doi:10.6041/j.issn.1000-1298.2026.09.039

基于侧链的水产品跨链交易模型研究

邹一波[1,2]　诸葛文豪[1]　张　枫[3]　葛　艳[1,2]　陈　明[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;
3. 光明食品集团上海崇明农场有限公司, 上海 201303)

摘要: 跨链技术解决了水产品供应链各企业区块链之间的信息孤岛问题,但是在跨链交易过程中存在着隐私泄露的风险。为了提高水产品跨链交易的安全性和隐私性,基于水产品交易业务流程,在常用跨链技术的基础上,提出了基于侧链的水产品跨链交易模型。模型设计了主链和侧链资产互操作流程,用智能合约实现主链和侧链资产的双向锚定;基于水产品跨链交易的业务特点设计跨链数据的数据结构和跨链交易流程;使用三阶段提交协议保证跨链交易的数据一致性,提高交易成功率,完善交易失败时的处理流程;同时,针对侧链有可能带来的双花问题,采用监听方式加以控制。最后,基于 Hyperledger Fabric 平台实现基于侧链的水产品跨链交易原型系统。实验结果表明,该模型能有效避免主链接入跨链的私钥暴露,降低隐私泄露风险。在交易量较大的情况下,平均交易成功率稳定高于 99%,平均交易延迟时间稳定低于 0.3 s。并且,通过使用侧链能有效分担主链查询压力,使用超过 10 000 条数据的并行查询测试表明,查询效率提升约 35%。

关键词: 水产品交易; 跨链; 侧链; 智能合约; 区块链

中图分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1000-1298(2026)09-0406-13　　**OSID**:

Cross-chain Trading Model of Aquatic Products Based on Side Chain

ZOU Yibo[1,2]　ZHUGE Wenhao[1]　ZHANG Feng[3]　GE Yan[1,2]　CHEN Ming[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*
3. *Guangming Food Group Shanghai Chongming Farm Co., Ltd., Shanghai* 201303, *China*)

Abstract: The cross-chain technology addresses the issue of information silos between the blockchains of different enterprises in the aquatic product supply chain. However, there is a risk of privacy leakage during cross-chain transactions. To enhance the security and privacy of cross-chain transactions for aquatic products, based on the business processes of aquatic product transactions and existing cross-chain technologies, a cross-chain transaction model for aquatic products was proposed by using sidechains. The model designed an interoperation process for assets between the main chain and sidechains, and a two-way anchoring of assets between the main chain and sidechains was implemented through smart contracts. Based on the characteristics of aquatic product cross-chain transactions, the model designed the data structure and transaction process for cross-chain data. A three-phase commit protocol was used to ensure data consistency in cross-chain transactions, improve the transaction success rate, and refine the handling process for transaction failures. Additionally, to address the potential double-spending issue introduced by sidechains, a monitoring method was adopted for control. Finally, a prototype system for cross-chain transactions of aquatic products using sidechains was implemented on the Hyperledger Fabric platform. The system architecture was structured with dedicated functional modules to support secure asset transfer, cross-chain data validation, and coordinated transaction management across participating enterprises, ensuring robustness and operational efficiency. Experimental results showed that this model effectively prevented the exposure of private keys when connecting the main chain to cross-chain operations, reducing the risk of privacy leakage. Under high transaction volumes, the average transaction success rate

收稿日期: 2025-01-17　修回日期: 2025-03-09

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

remained consistently above 99%, and the average transaction delay remained below 0.3 s. Furthermore, by using sidechains to offload the query pressure on the main chain, parallel query tests with over 10 000 data points demonstrated a query efficiency improvement of approximately 35%.

Key words: aquatic product trading; cross-chain; side chain; smart contract; blockchain

0　引言

我国水产品国内供应总量不断增加，食用消费量增长趋势明显[1]。水产品供应链具有链条长、环节多、跨区域流通广泛、对实时性和溯源要求高的特点，给供应链的信息管理和交易安全带来了挑战[2-3]。其中，数据存储分散且格式不统一，导致供应链信息不连贯、透明度不足，容易引发信任危机[4]。区块链由于具有去中心化、透明性、不可篡改性、匿名性、可审核性的特点[5-6]，被广泛用于各个领域[7-12]，在水产品供应链领域也得到广泛应用。在溯源方面，提高溯源查询效率[13]，确保供应链的透明度、可信任性和安全性[14]。在水产品交易方面，实现安全高效的交易过程[15-17]。然而，由于不同供应链环节可能采用不同的区块链网络，区块链间的数据孤岛问题成为新的挑战。单一链条难以覆盖整个水产品供应链，数据难以跨链交互，导致信息无法有效流通，进而影响交易效率和供应链协作[18]。

跨链技术可以实现不同区块链之间的数据互通，提升水产品供应链中的交易效率和协作能力[19-20]。目前，区块链的常用跨链技术主要有公证人机制[21]、哈希锁定[22]、分布式私钥控制[23]和侧链/中继[24]。基于公证人机制的跨链交易模型[25]解决了水产品跨链交易过程中产生的单点故障问题。但公证人机制去中心化程度更低[26]。哈希锁定主要用于简单的资产交换，难以支持复杂的跨链智能合约和多资产交易，并且交易难以追溯[27-28]。因此，它常与其它跨链机制结合使用[22]。分布式私钥控制系统通过在去中心化网络中分片保存私钥，实现了资产的所有权和使用权分离[29]。然而，这种方法可能导致较大的交易延迟[30]。这些跨链方法在应对跨链系统中可能出现的安全性和隐私性风险时，仍然存在一些挑战。如中继机制，通常需要主链私钥进行验证和资产转移，不可避免地增加了私钥泄露的风险[31]。侧链是一个独立于主链的区块链系统，能通过双向锚定实现与主链的价值流通和资产转移[32]。侧链可以为主链增加新的功能，并提供更高的安全性和隐私性[33]。侧链/中继作为可扩展的跨链技术，具备自行验证交易数据的能力，且侧链和中继两者之间没有严格的界限。从形式上看，侧链更强调链之间的主从关系，而中继则被视为实现跨链通信的技术或解决方案[34]。

基于上述情况，为了提高跨链交易过程中安全性和降低隐私泄露的风险，本文提出基于侧链的水产品跨链交易模型，与传统侧链和中继各自独立运作的方式不同，将中继功能内嵌于侧链架构中。该模型在各个水产品供应链企业节点主链的基础上引入侧链参与交易，隔离主链的敏感数据，再通过通信模块和验证模块实现水产品区块链的跨链交互和数据同步，通过监听避免侧链使用可能产生的双花问题，设计基于三阶段提交协议的跨链交易流程，以解决交易阻塞和数据不一致问题，并实现安全、可信的跨链交易。

1　基于侧链的水产品跨链交易模型构建

1.1　跨链交易拓扑结构

在水产品从生产到消费者购买的过程中，涉及到一个完整的供应链。水产品供应链是指从水产品生产到被消费者购买之间的整个供应链条，水产品供应链按照业务逻辑分为养殖、加工、仓储、销售和运输 5 个环节[35]。基于侧链的水产品跨链交易拓扑图如图 1 所示。

用户节点是水产品供应链中不同企业的服务节点，每个节点提供了其产品的关键信息，并通过区块链技术确保信息的可靠性。在跨链交易中，用户节点也作为跨链交易的发起方或者接受方。

主链与侧链互操作模型是通过交易存在证明和双向锚定实现主链与侧链水产品信息、资产的安全转移和交互。主链是在水产品供应链下企业所使用的区块链，企业通过区块链确保产品溯源、验证产品真实性、监测库存和物流等方面。不同企业可以通过区块链共享数据，提高透明度和效率。侧链备份主链部分水产品的信息，包括了水产品种类、采收日期、饲料类型、用药记录等。跨链交易的业务数据来自主链，跨链交易产生的数据存储到侧链。在主链和侧链的互操作过程中，通过智能合约实现侧链的交易存在证明和双向锚定，并防止同一份资产减少两次的情况，保证主链和侧链数据交互结果的一致性。

主链的私钥仅用于主链自身的操作，避免在跨链过程中暴露私钥。交易发生时，主链数据（如资

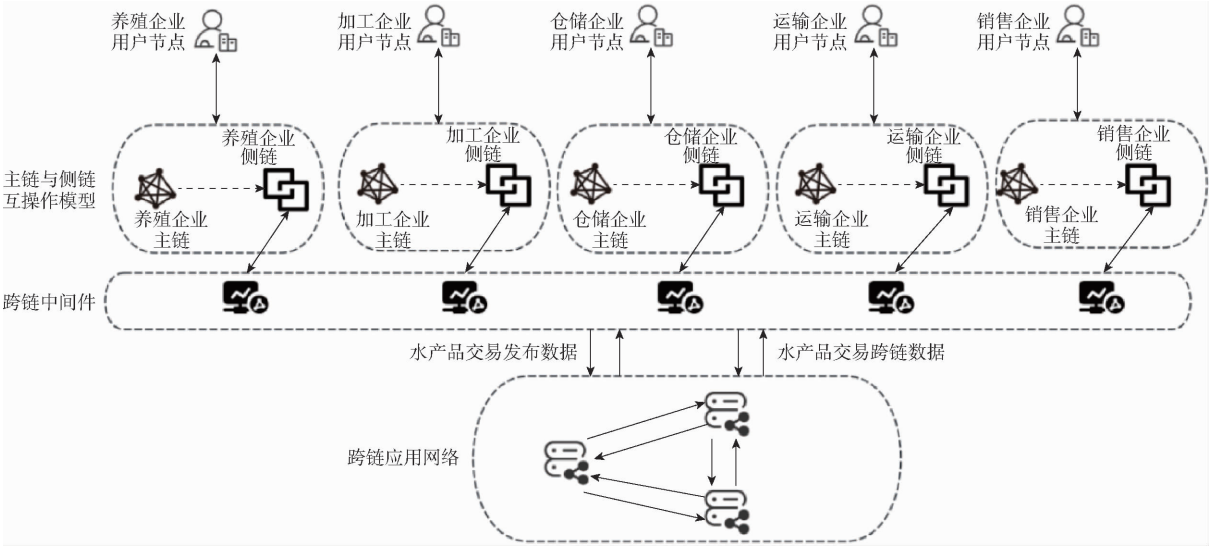


图 1 跨链交易拓扑图

Fig. 1 Topology of cross-chain transactions

产信息、敏感交易记录等)并不会直接在主链上进行跨链操作,而是通过在侧链上进行交易存证。只有当交易数据被提交到侧链时,才会涉及敏感信息的存储与验证。侧链作为一个独立的实体,确保了主链数据和敏感信息不被暴露,且主链的核心数据无法直接被篡改或访问。

跨链中间件和跨链应用网络共同组成跨链交易的通信模块和验证模块,实现中继的功能,完成不同企业用户节点的跨链交易。与水产品跨链业务相关的每条侧链都连接并适配了一个跨链中间件,用来连接到跨链应用网络。跨链中间件发布侧链中的水产品交易数据到跨链应用网络中。跨链应用网络传输水产品交易跨链数据进行跨链交易。

侧链、跨链中间件和跨链应用网络一起完成基于侧链的核心水产品跨链交易。侧链完成不同企业用户节点各自的跨链交易和存证。跨链中间件用于收集、传输交易信息、跨链交易信息,并适配接入侧链。跨链应用网络连接跨链中间件,实现对交易合同的签名、对交易信息的验证和展示跨链交易信息。水产品的跨链交易首先通过跨链应用网络完成水产品跨链交易的验证和确认,然后由跨链中间件传输水产品交易跨链数据,由侧链执行存证交易,最后由跨链应用网络完成确认。

1.2 主链与侧链互操作模型

交易过程借助主链与侧链协同完成时,需要考虑资产转移的安全性,交易的真实、有效性以及双花等问题。

双向锚定可以确保资产在主链与侧链之间安全转移,交易存在证明则可以验证跨链交易的真实性和有效性。主链与侧链的双向锚定和交易存在证明均可通过智能合约来实现。

双向锚定的原理是先在主链上锁定数字资产,侧链节点通过验证主链上的锁定交易后释放等值的数字资产。该等值数字资产在侧链上锁定并经过一定时间的确认后,主链上的数字资产在验证后被释放。主链和侧链的资产互相转移的过程中,通过对资产的锁定和释放,保证主链和侧链转移的原子性。

双花是一种常见的数据一致性攻击,指的是同一数字资产被用于两次支付[36]。为防止双花的出现,可以在主链和侧链添加资产的监听器。通过设计资产总量的数据结构,使用监听器对资产总量进行监听。如果主链与侧链交互时出现资产总量不一致的情况,则对该交互操作进行撤销,进而防止双花的出现,保证资产转移的安全性。

由此构建了主链与侧链互操作模型,如图 2 所示。在主链部署主链合约,其中包含与侧链通信的逻辑,在侧链部署侧链合约,其中包含与主链通信的逻辑。主链与侧链的互操作过程如下:

(1)根据水产品跨链业务需求,确认备份资产的范围。通过主链合约对侧链进行初始化,备份跨链所需的资产信息。

(2)通过主链合约将跨链所需的资产进行锁定。

(3)对锁定资产的操作进行存在性证明。查询锁定资产的数据,并对数据进行解析,将解析的数据与主链中的证书和实体进行对比,之后通过公钥解签背书策略中的签名对资产的操作进行存在性证明[37]。

(4)进行交易存在性证明后,通过侧链合约将主链对应锁定的资产增加到侧链资产。

(5)在侧链标记资产总量,主链的资产和侧链的资产合计后必须与标记的资产总量相等。设置主

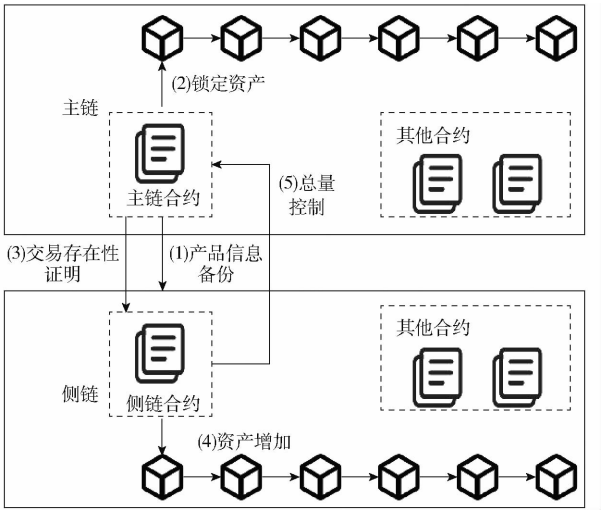


图 2　主链与侧链互操作模型

Fig. 2　Main chain and sidechain interoperability model

链和侧链资产变化的监听器，当侧链与其它区块链跨链交易后，才允许资产总量发生改变，从而有效地杜绝了双花现象。

2　水产品跨链交易业务数据定义

2.1　水产品交易基础数据定义

跨链中间件向跨链应用网络传递的水产品交易发布数据包括了供应链企业中不同种类水产品的资产数据。在水产品的跨链交易中针对不同企业间数据结构设计的差异性设计了通用数据结构和自定义数据结构。水产品交易跨链数据为水产品跨链交易过程中产生的数据。

由于水产品跨链交易中的不同环节在区块链中存储的数据结构各有不同，在跨链中需要有效的处理方法确保数据的完整性。本文根据水产品供应链不同环境的特点，设计通用数据结构，如表 1 所示，尽最大可能保证跨链过程中原有数据信息的完整性。然而，在实际应用中，部分环节可能涉及特殊业务需求，如水产品不同环节特定数据、特定企业标准等，这些数据无法完全适配通用数据结构。

表 1　水产品通用数据结构

Tab. 1　Generic data structure for aquatic products

参数信息	内容说明
supply_id	编号
supply_type	类型(养殖、加工、仓储、运输、销售)
batch_id	批次编号
quantity	数量
status	当前状态
custom	自定义

因此，本文允许对无法被通用数据结构涵盖的其他数据结构实现自定义存储，以满足跨链交易中不同业务场景的需求。例如，在加工企业的数据结构中，可能缺少用于存储养殖企业用药记录的字段，因此在跨链系统中，养殖企业需要创建自定义数据结构。跨链交易发生后，养殖企业该产品相关信息存储在加工企业的侧链中。加工企业需要获取养殖企业的生产数据时就不必通过跨链查询访问养殖企业侧链，既能减少跨链查询的频次，又能保证数据的完整性和可追溯性。

以养殖企业为例，表 2 为养殖企业自定义数据结构表。

表 2　养殖企业自定义数据结构

Tab. 2　Custom data structure for aquaculture enterprises

参数信息	内容说明
species	水产品种类
feed_type	饲料类型
harvest	采收日期
temperature	养殖水温范围
status	当前状态
medications	用药记录

以加工企业为例，表 3 为加工企业自定义数据结构表。

表 3　加工企业自定义数据结构

Tab. 3　Custom data structure for processing enterprises

参数信息	内容说明
plant	加工厂名称
processing_date	加工日期
method	加工方法
check	质量检查信息
accessories	加工辅料
operator	加工操作员

2.2　水产品交易跨链数据定义

水产品交易跨链数据是跨链交易模型中进行交易时产生的信息，具体参数信息如表 4 所示。参数 A、B 记录了交易双方主链的 ID(Identifier)，As、Bs 记录了此次交易中交易双方的侧链 ID。侧链通过 A、B 可以对主链锁定的产品持有数量进行验证。表 4 为跨链数据格式的内容。

S_Timestamp 记录了主链和侧链水产品资产转移的时间，能够确定交易顺序，并确保能够按照先后顺序执行跨链交易。S_Timestamp 能够防止系统堵塞，如果在跨链交易中执行跨链的时间超过一定时间则认定为堵塞，取消交易。通过查询 S_Timestamp 也能确认交易开始时间。

Message 保存了跨链交易的具体交易信息，由交易发起方提交，由跨链应用网络中的跨链应用传递给交易接收方进行确认，确认通过交易才能开始。

表 4 跨链数据

Tab. 4 Cross-chain data

参数信息	内容说明
A	主链交易证明
B	主链交易证明
As	发起链侧链 ID
Bs	目的链侧链 ID
S_Timestamp	权限转移时间戳
Message	跨链交易基本信息
A_Proof	跨链预执行证明
B_Proof	跨链预执行证明
Contract	双方签名后的合同
Extra_Proof	辅助验证信息

A_Proof、B_Proof 保存了跨链预执行信息,跨链应用通过 A_Proof 和 B_Proof 对 A、B 侧链的交易进行存在性证明。

Contract 是由交易合同产生的哈希字符串,交易时依次由跨链应用以及 A、B 签名。

Extra_Proof 存放跨链合同的地址,是签名和验证过程中使用的数据,作为辅助验证信息。

其中,跨链交易基本信息(Message)如表 5 所示,包含交易开始时间、交易数量、交易有效日期、付款方式、价格、附加条款和交易提交时间。交易提交时间(EndTime)为 0,并且不可修改,用于最后对交易进行提交和验证。

表 5 跨链交易基本数据

Tab. 5 Basic data for cross-chain transactions

参数信息	内容说明
StartTime	交易开始时间
TNumber	交易数量
Rxpiry	交易有效日期
Payment	付款方式
Price	价格
Additional	附加条款
EndTime	交易提交时间

3 基于侧链的水产品跨链交易流程设计

为了在跨链交易中保证交易数据的原子性,通常使用二阶段提交协议作为跨链交易的一致性协议[25]。然而二阶段提交协议只有“准备阶段”和“提交阶段”,在使用二阶段提交协议进行的跨链交易中,如果因为网络等原因在“提交阶段”发生崩溃时,交易的参与者可能会一直等待,导致交易阻塞。此外,在二阶段提交协议“提交阶段”时,若部分参与者因网络等原因未完成提交,会导致交易结果不一致。

因此,本文将交易分成了 CanCommit、PreCommit 和 DoCommit 共 3 个阶段,对侧链和跨链应用都引入了超时机制[38]。

以养殖企业和加工企业的跨链交易为例,水产品跨链交易的具体流程如下。

3.1 CanCommit 阶段

CanCommit 阶段流程时序图如图 3 所示。

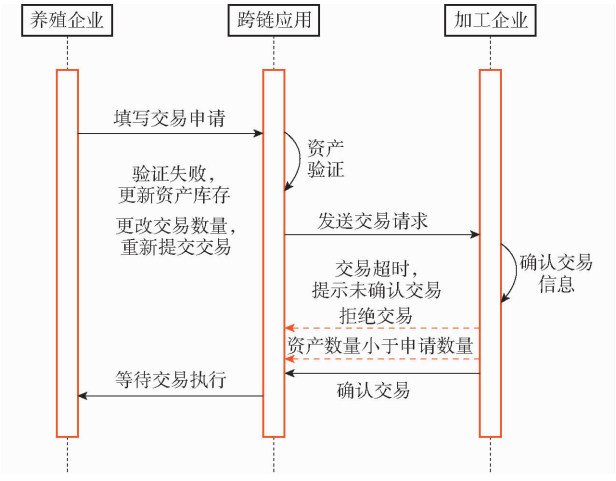


图 3 CanCommit 阶段流程时序图

Fig. 3 Sequence diagram of CanCommit phase process

(1)养殖企业通过跨链应用发起交易申请。养殖企业选择已在跨链应用中注册的交易对象,选择养殖企业链中需要交易的资产。交易申请内容分为 3 个部分:养殖企业链的资产信息、自定义信息和交易信息。交易信息中包含了交易开始时间、交易数量、价格、交易有效日期、附加条款以及合同。

跨链应用将交易信息中的合同上传到服务器中,将合同地址写入到跨链数据的辅助验证信息中。跨链应用对交易数量进行规则校验,当资产交易数量超过养殖企业链剩余数量时,提示非法交易申请。

(2)跨链应用通过跨链中间件调用智能合约查询该侧链资产的库存是否充足。如果查询失败则提示养殖企业查询失败或资产库存不足,如果查询成功但资产不足,则更新资产库存并提示修改资产交易数量。

(3)跨链应用将交易申请提交给加工企业。加工企业查看交易内容,并对交易进行确认。跨链应用等待加工企业确认交易,如果等待交易超过交易信息中的交易有效日期,则交易失败,向养殖企业提示“加工企业未确认交易”。如果加工企业拒绝交易,则跨链应用向养殖企业提示“加工企业拒绝交易”。

当跨链应用等待加工企业确认交易时,库存资产数量可能会由于养殖企业与其他企业交易而发生变化,所以当加工企业确认交易时会重新进行一次资产查询,确认需要交易的资产数量大于库存资产

数量。

(4)加工企业确认交易后,跨链应用对水产品交易资产进行锁定,防止在并发交易过程中出现水产品资产数量不一致的情况。资产状态从“正常”变更为“交易中”,交易进入 PreCommit 阶段。

3.2　PreCommit 阶段

PreCommit 阶段流程时序图如图 4 所示。

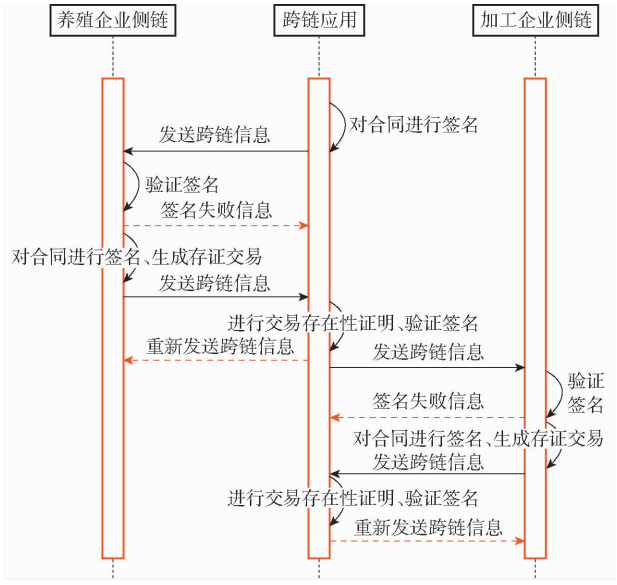


图 4　PreCommit 阶段流程时序图

Fig. 4　Sequence diagram of PreCommit phase process

(1)跨链应用使用私钥对合同地址进行签名,将生成的哈希字符串写入到跨链数据的 Contract 中。

(2)跨链应用通过跨链中间件将跨链数据发送到养殖企业侧链。

(3)养殖企业侧链调用智能合约,使用公钥对 Contract 字段进行验证,确认交易是否由跨链应用签名。如果验证失败,则通过跨链中间件返回签名失败信息,重新执行 PreCommit 阶段。

(4)养殖企业侧链使用私钥对合同签名,生成存证交易,将交易写入区块链中,并将交易存在证明字段写入 A_Proof 字段,最后通过跨链中间件将跨链数据发送到跨链应用。此时,养殖企业侧链将交易资产锁定,进入交易等待状态并生成存证交易。主链和侧链的资产总量不变,等待最终交易提交。

(5)跨链应用通过验证 A_Proof 字段验证交易是否执行,随后验证 Contract 是否已由养殖企业签名,验证成功后将跨链数据通过跨链中间件发送到加工企业侧链。如果验证失败,则重新发送跨链数据。

(6)加工企业侧链调用智能合约,使用养殖企业和跨链应用的公钥进行验证。加工企业侧链验证签名后,使用私钥对合同进行签名,生成存证交易,并将交易存在证明字段写入 B_Proof 字段,最后通过跨链中间件将跨链消息发送到跨链应用。如果验证失败,则通过跨链中间件返回签名失败信息,重新执行 PreCommit 阶段。

(7)跨链应用验证 B_Proof 字段验证交易是否执行,随后验证 Contract 是否已由加工企业签名,验证成功交易进入 DoCommit 阶段。如果验证失败,则重新发送跨链数据。此时,加工企业侧链将交易资产锁定,进入交易等待状态。

3.3　DoCommit 阶段

DoCommit 阶段流程时序图如图 5 所示。

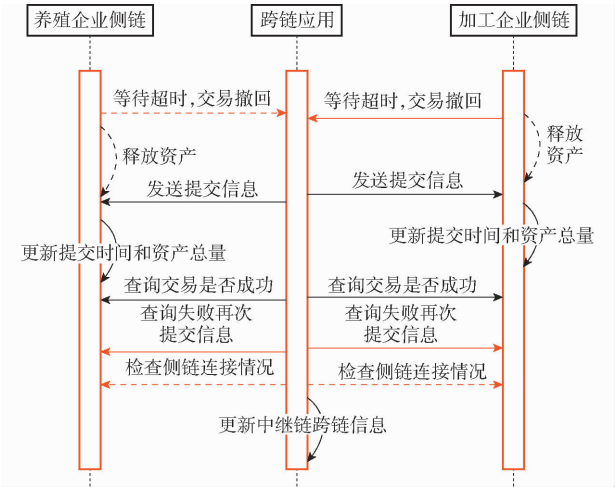


图 5　DoCommit 阶段流程时序图

Fig. 5　Sequence diagram of DoCommit phase process

(1)在提交最终交易前,若两方侧链等待超时,则判断为跨链失败,交易撤回,释放双方侧链锁定的资产。

(2)跨链应用记录提交时间,更新跨链数据中的交易提交时间,向跨链双方侧链发送提交信息。

(3)侧链收到提交信息后,更新交易提交时间和资产总量。

(4)跨链应用通过跨链中间件查询侧链区块,查询交易提交时间。如果查询结果为 0,则表示交易提交未成功,重新发送提交信息,并再次提交查询。

(5)若多次查询失败,并且交易超时,则将交易撤回,并检查跨链应用和侧链的连接情况。

(6)如果查询成功,则向养殖企业和加工企业提示跨链交易成功信息,并更新跨链应用中跨链双方的资产信息。

通过三段式的交易流程设计,将参与者双方的交易过程分为对交易的确认、交易的预执行以及交易的最终提交,并分别在 CanCommit 阶段、PreCommit 阶段、DoCommit 阶段执行。相较于二阶段提交协议,在 PreCommit 阶段向参与交易的双方

都增加了超时机制,如果因为网络等原因系统无法进行最终提交,参与交易双方会通过智能合约自动将交易撤回,防止了区块链因系统等待跨链应用的最终提交造成的堵塞问题。除此之外在最终提交后系统还会检查双方的执行结果,防止出现交易执行结果不一致的问题。

4 关键智能合约设计

4.1 主链与侧链互操作智能合约

主链和侧链分别部署各自的智能合约,通过双向锚定机制在主链上备份数据并锁定资产,同时在侧链上增加对应的资产。在侧链增加资产前,需要对主链锁定的资产进行操作存在性证明。设定主链和侧链的资产监听器,防止主链和侧链的资产总量因为双花发生变化。

(1)备份主链数据并导入到侧链

根据水产品跨链交易的业务需求确定需要转移的主链资产,然后创建主链该资产对应的数据结构数组,将主链数据保存到该数组后,转换成 JSON 格式传输到侧链中,算法如下:

```
//输入:需要备份的资产、侧链名称
//输出:资产导出结果
Function ExportAssets( ):
    // 查询需要备份的资产信息
    select_asset, err = Query asset information from blockchain
    //声明主链资产数组 assets,用于存放查询结果
    Declare assets as Array of Asset
    // 将资产信息转换为 JSON 格式
    assetsJSON = Convert assets to JSON
    // 调用侧链链码,将主链资产备份到侧链中
    Invoke chaincode on sidechain with assetsJSON
End Function
```

(2)在侧链中导入资产信息

根据业务需求创建与主链锁定资产相同的数据结构,将主链传入的 JSON 格式数据转换成该数据结构格式的数据。为了保证资产锁定和释放的原子性,在侧链导入资产信息时由于主链资产没有锁定,不涉及资产数量的变化,因此此时需要将资产数量设置为 0,算法如下:

```
//输入:主链传来的资产信息
//输出:资产导入结果
Function ImportAssets( ):
    // 声明侧链资产数组 assets
    Declare assets as Array of Asset
    // 初始化侧链资产数量为 0
    Set assets. value = 0
    // 保存查询的资产信息到区块链
    Store assets on the blockchain
End Function
```

(3)主链锁定资产

为了尽可能减少侧链接入对原先主链的影响,在对主链资产进行锁定时不对原先的数据结构进行改动,而是在原先数据结构基础上标记锁定资产数量,算法如下:

```
//输入:需要锁定资产的 ID 和数量
//输出:锁定资产的结果
Function LockAssets( ):
    // 根据锁定资产的 ID 查询资产信息
    assetJSON = Query asset information by assetID from blockchain
    // 声明主链资产和锁定资产的数组
    Declare asset as Asset
    Declare assetf as AssetF
    // 根据锁定资产的数量调整资产状态
    asset. value = asset. value - lock_value
    assetf. value = assetf. value + lock_value
    // 标记资产为锁定状态
    assetf. frozen = true
    // 保存更新后的资产信息到区块链
    Store asset and assetf on the blockchain
End Function
```

(4)验证锁定资产存在性证明

通过 Fabric SDK(Fabric software development kit)对主链资产锁定进行存在性证明。通过锁定资产的 ID 获取该资产进行锁定操作的区块 ID,对获取区块的的数据进行解签,将解签的数据与侧链保存的 MSPID(Membership service provider identifier)与序列化的证书信息对比后,根据公钥解签结果,如果对比正确,则证明主链锁定资产操作存在并且合法,算法如下:

```
//输入:主链证书地址、锁定资产的 ID 和数量
//输出:验证是否通过
Function LockProof( ):
    // 获取资产锁定 ID
    lock_id = Get transaction ID from response
    // 根据 ID 查询执行资产锁定的区块
    block = Query block information by lock_id
    // 从区块中获取链码执行的相关数据
    payload = Extract payload from block
    // 解析数据字段,获取 MSPID 和序列化的证
```

```
书信息
    lock_action_payload = Decode payload to extract MSPID and certificate details
    // 比对 MSPID 和证书,并使用公钥验证背书策略中的签名
    verification _ result = Compare MSPID and certificate, then verify signature
    // 返回验证结果
    Return verification_result
End Function
```

(5)侧链释放资产

验证存在性证明通过后,在侧链释放资产,算法如下:

```
//输入:需要释放资产的 ID 和数量
//输出:释放资产是否成功
Function UnlockAssets( ):
    // 根据锁定资产的 ID 查询资产信息
    assetJSON = Query asset information by assetID
    // 声明侧链资产对象
    Declare asset as Asset
    // 根据传入的资产数量释放资产
    asset. value = asset. value + unlock_value
    // 保存释放后的资产信息到区块链
    Store updated asset on the blockchain
End Function
```

(6)总量控制

为了防止双花,在主链和侧链上持续监听和标记资产总量的变化。在进行资产操作时,都要调用以下 HandleAsset( )方法,如果在未发生跨链交易,资产总量发生变化,则撤销此次操作。发生跨链交易时,根据交易内容更新资产总量。

```
//单独创建资产总量的数据结构
type TotalAssets struct{
    AssetsID int ‘json:“asstesid”’
    Total int ‘json:“total”’
    }
//在侧链上监听主链和侧链的资产总量变化
//输入:此次资产操作的资产 ID
//输出:资产总量是否发生变化
Function HandleAsset( ):
    // 获取当前资产总量
    totalAssetsJSON = Query total assets information
    // 根据资产 ID 查询侧链资产
    assetSideJSON = Query sidechain asset by assetID
    // 根据资产 ID 查询主链资产
    assetMainJSON = Query mainchain asset by assetID
    // 检查主链和侧链资产总量是否与总资产一致
    If totalAssets. total ! = assetSide. value + assetMain. value Then
        Return false // 数据不一致,返回错误
    End If
    // 数据一致,返回成功
    Return true
End Function
```

4.2 跨链智能合约

跨链智能合约是指在跨链交易 3 阶段提交过程中使用的智能合约,确保不同区块链数据和状态变更的一致性,确保跨链交易的原子性,并且在故障发生时进行数据恢复。

交易预执行阶段,修改侧链资产数量。修改侧链资产数量后,主链和侧链的资产总量发生变化,然而 TotalAssets 数据结构中存储的资产总量没有发生变化,如果此时执行总量监控函数 HandleAsset( ),则一定会发生错误。在交易预执行和等待交易提交时需要中断总量监控函数 HandleAsset( )。交易撤回阶段,在提交最终交易前,若交易失败,则交易撤回,重新执行总量监控函数 HandleAsset( )。交易提交阶段,通过更改 TotalAssets 数据结构中的资产总量对交易进行最终提交。以下为合同签名和验证合同签名。

(1)合同签名

在交易的 PreCommit 阶段,跨链应用使用私钥对合同进行签名。签名完成后,将数据写入到 Contract 字段,在其他企业进行存证交易前,对该字段使用跨链应用的公钥进行验证,即可证明该跨链数据可信。使用椭圆曲线数字签名算法(Elliptic curve digital signature algorithm,ECDSA)进行签名和认证,算法如下:

```
//输入:跨链数据字符串,私钥
//输出:跨链数据
Function RelaySign( ):
    // 声明存放跨链数据的变量
    Declare cross_info as CrossInfo
    // 生成合同地址的哈希值
    Hash = Hash ( cross _ info. Extra _ Proof using SHA - 256)
    // 使用私钥对合同地址的哈希值进行签名
    (r, s) = Sign(Hash using private key)
    // 将签名转换为字符串
```

```
    signature = Convert (r, s) to Base64 encoded string
    // 将签名写入跨链数据的 Contract 字段
    cross_info. Contract = signature
    // 返回跨链数据
    Return cross_info
End Function
```

(2)验证合同签名

在侧链对跨链数据中的 Contract 字段进行验证,算法如下:

```
//输入:跨链数据字符串,跨链应用公钥,侧链私钥
//输出:验证结果、跨链数据
Function VerifyAndSign( ):
    // 声明存放跨链数据的变量
    Declare cross_info as CrossInfo
    // 生成合同地址的哈希值
    hash = Hash ( cross _ info. Extra _ Proof using SHA - 256)
    // 解码存储在 Contract 字段中的签名字符串
    signature = Decode Base64 string from cross _ info. Contract
    // 分割签名为 r 和 s
    (r, s) = Split signature into two parts
    // 验证签名是否有效
    valid = Verify(Hash, r, s using public key)
    // 如果验证失败,返回错误信息
    If valid = = false Then
        Return "Error: Signature verification failed"
    // 使用私钥对合同地址的哈希值重新签名
    (r, s) = Sign(Hash using private key)
    // 将新签名转换为字符串并写入 Contract 字段
    signature = Convert (r, s) to Base64 encoded string
    cross_info. Contract = signature
    // 返回更新后的跨链数据
    Return cross_info
End Function
```

5 系统测试

5.1 系统实现

本文基于侧链的水产品跨链交易模型,开发了一个基于侧链的跨链交易系统,该系统以 Hyperledger Fabric 作为区块链的主链和侧链架构基础,采用 Go 语言搭建跨链应用的后端平台,使用 JavaScript 和 Vue 框架设计与开发前端界面。跨链中间件采用 Go 语言和 Shell 语言进行开发,将跨链中间件打包到跨链应用中供水产品供应链中的企业进行下载。其中,Go 作为主要逻辑处理,Shell 脚本负责区块链数据的操作、配置文件的修改、Docker 容器的部署。通过编写不同版本的 Shell 脚本能够使中间件适应各种复杂的区块链环境。

跨链系统的开发环境为 GO 1.21.3、Node 16.20.2、Vue 5.0.8。实验环境为 Ubuntu 22.04.6,Docker 的版本为 26.1.3,区块链框架 Hyperledger Fabric 版本为 2.2。在实验中,分别在水产品养殖链和加工链的主链中设置 3 个 Org(Organization)组织,并分别在其侧链中设立两个 Org 组织。

水产品跨链交易的上链数据采用 JSON 格式存储。以养殖企业自定义数据结构为例,以 JSON 格式存储的数据格式如下:

```
&Aquaculture{
"supply_id": "string"        //养殖编号
"supply_type": "string"      //类型(养殖)
"batch_id": "string"         //批次编号
"quantity": "number"         //数量
"status": "string"           //当前状态
"custom":{                   //自定义
    "species": "string"      //水产品种类
    "feed_type": "string"    //饲料类型
    "hatch": "date"          //孵化日期
    "harvest": "date"        //采收日期
    "temperature": "string"  //养殖水温范围
    "medications":"string"   //用药记录
        }
}
```

企业资产管理界面如图 6 所示,企业可以从该界面查看水产品资产信息。从企业资产管理界面点击详情查看水产品资产的详细信息,如图 7 所示。从企业资产管理界面点击交易申请可以填写交易申请信息,如图 8 所示。在填写交易申请信息界面,点击下拉条选择已注册的企业对象。填写的交易开始时间无法选中过去的时间,交易数量不能大于该资产剩余数量。

交易接受界面如图 9 所示,以加工企业 A 为例,加工企业在登录后可以看到养殖企业 A 对自己发起的交易申请,加工企业 A 点击查看详情可以查看到该水产品与图 7 相同的水产品详细信息,此时加工企业 A 可以选择是否接受交易。加工企业 A 确认交易后,该数量的资产会转移到加工企业侧链中,此时加工企业 A 可以在资产管理界面查看到已经接受的交易资产。



图 6　养殖企业 A 资产管理界面

Fig. 6　Asset management interface for aquaculture enterprise



图 7　水产品资产详细信息界面

Fig. 7　Detailed asset information interface for aquatic products



图 8　交易申请信息填写界面

Fig. 8　Transaction application information entry interface



图 9　交易接受界面

Fig. 9　Transaction acceptance interface

5.2　性能测试

本文采用 Caliper 作为性能测试工具，对基于侧链的跨链交易系统跨链交易的平均交易成功率和平均交易延迟进行测试。

设置 Caliper 的速率控制器为 fixed-rate 模式，以固定的每秒交易并发量（Transactions per second，TPS）发送交易。以控制固定数量交易测试交易的延迟和交易成功率。总交易量分别设定为 3 000、5 000、7 000，进行 10 轮测试，计算得出 10 轮测试的平均交易延迟和平均交易成功率。如图 10、11 所示，基于侧链的跨链交易平均延迟在 0.28 s 左右，平均交易成功率在 99% 以上。在侧链中使用预执行和最终确认执行的方式能有效防止交易双方结果不一致的情况，虽然等待最终确认的过程会导致交易延迟增加，但增加的时间不超过 100 ms，不影响实时交易。

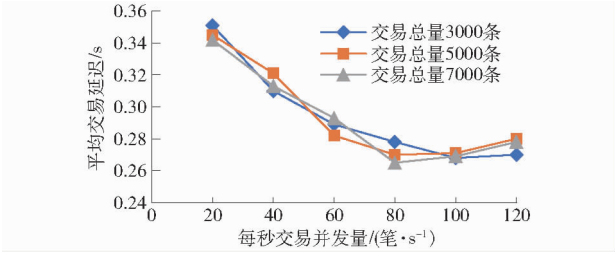


图 10　交易延迟对比结果

Fig. 10　Transaction delay comparison results

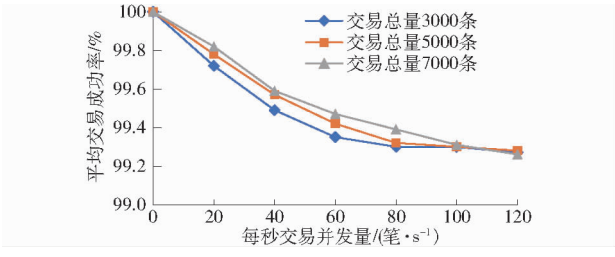


图 11　交易成功率对比结果

Fig. 11　Transaction success rate comparison results

在 Hyperledger 中，排序服务节点 Orderer 负责进行排序服务，多个交易在 Orderer 排序后打包成区块。在低 TPS 时，Orderer 需要等待交易填充，导致单笔交易延迟较高，随着 TPS 增加到 80 笔/s，区块更快被填满降低了交易延迟。随着总交易量的增加，平均交易延迟和平均交易成功率随着每秒交易数增加而减少。平均交易成功率的降低延缓了平均交易延迟下降的趋势，当平均交易成功率稳定在

99.27% 左右时,交易延迟反而会上升,此时每秒交易数接近系统上限。

根据主链和侧链的查询效率,分别分配主链和侧链的查询数量进行并行查询,能够在一定程度减少查询时间,并减少主链的查询压力。由于在侧链初始化后备份了部分主链的资产信息,并设置了资产总量监听器,在查询资产时从监听器中获得数据资产数量的数据,其它详细信息在主链中和侧链中相同。

由于不同侧链查询速度不同,根据不同查询速度的侧链分配最优主链和侧链的查询数量,能使用 Caliper 计算出最低的基于侧链并行查询消耗时间。最优分配查询数量的计算公式为

$$T_1 = \frac{q_1}{s_1} \tag{1}$$

$$T_2 = \frac{q_2}{s_2} \tag{2}$$

$$q_2 = Q - q_1 \tag{3}$$

$$T = |T_1 - T_2| \tag{4}$$

式中 T_1、T_2——主链、侧链的查询时间

q_1、q_2——待分配给主链、侧链的查询数量

s_1、s_2——主链、侧链的查询速度

Q——查询的总数

T——主链和侧链查询时间的差值

通过动态调整 q_1 和 q_2 的值使 T 达到最小。

性能测试的具体过程为:

(1)首先,使用测试工具对主链和侧链进行多次测试,获取主链和侧链查询速度平均值 s_1 和 s_2。由于主链和侧链的查询是并行执行,当 T 无限接近于 0 时,查询时间最短。设定固定数量 Q,联立公式(1)~(4)即可获得 q_1 和 q_2。

(2)其次,固定数量 Q,使用测试工具测得主链的查询时间 t_1 和将 Q 分配给 q_1、q_2 的侧链并行查询时间 t_2。

设置 Caliper 的速率控制器为 fixed-load 模式,通过修改每秒查询量确定系统的最短查询时间。由此可以计算出当 Q = 5 000 时,主链最快的执行时间为 23.811 s。分配为 q_1、q_2 后,测得基于侧链并行查询最优时间为 16.953 s。

使用同样的方法测试 Q 为 2 000、3 500、5 000、6 500、9 000 条交易时的 t_1 和 t_2 值,如图 12 所示。

(3)最后,用侧链的并行查询时间与单一主链查询时间进行比较,计算效率提升率,计算公式为

$$E = \frac{t_1 - t_2}{t_1} \times 100\% \tag{5}$$

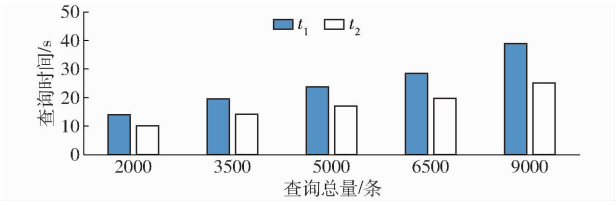


图 12 主链和基于侧链并行查询时间对比图

Fig. 12 Comparison of main-chain and side-chain-based parallel query times

式中 E——加入侧链后的架构相较于单链架构提升率,%

当查询总量 Q 分别为 2 000、3 500、5 000、6 500、9 000 条时,基于侧链的水产品交易架构相较于单一主链架构查询效率提升率 E 分别为 27.26%、28.18%、28.8%、31.06%、35.80%。当查询总量在 10 000 条以下时,查询效率增长率随着查询总量的增加而增长,当查询总量 Q 大于 10 000 条时,E 趋近于 35% 左右。由于侧链可以独立于主链并行处理查询操作,侧链与侧链间的负载也不会相互影响,所以提升的效率较为明显,并且侧链的性能越高,对主链查询效率的提升就会越大。

6 结论

(1)在安全性方面,在私钥的管理过程中需要避免私钥泄露的风险。使用其它跨链方式进行跨链时,由于对跨链节点的安全性和诚实性的过分依赖,如果跨链节点出现故障或被攻击,跨链交易信息和主链的数据可能会被篡改。本文提出的侧链的跨链方式,一旦私钥泄露,黑客和恶意方也只能对侧链进行篡改。并且主链留有数据备份,锁定的资产也能在主链释放,能将损失和风险降到最低。

(2)在隐私性方面,单独使用中继其它跨链方式进行跨链的所有交易数据都依赖中继跨链节点转发,并且可能在多个链上进行公开验证,缺乏对敏感数据的保护机制。在使用侧链跨链交易的访问控制机制失效时,也只会导致侧链的交易业务数据泄露,进而有效防止主链敏感信息泄露。

(3)在系统性能方面,基于侧链的水产品跨链交易系统平均交易成功率达 99% 以上,交易延迟在 0.28 s 左右。在侧链中使用超时机制能解决二阶段提交协议过程中的交易阻塞,使用预执行和最终确认执行的方式能在不影响实时交易的条件下有效防止交易双方结果不一致的情况。

(4)在系统效率方面,跨链交易的业务数据只在各自侧链上执行和记录,随着交易数量的增加,能有效防止主链的网络拥塞和性能瓶颈,并且减少了跨链交易和非跨链交易之间的冲突风险,进而防止

不同业务场景的交易混合可能导致意外的错误和不一致性。性能测试表明，侧链通过并行处理显著提升了查询效率，且侧链性能越高，对主链查询性能的提升效果越显著。由此可见，将部分查询需求和交易需求较高、非敏感的业务数据从主链转移到侧链，可以提升整个主链网络的吞吐量和效率。

参 考 文 献

[1] 中国居民水产品食用消费量. 测算与分析报告(2023)[EB/OL]. [2024 - 05 - 04]. https://www.crnews.net/cy/sc/959866_20231228104059.html.

[2] PIZZUTI T, MIRABELLI G, SANZ-BOBI M A, et al. Food track & trace ontology for helping the food traceability control[J]. Journal of Food Engineering, 2014, 120: 17 - 30.

[3] KUMAR A, MANGLA S K, KUMAR P. An integrated literature review on sustainable food supply chains: exploring research themes and future directions[J]. Science of the Total Environment, 2022, 821: 153411.

[4] 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)

[5] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352 - 375.

[6] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017: 557 - 564.

[7] TURKANOVIC M, HOLBL M, KOSIC K, et al. EduCTX: a blockchain-based higher education credit platform[J]. IEEE Access, 2018, 6: 5112 - 5127.

[8] LIANG G, WELLER S R, LUO F, et al. Distributed blockchain-based data protection framework for modern power systems against cyber attacks[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 3162 - 3173.

[9] BLOCK J H, COLOMBO M G, CUMMING D J, et al. New players in entrepreneurial fi-nance and why they are there[J]. Small Business Economics, 2018, 50: 239 - 250.

[10] ESPOSITO C, DE SANTIS A, TORTORA G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy? [J]. IEEE cloud computing, 2018, 5(1): 31 - 37.

[11] LAMBERTI F, GATTESCHI V, DEMARTINI C, et al. Blockchains can work for car insurance: using smart contracts and sensors to pro-vide on-demand coverage[J]. IEEE Consumer Electronics Magazine, 2018, 7(4): 72 - 81.

[12] KHAN M A, SALAH K. IoT security: review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2018, 82: 395 - 411.

[13] 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. 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)

[14] LUNA M, FERNANDEZ-VAZQUEZ S, TEREÑES CASTELAO E, et al. A blockchain-based approach to the challenges of EU's environmental policy compliance in aquaculture: from traceability to fraud prevention[J]. Marine Policy, 2024, 159: 105892.

[15] 王文娟, 汪海燕, 陈明, 等. 基于多链存储优化的水产品交易匹配模型研究[J]. 农业机械学报, 2024, 55(6): 272 - 283.
WANG Wenjuan, WANG Haiyan, CHEN Ming, et al. Aquatic product trading matching model based on multi-chain storage optimization[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(6): 272 - 283. (in Chinese)

[16] 王文娟, 张旭, 陈明, 等. 基于区块链的水产品撮合交易模型与系统实现[J]. 农业机械学报, 2023, 54(1): 364 - 375.
WANG Wenjuan, ZHANG Xu, CHEN Ming, et al. Trading matching model and system implementation for aquatic products based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(1): 364 - 375. (in Chinese)

[17] HUANG X R, SU C W, CHEN L B. A production and marketing platform model based on the AIoT and blockchain system for aquaculture[C]//2023 International Conference on Consumer Electronics - Taiwan (ICCE - Taiwan). IEEE, 2023: 623 - 624.

[18] DASAKLIS T K, VOUTSINAS T G, TSOULFAS G T, et al. A systematic literature review of blockchain-enabled supply chain traceability implementations[J]. Sustainability, 2022, 14(4): 2439.

[19] DING Y, ZHANG Y, QIN B, et al. A scalable cross-chain access control and identity authentication scheme[J]. Sensors, 2023, 23(4): 2000.

[20] SI H, LI W, SU N, et al. A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem [J]. Computer Communications, 2024, 223: 68 - 80.

[21] XIONG A, LIU G, ZHU Q, et al. A notary group-based cross-chain mechanism[J]. Digital Communications and Networks,

2022, 8(6): 1059 – 1067.
[22] SUN Y, YI L, DUAN L, et al. A decentralized cross-chain service protocol based on notary schemes and hash-locking[C]// 2022 IEEE International Conference on Services Computing (SCC). IEEE, 2022: 152 – 157.
[23] KATE A, GOLDBERG I. Distributed private-key generators for identity-based cryptography[C]// International Conference on Security and Cryptography for Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 436 – 453.
[24] WANG H, HE D, WANG X, et al. An electricity cross-chain platform based on sidechain relay[C]// Journal of Physics: Conference Series. IOP Publishing, 2020: 012189.
[25] 邹一波, 景虎, 陈明, 等. 基于公证人机制的水产品跨链交易模型研究[J]. 农业机械学报, 2024, 55(6): 262 – 271.
ZOU Yibo, JING Hu, CHEN Ming, et al. Cross-chain trading model of aquatic products based on notary mechanism[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(6): 262 – 271. (in Chinese)
[26] MOHANTY D, ANAND D, ALJAHDALI H M, et al. Blockchain interoperability: towards a sustainable payment system[J]. Sustainability, 2022, 14(2): 913.
[27] 李光柱, 李雷孝, 高昊昱. 跨链技术发展与应用研究进展[J]. 计算机工程与应用, 2024, 60(2): 32 – 45.
LI Guangzhu, LI Leixiao, GAO Haoyu. Cross-chain technology development and application research[J]. Computer Engineering and Applications, 2024, 60(2): 32 – 45. (in Chinese)
[28] YEH K H, YANG G Y, BUTPHENG C, et al. A secure interoperability management scheme for cross-blockchain transactions[J]. Symmetry, 2022, 14(12): 2473.
[29] MAO H, NIE T, SUN H, et al. A survey on cross-chain technology: challenges, development, and prospect[J]. IEEE Access, 2022, 11: 45527 – 45546.
[30] DUAN L, SUN Y, NI W, et al. Attacks against cross-chain systems and defense approaches: a contemporary survey[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10(8): 1647 – 1667.
[31] 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.
[32] YIN L, XU J, TANG Q. Sidechains with fast cross-chain transfers[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(6): 3925 – 3940.
[33] SINGH A, CLICK K, PARIZI R M, et al. Sidechain technologies in blockchain networks: an examination and state-of-the-art review[J]. Journal of Network and Computer Applications, 2020, 149: 102471.
[34] OU W, HUANG S, ZHENG J, et al. An overview on cross-chain: mechanism, platforms, challenges and advances[J]. Computer Networks, 2022, 218: 109378.
[35] 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)
[36] IQBAL M, MATULEVICIUS R. Exploring sybil and double-spending risks in blockchain systems[J]. IEEE Access, 2021, 9: 76153 – 76177.
[37] 梁瑞岿, 隋爱娜, 韩鹏斌, 等. 面向 Fabric 的跨链可行性方法研究[J]. 中国传媒大学学报(自然科学版), 2023, 30(1): 47 – 52.
LIANG Ruikui, SUI Aina, HAN Pengbin, et al. Research on cross-chain feasibility method for Fabric[J]. Journal of Communication University of China (Science and Technology), 2023, 30(1): 47 – 52. (in Chinese)
[38] KEIDAR I, DOLEV D. Increasing the resilience of distributed and replicated database systems[J]. Journal of Computer and System Sciences, 1998, 57(3): 309 – 324.