DOI:10.3969/j.issn.1007-9580.2022.01.007

基于区块链的水产品交易溯源系统研究与实现

冯国富,胡俊辉,陈 明
(1 上海海洋大学信息学院,上海 201306;
2 农业农村部渔业信息重点实验室,上海 201306)

摘要:针对传统水产品交易溯源系统存在的中心化易篡改、数据无法共享和可信溯源困难等问题,提出了基于区块链和星际文件系统(Inter Planetary File System,IPFS)结合的水产品交易溯源模型,通过分析水产品交易流程,将水产品养殖关键信息和订单交易信息等数据采用IPFS存储,并将IPFS地址上传至区块链网络。基于联盟链平台Hyperledger Fabric实现了该系统的原型,设计系统访问权限控制方案,提出了适用于该系统的智能合约,以保证交易数据的安全可靠存储。结果显示:该系统可以实现交易数据的发布和查询,消费者和监管部门可以实现对水产品养殖信息的可信追溯;系统吞吐量可以达到220笔/s的交易,基本满足水产品交易数据的存储和溯源业务需求。本研究可为水产品交易溯源技术提供一种参考。

关键词:区块链;水产品交易;溯源;IPFS;智能合约
中图分类号:S9-9;TP315 **文献标志码**:A **文章编号**:1007-9580(2022)01-0044-08

水产养殖业在农业经济发展中占有重要地位,据统计,2020年中国水产品总产量为6 549万t,其中养殖产品占比达到了79.8%[1]。近年来,水产品质量安全事件频发,不仅危及人们的身体健康,对水产养殖业发展也有不利影响[2-3]。在水产品交易环节中,交易数据的安全至关重要,这些数据不只是消费者进行水产品质量追溯的依据,还能让养殖企业带来更高经济收益。在传统水产品交易模式下,数据多采用中心化的存储方式,数据的安全可靠性得不到保证[4-5]。当存储数据的中心服务器出现故障时,数据就会存在丢失的风险,并且中心化存储的数据有可能会被篡改,数据可靠性存疑。除此之外,数据不能共享且溯源困难,水产品的养殖厂家、经销商以及消费者之间的数据是不互通的,因此导致交易链的上下游不能有效协同,数据溯源的透明性较低,出现问题无法第一时间定位。

区块链具有去中心化、可追溯和不可篡改的特点[6-9],区块链的出现为解决水产品交易中存在的数据安全问题提供了新的解决思路。首先,区块链是由多方参与共同维护的分布式数据库,不存在中心化的管理机构,解决了中心化存储数据不可靠的问题[10]。其次,区块链运用密码学技术,每个区块包含前一个区块链的哈希(Hash)值,形成有序的链式结构,确保数据不易被篡改[11]。最后,区块链具有可追溯性,共识机制保证节点间的数据共享和监督,存储于区块链之上的每一条记录、每一笔交易都可以进行可信溯源[12]。但是将区块链技术直接应用于水产品交易数据存储会存在问题,一是水产品交易环节中节点众多,产生的数据量较大,如果这些数据直接存储到区块链网络上,会给区块链存储容量造成压力。二是要保证交易的隔离性,即当前交易参与主体间的操作对其他主体是不可见的,数据加密之后再进行传输。

本研究以Fabric区块链平台为基础,通过对水产品交易流程分析,梳理并提炼出交易环节中关键主体和数据,提出基于区块链的水产品交易数据溯源系统模型。在该模型中,数据不直接存储在区块链网络中,而是结合星际文件系统(IPFS)存储原始数据,区块链网络中只需要存储IPFS的文件Hash地址降低链上存储压力。在此基础上,提出了系统访问权限控制方案,不同主体间进行数据交易时运行在独立的通道内,每个通

收稿日期:2021-10-10
基金项目:江苏现代农业产业关键技术创新(CX(20)2028)
作者简介:冯国富(1971—),男,博士,副教授,研究方向:嵌入式技术研究、区块链应用。E-mail:1586574214@qq.com
通信作者:陈明(1966—),男,博士,教授,研究方向:数据挖掘、农业信息技术。E-mail:892985538@qq.com

道有独立的账本和智能合约,不同通道间数据隔离,保证数据的隐私性和安全性。

1　相关背景

1.1　区块链

区块链是一种分布式去中心化账本[13-14],随着区块链在不同领域研究的深入,区块链的应用也越来越多样化,学者们提出了许多数据存储和溯源方案[15-17]。Xie 等[18]基于区块链提出了一种双链存储结构进行农产品数据的存储,利用链式数据结构存储交易的哈希值,然后将其与区块链链接在一起形成链式结构,保证数据不会被篡改。Hao 等[19]提出了一种基于 IPFS 和区块链的农产品数据存储模型,将传感器数据存入 IPFS 文件系统,然后利用区块链存储分布式文件系统 IPFS 的哈希值,确保数据安全。葛艳等[20]将区块链技术与危害分析及关键控制点(HACCP)结合,提出了生食牡蛎的质量溯源模型,通过设计智能合约,对链上和链下数据进行监控并进行质量判断。李梦琪等[21]通过分析水产品供应链的关键信息,提出了一种主从多链存储模型对供应链溯源信息进行管理,保证了溯源数据的真实性和追溯过程的透明化。赵磊等[22]从信息生态视角分析用户需求,提出追溯参与主体的风险补偿方案,并进行信息链流程再造,给出了一种基于区块链的生鲜食品追溯模型。以上基于区块链的数据溯源模型都有各自的优点,但是水产品交易数据溯源场景下数据量较大,直接存储在区块链之上会给链上造成很大压力,并且交易数据的隐私性应该进行控制。因此,本研究结合区块链技术的优势以及现有溯源系统的不足,提出区块链在水产品交易数据上的溯源模型。

1.2　星际文件系统

IPFS 是一个由所有参与的节点共同构成的分布式文件系统[23-24]。IPFS 在进行数据存储时不会受到文件大小的限制,因为它会将文件分为大小相等的数据块,每一块数据都有一个对应的 Hash 值,根据这些 Hash 值可以构建出一张文件检索表,从而可以实现将这些数据块分散存放在不同的服务器上[25]。

在进行数据查询时,只需要输入要查询的文件 Hash 值,IPFS 就会根据文件检索表去对应的文件服务器上查询数据并返回。IPFS 分布式的特点使其可以天然地与区块链结合,区块链网络中不再存放完整的数据,只需要存放对应数据文件的 IPFS 散列地址,从而节省区块链的网络带宽,降低链上存储压力。

2　系统模型

2.1　水产交易流程分析

在整个水产品交易流程中,首先要保证源头数据的真实可靠,即保证消费者购买到的水产品的养殖信息是真实可追溯的。水产品交易溯源流程如图 1 所示。

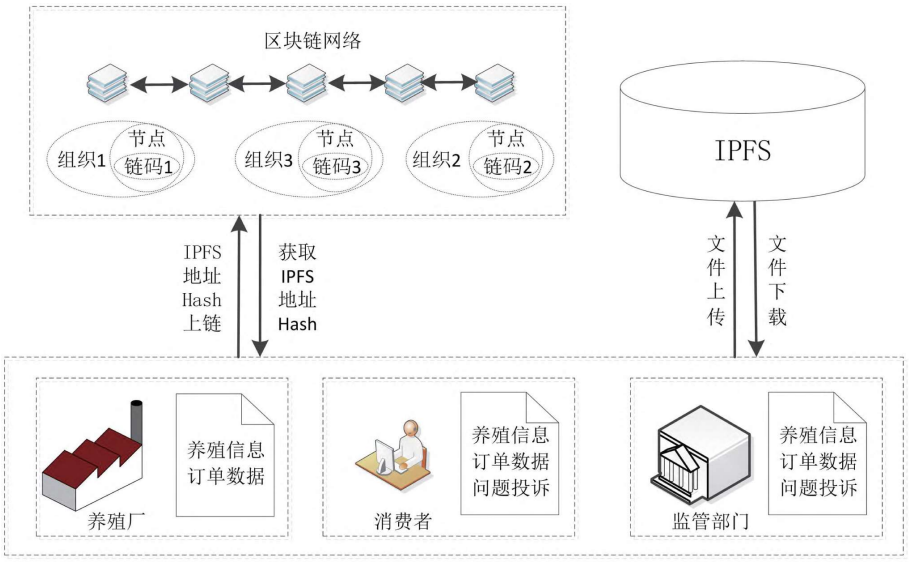

图 1　系统流程图

Fig.1　System flow chart

整个流程主要包括3个主体，分别为养殖厂、消费者和监管部门。在水产品流入市场进行交易前，养殖厂首先要将水产品的养殖信息，如池塘编号、水产品种类、入塘时间和捕捞时间等信息通过智能合约协调IPFS和区块链的工作，将原始数据存入IPFS中，再将返回的IPFS地址Hash值上传至区块链网络。消费者和养殖厂进行交易时，也需要将这些水产品的订单交易记录，包括买卖双方姓名、水产品名称、重量、单价和订单金额等信息结合IPFS进行存储。在交易完成之后，如果消费者发现购买的水产品出现食品质量安全问题，也可以将投诉信息上传至IPFS中进行存储。监管部门根据投诉信息在IPFS中找到对应交易订单信息和问题水产品的养殖信息，若该批次水产品存在质量问题，可以及时进行处理。

2.2 系统结构

联盟链Hyperledger Fabric平台具有去中心化、部署成本低、可扩展性高和数据安全可追溯等特点[26]。因此，通过对水产品交易流程分析，结合Hyperledger Fabric平台提出了系统整体架构。系统整体架构设计如图2所示，自上而下可分为应用层、数据库层、网络层和数据层。其中区块链技术主要用于数据库层和网络层。

图2 系统整体架构

Fig.2 System structure

应用层是在区块链网络的基础上，通过在区块链中编写智能合约对外提供API接口，设计一个水产品交易溯源平台，利用可视化的界面提供信息交互服务，面向的对象为水产品养殖厂、消费者和监管部门。

数据库层包括区块链网络中的分布式账本和IPFS文件系统。系统中所有的原始数据在IPFS中进行存储，数据存储完成后IPFS会返回对应文件的地址Hash值。区块链网络中的分布式账本存储的不再是原始数据，而是地址Hash值。为了实现数据隐私保护，文件地址Hash值在提交上链之前先通过对称加密的方式进行加密，然后再做上链处理。通过这种方式可以实现上传地址Hash值不会被通道内的其他用户看到，并且只有获得访问权限的用户才可以查看区块链网络中的地址Hash值，最终实现根据地址Hash值从IPFS文件系统中获取原始数据。

网络层采用共识算法解决用户之间的信任问题，通过共识机制选取背书节点进行数据验证。基于工作量证明的PoW共识算法会消耗很大的算力资源，不适合在商业领域应用[27]。因此，本研究使用了更加高效的Kafka共识算法，采用一组排序节点对消息进行处理，根据排序之后的结果进行上链处理[28]。网络层还要进行节点的访问权限控制，通过多通道机制实现通道间的数据隔离，通过证书颁发机构(Certification Authority，CA)签发证书控制节点对数据的访问，实现数据的隐私保护。

数据层作为最底层主要进行3部分数据信息的收集。一是水产品养殖过程中的数据，如池塘编号、水产品种类、入塘时间和捕捞时间等。二是交易过程中的订单数据，如买卖双方姓名、水产品名称、重量、单价和订单金额等。三是交易完成之后消费者给出的反馈数据，如质量问题的类型和描述、水产品名称和对应订单号等。

3 系统实现

3.1 Fabric网络环境模块

图3所示为根据系统流程图设计的Fabric网络结构模型，Fabric网络采用单机多节点的部署方式。在Fabric网络中，每1个参与主体对应1个组织节点，使用配置文件的方式创建系统所需要的养殖厂、消费者和监管机构3个组织节点，并通过Fabric模块生成对应的数字证书、数据文件和通道创始区块。每个组织下面包含2个Peer节点，用于实现各组织的背书、记账等功能。除此之外，需要配置CA证书节点和排序节点，CA证书节点用于给用户分发并且验证证书，排序节点用于对传递的消息进行排序以便后续生成相应的区块。在Fabric网络中，每一个组织都有相应的CA证书机

构给用户颁布证书进行身份验证,采用支持富查询的 CouchDB 数据库作为 Fabric 的状态数据库,每个组织配有相应的数据库进行数据存储。共识模块是由多个 Order 排序节点组成的 Kafka 集群来实现的,它具有高扩展性的特点,并且由于多个排序节点的存在,具有很高的容错能力。

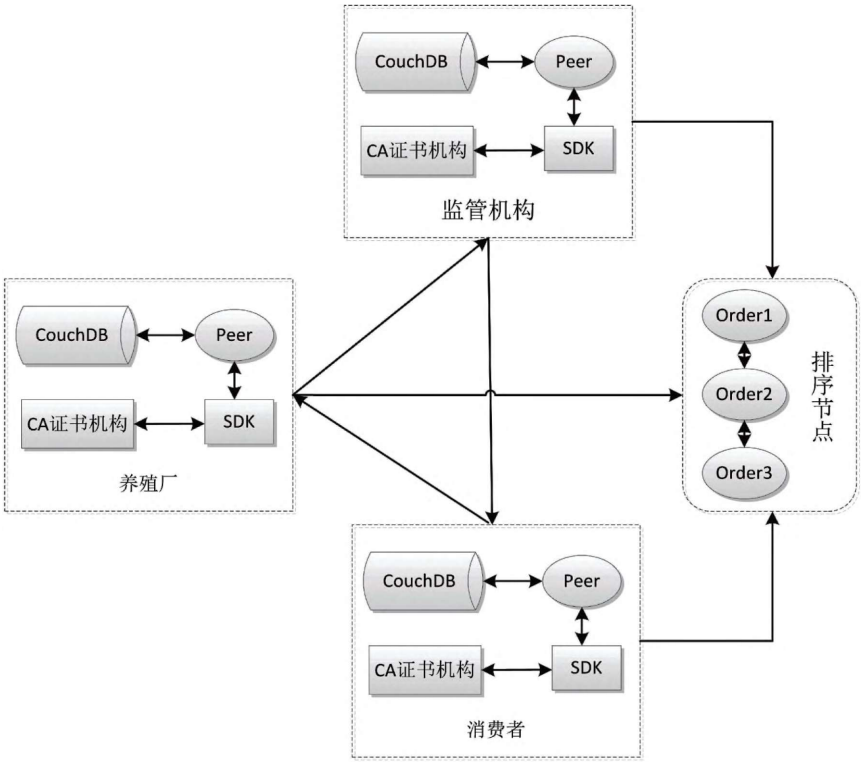

图 3　Fabric 网络结构模型

Fig.3　Fabric network structure model

系统中存在养殖厂、消费者和监管机构 3 个组织,其中,组织标志符、组织 ID 和各个组织安装的智能合约信息如表 1 所示。

表 1　系统组织表

Tab.1　System organization table

组织名称	组织标志符	组织 ID	智能合约名称
养殖厂	Org1	Org1MSP	cc_aqufarm
消费者	Org2	Org2MSP	cc_consumer
监管机构	Org3	Org3MSP	cc_authority

3.2　系统访问权限控制模块

在系统模型中,养殖厂、消费者和监管机构 3 个组织下存在不同的用户,用户之间应当是相互独立的,当消费者 A 进行数据查询时,对其他消费者来说应该是不可见的。因此,本研究在系统模型中配置了多条通道,每条通道拥有自己独立的账本和智能合约。从系统上看,通道仍然是由 Order 节点进行管理,划分目的只是为了将不同的通道信息进行隔离,保证数据交易信息的安全性和隐私性。

如图 4 所示为系统的通道设计模型,在该系统模型中,所有的节点会共同加入一个公共通道之中,他们共同维护一个账本并将自己的数据写入其中进行交易。channel1 和 channel2 是按照业务需求划分的私有通道,私有通道之间以及私有通道和主通道之间都是隔离的,可以保证数据的隐私性。在该模型中,养殖厂不希望养殖数据直接被其他养殖企业看到,消费者也不希望将自己的消费信息暴露出去。因此,养殖企业 BP1 和 BP2 分别订阅 channel1 和 channel2 通道,购买了相应企业水产品的消费者 C1 和 C2 也会订阅对应的通道,监管机构根据业务需求订阅需要监管的通道。在图 4 中,BP1 和 C1 在 channel1 通道中进行交易,BP2 和 C2 在 channel2 通道中进行交易,通道外组织节点无法查看交易数据。

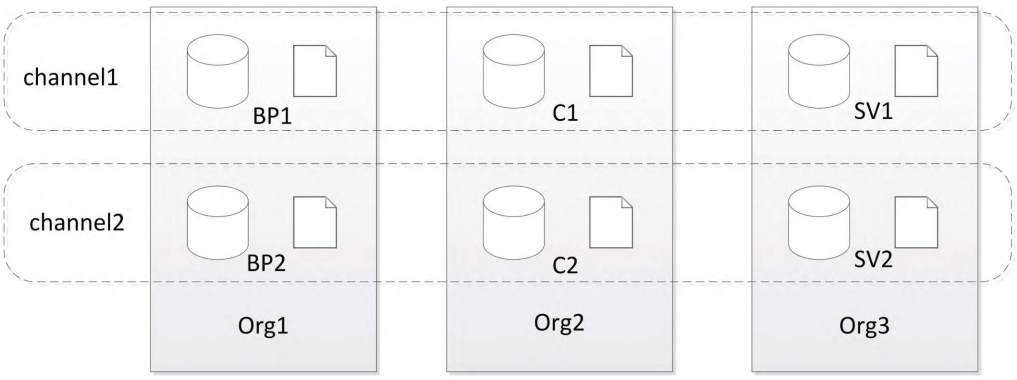

图 4 多通道设计模型

Fig.4 Multi-channel design model

除了对区块链网络进行多通道划分，数据在网络中应该以密文的方式进行传输，确保数据的隐私性。当用户不希望 IPFS 文件数据的地址 Hash 值直接被通道内其他用户看到时，可以对其加密后再进行上链操作。如当通道内用户 A 上传地址 Hash 值并且只希望同一通道内的用户 B 查看时，可以采用对称加密算法对地址 Hash 值进行加密，上链过程可以描述为：用户 A 首先获取用户 B 通过 AES（Advanced Encryption Standard）生成的密钥 K，对地址 Hash 值进行对称加密。加密函数定义为 encrypt（K，Hash），加密后的地址 Hash 值为 E_Hash，加密完成之后再将密文 E_Hash 上传至区块链网络。当用户 B 要查询原始数据时，首先会从区块链中获取加密之后的地址 Hash 值 E_Hash，然后使用密钥 K 对 E_Hash 进行解密获取地址 Hash 值，解密函数定义为 decrypt（K，E_Hash），最后再根据 IPFS 文件的地址 Hash 值执行查询操作获取原始数据。

3.3 智能合约模块

在 Fabric 平台中，智能合约又被称为链码，链码是连接客户端与 Fabric 网络的桥梁[29]。链码就是一段程序代码，用来表示系统流程的业务逻辑，也需要通过编译之后才能够运行，链码在经过编译和部署之后，一般运行于 Docker 容器之中。在 Docker 容器中，客户端可以通过调用链码，完成数据的发布和查询操作。链码可以由多种语言进行实现，本研究选用 Go 语言编写，系统编写的部分智能合约接口如表 2 所示。

表 2 智能合约接口说明

Tab.2 Description of smart contract interface

接口名称	接口描述
encrypt	数据加密接口
decrypt	数据解密接口
queryOrderInfo	查询交易订单信息
addOrderInfo	发布交易订单信息
queryProInfo	查询水产品养殖信息
addProInfo	发布水产品养殖信息

链码的主要功能包括发布和查询水产品养殖信息、水产品交易数据信息和问题投诉信息。根据组织的不同安装对应的链码，链码部署成功后首先会调用 Init 方法进行系统的实例化，然后执行 Invoke 方法发起交易执行定义的业务功能。以水产品养殖信息发布为例，当用户在客户端执行养殖信息发布操作时，数据存储的业务逻辑如图 5 所示。

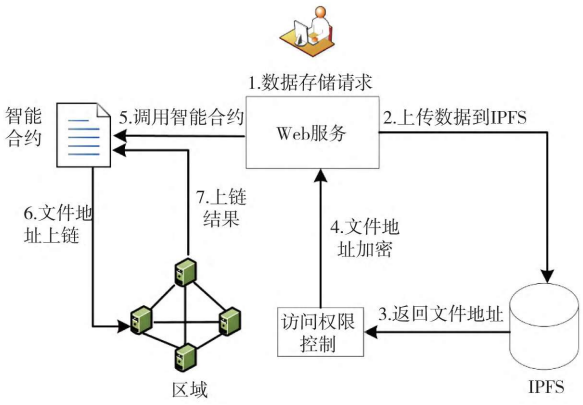

图 5 养殖信息上传流程图

Fig.5 Flow chart for uploading breeding information

用户登录成功后会发起数据发布请求,首先会进行权限认证验证节点身份信息,然后执行文件上传操作将数据提交到 IPFS 中并返回存储该文件的地址 Hash 值,再将返回的地址 Hash 值进行加密,最终通过调用智能合约将加密后的地址 Hash 值通过底层共识机制完成上链。

当用户需要查询水产品养殖信息时,数据查询的业务逻辑如图 6 所示,用户在前端界面发起查询请求后,节点首先进行身份验证获取访问权限,然后调用智能合约执行查询操作,从区块链上获取 IPFS 地址 Hash 值密文,再将地址 Hash 值进行解密,最终根据地址 Hash 值从 IPFS 中获取原始数据返回给前端用户。

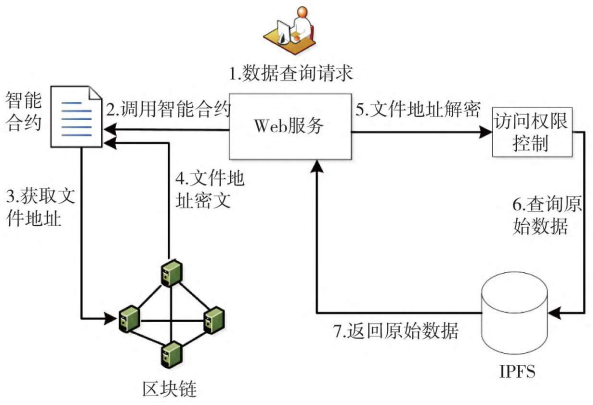

图 6　养殖信息查询流程图

Fig.6　Breeding information query flow chart

4　系统测试与分析

4.1　功能测试

在虚拟机 VMware 中完成水产品交易溯源系统环境的搭建,操作系统为 Ubuntu16.4。虚拟机的配置为内存 2 GB,硬盘为 40 GB,Hyperledger Fabric 版本为 1.2,采用 JavaScript 进行 Web 服务开发。

在 Fabric 网络环境中,系统采用单机多节点部署的方式,通过在 Cryptogen 模块中配置 3 个节点来模拟系统中的 Org1、Org2 和 Org3 共 3 个组织,每个组织下分别有 peer0 和 peer1 共 2 个节点。系统首先生成每个节点的证书文件并存放在本地,然后执行创建通道的命令,根据业务规则创建 2 个私有通道 channel1 和 channel2,同时执行命令将对应节点加入通道内,最后在每一个组织节点中安装链码完成网络启动。用户在登录时会对节点身份证书进行认证,只有在证书认证通过以后才可以进行操作。

水产品交易溯源系统提供的功能包括水产品养殖数据、订单数据和问题反馈信息的发布和查询。当用户登录系统后,系统访问权限控制模块会根据当前用户所在组织的权限,控制用户可以执行哪些业务功能。如当登录养殖厂用户 peer0org1,用户所在组织为 Org1MSP,节点发起交易订单数据发布请求后,首先需要在前端用户界面输入订单交易数据的相关信息,然后节点会调用安装在 Org1 组织内的智能合约执行上链操作。操作是在一个单独的通道内完成,对于未订阅该通道的组织和用户,所有的数据都是不可见的。订单数据发布成功之后,拥有权限的组织内的节点可以根据订单编号查询该订单的详细信息进行验证。如图 7 和图 8 分别为根据交易订单编号查询订单详细信息和根据水产品编号查询水产品养殖信息,系统首先验证当前 peer 节点的证书 keyStore 是否正确,验证成功后调用智能合约执行相应的业务逻辑返回结果。

图 7　交易订单数据查询界面

Fig.7　Transaction order data query interface

图 8　水产品养殖信息查询界面

Fig.8　Aquatic product breeding information query interface

4.2 性能测试

对于系统整体性能，主要关注系统的吞吐量（Transaction Per Second，TPS）。采用 HyperLeager 项目中的 Caliper 性能测试框架，测试在系统交易量为 100~700 笔/s 时，吞吐量的变化情况。如图 9 所示，横坐标表示交易的并发数，纵坐标表示系统吞吐量，当发送请求数量在 0~200 次/s 之间时，系统吞吐量呈稳步上升趋势。当发送请求数超过 200 次/s 时，系统吞吐量在 220 笔/s 左右波动，此时已经为系统最大吞吐量。

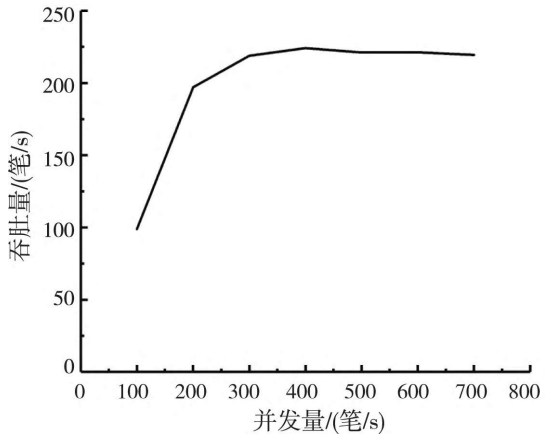

图 9 系统吞吐量测试结果

Fig.9 System throughput test results

通过对系统的功能和性能进行测试和分析可知，系统功能的有效性得到了验证，性能上 220 笔/s 交易的吞吐量可以应用于生产实践[30]，完成了预期的设计目标。将本研究提出的模型与其他几篇文献模型对比如表 3 所示。

表 3 方案性能对比

Tab.3 Scheme performance comparison

功能	文献[19]	文献[20]	文献[21]	文献[22]	本文方案
去中心化	是	是	是	是	是
访问控制	否	是	否	是	是
隐私保护	是	是	是	是	是
结合 IPFS	是	否	否	否	是

可以发现，5 篇文章的模型都是基于区块链去中心化的特点实现了数据的发布和追溯功能。文献[19]和文献[21]均没有访问控制机制，本模型进行了完善的通道设计，并且通过智能合约来进行访问控制，数据的隐私性较好。除此之外，文献[20-22]均未将区块链与分布式文件系统相结合，数据直接存储在区块链网络上，本模型结合 IPFS 的存储方案使得该模型在进行大文件存储时有更好的适用性。但是，本研究模型未采用物联网、传感器设备实时采集数据，下一步可将区块链技术与物联网技术相结合，进一步提升数据的可信性。

5 结论

本研究从水产品交易流程出发，提出了一种基于区块链的水产品交易溯源模型，基于 Fabric 技术框架和分布式数据存储方案 IPFS 实现了该系统。通过区块链去中心化的特点和共识机制解决了水产品交易数据在中心化存储模式下面临的安全问题，同时利用分布式文件系统 IPFS 降低了链上的数据存储压力。在此基础上，进行了多通道设计和访问权限控制，用户只能访问所在通道内的数据，提高了数据的隐私性。从性能上看吞吐量为 220 笔/s 左右，方案的可行性和有效性得到了验证。在水产品供应链交易中引入区块链技术，保证供应链中数据的完整性和安全性，防止信息孤岛和篡改。这些数据对于水产品的质量安全监控，以及提升养殖厂的经济效益具有很大的作用，为整个水产品供应链良性运转提供了保障。

□

参考文献

[1] 鲁泉，陈新军.改革开放 40 年来中国渔业产业发展及十四五产量预测[J].上海海洋大学学报，2021，30(2)：339-347.

[2] 陈艳，王路，韩立民.基于物联网的水产品冷链供应链集成管理体系—框架及运作机制[J].保鲜与加工，2020，20(1)：191-199.

[3] 郑建明，廖尹航.我国水产品质量安全可追溯治理问题考察及其对策[J].江苏农业科学，2018，46(24)：5-9.

[4] 王丽娟.基于区块链技术的水产品质量追溯体系研究[J].乡村科技，2019(9)：119-120.

[5] 苏庆玲，朱晓娜，许婷，等.基于区块链的水产品质量追溯体系的设计[J].中国渔业质量与标准，2019，9(4)：5-12.

[6] SHAMSHAD S，MAHMOOD K，KUMARI S，et al. A secure blockchain-based e-health records storage and sharing scheme[J]. Journal of Information Security and Applications，2020，55：102590.

[7] SADIQ A，JAVED M U，KHALID R，et al. Blockchain based data and energy trading in internet of electric vehicles[J]. IEEE Access，2020，9：7000-7020.

[8] 张亮，张翰林，孔凡玉.基于 Ethereum 的房地产供应链系统设计与实现[J].计算机工程与应用，2020，56(3)：214-223.

[9] RIFI N，RACHKIDI E，AGOULMINE N，et al. Towards using blockchain technology for IoT data access protection[C]. 2017 IEEE 17th international conference on ubiquitous wireless

broadband (ICUWB).IEEE,2017:1-5.
[10] 韩璇,袁勇,王飞跃.区块链安全问题:研究现状与展望[J].自动化学报,2019,45(1):206-225.
[11] 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.
[12] 蔡维德,郁莲,王荣.基于区块链的应用系统开发方法研究[J].软件学报,2017,28(6):1474-1487.
[13] REID F,HARRIGAN M.An analysis of anonymity in the bitcoin system[M].New York:Security and privacy in social networks.Springer,NY,2013:197-223.
[14] DENNIS R,OWEN G.Rep on the block:A next generation reputation system based on the blockchain[C].2015 10th International Conference for Internet Technology and Secured Transactions (ICITST).IEEE,2015:131-138
[15] 许继平,孙鹏程,张新.基于区块链的粮油食品全供应链信息安全管理原型系统[J].农业机械学报,2020,51(2):341-349.
[16] 魏立斐,朱嘉英,衡旭日.基于区块链技术和 HACCP 管理的智能化水产品质量安全溯源系统的设计与实现[J].渔业现代化,2020,47(4):89-96.
[17] 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.
[18] XIE C,SUN Y,LUO H.Secured data storage scheme based on block chain for agricultural products tracking[C].2017 3rd International Conference on Big Data Computing and Communications (BIGCOM).IEEE,2017:45-50.
[19] HAO J T,SUN Y,LUO H.A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking[J].Journal of Computers,2018,29(6):158-167.
[20] 葛艳,黄朝良,陈明.基于区块链的 HACCP 质量溯源模型与系统实现[J].农业机械学报,2021,52(6):369-375.
[21] 李梦琪,杨信廷,徐大明.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.
[22] 赵磊,毕新华,赵安妮.基于区块链的生鲜食品移动追溯平台框架重构[J].食品科学,2020,41(3):314-321.
[23] CHEN Y,LI H,LI K,et al.An improved P2P file system scheme based on IPFS and Blockchain[C].2017 IEEE International Conference on Big Data (Big Data).IEEE,2017:2652-2657.
[24] 范贤丽,范春晓,吴岳辛.基于区块链和 IPFS 技术实现粮食供应链隐私信息保护[J].应用科学学报,2019,37(2):179-190.
[25] 王可可,陈志德,徐健.基于联盟区块链的农产品质量安全高效追溯体系[J].计算机应用,2019,39(8):2438-2443.
[26] 黄立波,王伟,徐彦军,等.基于区块链的数字结业证书管理系统及其性能评估[J].华东师范大学学报(自然科学版),2020(6):72-81.
[27] 靳世雄,张潇丹,姚忠将,等.区块链共识算法研究综述[J].信息安全学报,2021,6(2):85-100.
[28] 赵文婷,沈蒙,金智新,等.区块链技术下的电力智能交易研究[J].太原理工大学学报,2020,51(3):331-337.
[29] 陈宇翔,张兆雷,刘地军,等.区块链的税收智能合约设计[J].通信技术,2018,51(6):1384-1390
[30] 张朝栋,王宝生,邓文平.基于侧链技术的供应链溯源系统设计[J].计算机工程,2019,45(11):1-8.

Research and implementation of aquatic product transaction traceability system based on blockchain

FENG Guofu,HU Junhui,CHEN Ming

(1 *College of Information Technology,Shanghai Ocean University,Shanghai* 201306,*China*;
2 *Key Laboratory of Fisheries Information,Ministry of Agriculture and Rural Affairs,Shanghai* 201306,*China*)

Abstract:Aiming at the problems of the traditional aquatic product transaction traceability system,such as centralized and easy to tamper,data cannot be shared,and credible traceability difficulties,a traceability model of aquatic product transactions based on the combination of blockchain and InterPlanetary File System (IPFS) is proposed. By analyzing the aquatic product transaction process,the key information of aquatic product breeding and order transaction information are stored in IPFS,and the IPFS address is uploaded to the blockchain network.Based on the alliance chain platform Hyperledger Fabric,the prototype of the system was realized,the system access control scheme was designed,and the smart contract suitable for the system was proposed to ensure the safe and reliable storage of transaction data.The results show that the system can realize the release and query of transaction data,and consumers and regulatory authorities can realize the credible traceability of aquatic product breeding information; the system throughput can reach about 220 transactions per second,which basically meets the aquatic product transaction data Business requirements for storage and traceability.This research can provide a reference for the traceability technology of aquatic product transactions.

Key words:blockchain; aquatic products trading; traceability; IPFS; smart contract