格式规范，保证了区块链与节点连接的安全性与易管理性；应用层面向不同的受众实现了不同的应用服务。

3.1.2　系统实现

本文实现了三文鱼冷链的全环节信息管理与监管溯源等功能。本节以运输环节为例进行展示。如图 5a 所示，该页面为某运输订单的信息页面，运输订单由物流节点创建并进行基本数据的录入，工作人员可以通过便携式设备将运输订单、商品二维码、运输车辆以及感知设备进行绑定，以便后续感知数据的上链。同时，订单页面可以实时更新货物的运输状态以及环境数据异常警告次数，更新信息均在运输链上链保存，图 5b 为上链区块信息，详细记录了数据上传过程中产生的区块高度以及数据上传的时间与交易哈希，与此同时，当智能合约检测到感知数据异常时，会在系统内生成预警并提醒操作人员处理，最后，永久上传带有异常标记的感知数据。

(a) 运输订单页面

(b) 订单预警以及上链信息查询

图 5　三文鱼冷链多链协同系统页面

Fig. 5　Salmon cold chain multi-chain collaborative system page

其次，本系统实现了监管链的数据查询功能，用户可以扫描商品包装二维码进行三文鱼冷链全环节数据的查询，从而满足政府的监管以及消费者的追溯需求。如图 6a 所示，该页面除了展示了三文鱼的商品信息以及物流信息之外，在页面顶部还设置有三文鱼全冷链的监管预警次数信息，预警次数较多，说明冷链企业对于环境参数的控制还存在不足，同时也说明了该三文鱼存在一定的质量问题。所展示的信息全部经过监管链的真实性验证并永久上链存储，上链信息如图 6b 所示。

3.2　实验测试与分析

基于以太坊实现了主从链协同原型系统，并与传统方案在通信数据大小与签名验证效率方面进行对比。最后，通过实验验证了多链架构相比于传统单链架构在存储与查询方面的优势。

以三文鱼冷链运输企业为例，本文对三文鱼运输过程产生的数据进行随机采样并进行上链，结果显示，三文鱼运输数据单次上链消耗 197 481 gas。根据以太坊规定，每个区块的目标大小为 1.5×10^7 gas。理论上一个区块可以存储大约 76 笔交易，但是在实际操作中，由于区块共识的实时性，区块中也会存储有其他节点产生的交易，因此，为了体现测试的真实性，本节将单区块交易数量划定在 5 ~ 75

(a) 物流监管信息查询 (b) 监管信息上链页面

图 6 系统监管功能实现页面

Fig. 6 Implementation pages of regulatory functions

的范围内进行测试。

3.2.1 通信消耗

在跨链通信中，传输信息 CTF 除了身份数据、感知数据与订单基本信息之外，还附带有验证数据真实性的节点签名信息。目前主流的区块链平台例如以太坊(Ethereum，ETH)、比特币和 HyperLedger Fabric 均采用椭圆曲线数字签名算法(Elliptic curve digital signature algorithm，ECDSA)，但由于标准不同，三者的签名长度在 64 ~ 72 B 之间。因此，为了便于比较，本文通过对以太坊 ECDSA 签名算法与 BLS 聚合签名算法的签名大小来展示 BLS 聚合签名算法在跨链通信中的优势。如图 7 所示，当签名数据为 5 条时，ECDSA 算法所需要的签名通信量为 325 B，而 BLS 算法签名即使在未压缩的情况下通信量也仅为 96 B，远低于 ECDSA 的通信量。同时，随着签名数量的增加，ECDSA 算法的签名大小呈线性增长趋势，在最大签名数量时，ECDSA 签名数据量达到 4 875 B，而 BLS 聚合算法签名通信量仍然保持不变。从实验结果可以看出，BLS 聚合签名算法可以有效降低跨链数据传输的通信量，从而提升三文鱼冷链多链协同模型的传输效率。

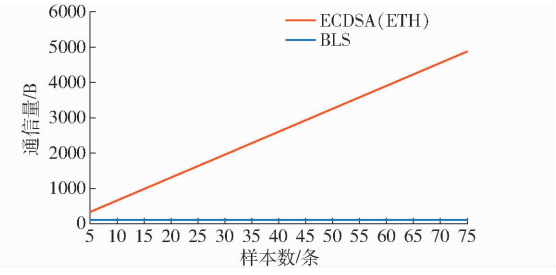

图 7 签名通信消耗

Fig. 7 Communication consumption

3.2.2 签名验证效率

数据真实性的验证是跨链通信过程中最为耗时的步骤，因此提高签名验证效率是提高系统整体运行效率的关键。本文以 ECDSA(以太坊)与 BLS 聚合签名算法时间开销对比为例，如图 8 所示。通过计算可知，当区块交易数在 5 ~ 75 区间内的条件下，ECDSA 算法验证时间曲线的趋势线斜率为 57.448，而 BLS 算法验证时间曲线的趋势线斜率仅为 0.553。因此，从实验结果可以看出，三文鱼冷链多链跨链通信中结合 BLS 聚合签名与验证技术可以极大地提高数据真实性验证的效率。

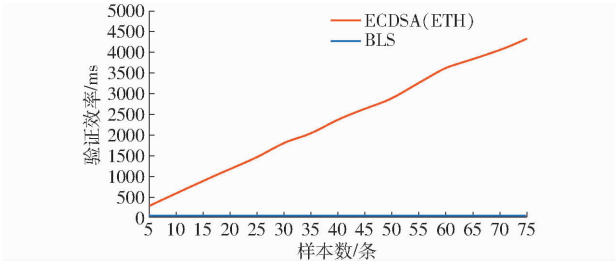

图 8 签名验证效率

Fig. 8 Signature verification efficiency

3.2.3 存储性能

多链模型的数据隔离机制不仅可以保证企业隐私数据的安全，同时也通过多链存储机制来分担传统单链架构所带来的存储压力，使监管链只面向存储监管类数据，而非企业内部的其他非监管类数据。本文分别测试了多链模型的监管链与传统单链在上传监管交易数量为 1×10^4 到 5×10^4 区间的存储消耗，如图 9 所示。由于单链架构会额外存储企业内部的非监管类数据，因此从图 9 可以看出多链架构中监管链的存储消耗低于传统单链架构；此外通过计算可知多链架构监管链存储曲线的趋势线斜率为 0.037，而传统单链架构存储曲线的趋势线斜率为 0.044，表明随着交易数量的增加，存储差距会不断变大。

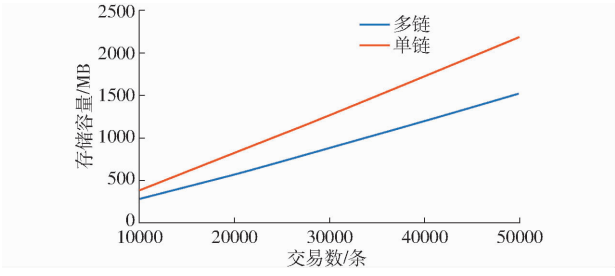

图 9 存储性能测试

Fig. 9 Storage performance testing

3.2.4 监管性能

为了体现多链架构在监管性能方面的优势，以包装二维码中的监管编号为查询索引，分别对多链架构和单链架构的监管交易查询进行测试。本次测试查询交易数量为 10 ~ 100 区间，测试结果如图 10 所示。区块链查询所需时间与查询交易数呈正相关；多链架构中监管链查询效率相较于单链架构平均提高 17.98%。由于区块链的查询性能与区块链

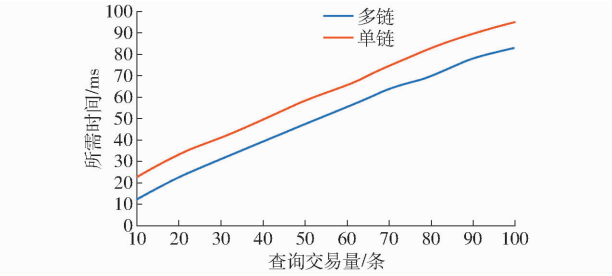

图 10　监管性能测试

Fig. 10　Regulatory performance

存储大小有关，因此结合 3.2.3 节分析可以得出，随着存储差距的增大，多链架构的监管性能优势将更加明显。

4　结论

（1）设计并实现了基于区块链的三文鱼冷链多链协同监管模型。该模型主从多链的设计既保证了企业内部隐私数据的安全，同时也缓解了传统单链架构因三文鱼冷链企业相关数据海量所带来的存储性能的问题。其次，本文提出的监管链注册机制适应于当前冷链行业集群式发展的特点与趋势，使得企业能够真正融入到全冷链监管的环境中，进而提升三文鱼冷链运输的质量。经测试，在存储性能方面，随着交易数量的提升，多链架构中监管链的存储消耗远低于单链架构；在监管性能方面，在同等条件下，由于单链架构的存储开销大于多链架构的监管链，因此多链架构的监管性能优于单链架构，并且随着区块链交易的增多，这一优势会不断加大。

（2）为了保障数据在跨链过程中的可靠性与验证效率，提升三文鱼冷链监管数据的可信度，本文在模型中实现一种基于聚合签名验证的数据真实性验证方法，在保证数据完整性的前提下，通过 BLS 算法提升跨链数据真实性验证的效率。实验结果显示，区块交易数在 5 ~ 75 区间内且趋势线拟合度趋近于 1 的前提下，ECDSA 算法验证时间曲线的趋势线斜率为 57.448，远高于 BLS 算法验证时间曲线 0.553 的趋势线斜率，在批量数据验证验证的情况下，具有良好的效率；在通信消耗方面，ECDSA 算法的签名通信量与签名数量呈正相关，所需要的签名通信量最多可达到 4 875 B，而 BLS 算法签名即使在未压缩的情况下通信量也一直保持在 96 B，远低于 ECDSA 的通信量。由此可见，在三文鱼冷链场景中，聚合签名与验证的方法在数据批量传输批量验证的条件下具有良好的效率优势。

参　考　文　献

[1] 刘婧懿，赵前程，程少峰，等. 鱼肉质构的影响因素及测定方法研究进展[J]. 食品安全质量检测学报，2020，11(9)：3035 - 3043.
LIU Jingyi, ZHAO Qiancheng, CHENG Shaofeng, et al. Research progress on the influencing factors and determination methods of fish muscle texture[J]. Journal of Food Safety & Quality, 2020, 11(9): 3035 - 3043. (in Chinese)

[2] 苏红，李雨欣，钱雪丽，等. 鳙鱼、金枪鱼和三文鱼鱼头的营养分析与品质评价[J]. 食品工业科技，2019，40(17)：212 - 217.
SU Hong, LI Yuxin, QIAN Xueli, et al. Nutrition analysis and quality evaluation of *Aristichthys nobilis*, *Thunnus obesus* and salmon salar head[J]. Science and Technology of Food Industry, 2019, 40(17): 212 - 217. (in Chinese)

[3] CUI Haoxin, NAYMUL K, JIANG Feng, et al. Evaluation of the impact of temperature fluctuations on the quality of pork and salmon during micro-freezing process[J]. Journal of Zhejiang University—Science B (Biomedicine & Biotechnology), 2022, 23(7): 578 - 603.

[4] 丁清龙，曾晓琮，周露，等. 三文鱼水产品掺假情况调查[J]. 食品安全质量检测学报，2019，10(13)：4080 - 4085.
DING Qinglong, ZENG Xiaocong, ZHOU Lu, et al. Investigation of adulteration in salmon seafood products[J]. Journal of Food Safety & Quality, 2019, 10(13): 4080 - 4085. (in Chinese)

[5] 白晨，马慧婕，宋昌彦，等. 2019 年上海生食三文鱼微生物抽检及消费者调查[J]. 食品工业，2020，41(10)：269 - 272.
BAI Chen, MA Huijie, SONG Changyan, et al. Microbiological sampling and consumer survey of raw salmon in Shanghai in 2019[J]. The Food Industry, 2020, 41(10): 269 - 272. (in Chinese)

[6] DONG Y, XU M, MILLER S A. Overview of cold chain development in China and methods of studying its environmental impacts[J]. Environmental Research Communications, 2021, 2(12): 122002.

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

[8] HAN J W, ZUO M, ZHU W Y, et al. A comprehensive review of cold chain logistics for fresh agricultural products: current status, challenges, and future trends[J]. Trends in Food Science & Technology, 2021, 109: 536 - 551.

[9] 于华竟，徐大明，罗娜，等. 杂粮供应链区块链多链追溯监管模型设计[J]. 农业工程学报，2021，37(20)：323 - 332.
YU Huajing, XU Daming, LUO Na, et al. Design of multi-chain traceability and supervision model for grain supply chain based on blockchain[J]. Transactions of the CSAE, 2021, 37(20): 323 - 332. (in Chinese)

[10] 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. Research on multi-chain model of blockchain for fruit and vegetable whole supply chain oriented to traceability subjects[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4): 416 - 427. (in Chinese)

[11] HALIM A H A, USMAN S. Implementation of IoT and blockchain for temperature monitoring in COVID19 vaccine cold chain

logistics[J]. Open International Journal of Informatics, 2021, 9(1): 78 - 87.
[12] 吴迪, 汪勇, 孙地冰, 等. 新冠疫情下港区农产品冷链物流监管平台构建与应用[J]. 农业大数据学报, 2022, 4(1): 62 - 68.
WU Di, WANG Yong, SUN Dibing, et al. Construction and application of cold chain logistics supervision platform for agricultural products in Hong Kong under COVID - 19 pandemic[J]. Journal of Agricultural Big Data, 2022, 4(1): 62 - 68. (in Chinese)
[13] RAMÍREZ C, ROJAS A E, GARCÍA A. A cold chain logistics with IoT and blockchain scalable project for SMEs: first phase [J]. IFAC-PapersOnLine, 2022, 55(10): 2336 - 2341.
[14] ZHANG Y, LIU Y, JIONG Z, et al. Development and assessment of blockchain-IoT-based traceability system for frozen aquatic product[J]. Journal of Food Process Engineering, 2021, 44(5): e13669.
[15] 何静,胡鑫月.基于量子区块链的食品冷链追溯系统构建[J].食品科学,2022,43(15):294 - 301.
HE Jing, HU Xinyue. Construction of food cold chain traceability system based on quantum blockchain[J]. Food Science, 2022, 43(15): 294 - 301. (in Chinese)
[16] 张森,叶剑,李国刚.面向冷链物流的区块链技术方案研究与实现[J].计算机工程与应用,2020,56(3):19 - 27.
ZHANG Sen, YE Jian, LI Guogang. Research and implementation of blockchain technology scheme for cold chain logistics [J]. Journal of Computer Engineering and Applications, 2020, 56(3): 19 - 27. (in Chinese)
[17] MERSHAD K, CHEIKHROUHOU O. Lightweight blockchain solutions: taxonomy, research progress, and comprehensive review[J]. Internet of Things, 2023, 24: 100984.
[18] WANG Q, ZHU X, NI Y, et al. Blockchain for the IoT and industrial IoT: a review[J]. Internet of Things, 2020, 10: 100081.
[19] 李莹,瞿红红,王佳,等.区块链多链防伪溯源模型设计与系统实现[J].湖南大学学报(自然科学版),2023,50(8):172 - 180.
LI Ying, QU Honghong, WANG Jia, et al. Blockchain multi-chain anti-counterfeit traceability model design and system implementation[J]. Journal of Hunan University (Natural Sciences Edition),2023,50(8):172 - 180. (in Chinese)
[20] 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. Research on 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)
[21] 孟博,王乙丙,赵璨,等.区块链跨链协议综述[J].计算机科学与探索,2022,16(10):2177 - 2192.
MENG Bo, WANG Yibing, ZHAO Can, et al. A survey on cross-chain protocols in blockchain[J]. Journal of Computer Science and Exploration, 2022, 16(10): 2177 - 2192. (in Chinese)
[22] 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. Research on rice origin traceability method based on blockchain and edge computing[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(5): 359 - 368. (in Chinese)
[23] 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. Research progress and prospect of blockchain traceability technology for agricultural product supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(1): 1 - 13. (in Chinese)
[24] 乔蕊, 刘敖迪, 陈迪, 等. 复杂物联网联盟链系统通信机制研究[J]. 自动化学报, 2022, 48(7): 1847 - 1860.
QIAO Rui, LIU Aodi, CHEN Di, et al. Research on communication mechanism of complex IoT consortium chain system[J]. Acta Automatica Sinica, 2022, 48(7): 1847 - 1860. (in Chinese)
[25] PENG X, ZHANG X, WANG X, et al. Multi-chain collaboration-based information management and control for the rice supply chain[J]. Agriculture, 2022, 12(5): 689.
[26] 谭海波, 周桐, 赵赫, 等. 基于区块链的档案数据保护与共享方法[J]. 软件学报, 2019, 30(9): 2620 - 2635.
TAN Haibo, ZHOU Tong, ZHAO He, et al. Archive data protection and sharing method based on blockchain[J]. Journal of Software, 2019, 30(9): 2620 - 2635. (in Chinese)
[27] 经普杰, 王良民, 董学文, 等. 分层跨链结构: 一种面向区块链系统监管的可行架构[J]. 通信学报, 2023, 44(3): 93 - 104.
JING Puje, WANG Liangmin, DONG Xuewen, et al. Hierarchical cross-chain structure: a feasible architecture for supervising blockchain systems[J]. Journal of Communications, 2023, 44(3): 93 - 104. (in Chinese)
[28] WEN L, ZHANG L, LI Y, et al. AVEI: a scientific data sharing framework based on blockchain[C] // Bench Council International Federated Intelligent Computing and Block Chain Conferences. Singapore: Springer Singapore, 2020: 264 - 280.
[29] 葛艳,姚海东,邹一波,等.基于区块链跨链技术的水产品交易模型研究[J].农业机械学报,2022,53(12):332 - 343.
GE Yan, YAO Haidong, ZOU Yibo, et al. Research on water product trading model based on blockchain cross-chain technology[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(12): 332 - 343. (in Chinese)
[30] 胡金有,王靖杰,朱志强,等.冷链物联网监测数据质量评估与优化研究进展分析[J].农业机械学报,2019,50(8):1 - 14.
HU Jinyou, WANG Jingjie, ZHU Zhiqiang, et al. Analysis of research progress on data quality evaluation and optimization of cold chain internet of things monitoring[J]. Transactions of the Chinese Society for Agricultural Machinery, 2019, 50(8): 1 - 14. (in Chinese)
[31] 贾志鑫. 三文鱼新鲜度和品质货架期预测模型研究[D]. 杭州: 浙江工商大学, 2020.
JIA Zhixin. Research on freshness, quality, and shelf life prediction model of salmon[D]. Hangzhou: Zhejiang Gongshang University, 2020. (in Chinese)