doi:10.6041/j.issn.1000-1298.2024.06.028

基于公证人机制的水产品跨链交易模型研究

邹一波[1,2]　景　虎[1,2]　陈　明[1,2]　葛　艳[1,2]　王文娟[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:随着水产品交易规模的扩大,区块链技术在产品溯源和数据共享方面得到广泛的应用,但不同企业内或同一供应链内的不同环节构建的区块链之间数据无法有效交互和共享,致使信息孤岛问题依然存在。因此提出了基于公证人机制的水产品跨链交易模型,旨在实现水产品不同环节之间的跨链交易,解决单点故障问题,并提升交易效率。同时针对水产品跨链交易业务特点,提出两阶段跨链交易流程,完善交易错误处理机制,从而解决跨链交易过程中的数据一致性、原子性需求,并基于 Hyperledger Fabric 平台构建系统原型。实验结果表明,在交易量较大的情况下,交易平均成功率高于 99%,平均延迟时间为 0.21 s 左右,模型在保证交易安全性的前提下,满足了水产品区块链跨链交易需求。

关键词:公证人机制;水产品;跨链交易模型;区块链

中图分类号:TP311.1　　**文献标识码**:A　　**文章编号**:1000-1298(2024)06-0262-10　　**OSID**:

Cross-chain Trading Model of Aquatic Products Based on Notary Mechanism

ZOU Yibo[1,2]　JING Hu[1,2]　CHEN Ming[1,2]　GE Yan[1,2]　WANG Wenjuan[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 expansion of the trading scale of aquatic products has led to the widespread application of blockchain technology in product traceability and data sharing. However, the inability of data exchange and sharing between blockchains constructed in different enterprises or different links within the same supply chain has led to the persistence of information silos. Therefore, a cross-chain transaction model for aquatic products was proposed based on a notary mechanism, aiming to achieve cross-chain transactions between different links of aquatic products, solve single point of failure problems, and enhance transaction efficiency. Meanwhile, addressing the characteristics of cross-chain transactions for aquatic products, a two-stage cross-chain transaction process was proposed, along with an improved transaction error handling mechanism, to address the requirements of data consistency and atomicity during cross-chain transactions. A system prototype was built based on the Hyperledger Fabric platform. Experimental results demonstrated that under high transaction volumes, the average success rate of transactions exceeded 99%, with an average latency of around 0.21 s. Thus, the model met the requirements of cross-chain transactions.

Key words: notary mechanism; aquatic products; cross-chain trading model; blockchain

0　引言

水产品作为我国重要食品来源之一,生产量和消费量都位居世界前列。在水产品供应链中,存在养殖、加工、销售、仓储、物流等环节[1]。环节众多导致水产品供应链透明度不足,从而引发质量安全风险[2]。区块链技术因为拥有去中心化[3]、可靠性[4]以及信息不可篡改性[5]等优点,已广泛应用于

收稿日期:2024-02-05　修回日期:2024-03-31

基金项目:广东省重点领域研发计划项目(2021B0202070001)

作者简介:邹一波(1983—),男,讲师,博士,主要从事区块链技术和机器视觉研究,E-mail:ybzou@ shou.edu.cn

通信作者:葛艳(1974—),女,副教授,博士,主要从事质量安全风险评价、溯源和农业信息化研究,E-mail:yge@ shou.edu.cn

工业、农业以及金融领域[6-10]，同时也推进水产品供应链的优化。通过增强水产品溯源的可信性[11-13]，从而保证食品质量安全，提高供应链透明度。如使用物联网和区块链结合，提高水产品冷链溯源效率和安全性[14]，构建区块链和星际文件系统(Inter planetary file system, IPFS)相结合的水产品交易溯源模型[15]。

区块链技术在水产品供应链中的应用，虽然提升了供应链效率和产品溯源能力，但传统交易方式的结构较为松散，导致交易过程中产生大量的数据，这些数据独立存在于不同的区块链中。然而，不同区块链网络之间存在数据同步[16-17]和业务流程协同[18-19]的困难，难以实现互相流通验证。这种局面造成了信息孤岛问题[1]，使得各个环节区块链之间难以实现互操作。

针对以上问题，国内外学者从理论上提出通过公证人机制[20]、侧链/中继[21]、哈希锁定[22]和分布式私钥控制[23]等各种区块链技术和方法[24-25]实现跨链过程中的互操作，解决信息孤岛问题。在应用领域，也有基于中继链方法的食品溯源跨链方案[26]，支持主流区块链之间跨链互操的跨境海产品供应链平台[27]，采用中继方式的水产品交易模型，改善不同区块链之间数据同步和业务流程协同的难题[1]。总体来说，中继方式实现跨链交易，容易出现单点故障，影响系统鲁棒性[1]；哈希锁定方式交易难以追溯[27]；分布式私钥控制方式管理密钥困难且复杂[28]。但是水产品跨链交易仍存在跨链网络去中心化程度低、单点故障影响大、可扩展性差、缺少交易失败处理机制等问题。

本文基于公证人机制，构建水产品的跨链交易模型，实现水产品跨链交易中不同区块链之间的互操作。在水产品交易环节中，允许不同的区块链网络通过选择不同的公证人来进行跨链交互，而不需要修改其原有的共识机制或数据结构，从而保障交易的独立性、鲁棒性和数据安全性。同时，优化水产品跨链交易流程，引入两段式交易流程，将跨链交易划分为预交易阶段和交易阶段，实现业务流程协同，保障跨链交易原子性。建立交易错误处理机制，保证交易事务安全性。

1　水产品供应链跨链交易业务分析

水产品供应链具有环节众多、企业间相互独立的特点。以水产品供应链中的业务功能逻辑为依据进行划分，可将其分为养殖、加工、仓储、销售和运输 5 个环节。水产品在供应链中按照交易流向，以养殖企业为交易起点，通过各个环节最终到达消费者手中。并且交易过程中不同环节的企业之间相互独立，各环节业务信息的数据结构也因各自业务需求而异[1]。

基于以上水产品供应链的特点，将水产品跨链交易中的业务信息分为产品信息和跨链交易信息：①产品信息用于记录当前交易产品的详细数据信息。②跨链交易信息用于满足跨链交易中的双方交易信息以及公证人信息。例如，在养殖企业记录水产品的养殖情况以及跨链交易信息，并通过公证人机制加入公证人信息后，与加工企业交易。而在加工环节需要对该批水产品的养殖情况等进行深入了解，同时添加商品名称、价格、保质期等信息，数据结构如图 1 所示。

2　基于公证人机制的水产品跨链交易模型架构

公证人机制是由公证人节点组成公证人组，来负责不同交易链间的跨链交易。每次数据传输都由特定的算法选取公证人节点，进行跨链交易验证以及跨链传输。通过公证人组的管理以及公证人之间的补充，单个节点的故障不影响整个跨链网络的运行[20]。新加入的交易链只需要准备好相关的区块链节点、身份证书、密钥等基础设施，不影响跨链交易网络。

因此，本模型引入公证人机制，构建水产品跨链交易拓扑结构和层次模型架构，在确保水产交易各环节企业区块链独立的情况下，实现区块链之间的互操作，解决跨链交易的数据同步和业务流程协同问题。同时本文针对现有的水产品跨链交易模型缺少超时、交易失败等问题的处理机制，在公证人机制的基础上，设计相应的两段式跨链交易流程，从而提升水产品跨链交易容错能力。

2.1　水产品跨链交易拓扑结构

本文提出的水产品跨链交易拓扑结构将企业用户作为交易双方，在公证人对交易的确认和验证下完成跨链交易。公证人机制建立在多个区块链网络之上，由公证人节点、跨链协议以及共识算法组成。公证人节点作为独立实体，利用智能合约规定跨链交易的规则和条件，负责在多个区块链网络之间的交易确认和验证。跨链协议负责数据的安全传输，共识机制负责在公证人节点之间达成共识，达成一致决策，保障数据可信。通过参与交易过程并提供公证人管理选择和数据传输功能，为水产品跨链交易提供了保障和互信机制，降低了跨链交易中的交易可信性风险。

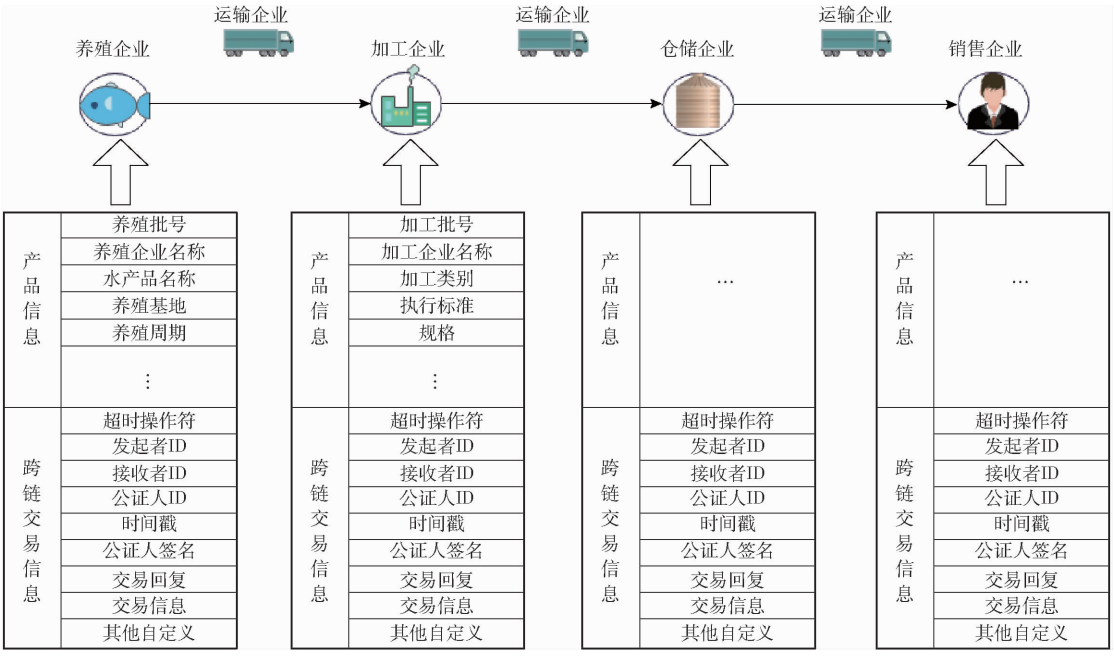

图 1 水产品交易部分环节数据结构

Fig. 1 Structural of data in various stages of water product transactions

模型拓扑结构如图 2 所示，由多条交易链以及公证人机制组成。可信的第三方公证人共同组成公证人机制，在交易用户节点提出交易到交易链，通过区块链网络提交给公证人机制，由公证人组分配此次交易的公证人，验证后提交给交易目标链。由接收交易的交易用户节点确认或拒绝交易后，再次递交给公证人，公证人验证交易并广播结果。公证人作为可信的中介机构，为跨链交易提供安全性保障。企业用户作为交易的参与者，由公证人机制进行数据传输，并在公证人节点验证下，完成跨链交易并实现跨链信息的传输。例如养殖企业用户节点与加工企业用户节点之间交易过程为：加工企业用户节点提交交易到销售交易链，再通过区块链网络提交给公证人机制，由其从公证人组中选取公证人承担交易的确认和验证；对应公证人验证交易后发送到养殖交易链，最终由养殖企业节点确认或拒绝后，回复公证人，最终由公证人确认并广播交易或取消交易。

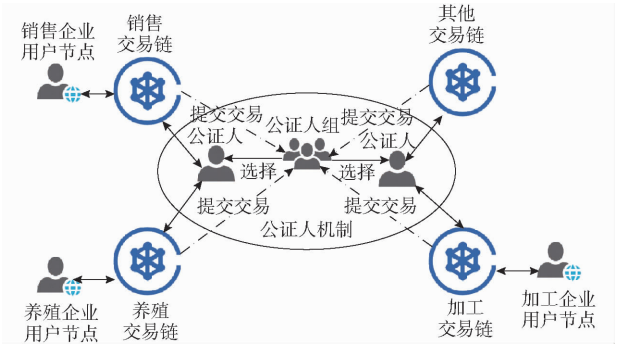

图 2 水产品跨链交易模型拓扑结构

Fig. 2 Model topology

2.2 水产品跨链交易层次模型架构

本文提出的水产品跨链交易层次模型涉及 5 个层次的架构，旨在解决上述业务分析的业务逻辑实现。如图 3 所示自下而上分别为：网络层、合约层、数据层、交互层和应用层，下面将对每个层次进行详细阐释。

图 3 系统架构图

Fig. 3 System architecture diagram

(1)网络层。该模型的核心是水产品供应链中各个企业的区块链结构。这些区块链采用分布式系统的设计，各节点通过 P2P 组网机制相互独立地构建区块链结构，并形成独立的通讯子网，用于维护各自的分布式账本管理。时间戳技术被应用于数据的存储，确保数据的时序性和完整性的共识机制，保证数据的不可篡改性。

(2)合约层规定了用户在区块链上的操作行为。在去中心化环境下，根据预设条件执行区块链操作，实现跨链交易的流程。合约层在水产品跨链交易业务逻辑的基础上构建查询跨链交易的查询合

约、实现建立跨链交易并控制跨链流程的跨链合约，以及建立跨链通道的系统合约，对用户的操作权限进行分层和限制，确保交易的安全性和可控性。

(3)数据层负责处理区块链中的跨链数据验证交易数据，以及负责错误处理的跨链数据管理，满足水产品跨链交易业务中的信息字段传输。并且根据水产品交易过程中合约超时失效和撤销问题，构建错误处理机制，调用相应函数终止交易并进行跨链交易撤销，以确保交易双方数据的一致性。

(4)交互层将跨链交易进行收集传输以及相应的跨链操作。跨链交易传输用于在交易过程中对跨链交易信息进行编码和解码，具体体现在将跨链信息、时间戳、哈希和背书信息打包成跨链交易，并进行跨链传输；跨链交易存储负责跨链交易过程中的交易储存，跨链交易验证用来验证跨链交易的一致性和合法性。

(5)应用层实现查询服务、公证人管理、跨链交易管理以及权限认证。该层直接面向企业用户，是模型功能的具象实现，企业用户在接入系统后，系统通过访问控制，发放数字证书，可直接接受或发起跨链交易、查询跨链交易。同时公证人管理对公证人的加入和退出进行管理，并对交易过程中的公证人进行选择，确保交易公平有效。

2.3　公证人机制设计

公证人机制包含图 3 中的公证人管理、跨链交易传输、跨链交易验证、权限认证、跨链交易储存、跨链交易验证。为应对水产品跨链实时交互、高并发和高吞吐量的需求，多个公证人组成公证人组能够将跨链交易分流，简化跨链交互，提高数据处理效率。同时针对水产品交易流程业务特点，在多个公证人的公证人组的基础上，强化公证人的选择机制，在公证人中不留存跨链交易相关信息，而是通过交易链各自上链跨链交易信息，从而维持去中心化和提高效率之间的平衡。

2.3.1　公证人管理

图 4 为公证人管理模型。公证人管理动态地管理公证人的加入和退出，并选取适当的公证人来执行跨链交易，确保跨链交易在公证人组中得到均衡的处理。当交易数量远大于公证人数量的情况下，通过在交易等待队列和交易队列对超量交易的延迟处理，对交易进行分流。在分流的优势下，避免了公证人组中某个公证人或正在参加跨链交易的公证人出现故障的单点故障问题，满足了实时交互和高吞吐量应用的需求，加强了水产品跨链模型的可靠性和去中心化。以跨链交易 A 为例，设置参数已存在的公证人数量 N，公证人优先级参数 P。公证人选取算法如下：

(1)当水产品跨链交易发起时，交易 A 首先提交给公证人组，进入交易等待队列。

(2)公证人组中 P 值为 1 的公证人被推选为执行该跨链交易的公证人，负责处理跨链交易的各个环节。

(3)若公证人存在故障，强制退出公证人，其余公证人的 P 值会减少 1，即 $P = P - 1$，并返回步骤(2)。

(4)交易 A 进入相应的交易列表，其余公证人的 P 值会减少 1，即 $P = P - 1$。

(5)公证人节点失效时返回到步骤(2)，并重新赋值 $N = N - 1$。

(6)当交易成功或交易终止时，公证人对交易

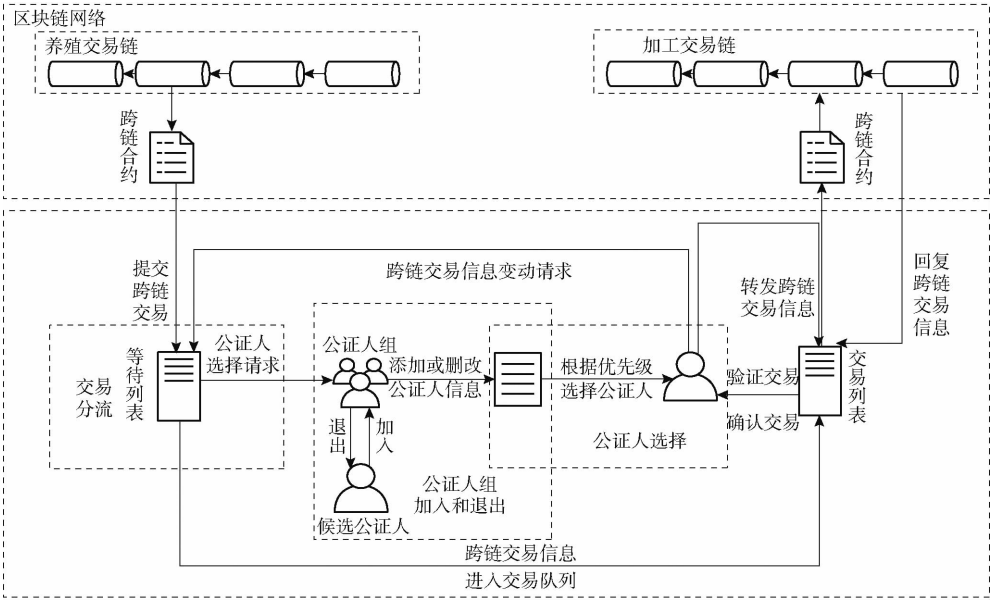

图 4　公证人管理模型图

Fig. 4　Notary management model diagram

进行验证。如果验证没有错误,公证人将重置 $P=N$,并重新进入公证人组进行排序。

(7)结束。

当交易数量远大于公证人数量时,需要通过交易等待队列和交易队列来对超量交易进行延迟处理,并对交易进行分流。这可以确保交易得到均衡的处理,并避免公证人组中某个公证人或正在参加跨链交易的公证人出现故障的单点故障问题。通过分流机制,可以提高交易的处理效率和网络的可靠性。

2.3.2 跨链交易传输

跨链交易传输在水产品跨链交易模型中发挥着连接交易链和公证人的关键作用。该模块负责接收来自提出链的交易数据信息,并进行解析和编码。随后,公证人将加入跨链信息,如时间戳等,将其打包成跨链交易信息,并发送给目标链。一旦目标链收到跨链交易信息,它会提供反馈,该反馈将被发送回公证人进行验证。最终,经过验证的跨链交易数据将被发送给双方链,完成整个跨链交易的数据交互过程,以确保交易双方依据交易既定流程处理交易。

2.3.3 跨链数据验证

跨链数据验证主要功能是在交易提交和结束时对交易的可信性进行验证。在跨链数据提交到公证人时,公证人会对跨链交易进行验证,确保跨链交易各个环节的可信性。交易完成时,公证人再次对跨链数据进行验证签名后,广播反馈以及跨链交易。通过公证人的参与,提供了对交易可信性的判断和反馈,从而保护了水产品跨链交易的安全性和可靠性。

2.3.4 权限认证

在跨链交易过程中,为了确保数据的流转具有明确的方向和可信性,采用了公钥基础设施(PKI)[10]和数字证书授权机构(CA)[12]技术构成权限认证。水产品参与者在跨链交易前,首先需要向数字证书授权机构(CA)申请数字证书。CA 通过验证身份后,颁发包含公钥和身份信息的数字证书用于加密和签名交易数据,通过以下环节,确保水产品跨链交易的安全性、完整性和可信性。

(1)跨链交易的发起:水产品的跨链交易发起方使用私钥对交易数据进行签名,同时将数字证书一同发送给接收方。

(2)数据传输和验证:加密的数据在跨链网络上传输。其他区块链成员可以通过接收方的公钥验证数据的真实性和完整性。

(3)公证人的应用:在交易过程中,公证人负责监听和验证交易。公证人通过验证签名,以区分不同的参与者身份确保数据可信。

(4)身份识别与交易有效性验证:公证人通过验证数据来识别交易双方的身份,同时验证交易的有效性。这包括检查数字签名的合法性和确保参与者的数字证书未被撤销。

(5)唯一标识码和智能合约:不同交易链之间使用唯一标识码进行区分。智能合约在不同交易链上具有不同的逻辑。这有助于公证人区分交易链的身份,识别不同的交易逻辑,确保数据流转的方向明确且可信。

2.3.5 跨链交易储存

跨链交易储存由交易等待队列和交易列表两部分组成。

交易等待队列是用于存放区块链发送过来但尚未执行的跨链交易的数据结构。这些交易暂时挂起等待执行,储存有交易跨链信息以及交易信息,并按照先进先出的原则进行排队。交易等待队列的目的是为了将未处理的跨链交易有序地分配给合适的公证人进行处理。当交易等待队列中的交易需要被执行时,根据一定的分配策略,交易会被分配给特定的公证人进行处理。

交易列表是每个公证人节点独有的数据结构,用于存储该公证人所负责的跨链交易。一旦交易等待队列中的交易被分配给某个公证人,该交易会被添加到该公证人的交易列表中进行处理。交易列表记录了公证人当前正在处理的交易信息,并在交易结束或被撤销后从列表中删除。

通过交易等待队列和交易列表的组织,整个跨链交易过程得以有序进行。交易等待队列确保了未处理的跨链交易按照时间顺序进行排队,而交易列表则用于存储每个公证人节点负责处理的交易信息。这种组织结构使得跨链交易能够有序地被分配和处理,从而提高了跨链交易的效率和可靠性。

2.3.6 跨链交易验证

为了验证交易的真实性和可信性,本文利用了区块链的密码学原理和哈希函数来保证数据的安全性和完整性。通过上述技术对跨链交易签名的运算,验证跨链交易的有效性,从而增强了交易的可信度和数据的安全性。此外,为了进一步保证数据的安全性和不可篡改性,本文采用 Merkle 树的结构来组织交易数据,可以快速验证交易数据是否存在于区块中,以及检测任何数据的篡改,来保障数据的不可篡改性,并使得跨链数据能够安全地在公证人和不同区块链之间流动。

3　水产品跨链交易流程设计

在保障水产品跨链交易安全性的前提下，本文将跨链交易分为两个阶段进行：预交易阶段和交易阶段。预交易是在交易提交后，选取公证人到交易确定的过程。交易阶段是在交易确定后，公证人验证签名后发送到区块链上链的过程，交易在这两个阶段中只能上链或终止，使得跨链交易具有原子性。通过将跨链交易数据和区块链进行隔离，本文有效提升了跨链交易事务管理过程的隔离性和数据一致性。在交易达成前，跨链交易数据处于隔离状态，避免了数据的泄露和不一致性问题，有利于提高跨链交易的安全性和可行性。

3.1　预交易阶段

预交易阶段是对跨链交易的达成过程中参与双方的交易确认和公证人的选择。如图 5 所示，该阶段流程如下：

(1)跨链交易的开始是由交易发起者提交交易信息、发起者 ID、发起链地址、目标链目标节点以及发起节点签名。

(2)提交给公证人组后，进入等待队列，根据 2.3.1 节的公证人选举算法，等待队列中排在前面的交易完成以及公证人组选举出首位公证人。

(3)在完成等待并选举出此次交易的首位公证人后，跨链交易信息首先退出等待对列，进入首位公证人交易列表。

(4)首位公证人验证跨链交易信息，并上传时间戳，对交易再次打包，打包完成后的交易，由公证人转发给目标链目标节点。

(5)在目标节点接收公证人转发的跨链交易后，首先检验交易合法性，验证交易和签名。再确认信息后，上传交易回复信息、目标节点签名后发送回执给公证人，交易阶段结束。

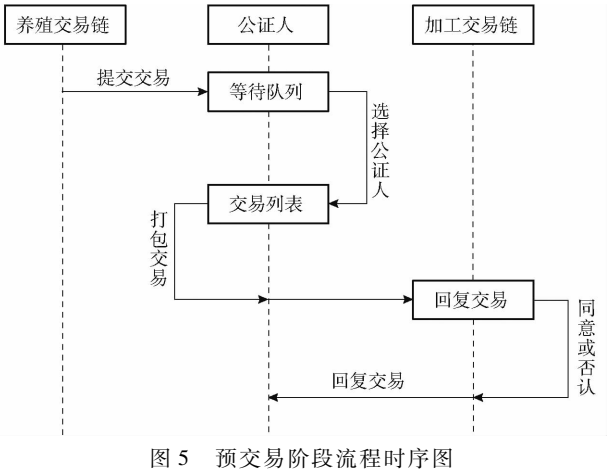

图 5　预交易阶段流程时序图

Fig. 5　Pre-trade phase process sequence diagram

3.2　交易阶段

交易阶段是在交易双方确定交易的情况下，公证人完成交易并广播交易，公证人不留存跨链交易信息，交易双方链分别对交易进行验证后上链更新区块链账本，从而达到水产品交易的目的。

首先公证人等待目标链的交易回执，如果接收方不同意交易或者在规定的时间内没有签名确认并发送给公证人，则交易不能达成，并启动交易撤销机制予以撤销，流程如图 6 所示。

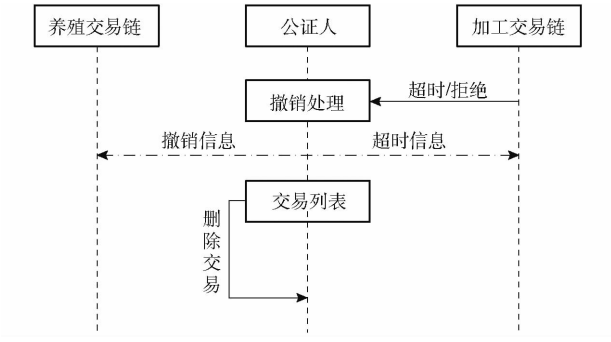

图 6　交易阶段错误处理时序图

Fig. 6　Transaction phase error handling sequence diagram

撤销处理返回超时信息如图 6 所示，包括交易信息、时间戳、公证人签名，发送到交易提出链和目标链。此次跨链交易从交易列表中删除，公证人不再接收目标链的此次交易回复。

交易阶段中若是在规定时间内获得交易回执，则流程如图 7 所示：首先公证人对交易信息双方签名进行验证，验证成功后上传公证人 ID、公证人签名，然后向交易双方链广播，公证人将交易从交易列表中删除。双方区块链上的节点验证确认后，打包交易上链更新账本，完成此次跨链交易。

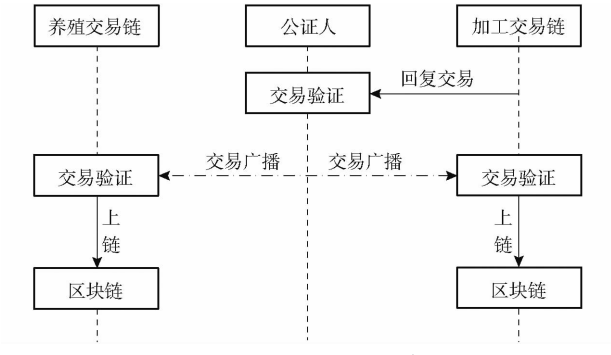

图 7　交易阶段流程时序图

Fig. 7　Transaction phase process sequence diagram

4　智能合约设计

4.1　预交易合约

预交易合约是指在跨链交易过程中使用的智能合约，用于实现预交易阶段的功能和流程。预交易合约可以在区块链上部署和执行，协调交易发起者、

公证人机制和目标节点之间的交互,算法如下:

输入:接收交易发起者提交的交易信息相关参数 Transaction(),其中包含发起者信息 ID、发起链地址 addA、目标链目标节点 addB 以及交易信息 text。

输出:预交易结果 result。

```
function PreTransaction(stub,args[])
    //提交交易到等待队列
        if Exit = transactionQueue.push(Transaction());    //查询交易是否存在
        TransactionAdded();    //加入队列
        //公证人分配
        assignTransaction()//选择首位公证人并分配交易
        //公证人验证交易信息和上传时间戳
        verifyTransaction()
    return result
    }
```

预交易合约包括交易提交、公证人分配、公证人验证以及交易信息获取,按执行逻辑分步执行,最终完成跨链预交易。提交交易需要提交者提交交易信息到公证人组,交易由此进入等待队列,算法如下:

输入:交易信息相关参数 Transaction(),跨链交易识别码 txID 以及交易信息 text。

输出:入队结果。

```
function submitTransaction(Transaction()) {
        transactionQueue.push(Transaction(txID, text));
        TransactionAdded(txID, text);
    return result
    }
```

交易进入等待对列后,等待公证人组分配公证人后进入交易列表,进行交易处理,公证人分配和交易处理算法如下:

输入:交易信息相关参数 Transaction(),公证人组信息 publicer()。

输出:交易处理结果。

```
function assignTransaction(Transaction(), publicer()) {
        require(transactionQueue.length > 0, "No transactions in the queue");
        //根据公证人系统的选择机制选取首位公证人地址
        address notary = selectNotary();
        //获取待处理的交易信息
            Transaction storage transaction = transactionQueue[0];
        //更新交易状态和标记为已处理
            TransactionAssigned(transaction.txID, notary);
    return result
    }
```

最后由公证人验证交易信息,算法如下:

输入:跨链交易识别码 txID。

输出:验证结果。

```
function verifyTransaction(txID) {
        //根据交易 ID 获取交易信息
            Transaction storage transaction = getTransaction(txID);
        //执行公证人验证逻辑,包括验证交易信息和上传时间戳等操作
        //更新交易状态和标记为已处理
        TransactionProcessed(transaction.txID);
    return result
    }
```

4.2 交易合约

交易合约是指在跨链交易过程中使用的智能合约,用于实现交易阶段的功能和流程。它是跨链交易的核心组成部分,承担着协调交易发起者、公证人机制和目标节点之间的交互任务,确保交易的顺利进行和可信性验证。算法如下:

输入:交易信息相关参数 Transaction(),公证人信息 notary。

输出:交易结果。

```
function Transaction(stub,args[]) () {
        //检查交易信息是否有效,例如检查交易时间戳、签名等
        //发送交易信息给接收方链上的节点
        ctx.GetStub().InvokeChaincode()
        //等待接收方链的交易回执
            response:= ctx.GetStub().GetTxValidationCode()
            if response != contractapi.TxValidationCodeValid {
            // 交易回执验证失败,启动交易撤销机制
            revokeTransaction(ctx, transactionInfo)
    }
        //如果超时,启动交易撤销机制
        if(time = =0){
            RevokeTransaction()// 执行撤销操作,例如发送撤销通知给交易发起方链
```

```
    }
    //交易回执验证成功,完成提交阶段
    return result
}
```

5　实验

5.1　系统实现

为了实现上述跨链交易模型框架和业务流程，在 Ubuntu 22.04.1、docker 20.10.21 环境下，使用 Hyperledger Fabric 2.2 来构建区块链架构。采用 javascript 16、go 1.17.13 完成底层框架开发，利用 Fabric 平台中的 JavaScript 接口实现系统设计，使用 Web 开发技术和框架实现用户友好的交互界面，通过与后端区块链网络的连接，实现与区块链的交互操作和数据传输。系统的前端设计还包括用户认证和权限控制功能，以确保系统的安全性和合规性。

实验环境中，为了每个环节的业务数据分离以及公证人的独立运行，每个通道设置 3 个 Org 作为生产链、加工链、销售链，公证人组中建立 4 个 Org 作为公证人。图 8 为遍历用户区块链跨链交易界面，图 9 为跨链交易详情界面用来查看跨链交易完整信息，图 10 为跨链交易的实现界面用来拟定交易详情，图 11 为查询交易界面用来查找特定交易。

图 8　遍历用户区块链跨链交易界面

Fig. 8　Navigate through user's blockchain cross-chain transaction page

ID	220812089172354243 21
发起人	生产公司A1
接受人	加工公司B1
公证人	公证人1
发起人签名	2beebfa35e4b68ab38451ededa7f4ddad6e62e321fbab735e78dea5df64b8012
接受人签名	2f5c8535d711642b72fb04401627aa9fbac30fb1903cc4db02258717921a4881
公证人签名	9a2d2ac4eb5e06fc361d32ea73fb919d1d0ba555d159301ed01aa42095cd637b
交易时间	2022-11-1
商品	name: 沙丁鱼 money: 200000 setaddress: 广东省东莞市 getDataaddress: 湖南省长沙市

图 9　跨链交易详情界面

Fig. 9　Cross-chain transaction details page

5.2　性能测试

针对基于公证人技术的水产品跨链交易，通过对比单个区块链交易，从交易性能的角度进行测试和分析。为了评估系统性能，采用 Caliper 性能测试工具，考察每秒交易并发量、平均交易成功率和平均延迟时间等指标。

图 10　跨链交易实现界面

Fig. 10　Cross-chain transaction implementation page

图 11　跨链交易查询交易界面

Fig. 11　Cross-chain transaction query page

如图 12 实验设置中，总交易量设定为 5 000 笔，并进行了 6 轮递增测试，逐渐提高每秒交易并发量。初步观察结果显示，在每秒交易并发量为 100 笔/s 之前，跨链交易成功率明显优于单链交易。这表明在较低的并发负载下，跨链交易性能表现较好。然而，在每秒并发量达到 120 笔/s 时，跨链交易成功率开始下降，当每秒交易并发量达到 60 笔/s 时，交易成功率稳定在 97% 以上。

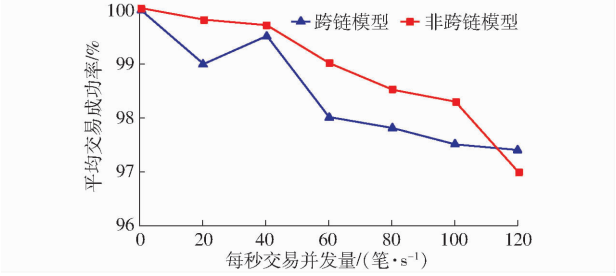

图 12　交易成功率测试结果

Fig. 12　Transaction success rate test results

如图 13 在总交易量为 5 000 笔的实验设置中，每轮实验逐渐增加每秒交易并发量，并观察平均延迟时间的变化情况。平均延迟时间大约稳定在 0.21 s 左右。随着每秒交易并发量的增加，平均延

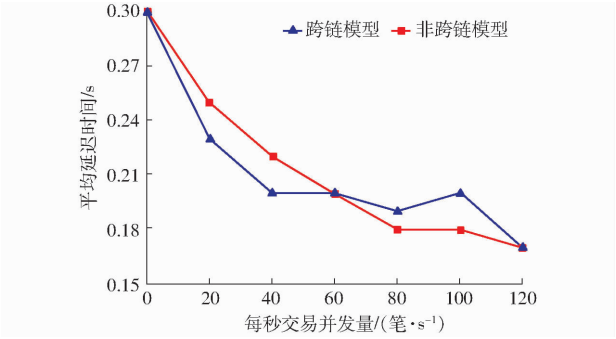

图 13　交易延迟对比结果

Fig. 13　Transaction latency comparison results

迟时间呈现出一定的趋势。初期阶段,系统在相对较低的交易并发量下表现出较低的平均延迟时间。这表明系统能够快速处理交易请求并迅速返回结果。当每秒交易并发量达到 60 笔/s,平均延迟时间在 0.21 s 附近趋于平缓。这意味着系统在这个交易量水平上能够稳定地维持较低的延迟性能。

如图 14 设置总交易量为 1 000、3 000、5 000 笔,每秒交易并发量不同。在总交易量为 1 000 笔和 3 000 笔时,成功率都在 98.4% 以上,并且两条曲线相近,表示交易成功率相近。这说明系统在处理这两个总交易量范围内的交易时表现稳定且高效。然而,当总交易量增加到 5 000 笔,成功率出现了骤降。

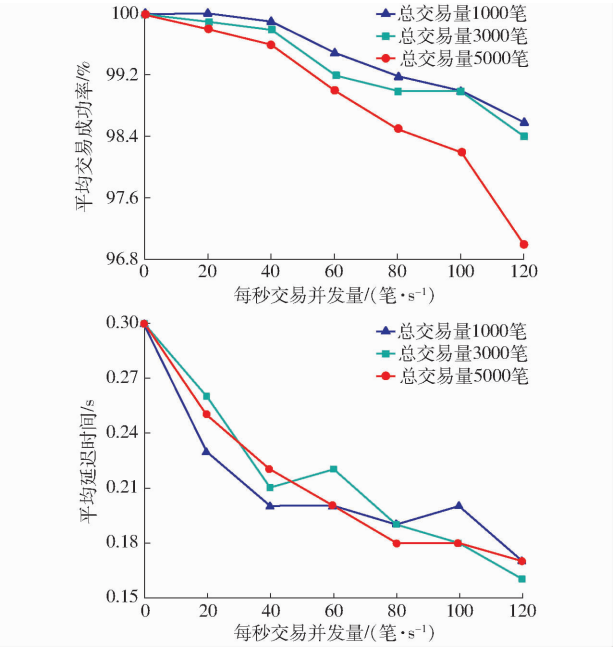

图 14 交易并发量结果对比

Fig. 14 Transaction concurrency comparison results

由上述性能分析表明,公证人机制能够确保更多的交易得到及时处理和验证,增强了整个跨链交易系统的可靠性和效率。在低交易并发量的情况下,跨链交易的效率与单链交易相比并没有明显差别。这是因为在低负载情况下,系统资源还未达到极限,跨链的中转和公证机制并未充分发挥作用,单链交易能够满足交易需求并具备相近的效率。因此,跨链中转节点和公证人的数量对于跨链交易的效率至关重要,尤其在高负载环境下能够显著提升系统性能。然而,在低负载情况下,跨链交易与单链交易的效率差别较小。在实际应用中,需要综合考虑交易成功率、延迟时间和效率等因素,根据具体需求进行合理的系统配置和优化。

6 结束语

基于公证人机制,构建水产品的跨链交易模型,通过可信第三方公证人的加入,提升交易的可信性和模型可扩展性、简化交易方式。采用两段式交易流程加入交易错误处理机制,保证了跨链交易安全性。通过构建交易相关的智能合约,在 Hyperledger Fabric 平台上实现模型应用,实现公证人机制、权限管理等跨链相关功能的模块化设计。系统性能实验结果表明,基于公证人的水产品跨链交易模型在较大交易规模情况下,跨链交易成功率高于 99%,延迟时间在 0.21 s 左右,满足了水产品跨链交易需求,同时具有较强的可靠性与安全性,并且系统可扩展性较好。

参 考 文 献

[1] 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 aquatic 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)

[2] JENNINGS S, STENTIFORD G D, LEOCADIO A M, et al. Aquatic food security: insights into challenges and solutions from an analysis of interactions between fisheries, aquaculture, food safety, human health, fish and human welfare, economy and environment[J]. Fish and Fisheries, 2016, 17(4): 893 - 938.

[3] RATHORE R. An overview on blockchain and its applications[J]. Asian Journal of Multidimensional Research, 2021, 10(10): 996 - 1000.

[4] PANDS S S, MOHANTA B K, SATAPATHY U, et al. Study of blockchain based decentralized consensus algorithms[C]// TENCON 2019—2019 IEEE Region 10 Conference (TENCON). IEEE, 2019: 908 - 913.

[5] TRELEAVEN P, BROWN R G, YANG D. Blockchain technology in finance[J]. Computer, 2017, 50(9): 14 - 17.

[6] BODKHE U, TANWAR S, PAREKH K, et al. Blockchain for industry 4.0: a comprehensive review[J]. IEEE Access, 2020, 8: 79764 - 79800.

[7] SABERI S, KOUHIZADEH M, SARKIS J, et al. Blockchain technology and its relationships to sustainable supply chain management[J]. International Journal of Production Research, 2019, 57(7): 2117 - 2135.

[8] AZARIA A, EKBLAW A, VIEIRA T, et al. Medrec: using blockchain for medical data access and permission management[C]// 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016: 25 - 30.

[9] OTHMANE F, MOHAMED A F, LEI S, et al. Internet of things for the future of smart agriculture: a comprehensive survey of

emerging technologies[J]. IEEE/CAA Autom. Sinica, 2021,8(4):718 – 752.
[10] ZHANG Y, LIU Y, JIONG Z, et al. Development and assessment of blockchain-IoT-based traceability system for frozen aquatic product[J]. Food Process Eng., 2021, 44(5): e13669.
[11] LEE H, YEON C. Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions [J]. Sustainability, 2021, 13(19): 11057.
[12] BARALLA G, PINNA A, CORRIAS G. Ensure traceability in European food supply chain by using a blockchain system[C]// 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE, 2019: 40 – 47.
[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 traceability based on blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(1):1 – 13. (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, 2021, 48(3): 80 – 89. (in Chinese)
[15] 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)
[16] WANG W, ZHANG Z, WANG G, et al. Efficient cross-chain transaction processing on blockchains[J]. Applied Sciences, 2022, 12(9): 4434.
[17] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. ACM Computing Surveys (CSUR), 2021, 54(8): 1 – 41.
[18] ALAM S. The current state of blockchain consensus mechanism: issues and future works[J]. International Journal of Advanced Computer Science and Applications, 2023, 14(8):84 – 94.
[19] BACK A, CORALLO M, DASHJR L,et al. Enabling blockchain innovations with pegged side-chains[J/OL]. http:// www.opensciencereview. com/papers/123/enablingblockchain-innvations-with-pegged-sidechains, 2014: 72.
[20] BUTERIN V. Chain interoperability[J]. R3 Research Paper, 2016, 9:1 – 24.
[21] FUSION Foundation. An inclusive cryptofinance plat-fom based on blockchain[M]. FUSION Whitepaper, 2017.
[22] HERLIHY M. Atomic cross-chain swaps[C]// Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing,2018: 245 – 254.
[23] 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. Survey on cross-chain protocols of blockchain [J]. Journal of Frontiers of Computer Science and Technology, 2022,16(10):2177 – 2192. (in Chinese)
[24] 魏济泽. 基于跨链的食品溯源系统设计与实现[D].南京:东南大学,2022.
WEI Jize. Design and implementation of food traceability system based on cross-chain[D]. Nanjing: Southeast University, 2022. (in Chinese)
[25] 吴欧,张贺,王岩泽,等.异构多链场景下跨境海产品供应链平台的架构设计与实现[J].应用科学学报,2022,40(4):539 – 554.
WU Ou, ZHANG He, WANG Yanze, et al. Architecture design and implementation of cross-border seafood supply chain platform in heterogeneous multi-chain scenario[J]. Journal of Applied Science, 2022, 40(4): 539 – 554. (in Chinese)
[26] XIAO X, FU Z, ZHANG Y, et al. SMS – CQ: a quality and safety traceability system for aquatic products in cold-chain integrated WSN and QR code[J]. Journal of Food Process Engineering, 2017, 40(1): e12303.
[27] POON J, DRYJA T. The Bitcoin lightning network: scalable off-chain instant payments[J/OL]. https://lightning. network/lightning-networkpaper. pdf.
[28] BERGAN T, ANDERSON O,DEVIETTI J,et al. CryptoNote v 2.0[EB/OL]. https://www. mendeley. com/research-papers/cryptonote-v-20.