doi:10.6041/j.issn.1000-1298.2024.06.029

基于多链存储优化的水产品交易匹配模型研究

王文娟[1,2]　汪海燕[1]　陈　明[1,2]　邹一波[1,2]　葛　艳[1,2]

(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:区块链技术应用到水产品线上交易架构中可以使交易双方隐私信息得到基本保障,然而,目前区块链水产品线上交易模型和系统存在海量数据存储负载大、维护成本高、数据查询效率低等问题。为进一步缓解以上问题,在梳理和分析水产品交易流程基础上,根据水产品交易业务技术需求,提出了基于多链存储优化的水产品交易匹配模型。该模型在智能合约中通过贪心算法实现了效率较高的多属性水产品线上交易匹配过程,通过区块链多通道技术构建了水产品交易多链架构,实现了用户交易信息分布式存储,提高了交易信息查询效率,同时,采用区块链与本地数据库双模式存储技术,缓解了区块链网络中各个节点海量数据存储的负载。基于 Hyperledger Fabric 平台实现了基于多链存储优化的水产品交易原型系统。该原型系统测试结果表明,临界值 900 s 平均最多可以完成 1 296 笔交易,说明系统在处理千条交易数据量时可以正常运行,满足水产品线上交易平台日常实际交易业务需求,同时在链上存储 1 600 条合同信息时查询 1 条用户合同信息平均时间为 4.018 s,多链存储结构提高了链上数据查询速度。

关键词:水产品交易;区块链;多链存储;交易匹配模型;贪心算法

中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1000-1298(2024)06-0272-12　　**OSID**:

Aquatic Product Trading Matching Model Based on Multi-chain Storage Optimization

WANG Wenjuan[1,2]　WANG Haiyan[1]　CHEN Ming[1,2]　ZOU Yibo[1,2]　GE Yan[1,2]

(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: The application of blockchain technology in the online trading architecture of aquatic products can provide basic protection for the privacy information of both parties involved in the transaction. However, currently, blockchain-based aquatic product online trading models and systems are suffering from problems such as large data storage loads, high maintenance costs, and low data query efficiency. To further alleviate the above problems, based on the sorting and analysis of the aquatic product trading process, and according to the technical requirements of aquatic product trading business, a trading matching model for aquatic products based on multi-chain storage optimization was proposed. This model achieved a highly efficient multi-attribute online trading matching process for aquatic products through greedy algorithms in smart contracts, and constructed a multi-chain architecture for aquatic product online trading through blockchain multi-channel technology, achieving distributed storage of user transaction information and thus improving the efficiency of transaction information query. Meanwhile, this trading matching model adopted a dual storage technology of blockchain and local database, which alleviated the load of massive data storage at various nodes in the blockchain network. Then, a prototype system for aquatic product online trading based on multi-chain storage optimization was implemented on the Hyperledger Fabric platform. The performance test results of the prototype system indicated that it took 900 s to complete 1 296 transaction matchings on average, indicating that the system can operate normally when processing a volume of thousands of transaction data, meeting the needs of the online trading platform for aquatic products. At the same time, when storing 1 600 contract information on the chain,

收稿日期:2024-03-22　修回日期:2024-04-19

基金项目:广东省重点领域研发计划项目(2021B0202070001)

作者简介:王文娟(1983—),女,副教授,博士,主要从事水产品质量溯源和撮合交易机制研究,E-mail:wangwj@shou.edu.cn

通信作者:陈明(1966—),男,教授,博士,主要从事智慧水产养殖和水产品追溯技术研究,E-mail:mchen@shou.edu.cn

the average time to query a user's contract information was 4.018 s, which indicated that the multi-chain data storage structure improved the speed of on-chain data queries.

Key words: aquatic product trading; blockchain; multi-chain storage; trading matching models; greedy algorithms

0　引言

联合国粮食及农业组织发布的《2022 年世界渔业和水产养殖状况》数据显示，我国水产品养殖基数庞大，占世界水产品养殖总量的 61.65%[1]。养殖户企业为了确保经济效益，需要对水产品进行快速交易。传统交易方式中，水产品养殖企业与买方均需进行线下交易，存在买卖双方严重信息不对称、交易效率低等问题。随着电子商务的快速发展，水产品线上交易占比逐年扩大，但水产品电子商务平台存在着海量交易数据易被篡改、存储负载大、交易效率低等问题[2]，亟需一种先进的水产品线上交易匹配解决方案，保障其交易的安全性，同时缓解数据存储压力并提高交易效率。

凭借其去中心化[3-6]、可追溯性[7-9]、集体维护、不可篡改[10]、公开透明[11]等特性，区块链可以作为保障水产品线上交易安全的底层技术，保障交易双方信息的真实可靠性。然而，目前国内外学者主要将区块链技术引入到水产品溯源领域，涵盖了水产品养殖关键信息存储[12-13]、水产品加工信息存储[14-16]、水产品流通环节跟踪[17-18]等内容，仅有部分学者尝试将其应用到水产品线上交易环节中。文献[19]提出了基于区块链的水产品交易溯源系统模型，但该模型仅能实现交易数据的上链发布和查询，不能涵盖线上交易业务过程。文献[20]使用鸟群觅食算法构建了水产品线上交易模型。文献[21]首次利用优化的蚁群算法，自动撮合一个时间段内的供应单与需求单进行交易，交易过程的数据通过区块链单链结构进行存储。文献[22]又将信用机制引入到水产品区块链撮合交易平台中，为交易双方提供透明的交易评估与信用信息，有效避免人为的故意违约行为，保障交易质量，提高交易双方的满意度，但其用户信息、水产品供需信息、合同信息等仍然采用区块链单链结构进行存储。将区块链技术引入到水产品交易环节中，保障其交易安全性，但海量交易数据存储以及交易信息查询效率优化的问题并未得到解决，区块链技术运用到水产品交易环节的研究仍处于初探阶段。

区块链多链技术在超级账本(Hyperledger)项目中被称为多通道技术，是该项目中的一个新功能[23]。当系统中的节点被分成多条链时，每条链由不同的节点组成并维护特定数据。在这种模式下，节点只需维护其所属链上的数据，这种分离数据的方式有助于降低区块链存储压力，减少数据处理负担。部分学者尝试将区块链多链技术应用到农产品[24-26]或水产品质量溯源与监管模型[27]中，提高数据存储和查询的效率，验证了多链结构的可行性和优越性。本文将继续拓展该领域研究，将区块链多链技术应用到水产品线上交易环节，用以优化线上海量交易数据存储结构，提升交易信息查询速度，提高水产品线上交易匹配效率。

本文首先对水产品交易过程的业务流程进行分析，构建基于多链存储优化的水产品交易匹配模型。然后，阐述模型设计的相关技术与智能合约设计方案。最终，在 Hyperledger Fabric 平台中实现以水产品养殖户企业为中心的水产品线上交易原型系统，并结合案例数据，对该原型系统性能进行测试分析。

1　基于区块链多链存储优化的水产品交易模型

1.1　水产品线上交易业务流程

水产品线上交易系统包含 3 类角色主体，即交易平台管理者、水产品养殖户企业、消费者。在不同的环境中交易的对象与交易的需求是不一样的，在以养殖户企业为中心的水产品交易中，由于水产品具备易腐蚀性，为了最大化销售力度，需要针对不同的消费者制订不同的价格优惠策略。从自身需求差异出发，水产品线上消费者可以分为批发商企业、餐饮企业与个体用户。因此，平台管理员首先需要对消费者进行身份认证与审核，同时为了减轻区块链数据存储压力，设计了一个具有 5 个通道的多链存储架构，使用 Kafka 共识协议，分别存储养殖户企业、批发商企业、餐饮企业、个体用户的注册信息以及供应单、需求单哈希值，以及交易合同明文信息。

水产品线上交易业务流程包括：用户信息注册与审核、养殖户企业发布供应单信息与消费者发布需求单信息、交易匹配、交易合同信息上链与合同信息查询 4 个阶段，如图 1 所示。

(1)用户信息注册与审核。在水产品交易系统中，用户需注册基本信息，管理员需对养殖户企业与消费者注册信息进行审核与身份认证，以确保交易的安全性和合法性，若用户注册的信息真实与合理，

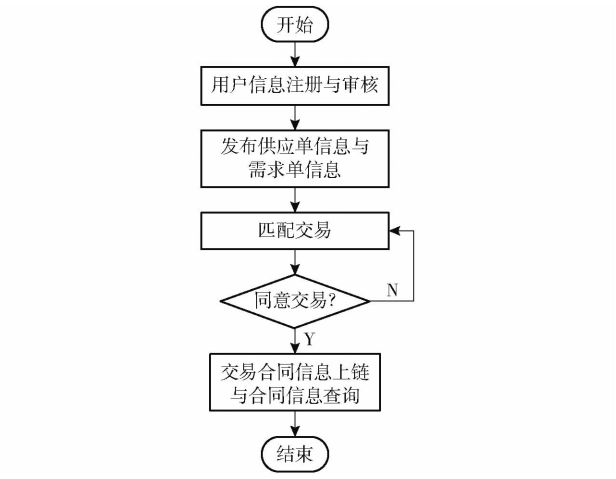

图 1 水产品线上交易匹配的业务流程

Fig. 1 Business process of aquatic product online trading matching

则审核通过,否则提示用户重新注册。在智能合约中调用 SHA-3-256 算法对审核通过的养殖户企业信息、批发商企业信息、餐饮企业信息与个体消费者信息分别进行哈希值计算,并将其哈希值上传至对应的通道中。

(2)养殖户企业发布供应单信息与消费者发布需求单信息。用户登录成功后,具备了自主发布水产品信息的权限。养殖户企业需要在发布供应单信息栏中,添加供应单信息。消费者根据实际需求,添加需求单信息。系统自动对提交的供应单信息与需求单信息进行格式化审查,核查供应单与需求单中水产品属性字段是否符合系统设置的属性约束,确保数据一致性与安全性。然后,在智能合约中调用 SHA-3-256 算法对供应单信息和需求单信息分别进行哈希值计算,并将其哈希值上传至对应的通道中。

(3)交易匹配。平台自动收集用户在上一个周期内新提交的供应单信息与需求单信息,以及上一周期内用户拒绝交易的供应单与需求单信息,在智能合约中调用匹配算法实现交易匹配,并将匹配结果返回给用户。

(4)交易合同信息上链与合同信息查询。用户根据平台自动匹配的结果来决定是否进行交易,如果匹配结果中有一方拒绝交易,用户对应的供应单或需求单将进入下一个周期重新进行交易匹配。若双方都接受匹配结果,则以双方报价的平均值作为成交价格,并按照消费者提出的数量自动生成交易合同,并调用智能合约将合同上链。之后,交易双方可以随时通过智能合约查看链上的历史交易合同信息。

1.2 水产品多链存储优化交易匹配模型

现有的水产品区块链交易模型均采用单链架构的存储方式,将不同类别的用户与交易信息直接上传到区块链网络中,随着交易数据越来越多,节点数量逐渐增加,数据不仅上传速度慢而且容易造成阻塞、丢失的问题,需要付出更多的维护成本。并且,在区块链单链结构中,查询用户信息、供应单信息、需求单信息或交易合同信息时均需要遍历整条链,查询效率较低[28]。针对以上问题,根据图 1 所示的水产品线上交易匹配的业务流程,搭建了如图 2 所示的水产品多链存储优化的交易匹配模型。整个交易匹配模型分为 4 个模块:区块链多通道网络、数据处理与优化存储、供应单与需求单交易匹配、链上信息查询。

(1)区块链多通道网络。该模型基于区块链多通道技术设计了具有 5 个通道的多链存储架构,利用 Kafka 共识协议分别存储养殖户企业注册信息及供应单信息哈希值(通道 1)、批发商企业注册信息及需求单信息哈希值(通道 2)、餐饮企业注册信息及需求单信息哈希值(通道 3)、个体户注册信息及需求单信息哈希值(通道 4)、交易合同明文信息(通道 5)。多通道网络实现了数据分布式存储,提高了链上信息的存储和查询效率。

(2)数据处理与优化存储。管理员完成审核与身份认证以及系统自动对供应单与需求单校对后,为减轻链上数据存储负载,需要对 5 个通道中的 5 类数据进行存储优化。该模型采用链上与本地数据库相互协同技术,除通道 5 存储了实际交易合同信息外,其他 4 个通道均存储对应明文信息的哈希值,大大节省了链上存储空间。

通道 1~4 数据存储优化的具体实现过程如下:将本地数据库存储的每一条用户注册信息、供应单信息或需求单信息作为一个信息对象,通过智能合约调用哈希算法 SHA-3-256 将其转换为 64 位十六进制的哈希值,再经过数字签名技术进行安全性验证,确认无误后将哈希值分别写入到相应的通道并返回其 key 键值,最后将 key 键的信息写入到本地数据库与之相对应的用户注册信息、供应单信息或需求单信息中。

通道 5 存储交易合同信息的明文信息,一旦合同信息被丢失或篡改,数据不可恢复。为了保证合同信息不被篡改,通道 5 里存储交易合同信息的明文信息,具体实现方式为:交易合同信息通过智能合约按时间顺序上链,数据在区块链中的存储结构,是通过计算出相邻交易合同信息的哈希值,进而两两结合形成新的哈希值,这些新的哈希值构成 Merkle tree,树根的哈希值存储在区块头部。同时,区块头部包含区块号、当前区块哈希

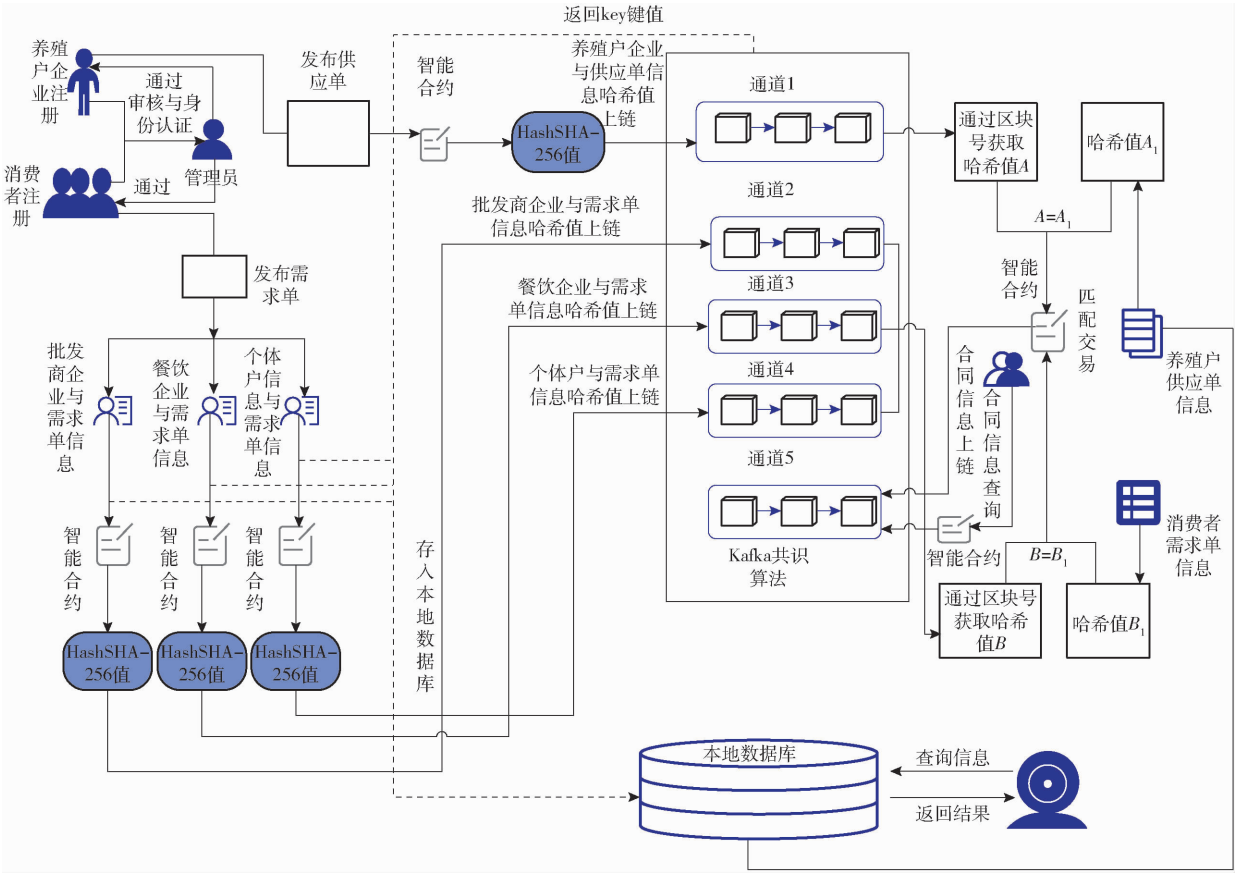

图 2　水产品多链存储优化交易匹配模型

Fig. 2　Trading matching model for aquatic products based on multi-chain storage optimization

值、前一区块哈希值、时间戳等信息，构建了区块链的链式结构。

(3)供应单与需求单交易匹配。供应单与需求单交易匹配环节中，交易匹配模型将 1 d 划分为 24 个周期，以整点作为周期开始和结束。在本模型中，养殖户企业和消费者可以在任意时间发布供应单与需求单信息。每个周期开始时，系统会自动地从本地数据库获取上一周期内养殖户企业的供应单信息和消费者的需求单信息，以及上一周期内拒绝交易的供应单信息与需求单信息，并对其信息进行逐条哈希计算与哈希值校对。以某个养殖户企业的供应单信息与某消费者的需求单信息为例，从对应通道中获得的链上数据分别为哈希值 A 与哈希值 B，系统同时通过本地数据库中区块号获取存储在区块链上某养殖户企业供应单信息的哈希值 A_1，以及某消费者需求单信息的哈希值 B_1。然后进行一致性校对，若 $A=A_1$，$B=B_1$，则证明数据未被篡改，允许正常交易；否则，系统将要求用户重新输入正确供应单或需求单信息，为了不影响本周期的执行时间，信息被篡改的用户需进入后续周期内再进行匹配。

在交易匹配过程中，系统需在 1/4 周期(15 min)内完成供应单与需求单信息的收集与哈希值校对，并在接下来的 1/4 周期(15 min)内在智能合约中调用贪心算法进行水产品自动交易匹配，匹配结果将返回给用户。在最后的 1/2 周期(30 min)内用户需做出反馈，若双方均同意交易，系统则自动生成交易合同并将其上传至链上通道 5 中；若任意一方拒绝交易，其对应需求单或供应单则自动进入下一个周期内重新进行匹配。

(4)链上信息查询。养殖户企业和消费者可以随时查询自己的注册信息或供应单、消费单信息，并自查信息是否被篡改。具体实现过程与交易匹配的第 1 阶段相似：从本地数据库检索自己信息，获取相关区块号，系统会自动地逐条计算用户信息、供应单信或需求单信息的哈希值，同时根据所获取的区块号查询对应在区块链网络中的哈希值，将二者进行校对，若两者相同则证明对应信息未发生篡改，系统将通过本地数据库将用户信息返回给用户；若两者不相同则证明相关信息已发生篡改，提示用户重新上传注册信息、供应单信息或需求单信息。当用户查询交易完成后的链上合同信息时，利用 key 键遍历查询，从最新的区块依次向前一个区块遍历，获得相匹配的 key 键，从而将交易合同信息的 value 值返回给用户。

2 关键技术

2.1 哈希算法

哈希算法是一种将任意长度的输入数据映射为固定长度输出数据(通常称为哈希值或散列值)的算法。安全散列算法(Secure Hash algorithm,SHA)是当前广泛使用的哈希算法之一,由美国国家安全局(National Security Agency,NSA)设计,其标准化和管理由美国国家标准与技术研究所(National Institute of Standards and Technology,NIST)负责[29]。SHA 算法是单向散列算法,通常难以逆向计算原始输入,且对相同的输入信息 M,函数总能计算出相同输出 $h(M)$。SHA 算法包括 SHA-1、SHA-2 和 SHA-3 等不同版本。目前,SHA-3 算法在区块链技术中被认为提供了较高的安全性和可靠性,其计算是非常敏感的,输入数据信息的微小变化,也会导致相应哈希值的显著差异[30],因此 SHA-3 在一定程度上解决了哈希值碰撞的问题。SHA-3 系列包含 4 个加密哈希函数:SHA-3-224、SHA-3-256、SHA-3-384 和 SHA-3-512[31-32]。SHA-3-256 提供了良好的安全性和计算效率平衡。相对 SHA-3-224 和 SHA-3-384,SHA-3-256 在与其他进制进行转换时更为方便;同时,SHA-3-256 输出长度相对较短,相比于 SHA-3-512 更节省存储空间。因此,本模型采用 SHA-3-256 算法,具体实施的方式是首先导入哈希算法库,然后信息对象直接调用 SHA 库生成一个 64 位十六进制字符的哈希序列值。

2.2 交易匹配算法

交易匹配算法使用贪心算法,贪心算法的核心思想是每次选择当前状态下的最优解,而不考虑其对未来决策的影响,即以局部最优解为先而可能导致无法获得全局最优解。这种算法的优点在于简单易实现,执行速度快。求解最小生成树[33-34]与背包问题[35]等是贪心算法的一些经典应用场景。

在水产品交易匹配中,将每一条供应单信息与需求单信息匹配视为一个子问题,在每个子问题中选择从多个交易属性进行匹配以达到局部匹配最优解,通过每次选择局部最优解,最终完成所有需求单与供应单的匹配,符合贪心算法的核心思想。每一次局部匹配不会影响接下来其他供应单与需求单的局部匹配,满足贪心算法的特性。因此,可以将贪心算法运用到水产品线上交易匹配。同时,贪心算法实现简单,不需要复杂的数据结构,能够快速进行交易匹配,从而提升买卖双方交易信息匹配效率。贪心算法用于水产品线上交易匹配的整体思路如图 3 所示。

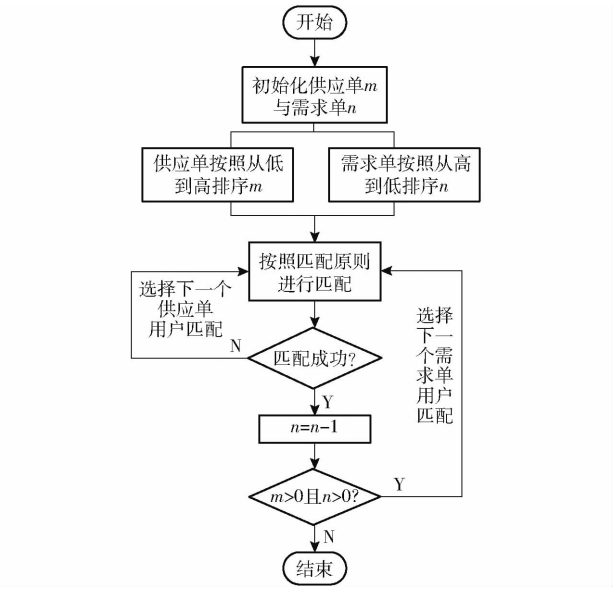

图 3 交易匹配算法流程图

Fig. 3 Flowchart of trading matching algorithm

本文选择贪心算法进行线上交易匹配时,每次局部匹配需满足以下 4 个属性约束条件:

(1)消费者报价大于等于养殖户企业报价。

(2)消费者订单数量小于等于养殖户企业库存数量。

(3)消费者收到水产品鲜活度不能低于需求单上的鲜活度。本文水产品鲜活度参考标准为 SC/T 3048—2014《鱼类鲜活度指标 K 值的测定》[36],具体新鲜度的等级核算参考文献[21],根据 K 值范围和水产品新鲜度等级划分如下:低于 10%,对应水产品新鲜度等级为 3(非常新鲜);[10%,20%),对应水产品新鲜度等级为 2(比较新鲜);[20%,50%],对应水产品新鲜度等级为 1(适度新鲜);高于 50%,对应水产品新鲜度等级为 0(不新鲜)。

(4)消费者收到的产品单体质量与需求单上的单体质量要求差异不能大于 50 g。

基于以上 4 个属性约束条件,本文中贪心算法(matchSupplyAndDemand)的设计如下:

```
1. sort.Sort(ByPrice(orders)) // 将供应单信息与需求单信息按照价格升序排列
2. for i := 0; i < len(orders) - 1; i++ {
3. supplyOrder := orders[i] // 如果当前订单是供应单,则寻找需求单进行匹配
4. if supplyOrder.Type == "养殖户企业" {
5. for j := i + 1; j < len(orders); j++ {
6. demandOrder := orders[j]
7. if (demandOrder.Type == "餐饮企业" || demandOrder.Type == "个体户" || demandOrder.Type == "批发商企业") &&demandOrder.Price >
```

= supplyOrder. Price&&demandOrder. Vividness < = supplyOrder. Vividness&&demandOrder. Quantity < = supplyOrder. Quantit{ //判断需求单是否满足条件进行交易,满足条件匹配成功

8. tradeQuantity : = min (supplyOrder. Quantity, demandOrder. Quantity) //拟计算交易数量

9. supplyOrder. Quantity - = tradeQuantity
demandOrder. Quantity - = tradeQuantity

10. tradeRecord : = TradeRecord{ SupplyOrderID: supplyOrder. ID, DemandOrderID: demandOrder. ID, Quantity: tradeQuantity, Price: supplyOrder. Price, //拟更新部分交易信息}

11. tradeRecords = append (tradeRecords, tradeRecord)

12. if supplyOrder. Quantity = = 0 { break} //供应单的数量已经减到 0,则表示供应单已经满足了需求,因此可跳出内层循环,继续下一个供应单匹配

}}}

2.3　智能合约设计

智能合约是部署在区块链网络节点上用来与分布式账本交互的程序代码。作为一种由事件触发而自动运行在区块链上的代码[37],智能合约能够促成线上水产品可信交易,并保障交易信息可追溯与防篡改性[38]。本文提出的基于多链存储优化的水产品线上交易匹配模型中涉及的智能合约如下:

(1)用户信息、供应单信息与需求单信息上链(Information_chain)。由于用户信息、供应单信息与需求单信息三者哈希值转化与信息上链类似,此处以用户信息上链为例进行详细说明。

输入:用户需上传用户名(name_ID)、企业名称(个体户不需要输入)(company_Name)、法定代表人(个体户不需要输入)(legalRepresentative)、密码(passWord)

输出:返回 key 键

1. import ("crypto/sha256" //计算信息的 SHA-3-256 哈希值
"encoding/hex" //将 256 位哈希值转换为十六进制字符串
"encoding/json" //将用户信息换为 JSON 字符串)

2. userInfo : = &user{ name_ID, company_Name, legalRepresentative, passWord} //创建用户信息

3. userInfoJSON, err : = json. Marshal(userInfo) //将用户信息转换为 JSON 字符串

4. if err ! = nil { return " ", fmt. Errorf("
failed to marshal user info: %w", err) } //返回错误,指明用户信息转换为 JSON 字符串失败

5. hasher : = sha256. New( )
hasher. Write(userInfoJSON)
hash : = hasher. Sum(nil) //计算用户信息的 SHA-3-256 哈希值

6. hashString : = hex. EncodeToString(hash) //将哈希值转换为十六进制字符串

7. err = ctx. GetStub( ). PutState("hashValue", []byte(hashString)) //将用户信息的哈希值存储到区块链上("hashValue" 作为存储在区块链的 key 键,"[]byte(hashString)" 作为存储在区块链的 value 值)

8. if err ! = nil { return "", fmt. Errorf("failed to put state: %w", err) } //返回错误,指明用户信息存储到区块链失败

9. return "hashValue", nil //返回用户信息哈希值的位置

(2)交易匹配(TransactionMatching)。本周期开始时,系统会自动地从本地数据库收集上一周期提交的供应单(suppleInfo)与需求单信息(demandOrder),以及上一周期内拒绝交易的需求单信息或供应单信息。首先使用哈希值校对(HashValueProofreading)智能合约对供应单信息和需求单信息的链上哈希值与本地数据库明文信息转换的哈希值进行校对。哈希值校对通过之后,再通过调用贪心算法进行供应单与需求单的的自动交易匹配,确认匹配结果,自动生成合同,存储在区块链上逻辑代码如下:

1. hashesJSON, err: = ctx. GetStub( ). GetState("hashValue") //从区块链状态数据库中获取键为 "hashValue" 的值(供应单或需求单的哈希值),并将结果存储在 hashesJSON 变量中

2. If err! = nil{ return false, fmt. Errorf ("failed to get state for hashes: %w", err) } //检查是否有错误发生,如果发生错误,说明无法获取状态值,返回一个错误信息

3. if hashesJSON = = nil{ return false, fmt. Errorf ("data not found for hashes") } //检查从区块链上获取的值是否为 nil,如果为 nil,说明在区块链上没有存储对应的值,返回一个错误信息

4. var hashes SupplyDemandHashes //声明一个变量 hashes,类型为 SupplyDemandHashes,用于存储从区块链上获取的供应单和需求单的哈希值

5. err = json. Unmarshal(hashesJSON, &hashes) //将从区块链上获取的哈希值的 JSON 表示解析为 SupplyDemandHashes 结构,并存储在 hashes 变量中

6. if err ! = nil { return false, fmt. Errorf("failed to

unmarshal hashes: %w", err) }//如果解析过程中发生错误,则返回错误信息

7. if strings. Compare (hashes. SupplyHash, supplyHash) = = 0 && strings. Compare (hashes. DemandHash, demandHash) = = 0

{//检查从区块链上获取的供应单和需求单的哈希值与本地计算的供应单和需求单的哈希值是否一致

8. func matchSupplyAndDemand (supplyInfo, demandInfo string) string {// 调用贪心算法实现匹配交易,代码逻辑参考 2.2 节匹配交易算法的设计} }

9. return match//匹配交易的结果返回给用户,用于用户确认交易

(3)合同信息上链(ContractInformationOnTheChain)。当养殖户企业与消费者确定交易后,系统会调用合同信息上链智能合约函数(ContractInformationOnTheChain)将交易合同明文信息上链,逻辑代码如下:

1. matchJSON, err := json. Marshal(match) //将交易匹配结果转换为 JSON 格式

2. if err ! = nil {return false, fmt. Errorf("failed to marshal match result: %w", err) }//如果转换失败,返回错误信息

3. err = ctx. GetStub ( ). PutState (" match", matchJSON)//将转换后的交易匹配结果存储在区块链上("match"表示 key 键,"matchJSON"表示 value 值(交易合同信息))

4. if err ! = nil {return false, fmt. Errorf("failed to put state for match result: %w", err) } //如果存储失败,返回错误信息

5. return true, nil//上链成功

(4)合同信息查询(QueryContract_Information)。该智能合约用以查询链上的交易合同信息,通过 key-value 形式实现,逻辑代码如下:

输入:交易合同的 key 值

输出:contractInfor(value 值)

1. contractInfo, err: = ctx. GetStub ( ). GetState ("match")//获取存储在区块链上的合同信息

2. if err ! = nil {

return nil, fmt. Errorf("failed to get state for contract info: %w", err) }//如果获取失败,返回错误信息

3. if contractInfo = = nil {

return nil, fmt. Errorf("contract info not found") }//如果合同信息为空,返回合同信息未找到的错误信息

4. return contractInfo, nil//返回合同信息

3 系统设计与实现

3.1 系统架构

基于图 2 所示的水产品多链存储优化的交易匹配模型,本文设计了图 4 所示的原型系统平台架构,包含应用层、合约层、共识层、网络层、数据层和功能层等 6 层结构。

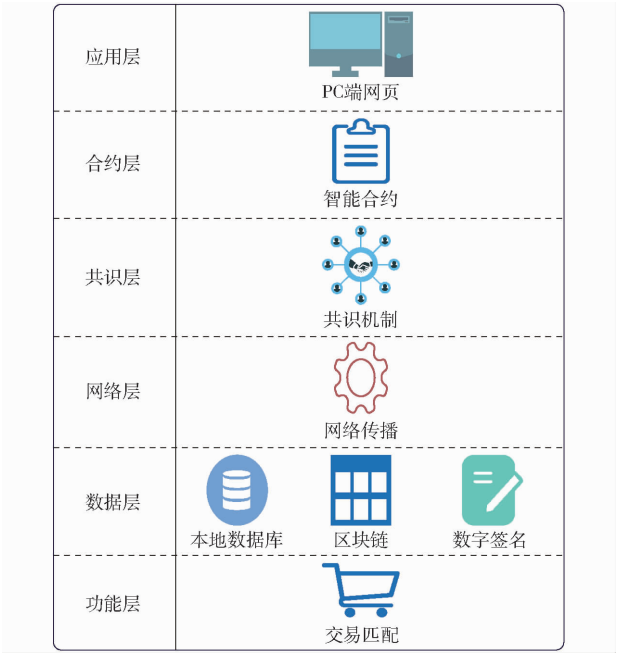

图 4 交易匹配系统架构

Fig. 4 Trading matching system architecture

应用层为用户操作提供可视化界面,平台通过网页前端获取用户上传的各种数据信息,包括用户注册信息、供应单信息、需求单信息等,同时用户也可以通过网页端查询注册基础信息、供应单或需求单信息、交易合同信息等。合约层中平台通过调用相应的智能合约函数,实现以下功能:用户信息、供应单信息、需求单信息的哈希值计算上链、哈希值校对、交易匹配、交易合同信息上链与查询等。共识层包括共识算法和节点身份认证,共识算法是一种可以在互不信任的节点之间建立信任的数学算法。网络层的核心是点对点(Peer-to-Peer,P2P)网络、数据传输、数据验证机制等。数据层包括区块数据、本地数据、数字签名、哈希值、Merkle 树等具体数据结构和存储方式。功能层展示了平台实现的主要功能为水产品线上自动交易匹配。

3.2 系统实现

本研究开发的原型系统,以 Hyperledger Fabric 的联盟链平台为底层架构,结合 MySQL 数据库,使用 JavaScript 和 Vue 框架设计与开发前端界面,采用 Go 与 Java 语言搭建后端平台。实验基于 64 位 Ubuntu,版本为 Ubuntu 16. 2. 5,内存 8 GB,磁盘空间

100 GB，Docker 版本 18.09.7，Hyperledger Fabric 版本 1.4.3，设计了 5 个通道，每个通道拥有 2 个组织与 4 个节点。以表 1 和表 2 的供应单、需求单信息为例，说明本系统实现过程和测试结果。

表 1　养殖户企业供应单信息

Tab.1　Information of supply order of farmers and enterprises

id	产品类型	个体户价格/元	餐饮企业价格/元	批发商企业价格/元	库存数量	鲜活度	单体质量/g	发货地址
famer_10495	鲫鱼	16	14	14	100 000	2	800	北京市
famer_10496	鲫鱼	19	15	14	10 000	1	800	北京市
famer_10497	鲫鱼	15	14	12	21 000	3	800	上海市

表 2　消费者需求单信息

Tab.2　Information of consumer demand list

id	产品类型	单价/元	购买数量	鲜活度	收货地址	身份	单体质量/g
329006	鲫鱼	14	900	2	北京市	餐饮	800
329009	鲫鱼	14	1 000	2	北京市	餐饮	750
329010	鲫鱼	18	2	2	上海市	个体户	800
329011	鲫鱼	14	2 000	1	河北省廊坊市	批发商	850

（1）用户信息注册与审核

在水产品交易系统中，用户在前端网页需要注册基本信息，如图 5 所示，以表 2 中 id 为 329006 的餐饮企业为例，注册信息包括：用户手动输入账号（id）、企业名称、账号、密码、确认密码与验证码。之后，企业用户需要通过图 6 界面上传营业执照照片作为认证材料，个体户消费者需通过上传身份证照片作为认证凭证。

图 5　用户信息注册界面

Fig.5　Aquatic product user information registration interface

管理员需要对养殖户企业与消费者注册信息进行审核与身份认证，以确保交易的安全性和合法性。图 7 为管理员在后台对 id 号为 329006 餐饮企业审核的界面图，审核的内容包括营业执照信息（或个人消费者身份信息）的真实性，以及用户角色与营业执照身份（或个人消费者身份证信息）是否相匹配。图 7 中 id 为 329006 用户注册的信息真实且角色与营业执照的身份相匹配，管理员则点击审核“通过”按钮，用户注册信息通过智能合约调用 SHA－3－256 哈希算法将其转化成哈希值进行上链，否则点击审核“不通过”按钮，提示用户重新输入正确的注册信息。

图 6　用户上传营业执照界面

Fig.6　User upload business license interface

图 7　管理员对消费者身份认证与审核

Fig.7　Administrator's authentication and review of consumer identity

（2）养殖户企业发布供应单信息与消费者发布需求单信息

认证通过的用户登录成功后，养殖户企业可以在“发布供应单信息”一栏中，添加供应单信息。如图 8 所示，id 为 famer_10495 的养殖户企业发布了

图 8 养殖户企业发布的供应单信息

Fig. 8 Supply order information issued by farmer companies

1 条供应单信息,信息包括:水产品类型为鲫鱼,个体户价格为 16 元,批发商企业价格为 14 元,餐饮企业价格为 14 元,库存为 100 000 条,单体质量为 800 g,鲜活度为 2,产地为北京市。消费者根据自己实际需求,在“发布需求单信息”一栏中,添加需求单信息。如图 9 所示,id 为 329006 的餐饮企业输入的 1 条需求单信息为:产品类型为鲫鱼,出价为 14 元,购买数量为 900 条,鲜活度为 2,单体质量为 800 g,收货地址为北京市。

图 9 消费者发布需求单信息界面

Fig. 9 Consumers publish demand order information interface

发布成功的供应单和需求单会通过智能合约中的 SHA-3-256 哈希算法将其转化成哈希值进行上链。

(3)交易匹配

本系统假定某一个周期内,收集到的供应单与消费单信息如表 1、2 所示。在进行交易匹配之前,需要调用智能合约对养殖户企业供应单信息与消费者需求单信息的哈希值进行校对。若数据未被篡改,则允许正常交易,调用含有贪心算法的智能合约进行自动交易匹配;否则,提示用户重新输入正确的需求单或供应单信息。

通过智能合约调用的贪心算法进行自动交易匹配后,匹配结果将返回给用户。图 10 为以 id 为 famer_10495 养殖户企业交易匹配结果返回的界面,养殖户企业 famer_10495 可以看到与图 7 输入的供应单自动匹配的全部需求单信息,包括需求单 id(系统对于每个需求单自动生成的账号)、产品类型、单价、消费者购买数量、收货地址、消费者账号(用户注册的 id 号)、消费者身份类别。养殖户企业 famer_10495 通过点击右侧的“交易”按钮,系统弹出如图 11 所示交易详情界面,当交易双方在 30 min 内都点击“确认交易”按钮时,系统自动生成交易合同信息;若有一方拒绝交易,则该供应单和需求单进入下一轮匹配。

图 10 交易匹配结果返回给养殖户企业用户界面

Fig. 10 Aquatic product matching results returned to user interface

图 11 交易匹配结果养殖户企业用户确认界面

Fig. 11 Aquatic product matching result user confirmation interface

(4)交易合同信息上链与合同信息查询

自动生成的交易合同信息调用智能合约将其上链。交易合同信息存储在第 5 个通道中,采用 key-value 的形式进行存储。当任何一方查询交易合同信息时,需要调用智能合约函数 QueryContract_Information,利用 key 键从最新区块依次向前一个区块遍历,获得相匹配的 key 键后,将交易信息的 value 值返回给查询用户。图 12 为养殖户 id 为 famer_10495 查询一个交易合同信息的界面。

3.3 系统性能测试

本文通过 Caliper 测试工具对基于多链存储优化的水产品线上交易系统进行性能测试。本研究以 1 h 为一个交易匹配周期 T,$T/4$ 的时间用于交易匹配,本实验测试临界值 900 s 平均最多可以完成 1 296 笔交易,说明系统在处理千条交易数据量时可以正常运行,满足水产品线上交易平台实际交易业务的需求,模型的有效性和实用性得到验证。为了进一步挖掘交易数据量与交易匹配时间之间的关联关系和变化趋势,本文分别对交易数据量为 100、

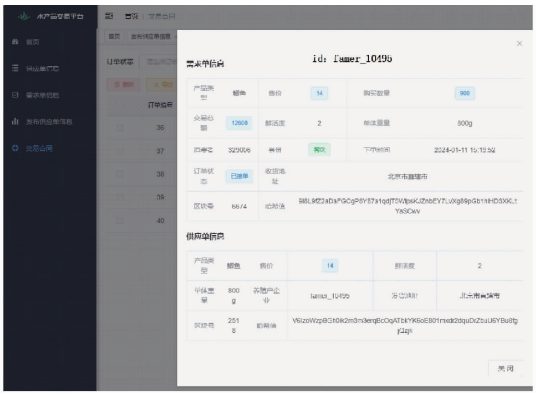

图 12　交易合同信息查询界面

Fig. 12　Contract information query interface

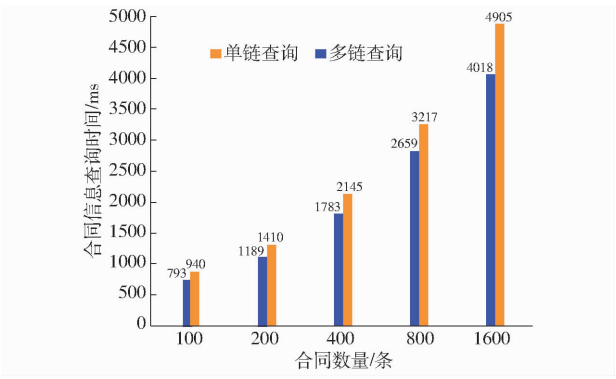

图 13　基于单链结构的原型系统与基于多链结构的原型系统交易合同信息查询时间对比

Fig. 13　Comparative time test of aquatic product contract information query between prototype system based on single-chain structure and prototype system based on multi-chain structure

200、400、800(成倍增长时)的平均交易完成时间进行测试,取 20 次测试结果的平均值可以看出,随着交易数据量的不断增加,交易匹配所需的时间呈现较为稳定的上升趋势,不会因为交易数据量的快速增加而导致系统性能出现严重问题,系统运行具有较高的稳定性。

现有的水产品区块链交易匹配模型均采用单链存储结构[21-22],将所有信息存储在一条链上,单链架构的系统按照水产品交易匹配流程的时间顺序依次存入用户注册信息、供应单信息、需求单信息与交易合同信息。当查询交易合同信息时,从最新区块依次向前一个区块逐渐遍历,由于单链结构查询交易合同时存在众多干扰信息(用户注册信息、供应单信息、需求单信息),花费时间较长。在基于多链架构的系统中,养殖户企业注册信息与供应单信息、批发商企业注册信息与其需求单信息、餐饮企业注册信息与其需求单信、个体消费者注册信息与其需求单信息、交易合同信息等分别为存储在 5 个不同的通道中。当查询任何一类链上信息时,系统均能够快速地定位到相应的通道中,其数据查询效率要明显比单链结构的水产品交易系统查询效率更高。以交易合同信息查询为例,本文设计了水产品多链架构交易系统与单链架构交易系统的对比实验。如图 13 所示,当链上交易合同数量分别为 100、200、400、800、1 600(成倍增长时)时,查询同一条合同信息时,水产品交易多链架构系统查询时间总是比单链架构系统查询时间短,查询效率更高。

从图 13 可以进一步分析出,当链上合同数量分别达到 100、200、400、800、1 600 时,多链架构水产品交易系统比单链架构交易系统查询效率分别提高 15.63%、15.67%、16.87%、17.3%、18.08%,其计算公式为

$$E = \frac{t_1 - t_2}{t_1} \times 100\%$$

E 表示多链比单链提升率,t_1、t_2 分别表示查询一条相同的交易合同信息时单链和多链所需要的时间。从测试与计算结果可以看出,随着链上存储的交易合同数量不断增加,水产品多链架构交易系统中链上交易合同信息查询效率的优势愈加明显,多链查询效率更快,性能更优,在确保数据安全的情况下,更能满足水产品线上交易平台中用户信息查询的效率需求。

4　结束语

作为一种分布式和去中心化的技术,区块链可以保证交易数据安全、提供交易记录可追溯性与用户隐私保护机制。本文提出的基于区块链多链存储优化的水产品交易匹配模型和原型系统,通过贪心算法,提升了用户交易匹配效率,采用区块链与本地数据库双模式存储技术以及多通道网络设计,降低了海量数据在区块链上存储的负载,节约了区块链存储空间,提高了链上合同信息查询效率并降低了存储成本,保障了用户信息、水产品交易供需信息和合同信息的安全,降低了水产品交易平台监管成本和难度,利于推进水产品线上交易平台进一步发展。

参　考　文　献

[1]　Food and Agriculture Organization of the United Nations. 2022 state report of world fisheries and aquaculture[EB/OL]. 2022-07-20. https://www.fao.org/3/cc0463zh/cc0463zh.pdf.

[2]　孙传恒,于毕竟,罗娜,等.基于智能合约的果蔬区块链溯源数据存储方法研究[J].农业机械学报,2022,53(8):361-370.
SUN Chuanheng, YU Bijing, LUO Na, et al. Research on fruit and vegetable blockchain traceability data storage method based

on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(8):361 - 370. (in Chinese)
[3] LI J, WANG Z, GUAN S, et al. ProChain: a privacy-preserving blockchain-based supply chain traceability system model[J]. Computers & Industrial Engineering, 2024, 187:109831.
[4] DHAR S, KHARE A, DWIVEDI A D, et al. Securing IoT devices: a novel approach using blockchain and quantum cryptography[J]. Internet of Things, 2024, 25:101019.
[5] GUO S, WANG F, ZHANG N, et al. Master-slave chain based trusted cross-domain authentication mechanism in IoT[J]. Journal of Network and Computer Applications, 2020, 172:102812.
[6] XU Z, WANG Y, DONG R, et al. Research on multi-microgrid power transaction process based on blockchain technology[J]. Electric Power Systems Research, 2022, 213:108649.
[7] YAP K Y, CHIN H H, KLEME J J. Blockchain technology for distributed generation: a review of current development, challenges and future prospect[J]. Renewable and Sustainable Energy Reviews, 2023, 175:113170.
[8] SHEN F, SHI L, JUN Z, et al. BMSE: blockchain-based multi-keyword searchable encryption for electronic medical records [J]. Computer Standards & Interfaces, 2024, 89:103824.
[9] ALI A A M, HAZAR M J, MABROUK M, et al. Proposal of a modifiedhash algorithm to increase blockchain security[J]. Procedia Computer Science, 2023, 225:3265 - 3275.
[10] ZOU Y, PENG T, WANG G, et al. Blockchain-assisted multi-keyword fuzzy search encryption for secure data sharing[J]. Journal of Systems Architecture, 2023, 144:102984.
[11] WANG T, HUA H, WEI Z, et al. Challenges of blockchain in new generation energy systems and future outlooks[J]. International Journal of Electrical Power and Energy Systems, 2022, 135:107499.
[12] ZHANG Y, LIU Y, ZHANG X, et al. Development and assessment of blockchain-IoT-based traceability system for frozen aquatic product[J]. Journal of Food Process Engineering, 2021, 44(5):13669.
[13] 魏立斐,朱嘉英,衡旭,等. 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.
WEI Lifei, ZHU Jiaying, HENG Xu, et al. Design and implementation of intelligent aquatic product quality and safety traceability system based on blockchain technology and HACCP management[J]. Fishery Modernization, 2020, 47(4):89 - 96. (in Chinese)
[14] 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.
LI Mengqi, YANG Xinting, XU Daming, et al. Design and implementation of aquatic product blockchain traceability information management system based on master-slave multi-chain[J]. Fishery Modernization, 2019, 48(3):80 - 89. (in Chinese)
[15] 王少然,王海陶. 基于“GS1 + 区块链”的水产品追溯技术研究[J]. 条码与信息系统,2020(6):8 - 13.
WANG Shaoran, WANG Haitao. Research on aquatic product traceability technology based on “GS1 + blockchain”[J]. Bar Code and Information System, 2020(6):8 - 13. (in Chinese)
[16] 李天明,张增年,严翔. 阳澄湖大闸蟹质量可信追溯模型研究[J]. 浙江万里学院学报,2021,34(2):86 - 91.
LI Tianming, ZHANG Zengnian, YAN Xiang. Research on credible traceability model of crab quality in Yangcheng Lake[J]. Journal of Zhejiang Wanli University, 2021, 34(2):86 - 91. (in Chinese)
[17] CRUZ E F, CRUZ A M R. Using blockchain to implement traceability on fishery value chain[J]. ICSOFT,2020, 1195: 501 - 508.
[18] PATRO P K, JAYARAMAN R, SALAH K, et al. Blockchain-based traceability for the fishery supply chain[J]. IEEE Access, 2022, 10: 81134 - 81154.
[19] 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)
[20] 周超,陈明,王文娟. 水产品线上交易匹配模型及算法研究[J]. 山东农业大学学报(自然科学版),2017,48(3):459 - 463.
ZHOU Chao, CHEN Ming, WANG Wenjuan. Research on online trade matching model and algorithm of aquatic products[J]. Journal of Shandong Agricultural University (Natural Science Edition), 2017,48(3):459 - 463. (in Chinese)
[21] 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. Model and system implementation of matching aquatic products based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(1):364 - 375. (in Chinese)
[22] WANG W, TENG D, CHEN M, et al. A trading matching model for aquatic products based on blockchain and credit mechanisms[J]. Mathematical Biosciences and Engineering, 2023, 20(11):19732 - 19762.
[23] 刘洋,林致远,张玉玺,等. 面向超级账本 Fabric 的多通道分片技术研究[J]. 应用科学学报,2023,41(4):614 - 625.
LIU Yang, LIN Zhiyuan, ZHANG Yuxi, et al. Research on multi-channel sharding technology for hyperledger Fabric[J]. Chinese Journal of Applied Sciences,2023,41(4):614 - 625. (in Chinese)
[24] 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及系统化实现[J]. 农业机械学报,2024,55(6):365 - 379.

ZHANG Xin, LIU Chongxuan, XU Jiping, 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. (in Chinese)

[25] 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 fruit and vegetable whole supply chain based on traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4):416 - 427. (in Chinese)

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

[27] 孙传恒,杨晓虎,罗娜,等.基于区块链的三文鱼冷链多链协同监管模型研究[J].农业机械学报,2024,55(1):360 - 370.
SUN Chuanheng, YANG Xiaohu, LUO Na, et al. Research on multi-chain collaborative regulatory model of salmon cold chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(1):360 - 370. (in Chinese)

[28] 朱燕超.面向区块链系统的查询处理研究[D].上海:华东师范大学,2020.
ZHU Yanchao. Research on query processing for blockchain systems[D]. Shanghai: East China Normal University, 2020. (in Chinese)

[29] KAMAL Z A, GHANI R F. A proposed hash algorithm to use for blockchain base transaction flow system[J]. Original Research, 2021, 9(4):657 - 673.

[30] 张晓蝶,黄郑正,赵金辉,等.基于区块链多链的农产品供应链追溯应用[J].重庆理工大学学报,2021,35(10):172 - 179.
ZHANG Xiaodie, HUANG Zhengzheng, ZHAO Jinhui, et al. Agricultural product supply chain traceability application based on blockchain[J]. Journal of Chongqing University of Technology, 2021, 35(10):172 - 179. (in Chinese)

[31] GUO J, LIAO G, LIU G, et al. Practical collision attacks against round-reduced SHA - 3[J]. Journal of Cryptology, 2020, 33: 228 - 270.

[32] LOU P, FEI Y, ZHANG L, et al. Differential fault analysis of SHA3 - 224 and SHA3 - 256[C]//2016 Workshop on Fault Diagnosis and Tolerance in Cryptography(FDTC). IEEE, 2016:4 - 15.

[33] 徐小小,周启银,娄成龙,等.基于贪心算法的自动路径规划送药小车[J].中国新技术新产品,2023,4(下):21 - 23.
XU Xiaoxiao, ZHOU Qiyin, LOU Chenglong, et al. Automatic path planning drug delivery vehicle based on greedy algorithm [J]. China New Technology and New Products, 2023,4(the second half):21 - 23. (in Chinese)

[34] 孙帅,许志远,玄世龙,等.基于贪心算法的无人船实时避碰算法[J].船舶工程, 2022, 44(4):14 - 18.
SUN Shuai, XU Zhiyuan, XUAN Shilong, et al. Real-time collision avoidance algorithm for unmanned ships based on greedy algorithm[J]. Ship Engineering, 2022, 44(4):14 - 18. (in Chinese)

[35] 林洪,邓艳.改进贪心算法求解扩展简化折扣{0 - 1}背包问题[J].西南师范大学学报(自然科学版),2022, 47(11):63 - 71.
LIN Hong, DENG Yan. Improved greedy algorithm to solve the extended simplified discount {0 - 1} knapsack problem[J]. Journal of Southwest Normal University (Natural Science Edition), 2022,47(11): 63 - 71. (in Chinese)

[36] 全国水产标准化技术委员会.鱼类鲜度指标 K 值的测定:高效液相色谱法:SC/T 3048—2014[S].北京: 中国农业出版社, 2014.

[37] 朱廷虎,刘洋,许立雄,等.基于区块链技术的微电网群分布式电能交易模式[J].电力建设,2022,43(6):12 - 23.
ZHU Tinghu, LIU Yang, XU Lixiong, et al. Microgrid group distributed electric energy transaction model based on blockchain technology[J]. China Electric Power Construction,2022,43(6):12 - 23. (in Chinese)

[38] 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. Design and system implementation of blockchain multi-chain anti-counterfeiting traceability model[J]. Journal of Hunan University (Natural Science Edition),2023,50(8):172 - 180. (in Chinese)