doi:10.6041/j.issn.1000-1298.2023.12.037

基于属性访问控制模型的果蔬跨链追溯系统设计与实现

杨信廷[1,2]　李金辉[1,2]　罗　娜[2,3]　邢　斌[2,3]　孙传恒[2,3]

(1.江苏大学农业工程学院,镇江 212013;2.北京市农林科学院信息技术研究中心,北京 100097;
3.农产品质量安全追溯技术及应用国家工程研究中心,北京 100097)

摘要:针对现有果蔬农产品供应链中存在的上下游区块链间追溯数据差异化、细粒度共享困难以及数据隐私保护等问题,通过分析果蔬农产品供应链各环节业务流程,在果蔬农产品质量安全追溯场景下,提出了一种支持异构多链的基于属性的果蔬跨链追溯访问控制模型。该模型利用基于中继链的跨链技术将跨链信息标准化从而实现异构多链之间的跨链通信,并结合果蔬跨链追溯需求,采用基于 ABAC(Attribute-based access control)的访问控制模型实现对数据资源灵活、细粒度访问控制。为验证模型有效性,利用 BitXHub 中继链技术在 Hyperledger Fabric 和 Ethereum 构成的异构链中实现跨链数据访问,在跨链合约中实现基于属性的访问控制流程,构建出果蔬追溯跨链访问控制模型的原型系统。系统测试结果表明,中继链处理跨链交易的发送率平均最高值分别约为 600 笔/s 和 400 笔/s,策略判定时间不会随着策略数目的增加而有较大波动,基本稳定在 2 000 ms 左右,能够满足果蔬供应链在异构区块链之间跨链数据差异化、细粒度共享的需求,也保证了数据共享过程中的数据隐私性。

关键词:果蔬供应链;异构多链;跨链;访问控制;属性访问控制

中图分类号:TP309.2　　**文献标识码**:A　　**文章编号**:1000-1298(2023)12-0376-13　　**OSID**:

Fruit and Vegetable Cross-chain Traceability System Based on Attribute Access Control Models

YANG Xinting[1,2]　LI Jinhui[1,2]　LUO Na[2,3]　XING Bin[2,3]　SUN Chuanheng[2,3]

(1. *College of Agricultural Engineering*, *Jiangsu University*, *Zhenjiang* 212013, *China*
2. *Research Center of Information Technology*, *Beijing Academy of Agriculture and Forestry Sciences*, *Beijing* 100097, *China*
3. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*)

Abstract: Aiming at the problems of traceability data differentiation between upstream and downstream blockchains, difficulties in fine-grained sharing, and data privacy protection existing in the existing supply chain of fruits and vegetables and agricultural products, an attribute-based cross-chain traceability access control model of fruits and vegetables supporting heterogeneous multi-chain was proposed by analyzing the business processes of various links in the supply chain of fruits and vegetables and agricultural products, and in the context of fruit, vegetable and agricultural products quality and safety traceability scenarios. The model used relay chain-based cross-chain technology to standardize cross-chain information to achieve cross-chain communication between heterogeneous multi-chains, and combined the cross-chain traceability requirements of fruits and vegetables with the attribute-based access control (ABAC) model to achieve flexible and fine-grained access control on data resources. In order to verify the effectiveness of the model, BitXHub relay chain technology was used to realize cross-chain data access in the heterogeneous chain composed of Hyperledger Fabric and Ethereum, and the attribute-based access control process was implemented in the cross-chain contract, so as to construct a prototype system of the cross-chain access control model for fruit and vegetable traceability. The system test results showed that the average maximum value of the sending rate of the relay chain for processing cross-chain transactions was about 600 t/s and 400 t/s, respectively, and the policy determination time did not fluctuate greatly with the increase of the number of policies, and was basically stable at about 2 000 ms,

收稿日期:2023-08-11　修回日期:2023-09-18

基金项目:国家重点研发计划项目(2022YFD2001804-2)和江苏省科技计划(重点研发计划现代农业)项目(BE2023315)

作者简介:杨信廷(1974—),男,研究员,博士,主要从事农产品智慧供应链研究,E-mail:yangxt@nercita.org.cn

通信作者:孙传恒(1978—),男,研究员,博士,主要从事农产品追溯技术研究,E-mail:sunch@nercita.org.cn

which was able to satisfy the needs of the fruit and vegetable supply chain for the differentiated and fine-grained sharing of cross-chain data among heterogeneous blockchains, and also ensured the data sharing process of the data privacy.

Key words: fruit and vegetable supply chain; heterogeneous multi-chain; cross-chain; access control; attribute-based access control

0　引言

随着人们健康饮食的意识不断加强，水果、蔬菜作为营养丰富、健康无害的食品，受到越来越多的关注。然而近年来果蔬行业频繁出现的农药残留超标、过量使用食品添加剂、违规使用化学药品、生产环境不达标等事件严重危害了社会公众信任和消费者的健康安全[1-2]。果蔬供应链涉及生产、仓储、加工、运输、销售和食用等多个环节，各环节以物资流向连载整合通过信息共享提升整个农产品供应链的运作效率[3-5]。区块链技术具有不可篡改、分布式、去中心化、可追溯等特点，可以解决传统农产品追溯体系存在的信息中心化存储、易篡改、数据不透明、共享性差等问题[6-8]。

然而随着区块链技术的快速发展，不同区块链应用之间形成通信壁垒，导致果蔬供应链上下游各环节之间形成了数据孤岛。果蔬农产品具有季节性销售、区域特征明显、贮存寿命短而鲜度要求高的特点，因此要求供应链中的各个环节需要有效的信息共享和沟通机制，实现快速、高效的物流和运输系统来保持其新鲜度，减少出现产品损耗和浪费、供货不稳定等问题，更好地满足消费者的需求[9-10]。果蔬供应链上下游融合交互需求日益增长，打破不同区块链间通信壁垒是区块链间协同操作和消息共享的关键[11-13]。

在实现区块链链间协作和互联互通方面，国内外学者进行了相关研究。文献[14]为解决现有水产品供应链中各企业环节的区块链间信息孤岛的问题以及实现各企业间的安全交易，提出了基于区块链跨链技术的水产品交易模型。文献[15]针对供应链上各组织采用无法进行数据交换和功能互补的异构区块链带来的价值孤岛问题，设计并实现了一个支持主流区块链互操作的跨境海产品供应链平台。文献[16]基于并行区块链理论和智能合约技术构建了适用于大米供应链复杂数据的监管跨链模型以增强疫情下大米供应链的监管能力。跨链技术在农业领域的应用偏向于跨链信息共享以及交易。由于链间通信涉及到链上不同类型的数据，如果不对跨链行为作出限制，区块链上隐私信息将会有泄露风险，跨链技术的出现使得各区块链系统之间数据交换共享的安全需求变的更为复杂。

同时，国内外学者对跨链访问控制也进行了研究。文献[17]提出了一种基于跨链的医疗数据安全共享方案以解决医疗机构之间医疗数据共享困难的问题。该方案同时结合 AES(Advanced encryption standard) 和 CP - ABE(Ciphertext-policy attribute-based encryption) 加密算法进行细粒度的医疗数据访问控制，虽实现了细粒度的访问控制，但 ABE 机制中的权限更新问题尤为突出。文献[18]在知识付费应用场景下提出一种支持异构多链的数据隐私保护方案，实现了联盟链上知识分享及公有链上知识付费，但这种方案在效率方面仍有一定的提升空间。文献[19]提出了一种以属性访问控制(Attribute-based access control, ABAC) 模型为基础的域间访问控制模型，为域间访问提供自主且细粒度的访问控制，但该方案是通过遍历所有区块检索属性与策略，导致策略判定时间会随着策略数量的增加而变长。因此实现高效、细粒度的跨链访问控制是一个亟待解决的问题。

本文通过借鉴 ABAC 并结合果蔬追溯实际跨链需求提出基于属性的跨链访问控制模型方案。该方案采用基于中继技术的跨链解决方案实现不同区块链之间的通信，中继链用于实现业务链和服务的管理与跨链消息的转发；然后利用基于属性的访问控制机制设计跨链访问控制方案，增加对整个动态系统管理的灵活性；最后基于 BitXHub 中继平台搭建实现区块链互操作性的中继链，并基于 Hyperledger Fabric 和 Ethereum 平台分别搭建 2 条异构业务链以实现果蔬追溯跨链访问控制模型的原型系统并对其进行相关测试。

1　果蔬供应链关键信息分析及跨链追溯模型

1.1　果蔬供应链关键信息

果蔬供应链涉及多个环节，从生产、加工、仓储、运输到批发和零售等各个环节都是供应链中必不可少的组成部分。各个环节分属的企业之间相互独立，企业间通过协调和合作，以确保产品从生产到销售的顺畅流动[20]。果蔬供应链信息多源异构，种类繁多。然而，并非所有关键信息都与质量或安全有关，也不是所有数据都可以完全共享。在实际生产

中,除了进行逆向追溯,还需要兼顾供应链上下游的协作和政府监管等问题[21]。因此,有些信息需要在不影响供应链运作和隐私性的前提下共享。为解决以上问题,保障供应链信息的隐私性,本研究将果蔬追溯链划分为生产链、加工链、运输链、仓储链、销售链。每条链在相应阶段不但会有来自传感器等外部设备的信息上传,还可能需要接收来自上一阶段的信息输入和对下一阶段的信息输出。当追溯单元由一个组织转移到另一个组织时产生外部追溯信息,外部追溯信息包括接收信息和输出信息。若追溯单元仅在组织内部各部门之间流动,产生内部追溯信息即处理信息。因此,根据从上述环节中提取出的关键信息并根据实际情况和相关质量与安全标准,筛选并分类为内部追溯数据、外部追溯有限共享数据、外部追溯完全共享数据。分类结果如表 1 所示。

表 1 果蔬供应链关键信息

Tab. 1 Key information of fruit and vegetable supply chain

所处阶段	内部追溯数据	外部追溯有限共享数据	外部追溯完全共享数据
生产阶段	生产人员信息、生产成本、生产数量	交易信息、产品来源、产品标识、质量信息、产品去向、出货数量、产品批次	生产企业、生产资质、产地信息、种植信息、采收信息、生产标准、作业方法
加工阶段	加工人员信息、原料成本、加工成本	交易信息、产品来源、产品标识、质量信息、产品去向	加工企业、加工资质、加工日期、加工方式、加工环境、处理量、包装信息
仓储阶段	仓储人员信息、仓储成本	交易信息、产品来源、产品标识、质量信息、产品去向	仓储企业、仓储资质、存储方式、仓库编号、始末时间、温湿度
运输阶段	运输人员信息、运输成本	交易信息、产品来源、产品标识、质量信息、产品去向	运输企业、运输资质、运输工具编号、运输路线、运输成本、收购批次、收购成本
销售阶段	销售人员信息、进货数量、进货价格	交易信息、产品来源、产品标识、质量信息、产品去向	销售企业、销售资质、进货时间、销售时间、销售价格

内部追溯数据是指在供应链各环节内部进行追溯活动所涉及的不与外部企业分享的隐私数据,该类数据的泄露将会对本企业的商业发展造成严重影响。外部追溯有限共享数据是指在供应链上下游的协作和政府监管场景下共享的数据,此类共享的数据不影响供应链运作和隐私性。此类数据主要包括追溯单元及本阶段添加物、包装物等产品来源信息,入库验收检验信息、温度等关键控制点要求以及追溯单元接收方等产品去向信息以及相关交易信息。外部追溯完全共享数据是指在供应链各环节内部进行追溯活动时对外部完全公开的数据,主要是面向消费者的溯源需求。

由于不同环节涉及到的数据类型和格式存在差异,使得在供应链管理过程中,数据的采集、整合和共享变得相对困难,需要进行数据转换、数据标准化等工作来解决这些问题。因此,为了实现供应链数据的有效整合和共享,本文对多源异构数据通过制定统一的数据规范和标准,以及采用数据转换技术,将供应链中的异构数据在共享时自动转换为统一的数据格式,以实现多源异构数据共享。

1.2 果蔬供应链跨链追溯架构

果蔬供应链跨链追溯通常涉及多个参与方、多个环节和多个区块链网络,而不同的参与方、不同的环节通常采用不同的区块链网络,为实现跨链追溯,需要建立统一的跨链格式和标准,实现不同区块链网络之间的关联性和可追溯性。中继链作为一种跨链技术,可以提供跨链标准化的数据格式和交易协议,具有较高的互操作性。中继链作为联通所有业务链的枢纽,和多个业务链组成联盟,因此中继链各节点由各业务链共同维护,是联盟链,负责管理接入的所有业务链以及业务链之间跨链消息的验证、持久化和路由。跨链网关主要负责跨链交易的收集以及跨链交易的转发等任务。当有部分数据需要在不同组织之间流动时,业务链通过跨链网关接入中继链中,然后通过跨链智能合约实现外部追溯数据在不同组织之间的流动。外部追溯完全共享数据通过跨链合约和数据转换合约进行统一格式转换实现跨链通信;外部追溯有限共享数据除了涉及跨链合约和数据转换合约外,还将调用访问控制合约和策略管理合约来实现对数据权限的判定及访问控制。其示意图如图 1 所示。

跨链追溯包括以下内容:

(1)数据采集:通过物联网技术收集果蔬供应链的各种数据,包括种植信息、加工信息、包装信息、运输信息等内容。

(2)上链处理:将采集到的数据进行处理后上链,按照供应链阶段划分,不同数据上不同的链,确保数据的安全、可信和不可篡改。

(3)跨链标准化:建立跨链格式和标准,使得不同区块链网络之间可以相互交流,构建关联性和可

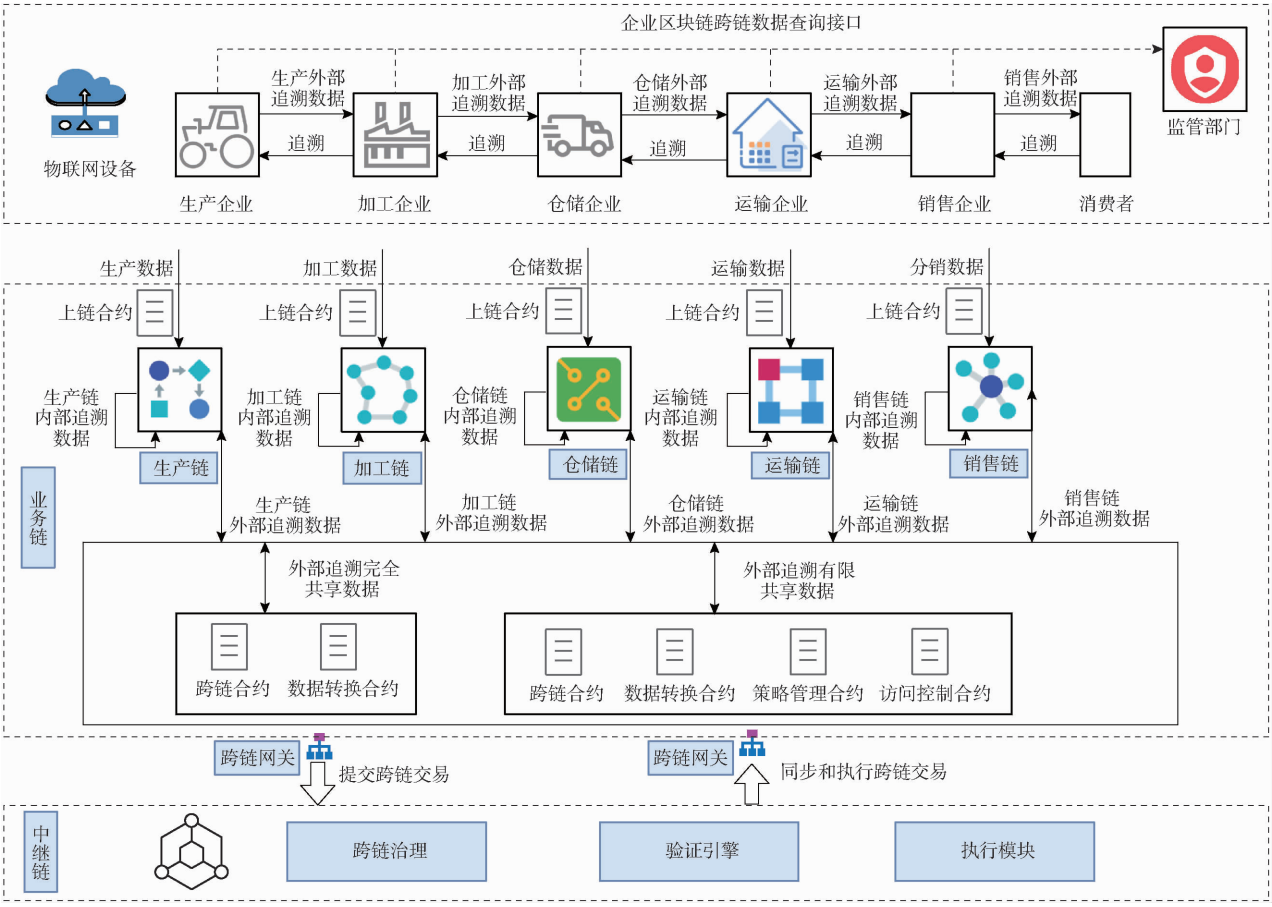


图 1　果蔬供应链跨链溯源架构

Fig. 1　Cross-chain traceability architecture for fruit and vegetable supply chain

追溯性。

(4)隐私保护:控制数据的访问权限,通过数据加密和访问控制等方法来保护个人隐私和商业秘密。

(5)数据查询:参与方可以通过跨链查询系统获取到相关的数据,对于有疑问或者需要追溯的数据进行查询和追溯,并且能够确认数据的真实性和完整性。

1.3　基于中继链的跨链追溯模型

跨链技术为解决区块链异构互联互通问题、提升区块链的互操作性和可扩展性提供技术解决方案[22]。目前跨链技术的主流方法有 4 种,分别是公证人机制、侧链/中继链、哈希锁定和分布式私钥控制[23-24]。中继链作为一种跨链技术不但可以提供跨链标准化的数据格式和交易协议,而且可以通过多种安全机制来保护跨链传输的安全,中继机制能支持跨链价值转移、资产质押和跨链合约,具有较高的通用性和可扩展性[25]。本文结合果蔬供应链跨链追溯实际业务场景,设计了一种基于中继链的跨链追溯模型,在跨链通信网络系统中实现访问控制和保护数据所有者隐私,如图 2 所示。

图 2 描述了在一个跨链通信网络系统中实现访问控制和保护数据所有者隐私的跨链追溯模型和消息流,左边是中继链,右边是业务链。跨链网关节点部署在业务链中,是由相应的业务链维护的服务程序,担任着业务链和中继链之间收集、转换和传播消息的角色,简化业务链接入跨链系统的过程,增强接入跨链系统的便捷性。中继链用于跨链治理以及跨链验证与执行,是一种实现通用跨链传输协议的开放许可链。跨链治理模块主要负责业务链以及跨链服务的注册、审核和冻结等操作,为不同区块链的不同用户分配统一的身份,对管理过程中的投票策略进行管理。中继链由多个节点组成,由所有节点共同维护。接入链在接入中继链时,首先要在中继链中进行注册,经过中继链上的大多数节点投票同意后方可接入,然后在中继链中给接入链分配跨链数字身份,实现身份在多条链间的互通互认,可以更加方便地实现以身份为中心的数据在不同链间的可信流通。

中继链通过验证引擎实现跨链交易可信验证。当新的业务链注册到中继链时,需要通过合约的方式将业务链对应的验证规则上传。业务链产生一笔跨链交易,中继链接收之后,将跨链交易传入验证引擎,验证引擎解析通用跨链传输协议以后,获知来源

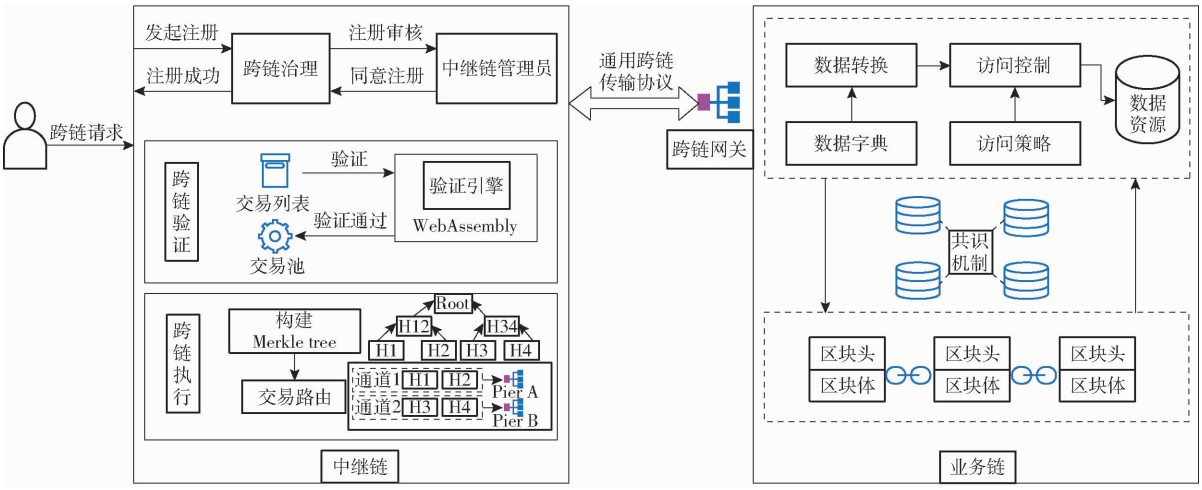


图 2 跨链追溯模型

Fig. 2 Model for cross-chain traceability

链的 ID,并根据 ID 检索出对应的验证规则脚本。然后验证引擎会用虚拟机调用规则脚本,虚拟机会对通用跨链传输协议解析出的 Proof 字段进行校验,从而确定交易的合法性。

跨链交易验证通过后,一个区块中所有跨链交易会被构建成默克尔树(Merkle tree),然后默克尔根(Merkle root)在经过验证节点的签名后被发送到目的链执行。中继链将所有的跨链交易分类放到对应的队列中供跨链网关获取和调用。

智能合约是一种可以在没有可信第三方的情况下自动执行的多方协议[26]。智能合约通过事件触发的机制而执行,其赋予对象以数字的特征并将其部署至区块链[27]。智能合约在供应链网络的所有网关节点上实现,以实现网络中的互操作性。各个区块链网络的管理机构决定哪些信息可以共享,哪些数据可以在本地应用,并通过访问控制合约实现。数据字典合约用于管理本地业务链与其他业务链的数据字典,确定数据结构、数据类型、取值范围以及转换规则。数据转换合约对来自其他业务链的请求字段通过查询数据字典转换为本业务链上相应的字段。访问策略合约负责根据实际情况对本业务链上的数据制定访问控制策略,并对过时的访问控制策略进行更新或删除。访问控制合约则根据链上的访问控制策略对跨链请求进行判定,如果符合访问策略则同意访问,通过数据转换合约转换为对应的格式然后返回,否则拒绝该请求。数据字典相关内容以及访问控制策略均存储在链上。

下面以果蔬加工企业跨链访问生产链上的外部追溯部分共享数据为例介绍跨链流程,具体流程如图 3 所示。

(1)注册阶段:对于需要加入跨链网络,使用中继链进行跨链的业务链,首先需要由业务链管理员向中继链注册业务链,即向中继链发送一笔业务链注册的交易,跨链网关将消息封装成通用跨链协议格式提交到中继链。中继链以交易的来源(即当前跨链网关公钥的地址)作为业务链的 ID,生成一个业务链注册的提案。提案由中继链上的管理员进行投票,审核通过或失败后中继链发送一条消息回执提示注册成功或失败。注册成功后的业务链以同样流程将跨链服务注册。

(2)请求阶段:加工链需要跨链请求数据时,调用跨链合约抛出跨链事件即发送一条跨链访问请求 Req,跨链网关捕获该跨链事件,并将其封装成通用跨链协议格式后向中继链发送。中继链验证跨链消息的来源链、目的链状态,并对跨链消息中的跨链消息证明进行验证,验证通过后中继链从已验证的交易列表中构建 Merkle tree 并对该 Merkle root 签名,然后通过跨链路由到生产链对应的跨链网关。

(3)执行阶段:跨链网关对跨链消息进行解析,然后生产链使用中继链的公钥验证中继链的签名是否有效。通过验证后,生产链上的访问控制合约根据访问主体、客体的属性以及访问控制策略对访问请求进行决策。对符合访问策略的数据经数据转换合约转换为统一的数据格式后返回。

(4)回执阶段:生产链将返回的外部追溯部分共享数据封装成消息回执 Res,经跨链网关封装成通用跨链协议格式后提交到中继链,中继链验证回执消息可信后路由转发到加工链对应跨链网关,解析回执后加工链获得数据,至此一次跨链访问过程结束。

2 果蔬跨链追溯访问控制模型

2.1 基于属性的跨链追溯访问控制模型

访问控制是对计算、存储、服务等资源的访问设

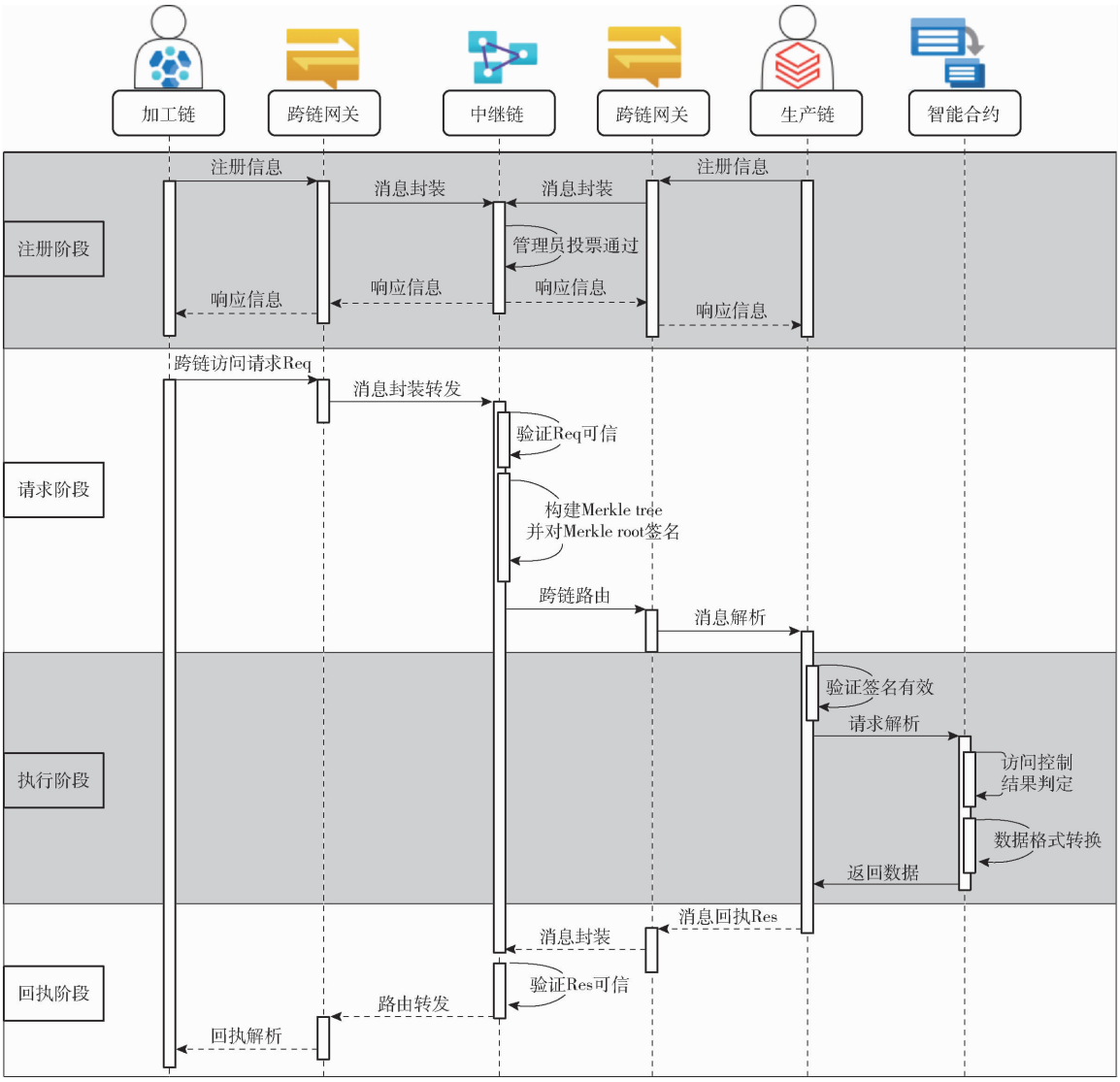


图 3　跨链追溯时序图

Fig. 3　Sequence diagram for cross-chain traceability

置访问条件，从而有效避免恶意应用对资源的不正当访问以及合法应用对资源的越权访问，是确保各应用安全访问资源的一种有效手段[28]。在果蔬农产品追溯领域，果蔬供应链存在着追溯链条长、涉及主体多且复杂、季节性销售、区域特征明显、贮存寿命短、鲜度要求高等问题，供应链各环节之间需要建立快速高效的信息共享沟通机制以提升供应链透明度，确保产品新鲜度达标以及质量安全可追溯。然而传统的访问控制技术难以满足果蔬跨链追溯环境下对访问控制的需求[29]，为解决上述问题，本文提出一种基于 ABAC 的跨链追溯访问控制模型。

ABAC 是一种基于属性的访问控制模型，此模型中，访问请求被授权策略引擎处理，该策略引擎评估请求中的主体属性、对象属性和上下文属性，并基于这些属性决定是否允许或拒绝访问[30-31]。ABAC 将主体和客体的属性作为基本决策要素，使用属性或属性集合来描述实体，基于属性的逻辑语义描述访问控制策略，将策略管理和权限判定解耦。通过更加细粒度的属性或属性集合，从多个角度描述实体，并加入了环境实体作为另一种约束，从而可以针对实际情况对策略进行更改，具有相当程度的灵活性。由于属性是实体固有的特性，通过实体属性发现机制，可以挖掘出独立、完备的实体属性集合，不需要事先手动分配，根据请求者以及访问资源所需求的属性进行授权，使得 ABAC 管理相对简单；并且在 ABAC 模型中，策略随用户和资源的增多呈线性增长，面对海量的用户和数据，系统开销较小并且可以有效解决动态性问题；同时，ABAC 所具有的细粒度性以及低复杂度且表达丰富的策略描述语言，可以使其恰当地应用在果蔬供应链跨链追溯场景中。

在 ABAC 模型中，策略决策点利用基于属性的访问请求查询符合要求的访问控制策略，并将这些访问控制策略整合为策略集发送回策略决策点进行

策略判决。在本文所述模型中,访问控制策略由各业务链根据各自的安全需求,使用标准化、统一的细粒度属性信息进行描述,针对访问控制策略制定。从技术上看,共享的数据虽然是由企业决定的,但企业应该根据监管要求和政策制定相应的访问控制策略,包括给予监管部门一定的主动权。同时从管理方面来讲,监管部门可以通过相关法律法规,以约束企业的行为,并规定数据使用和共享的要求,并对企业进行定期的审计和监测,以确保其对数据的使用和共享符合相关规定。为方便描述,做如下定义:基于属性的访问请求由主体属性、客体属性、操作属性、环境属性的集合构成,基于属性的访问请求的含义为:"主体属性为 Subject 的主体在环境属性 Environment 条件下,对客体 Object 进行 Action 的操作请求。"[19]本文结合果蔬供应链中的实际情况对属性作出进一步划分,具体描述如表 2 所示。

表 2 访问控制模型属性描述

Tab.2 Attribute descriptions of access control model

属性分类	表示	描述
主体属性	ID 标识	果蔬供应链中请求主体唯一性标识
	Role 角色	果蔬供应链中请求主体所属角色,可为管理员或普通用户
	Org 组织	果蔬供应链中请求主体所属的某个组织
	Stage 阶段	果蔬供应链中请求主体所处阶段,可为生产、加工、仓储、运输、销售阶段中的某个阶段
客体属性	ID 标识	果蔬供应链中被请求客体唯一性标识
	Level 等级	果蔬供应链中被请求客体所属资源等级,可为内部追溯数据、外部追溯有限共享数据或外部追溯完全共享数据
	Org 组织	果蔬供应链中被请求客体所属的某个组织
	Stage 阶段	果蔬供应链中被请求客体所处阶段,可为生产、加工、仓储、运输、销售阶段中的某个阶段
操作属性	Type 操作类型	请求中的操作类型,可为读或写
环境属性	Geolocation 请求来源	发起请求时的来源地址
	StartTime 请求开始时间	发起请求时的开始时间
	EndTime 请求结束时间	发起请求时的结束时间

本模型将智能合约技术和 ABAC 访问控制模型结合,根据果蔬供应链跨链追溯场景和实际需求进行进一步设计,其框架如图 4 所示。

具体步骤如下:

(1)加工链请求者发送一个事务来向访问控制合约发送访问请求,该事务包含它的 ID[0x2569…]、客体对象 ID[0x7583…]和要执行的操作{Read}。

(2)访问控制合约通过调用属性管理合约,调用参数包含主体 ID 和客体 ID,从属性管理合约检索主体和客体属性。

(3)属性管理合约向访问控制合约返回相应的主体属性和客体属性。图 4 中检索的主体属性代表含义为主体所处供应链阶段为 2(加工阶段),所属组织值为 process(加工组织),主体角色值为 admin(管理员);客体属性代表含义为资源级别值为 semi-share(外部追溯部分共享数据),所属组织值为 production(生产组织),所处供应链阶段值为 1(生产阶段)。

(4)访问控制合约调用策略管理合约,调用参数包含客体属性,以查询相关策略。

(5)策略管理合约通过键值查询来搜索相关策略,并将找到的策略返回给访问控制合约。图 4 中检索的访问控制策略代表含义是主体和客体的 ID 不为空,主体角色值为 admin、所属组织值为 process(加工组织)、所处阶段值为 2(加工阶段),客体资源级别值为 semi-share(外部追溯部分共享数据)、所属组织值为 production(生产组织),访问主体角色值为 admin,访问客体的资源级别值为 semi-share(外部追溯部分共享数据)、所处阶段值为 1(生产阶段),执行操作类型值为 read,访问 IP 定位为境内,访问时间为 09:00—21:00,满足以上条件即可通过。

(6)根据得到的主体属性、客体属性、操作类型、操作环境以及策略集和结果合并算法,确定主体是否有权对对象执行操作,判断出该访问请求满足访问策略。

(7)访问控制合约将判定结果返回,根据判定结果决定是否将数据返回给请求主体。

2.2 智能合约设计

针对果蔬追溯实际业务场景,本研究结合果蔬跨链追溯模型设计出策略管理、属性管理、访问控制、数据查询的智能合约方法,在链中的各追溯节点发起跨链追溯时,即可自动触发访问控制合约实现访问控制逻辑的自动执行。针对供应链主体的追溯需求,本研究设计相关合约功能,智能合约设计细节如表 3 所示。

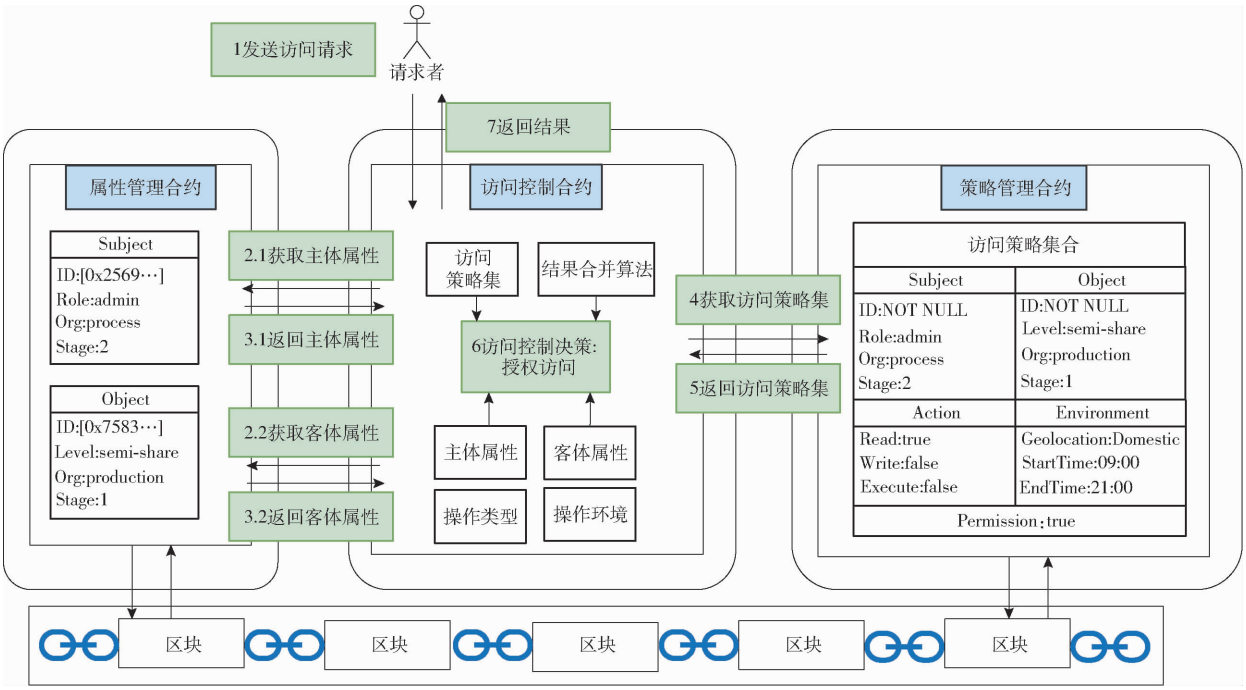


图 4　访问控制框架

Fig. 4　Access control framework

表 3　智能合约设计

Tab. 3　Design of smart contract

合约功能	合约方法	输入	输出	描述
策略管理合约	addPolicy( )	策略 ID/策略内容	True/false	添加访问策略
	queryPolicy( )	策略 ID	访问策略集合	查询访问策略
属性管理合约	querySubAttr( )	主体 ID	实体属性集	获取主体属性集
	queryObjAttr( )	客体 ID	客体属性集	获取客体属性集
	queryEnv( )		环境属性集	获取环境属性集
访问控制合约	isPermission( )	主体属性集/客体属性集/操作类型/环境属性集/访问策略	true/false	根据提供的实体属性集和访问策略对请求做出判定
	isEqual( )	结构体 A/结构体 B	true/false	比较两个类型的结构体是否相等,若其中一个结构体的字段为空,则默认相等
	conbineResult( )	判定结果集合/合并算法	true/false	根据预定义合并算法对匹配的策略集的判定结果集合进行合并
数据查询合约	set( )	key/value	true/false	链内查询
	get( )	key	value	链内上传
	interchainGet( )	目的链 ServiceID/key	true/false	根据 key 跨链查询
	interchainSet( )	目的链 ServiceID/key/value	value	跨链上传 key/value

相关访问控制策略使用区块链存储,访问控制策略数量会随着链上数据的逐步膨胀而逐渐增多,为了兼顾访问控制策略的灵活性和策略的查询效率,本文在利用 ABAC 设计策略管理智能合约时提出了特定访问控制策略和通用访问控制策略的概念。特定访问控制策略即针对某一个特定资源所制定的访问策略,通用访问控制策略是指针对具有同类属性的一批资源所制定的访问控制策略。访问控制策略以(key,value)的形式存储在链上,以客体属性集的序列化信息作为 key,以其对应的访问策略集为 value,针对相同 key 的多条访问策略,访问策略集以数组形式进行序列化和反序列化。在进行策略判定时,先获取特定访问控制策略进行判定,如果不存在该策略,再通过通用访问控制策略进行判定,相关智能合约伪代码描述如下:

算法 1:策略查询智能合约

输入:客体属性集 Object

输出:访问策略集 policyArray

Begin

objectAsBytes = 客体属性集 Object 序列化

policyArrayAsBytes = 通过 objectAsBytes 键值查询到序列化信息

```
        policyArray = 将序列化信息反序列化为访问策略集结构
        return 访问策略集
    End
```

算法 2:策略判定智能合约

输入:主体属性集 Subject,客体属性集 Object,操作类型 Action,环境属性集 Environment,策略集结果合并算法 combineAlgorithm

输出:策略判定结果(Result)

```
    Begin
        //以客体属性集为 key,获取特定访问策略进行判定
        specificPolicy = 获取特定访问策略集
        for (遍历特定访问策略集数组){
          if (输入属性与访问策略中属性匹配){
            results = 单条策略判定结果追加到结果集
          }
        }
        //将客体属性集中的客体 ID 置空,获取通用访问策略进行判定
        generalPolicy = 获取通用访问策略集
        for (遍历通用访问策略集数组){
          if (输入属性与访问策略中属性匹配){
            results = 单条策略判定结果追加到结果集
          }
        }
        Result = 策略集结果合并
        return 最终结果
    End
```

3 性能测试

本文所提出方案的测试实验在 Virtual Machine ware 虚拟机中进行。虚拟机操作系统为 Ubuntu 16.04,处理器内核 8 个,内存 8 GB。在 Ubuntu 下搭建 BitXHub 2.0 跨链技术平台、Ethereum 1.2.0 和 Hyperledger Fabric 1.4 区块链平台,环境配置包括 go 1.15.6、docker 20.10 和 docker compose 2.3 等服务。本文实验以太坊上的智能合约采用 solidity 语言进行编写,Fabric 1.4 上的链码采用 go 语言进行编写。

3.1 性能测试

本研究的中继链基于 BitXHub 跨链技术平台实现,使用 Premo 测试框架对本文所提出的系统进行压力测试。通过逐步增加每秒并发量,观测实际处理交易量,分别针对中继链的链内交易和跨链交易进行发送率性能测试。随着预设发送率的逐步增加,中继链实际处理链内交易速率也同步增加,随后趋于稳定(图 5a),中继链实际处理链内普通转账交易最大值稳定在 4 000 笔/s 左右,实际处理链内调用 BVM 交易(BVM 即链上内置合约,用以实现中继链管理业务链)最大值稳定在 2 000 笔/s 左右。当对中继链处理跨链交易性能进行测试时,中继链实际处理跨链交易速率出现较大波动(图 5b),随着预设发送率的逐步增加,业务链类型为 Fabric 的跨链交易处理速率先逐渐增加然后稳定在 600 笔/s 左右,用链类型为 Ethereum 的跨链交易处理速率先逐渐增加然后逐渐下降,最高值为 400 笔/s 左右。通过后台的机器资源监控可知,该情况是由于内存爆满所导致。

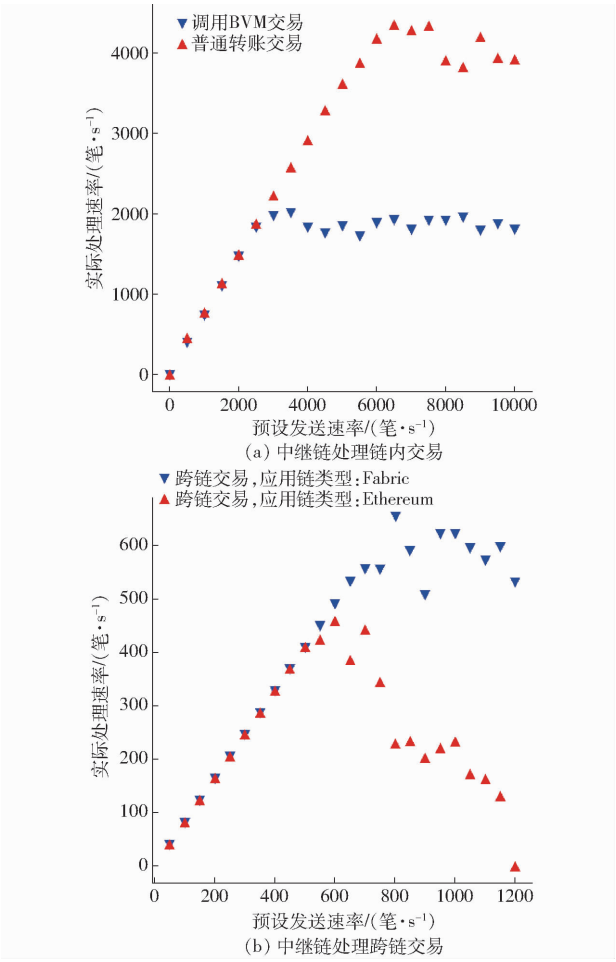


图 5 中继链性能测试结果

Fig. 5 Performance testing of relay chain

3.2 对比测试

通过对比来评估本文提出的访问控制模型,表 4 描述了同已有研究进行对比,分析本文模型的优势。

本文所设计的基于属性的访问控制模型将访问控制策略以(key,value)的形式存储在链上,以客体

表 4　本模型和已有研究方案对比分析

Tab. 4　Comparison between this model and existing model

方案来源	便于访问	安全性	自主授权	权限便于更新	效率
文献[17]	访问 IPFS 上的密文并解密	对称加密 属性基加密 区块链	使密文和密钥与属性集合和访问结构产生关联	否	权限更新时需要重新加密
文献[18]	访问 IPFS 上的密文并解密	对称加密 代理重加密 区块链	不支持	否	效率方面有待提升
文献[19]	直接返回数据	访问控制机制 区块链	自主制定策略	是	策略判定时间随着策略数目的增加而快速增加
本文方案	直接返回数据	访问控制机制 区块链	自主制定策略	是	高

属性集的序列化信息作为 key，以其相应的访问控制策略集为 value，这种通过键值检索数据的方式会利用索引减少数据检索的时间。为了测试策略判定时间与策略数目之间的关系，本方案与文献[19]中的方案进行对比，结果如图 6 所示。由图 6 可知，文献[19]的策略判定时间随着策略数目的增加而快速增加，这是因为在文献[19]中策略的检索是通过遍历所有区块进行的，本文所设计的方案随着策略数目的增加并无明显变化，稳定在 2 000 ms 左右，是因为本文通过键值检索数据的方式检索策略，通过索引查询数据的时间一般不会随着数据量的增加而减慢[32]。

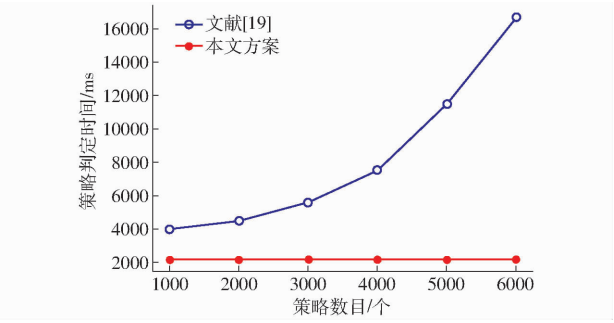


图 6　策略判定时间测试

Fig. 6　Analysis of policy decision time testing

4　原型系统设计及实现

4.1　系统架构

基于果蔬供应链跨链追溯的业务分析，本文设计了果蔬供应链跨链追溯模型的架构，如图 7 所示。模型架构共分为 5 层，根据实现功能自下而上分别是基础层、跨链服务层、接口层、智能合约层和业务层。

基础层包含区块链本身需要具备的模块，如网络模块、存储模块、共识模块等。不同类型区块链的基础层可能略有不同。P2P 网络是节点之间共识和信息传递的通道，是平台的网络通信基础。默克尔

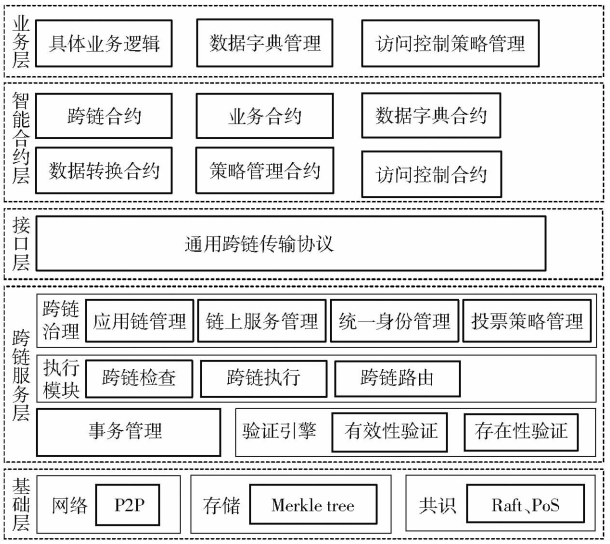


图 7　跨链溯源技术架构图

Fig. 7　Technology architecture of cross-chain traceability

树是一种基于哈希的树形数据结构，采用默克尔树来存储数据，可以提高数据的安全性和效率，保障了区块链系统的稳健运行。共识机制指的是区块链网络中各节点之间通过协商达成一致的过程，从而确保区块链系统的安全性和一致性。本文在系统中使用数据管理智能合约来对果蔬产业链数据进行管理，区块链共识机制不仅适用于区块链网络中的交易数据，也同样适用于智能合约数据。

跨链服务层包括跨链治理模块、执行模块、事务管理模块、验证引擎模块，各模块互相协作完成中继跨链流程。跨链治理模块主要负责业务链注册、审核和冻结等操作；执行模块负责跨链交易的检查、处理和验证工作；事务管理模块负责跨链交易在整个系统处理的一致性；验证引擎模块在虚拟机之上实现了跨链交易存在性和有效性的验证逻辑。

接口层采用通用的跨链传输协议，实现异构区块链之间的跨链交易路由和可信验证，允许异构数据及服务进行跨链调用。

智能合约层对跨链追溯流程的相关功能设计了相应的智能合约,包括业务合约、跨链合约、数据字典合约、数据转换合约、策略管理合约以及访问控制合约。业务合约主要包含具体的业务逻辑,如跨链读取或跨链写入相关数据。跨链合约负责对接跨链网关,业务合约需要跨链时,要统一将跨链请求提交到跨链合约上,跨链合约统一和跨链网关进行交互。数据字典合约维护存储在链上的数据字典,为数据转换合约提供数据元素映射规则模板。而数据转换合约则根据数据字典对来自不同数据源的异构数据转换为通用格式,以便后续进行数据访问。数据访问时还需要考虑数据权限和数据安全问题,采用数据授权、身份验证等技术来保护数据。策略管理合约是对链上数据制定的访问控制策略进行管理,而访问控制合约则是根据访问控制策略来对访问请求进行权限的判定,来决定是否同意访问请求。

业务层可实现具体的跨链追溯流程。果蔬供应链不同环节的企业将自己的业务链接入跨链系统后,既可以跨链请求其他业务链的数据,也可以被其他业务链进行请求访问。将自己业务链的数据结构和数据类型进行上传更新数据字典以便于数据转换,然后通过制定或更新本业务链数据的访问控制策略以保证数据安全。

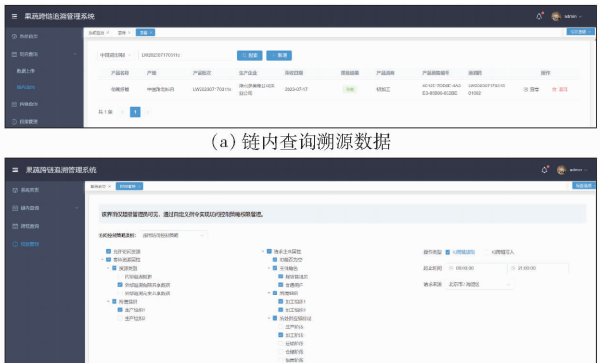
4.2 原型系统实现

本研究根据基于属性的跨链访问控制模型实现果蔬供应链跨链溯源系统。果蔬供应链跨链溯源系统采用基于中继链的跨链追溯模型。中继链用于连接和管理多个并行运行的子链,负责协调和处理不同子链之间的交互和通信。针对不同类型框架的区块链,基于中继链的跨链技术可以屏蔽不同框架的底层差异,简化业务链的接入流程,能够支持业务所在区块链便捷、快速地接入到中继链中,从而实现和其他业务区块链的跨链操作。

图 8a 显示了根据批次号查询进行链内查询溯源数据的结果,该数据为生产阶段企业的链上数据,数据资源拥有者可以根据数据资源的属性来制定访问控制策略。如图 8b 所示,生产企业根据实际情况制定外部追溯有限共享数据的通用访问控制策略。图 8c 展示了加工企业进行跨链获取生产企业的数据,跨链请求中指定目的链服务地址以及批次号,获取成功后数据将会写入加工链上。图 8d 展示了跨链网关日志输出。

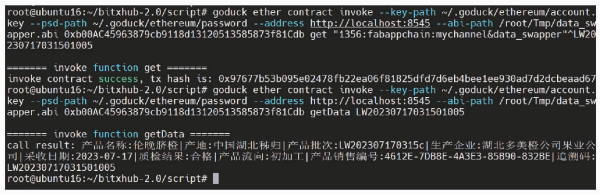
5 结论

(1)基于属性的果蔬追溯访问控制模型利用基

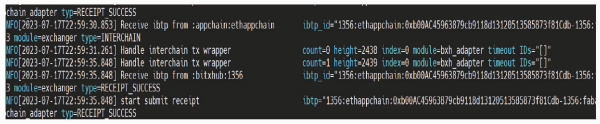


(a) 链内查询溯源数据

(b) 制定访问控制策略



(c) 跨链获取数据



(d) 跨链网关日志输出

图 8 果蔬供应链跨链溯源系统界面和后端

Fig. 8 Front-end and back-end of cross-chain traceability system for fruit and vegetable supply chain

于中继链的跨链技术实现异构多链之间的跨链通信,然后通过借鉴 ABAC 并结合实际跨链需求设计出一种基于属性的访问控制模型实现对数据灵活、细粒度地访问控制,最后针对果蔬供应链的多源异构数据设计共享方案实现供应链数据的有效整合和共享。

(2)本文构建并实现了业务链 + 跨链网关 + 中继链模式的果蔬质量安全跨链追溯原型系统。系统测试结果表明,中继链处理业务链类型为 Fabric 和 Ethereum 的跨链交易的发送速率平均最高值分别约为 600 笔/s 和 400 笔/s,策略判定时间稳定在 2 000 ms 左右,而且策略判定时间不会随着策略数目的增加而有较大波动,本文方案与已有研究方案对比分析,结果表明具有一定优势。

(3)本文所设计的方案能够解决果蔬供应链中上下游企业存在的信息孤岛问题以及隐私数据的细粒度访问控制问题,对提高果蔬供应链上下游企业的协作效率有一定推进作用。随着跨链技术的进一步发展,未来实现区块链的互联互通是一个必然趋势,果蔬供应链具有季节性变化、区域性生产、产品易腐而保鲜度要求高的流转特性,跨链追溯对优化果蔬供应链的效率、实现果蔬质量安全数据的有效整合以及数据价值的深度挖掘,促进果蔬产业的安全可持续发展具有重要意义。

然而，在果蔬农产品供应链领域，不仅要实现上下游流通，对流通过程中的监管也是值得研究的问题，如何实现农产品安全追溯，构建跨域监管模型，实现多环节、全链条跨域监管以及探究协同互作监管机制与控制策略均是值得进一步研究的问题。

参 考 文 献

[1] 曹裕，杜志伟，万光羽. 不同农药残留标准下家庭农场种植行为选择[J]. 系统工程理论与实践，2018，38(6)：1492－1501.
CAO Yu, DU Zhiwei, WAN Guangyu. Family farms' choice of cropping behavior under different pesticide residue standards [J]. Systems Engineering-Theory & Practice，2018，38(6)：1492－1501. (in Chinese)

[2] 叶兴乾，任艳明，陈健乐，等. 果蔬营养新功能：益生元[J]. 中国食品学报，2021，21(6)：1－10.
YE Xingqian, REN Yanming, CHEN Jianle, et al. The new nutritional function of fruit and vegetable: prebiotic[J]. Journal of Chinese Institute of Food Science and Technology, 2021，21(6)：1－10. (in Chinese)

[3] DEMESTICHAS K, PEPPES N, ALEXAKIS T, et al. Blockchain in agriculture traceability systems: a review[J]. Applied Sciences-Basel，2020，10(12)：4113.

[4] 葛宏义，吴旭阳，蒋玉英，等. 基于区块链技术的粮油食品溯源研究进展及展望[J]. 农业工程学报，2023，39(5)：214－223.
GE Hongyi, WU Xuyang, JIANG Yuying, et al. Research progress and prospect of grain and oil food traceability based on blockchain technology[J]. Transactions of the CSAE，2023，39(5)：214－223. (in Chinese)

[5] KAMILARIS A, FONTS A, PRENAFETA-BOLD'Y F X. The rise of blockchain technology in agriculture and food supply chains [J]. Trends in Food Science & Technology，2019，91：640－652.

[6] 于戈，聂铁铮，李晓华，等. 区块链系统中的分布式数据管理技术——挑战与展望[J]. 计算机学报，2021，44(1)：28－54.
YU Ge, NIE Tiezheng, LI Xiaohua, et al. The challenge and prospect of distributed data management techniques in blockchain systems[J]. Chinese Journal of Computers, 2021，44(1)：28－54. (in Chinese)

[7] 曾诗钦，霍如，黄韬，等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报，2020，41(1)：134－151.
ZENG Shiqin, HUO Ru, HUANG Tao, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020，41(1)：134－151. (in Chinese)

[8] KRITHIKA L B. Survey on the applications of blockchain in agriculture[J]. Agriculture-Basel，2022，12(9)：1333.

[9] 卞靖，陈曦. 中国蔬菜价格波动的特征、原因及调控思路研究[J]. 宏观经济研究，2020(4)：142－152.
BIAN Jing, CHEN Xi. A study on the characteristics, reasons and regulation of vegetable price fluctuation in China[J]. Macroeconomics, 2020(4)：142－152. (in Chinese)

[10] 郭秋生，韩晓媛. 我国水果价格波动特征及横向溢出效应研究——以梨、苹果和葡萄为例[J]. 价格理论与实践，2023(3)：103－107.
GUO Qiusheng, HAN Xiaoyuan. A study on the fluctuation characteristics and horizontal spillover effects of fruit prices in China: taking pears, apples, and grapes as examples[J]. Price: Theory & Practice，2023(3)：103－107. (in Chinese)

[11] 王群，李馥娟，倪雪莉，等. 区块链互操作性及跨链技术研究[J]. 计算机科学与探索，2023，17(8)：1749－1775.
WANG Qun, LI Fujuan, NI Xueli, et al. Research on blockchain interoperability and cross-chain technology[J]. Journal of Frontiers of Computer Science and Technology, 2023，17(8)：1749－1775. (in Chinese)

[12] 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 traceabilty based on blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery，2021，52(1)：1－13. (in Chinese)

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

[14] 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)

[15] 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 seafood-oriented supply chain platform based on multiple heterogeneous blockchains[J]. Journal of Applied Sciences，2022，40(4)：539－554. (in Chinese)

[16] PENG X, ZHANG X, WANG X, et al. Research on the cross-chain model of rice supply chain supervision based on parallel blockchain and smart contracts[J]. Foods，2022，11(9)：1269.

[17] 何全文，林庆新，林晖，等. 基于跨链的医疗数据安全共享方案[J]. 计算机系统应用，2023，32(5)：97－104.
HE Quanwen, LIN Qingxin, LIN Hui, et al. Cross-chain-based medical data security sharing scheme[J]. Computer Systems & Applications，2023，32(5)：97－104. (in Chinese)

[18] 王思蝶，马兆丰，罗守山，等. 面向异构多链的区块链链上数据隐私保护方案[J]. 信息网络安全，2022，22(12)：67－75.
WANG Sidie, MA Zhaofeng, LUO Shoushan, et al. Data privacy-preserving scheme on blockchain for heterogeneous multi-

chain[J]. Netinfo Security,2022,22(12):67 - 75. (in Chinese)
[19] 张建标,张兆乾,徐万山,等.一种基于区块链的域间访问控制模型[J].软件学报,2021,32(5):1547 - 1564.
ZHANG Jianbiao, ZHANG Zhaoqian, XU Wanshan, et al. Inter-domain access control model based on blockchain[J]. Journal of Software,2021,32(5):1547 - 1564. (in Chinese)
[20] PATELLI N, MANDRIOLI M. Blockchain technology and traceability in the agrifood industry[J]. Journal of Food Science, 2020,85(11):3670 - 3678.
[21] 于合龙,陈邦越,徐大明,等.基于区块链的水稻供应链溯源信息保护模型研究[J].农业机械学报,2020,51(8):328 - 335.
YU Helong, CHEN Bangyue, XU Daming, et al. Modeling of rice supply chain traceability information protection based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery,2020,51(8):328 - 335. (in Chinese)
[22] 孙浩,毛瀚宇,张岩峰,等. 区块链跨链技术发展及应用[J].计算机科学,2022,49(5):287 - 295.
SUN Hao, MAO Hanyu, ZHANG Yanfeng, et al. Development and application of blockchain cross-chain technology[J]. Computer Science,2022,49(5):287 - 295. (in Chinese)
[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] OU W, HUANG S, ZHENG J, et al. An overview on cross-chain: mechanism, platforms, challenges and advances[J]. Computer Networks,2022,218(12):109378.
[25] 叶少杰,汪小益,徐才巢,等. BitXHub:基于侧链中继的异构区块链互操作平台[J].计算机科学,2020,47(6):294 - 302.
YE Shaojie, WANG Xiaoyi, XU Caichao, et al. BitXHub: side-relay chain based heterogeneous blockchain interoperable platform[J]. Computer Science,2020,47(6):294 - 302. (in Chinese)
[26] HU B, ZHANG Z, LIU J, et al. A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems[J]. Patterns,2021,2(2):100179.
[27] 贺海武,延安,陈泽华.基于区块链的智能合约技术与应用综述[J].计算机研究与发展,2018,55(11):2452 - 2466.
HE Haiwu, YAN An, CHEN Zehua. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development,2018,55(11):2452 - 2466. (in Chinese)
[28] 徐恪,凌思通,李琦,等. 基于区块链的网络安全体系结构与关键技术研究进展[J].计算机学报,2021,44(1):55 - 83.
XU Ke, LING Sitong, LI Qi, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers,2021,44(1):55 - 83. (in Chinese)
[29] ZHANG Y, YUTAKA M, SASABE M, et al. Attribute-based access control for smart cities: a smart-contract-driven framework [J]. IEEE Internet of Things Journal,2021,8(4):6372 - 6384.
[30] 房梁,殷丽华,郭云川,等.基于属性的访问控制关键技术研究综述[J].计算机学报,2017,40(7):1680 - 1698.
FANG Liang, YIN Lihua, GUO Yunchuan, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers,2017,40(7):1680 - 1698. (in Chinese)
[31] 景旭,邢胜飞.基于 PBFT 的猕猴桃溯源联盟链应用访问控制方案[J].农业机械学报,2023,54(1):183 - 195.
JING Xu, XING Shengfei. Access control scheme of kiwifruit traceability consortium blockchain application based on PBFT [J]. Transactions of the Chinese Society for Agricultural Machinery,2023,54(1):183 - 195. (in Chinese)
[32] 潘恒,钱海洋,姚中原,等.典型区块链存储与查询技术综述[J].郑州大学学报(理学版),2022,54(6):34 - 50.
PAN Heng, QIAN Haiyang, YAO Zhongyuan, et al. A survey of typical blockchain storage and query technologies[J]. Journal of Zhengzhou University (Natural Science Edition),2022,54(6):34 - 50. (in Chinese)