doi:10.6041/j.issn.1000-1298.2025.06.003

基于区块链的食品供应链跨域追溯监管数据共享方法研究

孙传恒[1,2]　孙甄真[2,3]　罗　娜[1,2]　邢　斌[1,2]　王少华[2,3]　高官岳[1,2]　杨信廷[1,2]

(1. 国家农业信息化工程技术研究中心, 北京 100097;
2. 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;
3. 天津农学院计算机与信息工程学院, 天津 300384)

摘要: 食品安全追溯体系的广泛应用,一方面能够降低监管部门信息获取成本,提升监管效率,另一方面也能倒逼企业提高安全意识,主动进行风险控制。然而,由于不同食品监管部门技术和管理的原因,食品供应链中的监管数据分散、各监管域之间缺乏信任、数据难共享。针对上述问题,利用区块链技术在身份验证和权限管理方面的去中心化、不可篡改等优势,提出了一种面向食品供应链的跨信任域监管数据共享方法。首先通过引入 Schnorr 签名算法实现跨域身份认证,其次在基于属性的访问控制(Attribute-based access control,ABAC)基础上加入属性映射机制,实现食品供应链追溯监管数据的动态细粒度访问控制,最后基于 Hyperledger Fabric 开发食品供应链跨域安全传输原型系统,并进行了性能测试。结果表明,当交易负载数为 300 条时,跨域监管数据共享方法中的策略写入最小时延为 0.56 s,最大吞吐量为 113 个/s;当交易负载数为 600 条时,策略决策最小时延为 0.01 s,最大吞吐量为 414 个/s。本研究提出的食品供应链跨域监管数据共享方法性能良好,为实现食品供应链监管数据跨域共享提供新的方法和思路。

关键词: 食品供应链; 跨域; 区块链; 身份认证; 访问控制

中图分类号: TP311.11　　**文献标识码**: A　　**文章编号**: 1000-1298(2025)06-0033-14　　**OSID**:

Cross Domain Traceability and Regulatory Data Sharing Method for Food Supply Chain Based on Blockchain

SUN Chuanheng[1,2]　SUN Zhenzhen[2,3]　LUO Na[1,2]　XING Bin[1,2]　WANG Shaohua[2,3]　GAO Guanyue[1,2]　YANG Xinting[1,2]

(1. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
2. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*
3. *College of Computer and Information Engineering*, *Tianjin Agricultural University*, *Tianjin* 300384, *China*)

Abstract: The widespread application of food safety traceability system can not only reduce the cost of information acquisition for regulatory authorities and improve regulatory efficiency, but also force enterprises to raise safety awareness and actively control risks. However, due to the technical and management reasons of different food regulatory departments, regulatory data in the food supply chain was scattered, there was a lack of trust between regulatory domains, and data sharing was difficult. In response to the above issues, a cross trust domain supervision data sharing method for the food supply chain was proposed by utilizing the decentralized and tamper proof advantages of blockchain technology in identity verification and permission management. Firstly, cross domain identity authentication was achieved by introducing the Schnorr signature algorithm. Secondly, an attribute mapping mechanism was added to attribute-based access control (ABAC) to achieve dynamic fine-grained access control of food supply chain traceability and supervision data. Finally, a prototype system for cross domain secure transmission of food supply chain was developed based on Hyperledger Fabric, and performance testing was conducted. The results showed that when the transaction load was 300, the minimum delay for policy writing in the cross domain supervision data sharing method was 0.56 s, and the maximum throughput

收稿日期: 2025-02-04　修回日期: 2025-03-19

基金项目: 国家重点研发计划项目(2023YFD2001304)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: 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

was 113 transactions per second. When the transaction load was 600, the minimum delay for policy decision-making was 0.01 s, and the maximum throughput was 414 transactions per second. The cross domain regulatory data sharing method proposed had good performance, providing methods and ideas for achieving cross domain sharing of food supply chain regulatory data.

Key words: food supply chain; cross domain; blockchain; identity authentication; access control

0 引言

随着社会经济的发展,人们对食品安全关注程度不断提高[1-2]。食品安全风险存在于整个食品供应链过程中[3-5]。为了更好地确保食品安全性,国家已经建立并完善了市场监管体制,提出一系列与食品安全相关的措施[6]。我国的食品安全监管体制仍是一个多部门协作的体系[7],涉及多个领域和学科。在食品供应链监管以及食品安全追溯体系中[8-10],现有的监管模式仍然存在一些问题,各监管域之间缺乏有效的信息共享和协同机制[11]。在分布式网络环境中,各监管域组织形成了多个相对独立的信任域,这种独立性会导致信息孤岛和数据难以共享的问题[12-13]。跨监管域数据共享是指在多个独立的监管域之间实现数据的共享与协同,可将各种监管力量有效结合起来,构建更加高效和公开的食品安全监管体系[14-15]。因此,有必要进行跨域研究,实现食品供应链的跨监管域数据共享。

跨监管域数据的安全共享需解决身份认证和访问控制的问题。然而在监管域追溯数据跨域共享中,未经授权访问和非法数据篡改等安全问题时有发生,建立统一的身份认证体系以及细化数据访问的权限管理,可以有效保障数据共享的安全性。早期的身份认证主要是公钥基础设施 PKI(Public key infrastructure)和基于身份的密码体制 IBC(Public key infrastructure)的认证机制,但都是基于中心化的认证方法,依赖于第三方可信机构,存在较大的安全隐患。区块链是一种分布式记账技术,实现了去中心化管理,其数据被存储在多个网络节点中,不依赖于任何一个中心化的管理点,从而有效规避了单点失效的风险。已有相关研究结合区块链实现跨域认证,参与者在多个可信区域之间完成一致的身份验证[16]。相关理论和实践研究[17-29]表明实现跨域数据的高效、安全和细粒度的安全共享是一个亟待解决的问题。

区块链不可篡改、公开透明的特性可以帮助不同域的组织迅速建立起信任、促进跨域合作[30-31],本文结合食品供应链的追溯需求,针对跨监管域数据共享问题,提出基于区块链的食品供应链跨域追溯监管数据共享方法。利用基于 Schnorr 签名算法构建零知识证明的身份认证方案实现不同信任域之间的身份认证,确保参与者身份的真实性;然后利用加入属性映射机制的 ABAC 实现不同域间的细粒度访问,增加数据共享时的灵活性;最后基于 Hyperledger Fabric 平台实现食品供应链跨域追溯监管数据共享的原型系统并对其进行相关测试。

1 食品供应链跨域追溯监管数据共享模型

1.1 食品供应链监管信息分析

食品供应链是指从原料的生产、加工、运输、储存到最终的零售商和消费者手中的全过程,食品供应链监管又是一个涉及多个领域和部门的复杂过程[32]。对食品供应链进行监管的目的是确保食品从生产到消费的每一个环节都符合安全标准。因此,将食品供应链各阶段所涉及的监管数据进行概括,如表 1 所示。不同食品类型的供应链可能涉及不同的监管部门和数据类型,但跨监管域数据共享中的数据分散、监管域间缺乏信任等核心问题是普遍存在的。本文主要聚焦于加工食品类型,具有广泛的适用性,覆盖从初级农产品到深加工食品的整个食品供应链,通过对各阶段监管数据进行简单分类,可以为跨域数据共享提供通用的框架。

表 1 食品供应链追溯监管数据分类

Tab. 1 Classification of food supply chain traceability and regulatory data

所处阶段	监管数据类型
生产	农产品生产者的认证信息 农药、兽药使用记录 食品添加剂和包装材料使用标准等
加工	食品生产许可证信息 食品加工记录,包括原料来源、加工流程、员工健康等 食品安全标准和检验报告等
流通	食品经营者的许可信息 食品储存和运输记录 进出口食品的检验检疫报告等
销售	食品经营许可证 食品标签和广告 销售记录和消费者投诉 食品安全风险评估报告 消费者健康和营养指导信息 食品安全事故调查报告和处理结果等

跨域数据访问结构如图 1 所示,食品供应链的

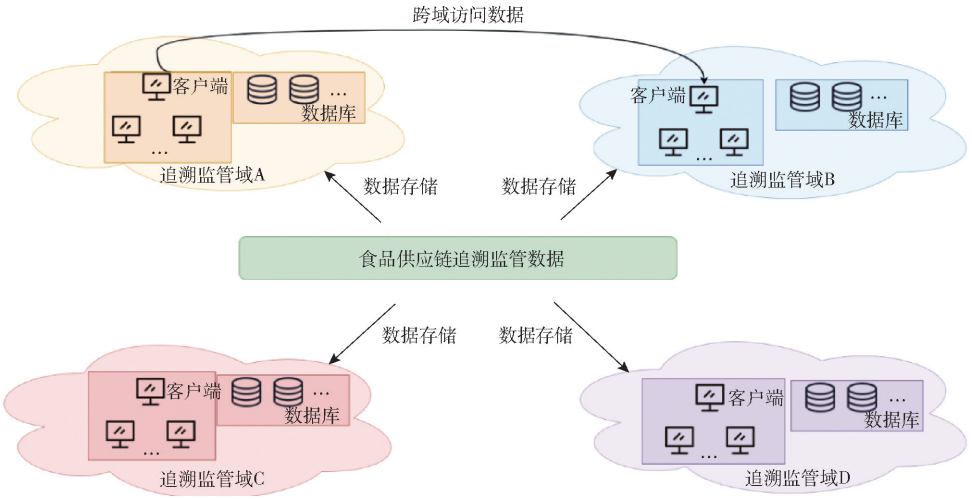


图 1　跨域访问结构图

Fig. 1　Cross domain access structure diagram

追溯监管数据广泛分布在多个监管部门，这些监管部门依据其特定的监管职责分别负责不同类型的数据收集与管理，形成了多个相对独立的监管域。各监管部门在食品供应链的分工上各有侧重，在保障食品安全的共同目标下又存在着紧密的协作关系。当前的数据存储与访问机制限制跨域协作的效率与深度，监管部门在应对食品安全问题时难以形成合力。因此，基于对跨域数据访问结构分析，设计跨域追溯监管数据共享模型，打破数据孤岛。

1.2　跨域追溯监管数据共享模型

由于现有食品供应链的监管存在问题，缺乏针对信任域数据孤岛、监管数据难共享的解决方法，众多监管部门形成互不信任的监管域，而区块链可以解决这种多方间的信任问题[33-34]。区块链根据不同场景下的信任构建方式可分为公有链、联盟链和私有链 3 类[35]。在食品供应链的场景中，跨监管信任域实现食品监管数据的共享，多个监管机构或组织相互独立，联盟区块链由多个独立的组织共同管理，因此，选用联盟区块链开展针对跨监管域数据共享的模型研究。

针对食品供应链提出跨域监管数据共享模型，如图 2 所示。模型主要由 3 部分构成：食品供应链环节、涉及监管域（模型中只展示 4 个监管域）以及区块链网络。食品供应链多环节中会产生大量监管数据，按照监管部门的不同监管职责划分存储，分散在不同监管域中。例如食品供应链的监管数据会涉及农业生产相关数据、卫生标准相关数据、食品检测相关数据和市场监管相关数据等，各监管部门由于

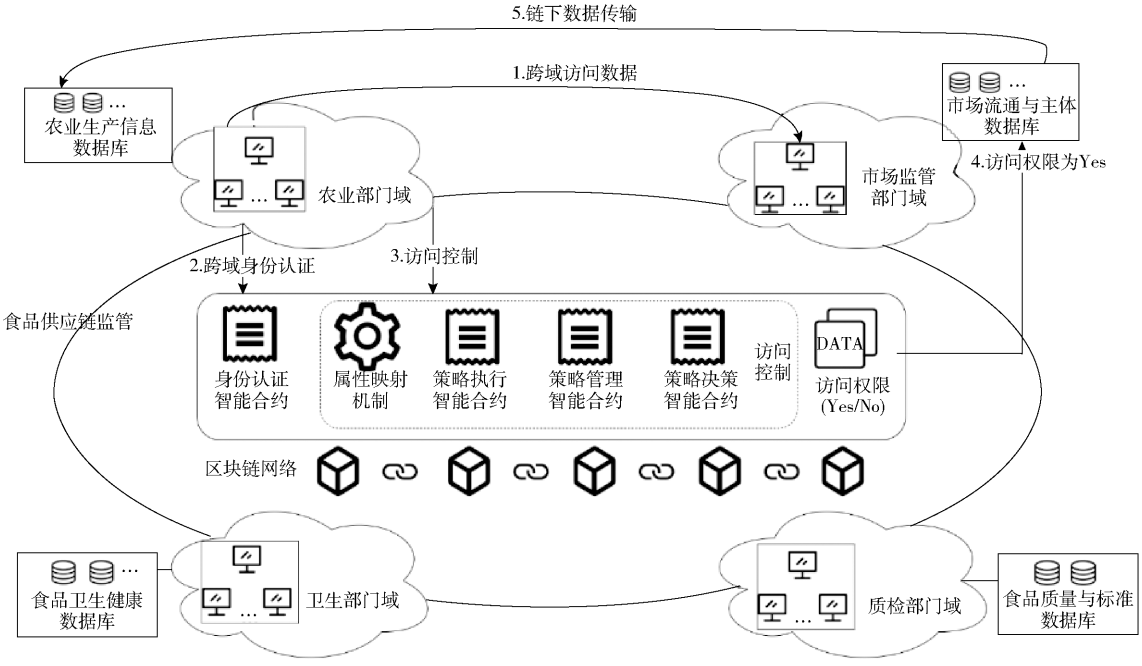


图 2　食品供应链跨域追溯监管数据共享模型

Fig. 2　Cross domain traceability and regulatory data sharing model for food supply chain

在供应链的分工不同而无法共享所有的监管数据，但在食品安全监管体系中，各部门之间又存在协作关系，需要各部门之间进行频繁的数据共享和信息交互，例如市场监管部门为确保食品源头追溯的准确性和及时性，有效应对农药残留等食品安全问题，可以和农业相关部门进行协作共享。为便于后续的实验验证，本模型特选 4 个不同监管域作为示例，模型中的监管域分别表示农业部门域、市场监管部门域、卫生部门域和质检部门域，不同域的设备在应用层进行注册。这 4 个监管域功能不仅覆盖了食品供应链的关键节点，也体现了多部门协同监管的复杂性与必要性。

以农业部门域跨域访问市场监管部门域为例说明模型工作流程：首先，农业部门域向市场监管部门域请求跨域访问（步骤 1）；然后，市场监管部门域在区块链上完成对农业部门域的身份认证，认证失败则拒绝访问，认证成功则进一步在区块链上执行访问控制（步骤 2）。农业部门域通过属性映射机制构建基于属性的访问请求到市场监管部门域，通过区块链上的策略执行、策略管理、策略决策等智能合约决定访问权限结果（步骤 3），决策失败则拒绝访问，决策成功则其访问权限为 Yes（步骤 4），可进一步实现链下数据传输（步骤 5）。模型的设计确保数据共享的安全性、高效性和隐私性，同时利用区块链技术提高身份验证和权限管理的可靠性。

2 食品供应链跨域追溯监管数据共享方法

在深入探讨基于区块链的食品供应链跨域追溯监管数据共享方法时，鉴于食品供应链涉及多环节、多参与方，且多为不同的信任域，确保每一个参与者都具备真实合法的身份标识，可为后续的数据共享与协同工作奠定信任基础。传统的中心化认证机制在面临跨域环境时，因信任缺失、效率低下而难以胜任；在复杂多变的食品供应链环境中，不同域间数据敏感性与访问需求各异，传统的基于角色的访问控制难以满足动态变化的权限管理需求，仅依靠 ABAC 也无法解决域间数据属性的差异问题。因此，利用区块链的去中心化特性，引入 Schnorr 签名算法实现跨域身份认证，以及在 ABAC 基础上加入属性映射机制，实现食品供应链追溯监管数据的动态细粒度访问控制，实现可靠的跨域追溯系统。

2.1 基于 Schnorr 签名算法的身份认证

食品供应链跨监管域数据共享的场景涉及众多参与域，在数据共享中，身份认证技术确保参与方经过必要的验证和授权，降低由于身份欺诈或未授权访问而引发的风险。身份认证是一项对网络实体身份的有效性进行鉴别的技术[36]。跨域身份认证方案基于区块链的分布式信任，通过编写智能合约实现，提供了实时的、自动化的验证机制，解决域间设备的身份认证问题。随着数字身份认证在各行各业的广泛应用，特别是在需要高安全性和高效率的跨域环境中，选择合适的签名算法尤为重要。

在多方跨监管域数据共享场景中，选择 Schnorr 签名算法为本研究身份认证中的优选方案，主要有以下几点理论依据：

（1）简洁性与高效性：Schnorr 签名算法基于离散对数问题，具有较高的计算效率，适合在区块链环境中进行快速验证。其签名生成和验证过程简单且计算量小，仅需一次点乘运算和一次哈希运算，在保证安全性的同时，降低系统的计算负担。

（2）多签名支持：Schnorr 签名算法支持多签名配置，不同监管实体可以共同验证和批准跨域数据交换，增强系统的协作能力。多签名聚合可以将多个签名合并为一个签名，减少通信开销。例如：多个签名者的签名 (R_1,s_1)，(R_2,s_2)，…，(R_n,s_n) 可以聚合为 (R_{agg},s_{agg})，其中

$$R_{agg}=R_1+R_2+\cdots+R_n \tag{1}$$

$$s_{agg}=s_1+s_2+\cdots+s_n \tag{2}$$

验证时只需验证 $s_{agg}G=R_{agg}+eY_{agg}$ 等式是否成立，其中 Y_{agg} 是多个公钥的聚合。

（3）隐私保护：Schnorr 签名算法通过零知识证明技术，在不泄露私钥的情况下证明签名的有效性。确保签名的安全性和零知识性，适用于需要保护用户隐私的跨域数据共享场景。

（4）兼容性：Schnorr 签名算法与现有的公钥基础设施（PKI）和区块链技术具有良好的兼容性，能够无缝集成到现有的系统。

2.1.1 Schnorr 签名算法

Schnorr 签名算法以其简洁性、高效性及基于离散对数问题的安全性在密码学领域内占据重要地位[37]。在本框架中，聚焦于如何利用该算法实现一种在不泄露私钥 x 的前提下，向验证方（如证书颁发机构 CA）证明私钥持有者身份的机制。关于系统参数的设定，系统构建于一个椭圆曲线 $E(a,b)$ 之上，其中 a 和 b 定义了曲线的方程。此外，选定一个基点 g，并定义一个大素数 p 作为椭圆曲线的模数，确保运算的有限域。椭圆曲线的阶 q 是另一个关键参数，用于确保离散对数问题的难解性。私钥 x 是随机选取于 $[1,q-1]$ 的一个整数，其对应的公钥 y 则通过椭圆曲线上的点乘运算得出，公式为

$$y=g\cdot x \bmod p \tag{3}$$

Schnorr 签名算法流程如图 3 所示。

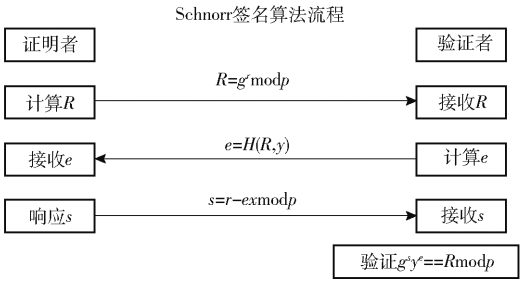


图 3　Schnorr 签名算法流程图

Fig. 3　Flowchart of Schnorr signature algorithm

签名生成：由证明者（设备）操作，选择一个随机整数 $r \in [1, q-1]$ 作为临时私钥；计算承诺值 R，并将 R 发送给验证者作为初步承诺，公式为

$$R = g^r \bmod p \tag{4}$$

挑战与响应：验证者（CA）接收 R 后，计算挑战 $e = H(R, y)$，其中 H 是一个安全的哈希函数，将承诺值 R 和公钥 y 作为输入；证明者（设备）收到挑战 e 后，计算响应值 s，并将 s 发送给验证者，公式为

$$s = r - ex \bmod p \tag{5}$$

签名验证：验证者（CA）使用接收到的 s、已知的 R、y 以及挑战 e，验证等式

$$g^s y^e = = R \bmod p \tag{6}$$

是否成立，若等式成立，则证明者成功证明了其知道私钥 x，签名被视为有效，从而验证了证明者的身份；否则，签名无效。

2.1.2　链上身份认证过程

跨域身份认证中，Schnorr 算法通过零知识证明的方式保护了用户的私钥和身份信息，在不泄露私钥的情况下证明私钥的存在，确保签名的安全性和零知识性。此外，区块链的不可篡改性和分布式特性可为设备的注册、证书颁发和验证提供安全可靠的环境。具体而言，通过在区块链上部署一个 CA（证书颁发机构）的智能合约，实现对设备注册、证书生命周期管理的自动化与透明化。

链上身份认证过程如图 4 所示，具体过程可分为 3 个阶段：

注册阶段：有跨域访问需求的设备首先向区块链网络中的 CA 服务发起注册请求，并提交其身份信息（info）。CA 服务在审核通过后，为该设备生成一对非对称密钥对（公钥 pk_{req} 和私钥 sk_{req}），其中私钥 sk_{req} 通过安全通道发送至设备端进行秘密存储。随后，CA 服务利用其私钥 sk_{ca} 对设备的公钥 pk_{req} 及身份信息 info 进行数字签名，生成相应的数字证书 cert，并将此证书永久记录在区块链上，以确保其不可篡改性与可追溯性。

零知识证明生成阶段：设备需要进行身份认证时，向 CA 服务发送认证请求。请求中包含需通过 Schnorr 算法进行签名的内容，在不泄露私钥的前提下，向 CA 服务证明其身份的有效性。设备据此生成零知识证明请求 zkp，并发送至 CA 服务以待验证。

零知识证明验证阶段：CA 服务接收到零知识证明请求后，利用 Schnorr 算法对其进行验证分析。若验证成功，则确认该设备身份的真实性与有效性，向设备发送认证成功的响应，为后续访问控制流程奠定基础。

2.2　基于属性映射机制跨监管域实现访问控制

传统的跨域访问控制依赖中心化的认证和权限管理系统，在去中心化的区块链上实施跨域访问控制增加系统的安全性，同时也为跨域访问控制提供

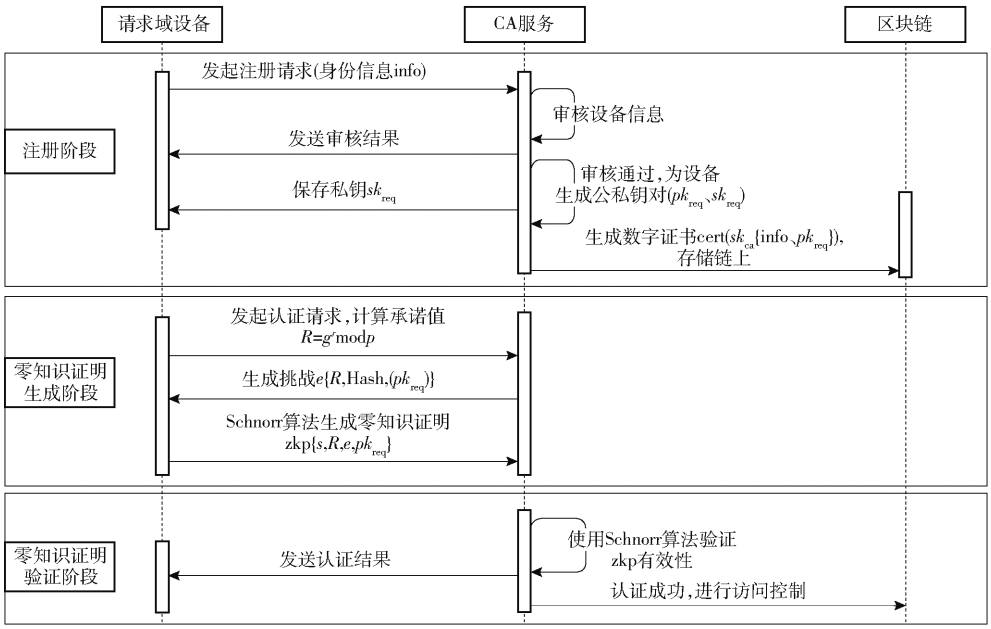


图 4　链上身份认证时序图

Fig. 4　Identity authentication timing diagram

了不可篡改的审计跟踪,增强了系统的信任度。在不同的监管域中,各部门因其特定的数据访问需求与操作权限,会制定差异化的访问策略。然而,由于命名规则、标准或架构的多样性,基于属性的跨域访问控制常面临属性不一致的挑战。因此,引入属性映射机制,通过区块链技术记录并保存这种映射关系,确立不同监管域间属性的对应关系,从而有效实现跨域访问控制。在区块链环境中,用户和资源的属性实现去中心化存储与验证,显著降低了对中心化身份提供商的依赖。属性值变更在区块链上实时记录并传播,确保访问决策基于最新且经过验证的属性信息,从而提高了安全性和响应速度。

基于属性映射的访问控制主要分为以下 3 个步骤:定义标准属性,确定各信任域间的属性映射关系,制定标准的属性命名规范;智能合约中实现属性映射,在智能合约中实现属性映射逻辑,将不同信任域的属性映射到标准的属性命名;动态访问控制规则设计,利用智能合约实现动态访问控制规则,基于标准属性进行访问权限控制。

2.2.1 属性的定义和映射机制

在访问控制系统中,属性指的是与实体相关的一组描述符,比如用户的职位、操作时间等,对于属性的使用允许系统基于这些描述符来制定访问决策,从而提供更具细粒度的访问控制。在 ABAC 模型中,属性为系统提供了一种灵活且动态的方式来适应变化的访问需求和环境条件。因此,分析提取了食品供应链跨监管域数据访问的主要属性信息,并对其进行进一步的划分,其属性描述如表 2 所示。

表 2 食品供应链跨监管域数据访问属性描述

Tab. 2 Description of cross regulatory domain data access attributes in food supply chain

属性分类	表示	统一命名
主体属性	UserID	请求访问主体的唯一性标识
	Role	请求访问主体所属角色,每个域命名会有不同
	Department	请求访问主体所属部门,每个域命名会有不同
	Domain	请求主体所属监管域
	AccessLevel	请求主体的访问权限级别,每个域命名会有不同
客体属性	ID 标识	被请求客体的唯一性标识
	DataType 数据类型	被请求客体的数据类型
	DataDomain 数据所有域	被请求客体所属域
	SensitivitLevel 敏感度	被请求客体的敏感度级别
	DataStatus 数据状态	被请求客体的数据状态
操作属性	OperationType 操作类型	请求中的操作类型
环境属性	Time	发起访问请求的时间
	Location	发起访问请求的地址来源

跨域访问控制基于 ABAC 模型,通过以上的属性描述,可以制订较为详细的访问控制策略。但不同域对多个属性的命名方式存在差异,跨域的环境会导致属性和策略不兼容问题的出现。因此,提出基于属性映射的 ABAC 模型,通过映射机制将请求主体属性映射为符合目标域策略的属性。在跨域数据访问的时候,目标域会接收到来自请求域的请求信息,为满足目标域的访问策略相匹配,就要对请求域发来请求的主体属性进行映射,主要是针对具有不同命名方式的请求主体身份的相关描述。映射机制中对于映射关系的描述为

$$\mathrm{CONDS}(C_1 \text{ AND } \cdots \text{ AND } C_n)S \Rightarrow \mathrm{TRANSFORM}(A_1, A_2, \cdots, A_n)S \Rightarrow \mathrm{ATTRBS}(B_1, B_2, \cdots, B_n)T$$

该映射关系主要由 3 部分组成。$\mathrm{CONDS}(C_1 \text{ AND } \cdots \text{ AND } C_n)S$:第 1 部分表示源域 S 中的属性条件集合,当且仅当所有条件 C_i 都为真时,才会触发映射关系;$\mathrm{TRANSFORM}(A_1, A_2, \cdots, A_n)S$:第 2 部分是一个转换函数,它接收源域 S 中的属性集合作为输入,并计算目标域 T 中的新属性值。这个转换函数可以是简单的赋值,也可以是复杂的逻辑或数学运算;$\mathrm{ATTRBS}(B_1, B_2, \cdots, B_n)T$:第 3 部分是目标域 T 中的属性赋值集合,每个 B_j 是转换函数输出的新属性值。为明确阐述映射机制的实现,依据请求者的职位和部门,映射其在目标域的相关属性以及访问级别,即

$$\mathrm{CONDS}(\mathrm{Role} = \text{"Inspector"} \text{ AND } \mathrm{Department} = \text{"Public Affairs Department"})S \Rightarrow \mathrm{TRANSFORM}(\mathrm{Role}, \mathrm{Department})T \Rightarrow \mathrm{ATTRBS}(\mathrm{ROLE} := \text{"Censor"}, \mathrm{Department} = \text{"Regulatory Affairs Department"}, \mathrm{ACCESS_LEVEL} := \text{"BasicAccess"}))T$$

具体来说,源域主体属性中职位为"Inspector",部门为"Public Affairs Department",经过映射,其在目标域中职位为"Censor",部门为"Regulatory Affairs Department",该属性组合拥有的访问级别为"BasicAccess"。该映射机制结构清晰地区分了条件(CONDS)、转换(TRANSFORM)和赋值(ATTRBS)3 个部分,结构化的描述方式使得映射关系更加易于管理和维护,方便后续的修改和扩展。此外,转换函数的引入允许在映射过程中进行更复杂的计算或逻辑处理,而不仅是简单的赋值,这也使得映射机制更加灵活。

针对属性取值范围有限的特性设计了高效的键值对检索方案。首先,对用户和资源的相关属性进行细致梳理,确定用户的职位、部门、所属域、访问级别以及资源的资源 ID 标识、数据类型、数据所有域、敏感度级别、数据状态等属性的有限取值集合。对

于用户属性，依据各属性取值种类构建相应维度的向量。例如，假设系统中存在 n_1 种职位、n_2 个部门、n_3 个所属域和 n_4 种访问级别，构建一个长度为 $L_u = n_1 \times n_2 \times n_3 \times n_4$ 的一维向量。通过特定的映射规则，将用户的属性组合唯一映射至向量下标。如用户 user2 具有特定属性集合，经计算得到对应下标 i_u，并于该下标位置存储其访问策略信息。同理，针对资源属性构建多维向量。假设资源属性取值种类分别为 m_1（资源 ID 标识）、m_2（数据类型）、m_3（数据所有域）、m_4（敏感度级别）、m_5（数据状态），构建一个大小为 $L_r = m_1 \times m_2 \times m_3 \times m_4 \times m_5$ 的 5 维向量，如对于资源 resource1，依据其属性组合经映射规则确定下标 i_r，存储相关访问控制信息。在检索时，如当用户 user2 发起对资源 resource1 的访问请求，分别提取用户与资源属性信息，依据映射规则计算出对应向量下标 i_u 和 i_r。由于向量的随机访问特性，检索过程直接定位下标获取信息，时间复杂度为 $O(1)$。

2.2.2　访问控制框架及工作流程

ABAC 是一种灵活的访问控制模型，使用预定义的策略和属性来决定用户是否有权访问特定的资源。在 ABAC 模型中，访问控制决策基于主体（请求访问的用户）属性、客体（被请求的信息或服务）属性、操作（用户希望执行的操作，如读取、写等）属性以及环境（当前的上下文状态，如时间）属性。可扩展访问控制标记语言（eXtensible access control markup language，XACML）定义了策略的标准表示格式以及做出授权决策的标准方法，比较适用于与分布式环境下的访问控制策略描述，已被广泛应用于 ABAC 的研究中[38-39]。XACML 架构包括几个关键组件：策略管理点（Policy administration point，PAP）、策略执行点（Policy enforcement point，PEP）、策略决策点（Policy decision point，PDP）和策略信息点（Policy information point，PIP）。

为满足跨域访问控制，对传统的 ABAC 模型加入属性映射机制，使用 XACML 标准来描述访问控制策略，将访问控制技术与区块链技术相结合，跨监管域访问控制框架如图 5 所示，包括准备阶段、执行阶段和区块链网络。

跨监管域访问控制是在区块链上通过智能合约进行交互实现的。以监管域 A（即数据请求者所在监管域）访问监管域 B（即数据拥有者所在监管域）的过程为例，描述跨监管域访问控制工作流程，具体如下：

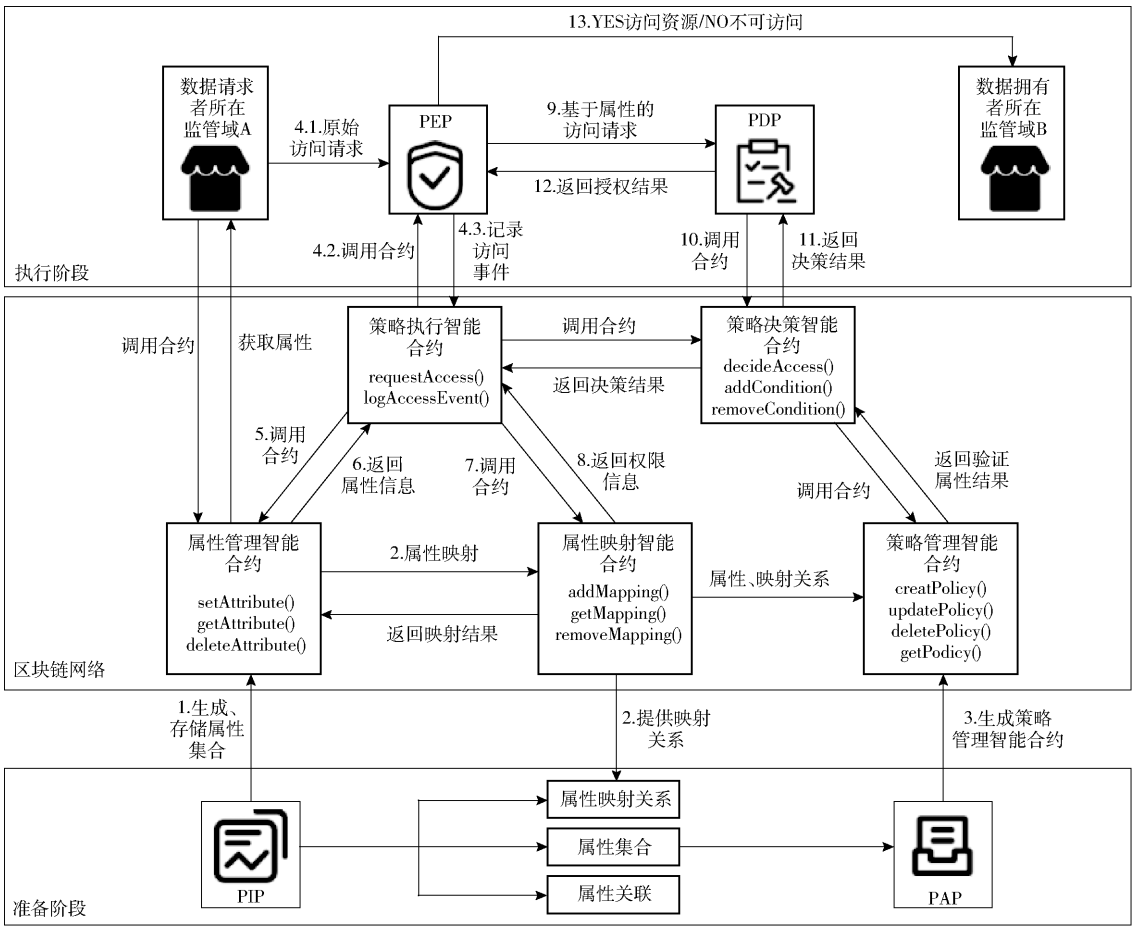


图 5　跨监管域访问控制框架

Fig. 5　Cross regulatory domain access control framework

首先,准备阶段与区块链网络交互,PIP 在区块链上生成、存储和管理属性集合,包括监管域 A 和监管域 B 中所涉及的用户、资源和环境等属性。生成的属性管理智能合约由各监管域共同维护;通过区块链网络中的属性映射智能合约获取属性映射关系,将属性映射关系、属性、属性关联等信息发送给 PAP;PAP 基于属性及其映射到权限的关系,在区块链上生成策略管理智能合约,便于动态调整策略、响应属性或环境的变化。以上过程如图 5 中步骤 1 ~3 所示。

其次,执行阶段与区块链网络交互,当监管域 A 发送原始访问请求到 PEP 请求执行时,PEP 基于请求信息在区块链上生成策略执行智能合约,记录监管域 A 的相关访问事件,此过程如图 5 中步骤 4 所示。PEP 通过策略执行智能合约调用属性管理智能合约获取到与监管域 A 相关的属性信息,并调用属性映射智能合约获取到监管域 A 的属性映射信息及相关属性权限。基于获取到的信息,PEP 为监管域 A 构建基于属性的访问请求并发送到 PDP 请求决策。以上过程如图 5 中步骤 5 ~9 所示。PDP 通过策略决策智能合约调用策略管理智能合约验证监管域 A 的所有属性数据;再由策略决策智能合约评估监管域 A 的基于属性的访问请求,决定是否授权访问,PDP 将授权结果返回给 PEP;PEP 根据该结果对监管域 B 资源执行操作:决策结果为 YES 时,可访问数据资源,决策结果为 NO 时,拒绝对资源的访问。以上过程如图 5 中步骤 10 ~13 所示。

2.3 智能合约设计

针对食品供应链跨监管域数据共享场景实现身份认证和访问控制,使用 Fabric 区块链平台,用 go 语言开发智能合约,主要分为身份认证、属性管理、属性映射、策略执行、策略管理、策略决策的智能合约方法。链上收到跨域访问请求,节点收到请求自动触发合约实现身份认证以及动态授权访问。智能合约设计如表 3 所示。

表 3 智能合约设计

Tab. 3 Smart contract design

合约功能	合约方法	输入	输出	描述
身份认证	registerIdentity ( )	域名称 Domain 注册身份信息 info	用户身份唯一标识 userID	注册域间新用户
	createCertificate( )	身份信息 userID、域名称 Domain、公钥 PublicKey	证书 Cert、证书哈希值 HashStr	创建数字证书
	requestAuthentication( )	用户身份唯一标识 userID、零知识证明请求 zkp	True/False	用户发起身份认证请求
	verifyProof( )	零知识证明请求 zkp、公钥 PublicKey	True/False	验证用户身份
属性管理合约	setAttribute( )	用户 ID(或资源 ID)、属性名、属性值/集	True/False	存储或更新属性值
	getAttribute( )	用户 ID(或资源 ID)、属性名	属性值/集	返回请求的属性值/集
	deleteAttribute( )	用户 ID(或资源 ID)、属性名	True/False	从存储中删除属性值/集
属性映射合约	addMapping( )	属性名、属性值、权限集合	True/False	添加新的映射规则
	getMapping( )	属性名、属性值	权限集合	返回基于属性的权限集合
	removeMapping( )	属性名、属性值	True/False	删除指定映射规则
策略执行合约	requestAccess ( )	用户 ID、资源 ID、操作类型	Allow/Refuse	接收访问请求,获取决策结果,执行决策结果
	logAccessEvent ( )	用户 ID、资源 ID、操作类型、访问结果	True/False	将访问事件记录到区块链上
策略管理合约	creatPolicy( )	策略 ID、策略规则	True/False	在合约中添加新的策略,用于后续访问控制判断
	updatePolicy( )	策略 ID、新的策略规则	True/False	修改已存在的策略,适用于变更环境或需求
	deletePolicy( )	策略 ID	True/False	从合约中删除指定的策略
	getPolicy( )	策略 ID	策略规则	返回指定策略的详细规则信息
策略决策合约	decideAccess( )	用户 ID、资源 ID、操作类型	Allow/Refuse	检查用户请求与策略规则的匹配情况,决定是否允许访问
	addCondition( )	策略 ID、条件表达式	True/False	向特定策略添加新的条件,提高策略的适应性和灵活性
	removeCondition( )	策略 ID、条件表达式	True/False	从策略中移除指定的条件,适用于策略简化或调整

身份认证合约执行时，通过用户注册生成数字证书，实现用户身份的可验证性和唯一性。关键功能包括用户注册、数字证书生成、身份验证及零知识证明验证。访问控制执行时，先由策略执行合约接收访问请求并记录访问事件用于审计和监控，有助于追踪潜在的安全问题和不当行为。策略执行阶段是访问控制流程的实际应用点，依据预设的策略规则来直接控制对资源的访问；策略管理负责策略的创建、更新和删除，这一环节确保了访问控制策略可以灵活应对组织需求的变化；策略决策合约作为智能合约的形式，提供了一种自动化和去中心化的方法来实施访问控制决策，使得访问控制不仅自动化且透明，同时增强了安全性和可信度。相关智能合约伪代码描述如下：

算法 1：身份认证智能合约

输入：源域用户身份信息 userID，域信息 Domain

输出：认证结果 AuthResult

```
1. Function creatCertificate (userID, Domain, PublicKey) //为用户生成数字证书
2.  return encodePacked(Cert, HashStr)
3. Function requestAuthentication (userID, zkp) //用户发起认证请求
4.  require(user[userID].isRegistered, "User not registered")
5.  bool isValid = verifyProof(zkp, PublicKey) //验证零知识证明
6.  if (isValid)
7.  emit AuthSuccess(userID)
8.  else
9.  emit AuthFailed(userID)
10. FunctionverifyProof (zkp, PublicKey) //验证零知识证明
11.  if keccak256 (zkp) == keccak256 (publicKey)
12.  return AuthResult
```

算法 2：策略执行智能合约

输入：用户 ID UserID，资源 ID ResourceID，操作类型 ActionType

输出：访问结果 AccessResult

```
1. Function requestAccess (UserID, ResourceID, ActionType) //处理访问请求
2. decisionResult = decideAccess (UserID, ResourceID, ActionType) //转发请求至策略决策合约以获取决策结果
3. if (decisionResult == "Allow") //根据决策结果执行允许或拒绝操作
4.  AccessResult = "Allow"
5. else
6.  AccessResult = "Refuse"
7. return AccessResult
8. Function logAccessEvent (UserID, ResourceID, ActionType, AccessResult) //记录访问事件到区块链
9. access_event = new AccessEvent (current_timestamp, UserID, ResourceID, ActionType, AccessResult) //创建访问事件对象
10. blockchain.write(access_event) //将访问事件写入区块链
```

算法 3：策略决策智能合约

输入：用户 ID UserID，资源 ID ResourceID，操作类型 ActionType，策略 ID PolicyID，条件表达式 ConditionExpression

输出：访问决策 AccessDecision (Allow/Refuse)，操作结果 OperationResult (True/False)

```
1. Function decideAccess (UserID, ResourceID, ActionType) //决定是否允许访问
2. if (policyMatching (UserID, ResourceID, ActionType)) //检查用户请求与策略规则的匹配情况
3.  return "Allow" //允许访问
4. else
5.  return "Refuse" //拒绝访问
6.  Function addCondition (PolicyID, ConditionExpression) //向特定策略添加新的条件
7. if (policyExists (PolicyID)) //策略已存在
8.  updatePolicy(PolicyID, NewPolicyRules) //向策略添加条件
9. return True
10. else
11.  return False //策略不存在
12.  Function removeCondition (PolicyID, ConditionExpression) //更新已存在的策略
13. if (policyExists(PolicyID))
14. else
15.  return False //策略不存在
16. Function deletePolicy(PolicyID) //从策略中移除指定的条件
17. if (policyExists (PolicyID) &&addCondition (PolicyID, ConditionExpression))
18.  removeCondition (PolicyID, ConditionExpression) //从策略中移除条件
19. return True
```

```
20. else
21.     return False //策略或条件不存在
```

3 实验测试

实验测试在 Virtual Machine ware 虚拟机中进行,虚拟机操作系统为 Ubuntu 20.04,内存容量 8 GB,处理器内核 8 个。在 Ubuntu 下搭建 Hyperledger Fabric 2.2 区块链平台,其中包含 1 个通道、2 个组织、4 个 peer 节点以及 3 个 Orderer 节点,选择 Raft 作为区块链平台的共识机制,选择该共识主要是通过其直观的领导者选举和日志复制机制,确保数据的一致性和高可用性,对支撑跨域身份认证和访问控制实验的基本需求至关重要,共识算法的选择并非核心讨论内容,只是作为实验环境搭建的一部分被采用,以便专注于跨域身份认证和访问控制机制的研究与实现。实验中的链码均使用 go 语言进行编写。

3.1 性能测试

依据 Hyperledger Fabric 的主要性能评估关键指标,包括交易时延和交易吞吐量,将其作为系统的性能评估指标。实验中使用 Caliper 测试工具对区块链上实现跨域访问控制的策略写入交易活动和策略判定交易活动进行性能测试。其中对于策略写入的测试在交易负载为 50 ~ 300 条范围内分别进行,其时延和吞吐量如图 6 所示,在交易负载最大时的最小时延为 0.56 s,最大吞吐量为 113 个/s;对于策略决策的测试在交易负载为 100 ~ 600 条范围内分别进行,其时延和吞吐量如图 7 所示,在交易负载最大时的最小时延为 0.01 s,最大吞吐量为 414 个/s,测试结果均处于可接受范围。

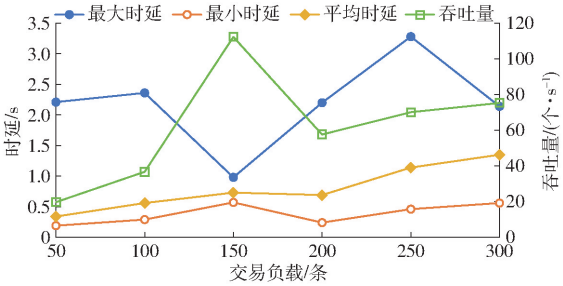


图 6 策略写入的时延和吞吐量

Fig. 6 Delay and throughput of policy writing

模拟并量化系统在接收到访问请求后,执行策略查询和策略决策过程的时间效率,实验共进行 100 轮请求,分别模拟属性个数为 6、12、18 时的请求,时间消耗如图 8 所示,可以观察到策略判定时间稳定在 2.05 s 左右,表明系统对于属性数量的增加具有较好的可扩展性。在高频次访问请求场景下,稳定的判定时间能够确保系统资源的合理分配与有效利用,避免因处理延迟而导致的服务中断或性能瓶颈。

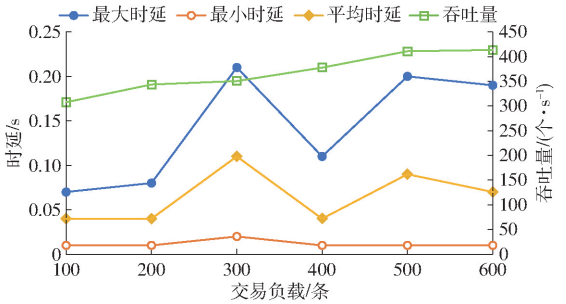


图 7 策略决策的时延和吞吐量

Fig. 7 Delay and throughput of strategy decisions

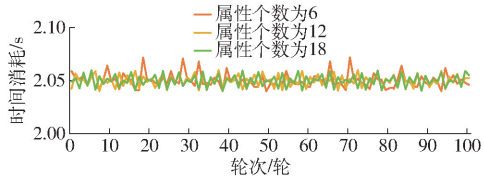


图 8 策略判定时间消耗

Fig. 8 Strategy determination time consumption

3.2 对比

通过对比分析来评估提出的基于区块链技术的跨域监管数据共享方法,结合表 4 可以看出,在安全性、自主授权、存储成本、数据传输效率、可审计性及判决透明度等方面的优势。

表 4 本研究与已有研究对比

Tab. 4 Comparative analysis between this study and existing research

来源	基于区块链	安全性	自主授权	存储成本	数据传输效率	可审计	判决透明
文献[26]	是	访问控制机制	具备	高	低	具备	具备
文献[28]	是	访问控制机制 非对称加密	具备	高	高	具备	具备
文献[29]	是	访问控制机制 非对称加密	具备	高	低	具备	具备
本研究	是	身份认证机制 访问控制机制 非对称加密	具备	低	高	具备	具备

进一步探究策略判定时间与策略数量之间的关联性,分别测试策略数量为 1 000、2 000、3 000、4 000、5 000 的策略判定时间,体现策略响应请求的时间长短。随机选择 20 条请求,每条请求中属性个数为 6,与文献[29 - 30]的测试结果进行对比,结果如图 9 所示。由图 9 可知,随着策略数量的递增,文

献[29－30]策略判定时间消耗显著增加，而本研究策略判定时间基本维持在 2.05 s 左右，无明显波动。这一显著差异是由于本研究采用基于向量的键值对检索方式，本质是通过对用户和资源属性的离散取值进行编码，转化为向量中的下标索引，属性的取值范围和种类不变，存储策略信息的向量维度和大小没有发生变化，因此随着策略数量的增加，检索时间基本保持不变，避免了传统遍历区块检索方式中因数据量增长而导致的性能下降问题，从而确保了查询效率的稳定性和高效性。

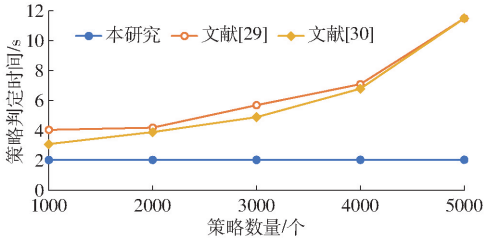


图 9　策略判定时间对比测试

Fig. 9　Comparison test of strategy judgment time

3.3　系统架构

基于食品供应链跨域追溯监管数据共享的业务分析，本文设计了系统整体架构图，如图 10 所示。系统架构共分为 5 层，根据实现功能自下而上分别是数据存储层、传输层、服务层、区块链网络层和应用层。

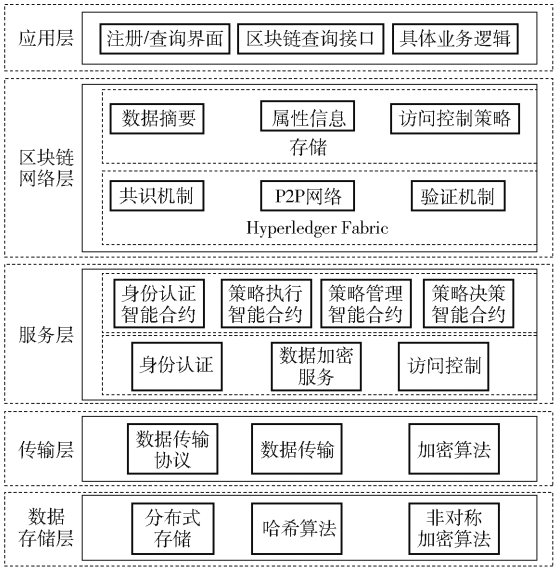


图 10　系统整体架构图

Fig. 10　Overall system architecture diagram

数据存储层：利用分布式存储技术，各监管域在本地服务器存储食品全链条不同追溯阶段的监管数据，数据在存储前，会经过服务层的加密处理，确保数据的安全性和隐私性。利用哈希算法来验证数据的完整性。

传输层：负责数据的加密和安全传输。数据传输模块负责数据的实际传输工作，包括网络协议的选择、数据包的封装与解析等。在数据传输过程中，使用加密算法对数据进行二次加密，确保数据在节点之间传递时的安全性和完整性。

服务层：主要包括身份认证和访问控制两大模块，以及数据加密服务。利用区块链的去中心化和透明特性，在链上通过智能合约实现域间参与者的身份认证和细粒度的访问控制，确保只有经过认证的监管域才能访问和共享数据。数据加密服务负责在数据进入存储层或传输层之前，对数据进行加密处理。

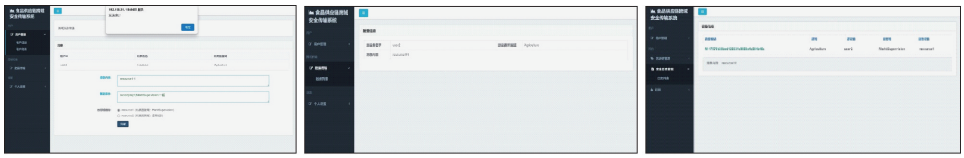
区块链网络层：构建基于区块链的底层框架。存储模块中，数据摘要信息用于快速验证数据的完整性和真实性，完整的属性信息包括参与者主体以及资源客体等，便于追溯和查询；利用 Hyperledger Fabric 作为区块链框架，支持模块化和高度可配置的架构，采用合适的共识算法，确保区块链网络中各节点之间数据的一致性和正确性，P2P 网络实现节点之间的直接通信和数据交换，验证机制对区块链上的交易和数据进行验证，确保数据的合法性和有效性。

应用层：提供注册/查询界面，有跨域访问需求的用户进行注册、登录以及查询食品供应链追溯信息；区块链查询接口允许用户通过 API 等方式查询区块链上的数据和交易；具体业务逻辑根据业务需求，实现具体的业务逻辑处理。

3.4　原型系统实现

web 前端实现食品供应链安全传输系统，多个监管域用户或者设备注册所在域的身份信息，聚焦于链上身份认证和访问控制机制的核心贡献，进行数据跨域访问请求到达时的身份认证和访问控制的实现。以用户 user2 要跨域访问数据 resource1 为例，user2 首次注册时的身份信息为：职位 Inspector，部门 PublicAffairsDepartment，所属域 Agriculture，访问级别 Level1Access。具体访问请求为：用户 user2，职位 Inspector，部门 PublicAffairsDepartment，所属域 Agriculture，访问级别 Level1Access，访问数据 resource1，执行操作 read。资源 resource1 有多个属性：资源 ID 标识 resource1，数据类型 record，数据所有域 MarktSupervision，敏感度级别 Public，数据状态 Published。

图 11 为食品供应链跨域安全传输系统实现。如图 11a 所示，用户 user2 向目的域发送消息；成功经过身份认证和访问控制后，目的域可以收到请求域传来的消息，如图 11b 所示；图 11c 为管理员可以查看的跨域消息具体信息，便于后续的审计。



(a) 请求域访问 (b) 目的域访问 (c) 管理员日志管理

图 11 食品供应链跨域安全传输系统实现

Fig. 11 Front end implementation of cross domain security transmission system for food supply chain

4 结束语

针对食品供应链监管数据跨域难共享的问题,提出了一种跨监管域数据共享模型。首先,依赖 CA 服务,为跨域用户分配证书和密钥以及属性信息,基于 Schnorr 签名算法实现域间身份认证。其次,在 ABAC 框架下,建立了属性映射机制,系统能根据不同监管主体的属性及实时的授权规则动态调整访问权限,增强了系统的灵活性和适应性,在区块链上进行访问控制可以帮助监管部门更为精确地追踪和记录用户对资源的访问与操作,便于后续的审计和监测,提高了系统的安全性和透明度,身份认证和访问控制成功实现可进行链下数据传输,确保监管实体最终获取数据时的合法性与安全性。

参 考 文 献

[1] BOSONA T, GEBRESENBET G. The role of blockchain technology in promoting traceability systems in agri-food production and supply chains[J]. Sensors, 2023,23(11):5342.

[2] 陆丹, 陆维福. 行政法视角下的食品安全风险监测与评估[J]. 食品科学, 2024,45(14): 366 – 373.
LU Dan, LU Weifu. Food safety risk monitoring and assessment from the perspective of administrative law[J]. Food Science, 2024, 45(14): 366 – 373. (in Chinese)

[3] 黄振彬, 顾艺. 新媒体技术在食品安全监督管理中的应用[J]. 食品与机械, 2024,40(3): 250 – 251.
HUANG Zhenbin,GU Yi. The application of new media technology in food safety supervision and management[J]. Food and Machinery, 2024,40(3): 250 – 251. (in Chinese)

[4] ZHANG W, TANG Y, HAN Y, et al. Microplastics boost the accumulation of tetrabromobisphenol A in a commercial clam and elevate corresponding food safety risks[J]. Chemosphere, 2022,292: 133499.

[5] 董云峰, 张新, 许继平, 等. 基于区块链的粮油食品全供应链可信追溯模型[J]. 食品科学, 2020,41(9): 30 – 36.
DONG Yunfeng, ZHANG Xin, XU Jiping, et al. Blockchain-based traceability model for grains and oils whole supply chain [J]. Food Science, 2020, 41(9): 30 – 36. (in Chinese)

[6] 王逍静. 企业食品安全合规建设研究:以食品召回制度为视角[J]. 食品科学, 2024,45(21): 368 – 377.
WANG Xiaojing. Compliance construction of enterprise food safety governance: from the perspective of food recall system[J]. Food Science, 2024, 45(21): 368 – 377. (in Chinese)

[7] 张新, 谭学泽, 王小艺, 等. 基于区块链和联邦学习的食品全程全息风险信息可信共享模式[J]. 食品科学, 2024, 45(15): 1 – 12.
ZHANG Xin, TAN Xueze, WANG Xiaoyi, et al. A trusted sharing model for risk information of food full-process and all-information based on blockchain and federated learning[J]. Food Science, 2024, 45(15): 1 – 12. (in Chinese)

[8] 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 blockchain hierarchical supervision model for wheat supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery,2023,54(3):363 – 371. (in Chinese)

[9] 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)

[10] 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. Blockchain multi-chain model of fruit and vegetable supply chain for traceability subjects[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(4): 416 – 427. (in Chinese)

[11] LUISANNA C, KATIUSCIA M. Blockchain in agri-food traceability systems: a model proposal for a typical italian food product [C]//2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2021: 669 – 678.

[12] 经普杰, 王良民, 董学文, 等. 分层跨链结构:一种面向区块链系统监管的可行架构[J]. 通信学报, 2023,44(3): 93 – 104.
JING Pujie, WANG Liangmin, DONG Xuewen, et al. CHA: cross-chain based hierarchical architecture for practicable blockchain regulatory[J]. Journal on Communications, 2023, 44(3): 93 – 104. (in Chinese)

[13] 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)
[14] JAYASHREE K, PRATHAMESH I, PRATHAMESH J, et al. A block-chain based approach for food supply chain management[C]//2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2022: 1 - 5.
[15] 杨信廷, 李瑞, 李金辉, 等. 基于区块链技术的农业食品溯源研究进展[J]. 食品科学, 2024,45(20): 299 - 310.
YANG Xinting, LI Rui, LI Jinhui, et al. Research progress on agricultural food traceability based on blockchain technology [J]. Food Science, 2024, 45(20): 299 - 310. (in Chinese)
[16] 魏松杰, 李莎莎, 王佳贺. 基于身份密码系统和区块链的跨域认证协议[J]. 计算机学报, 2021,44(5): 908 - 920.
WEI Songjie, LI Shasha, WANG Jiahe. A cross-domain authentication protocol by identity-based cryptography on consortium blockchain[J]. Jouenal of Computers, 2021,44(5): 908 - 920. (in Chinese)
[17] WANG M, RUI L, YANG Y, et al. A blockchain-based multi-ca cross-domain authentication scheme in decentralized autonomous network[J]. IEEE Transactions on Network and Service Management, 2022,19(3): 2664 - 2676.
[18] WANG W, HU N, LIU X. BlockCAM: a blockchain-based cross-domain authentication model[C]// 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 2018: 896 - 901.
[19] GU P, CHEN L. An efficient blockchain-based cross-domain authentication and secure certificate revocation scheme[C]// 2020 IEEE 6th International Conference on Computer and Communications (ICCC), 2020: 1776 - 1782.
[20] 杨信廷, 王杰伟, 邢斌, 等. 基于区块链的畜牧养殖资产监管身份认证研究[J]. 农业机械学报, 2021,52(11): 170 - 180.
YANG Xinting, WANG Jiewei, XING Bin, et al. Identification of animal husbandry assets supervision based on blockchain [J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(11):170 - 180. (in Chinese)
[21] 景旭, 蒋炎. 集群式农产品供应链区块链密文策略可验多部门监管方案[J]. 农业工程学报, 2023,39(3): 227 - 236.
JING Xu, JIANG Yan. Multi-department supervision scheme of the verifiable blockchain ciphertext policy for cluster agricultural supply chain[J]. Transactions of the CSAE, 2023, 39(3): 227 - 236. (in Chinese)
[22] 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与系统化实现[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)
[23] FENG C, LIU B, GUO Z, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones [J]. IEEE Internet of Things Journal, 2022,9(8): 6224 - 6238.
[24] 诸天逸, 李凤华, 成林, 等. 跨域访问控制技术研究[J]. 网络与信息安全学报, 2021,7(1): 20 - 27.
ZHU Tianyi, LI Fenghua, CHENG Lin, et al. Research on cross-domain access control technology[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 20 - 27. (in Chinese)
[25] ABDELFATTAH D, HASSAN H A, OMARA F A. A novel role-mapping algorithm for enhancing highly collaborative access control system[J]. Distributed and Parallel Databases, 2022,40(2): 521 - 558.
[26] 杨信廷, 李金辉, 罗娜, 等. 基于属性访问控制模型的果蔬跨链追溯系统设计与实现[J]. 农业机械学报, 2023, 54(12): 376 - 388.
YANG Xinting, LI Jinhui, LUO Na, et al. Fruit and vegetable cross-chain traceability system based on attribute access control models[J]. Transactions of the Chinese Society for Agricultural Machinery,2023,54(12):376 - 388. (in Chinese)
[27] SALEHI S A, HAN R, RUDOLPH C, et al. DACP: enforcing a dynamic access control policy in cross-domain environments [J]. Computer Networks, 2023,237: 110049.
[28] 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)
[29] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019,30(9): 2636 - 2654.
LIU Aodi, DU Xuehui, WANG Na, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636 - 2654. (in Chinese)
[30] LUO F, HUANG R, XIE Y. Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks[J]. Journal of King Saud University-Computer and Information Sciences, 2024,36(2): 101946.
[31] XUE L, HUANG H, XIAO F, et al. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums[J]. IEEE Transactions on Network and Service Management, 2022,19(3): 2409 - 2420.
[32] 李兆丰, 刘炎峻, 徐勇将, 等. 数字化食品在新时代下的发展与挑战[J]. 食品科学, 2022,43(11): 1 - 8.
LI Zhaofeng, LIU Yanjun, XU Yongjiang, et al. Development and challenges of digital foods in the new area[J]. Food Science, 2022, 43(11): 1 - 8. (in Chinese)
[33] 邵奇峰, 金澈清, 张召, 等. 区块链技术:架构及进展[J]. 计算机学报, 2018,41(5): 969 - 988.
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Jouenal of Computers, 2018,41(5): 969 - 988. (in Chinese)
[34] 王利朋, 关志, 李青山, 等. 区块链数据安全服务综述[J]. 软件学报, 2023,34(1): 1 - 32.

WANG Lipeng, GUAN Zhi, LI Qingshan, et al. Survey on blockchain-based security services[J]. Journal of Software, 2023, 34(1): 1 - 32. (in Chinese)

[35] 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)

[36] 黄穗, 李健, 范冰冰. IABC:一种基于区块链和布谷鸟过滤器的跨域认证方法[J]. 小型微型计算机系统, 2020, 41(12): 2620 - 2625.
HUANG Sui, LI Jian, FAN Bingbing. IABC: a cross-domain authentication method based on blockchain and cuckoo filter[J]. Journal of Chinese Computer Systems, 2020, 41(12): 2620 - 2625. (in Chinese)

[37] IMGHOURE A, OMARY F, EL-YAHYAOUI A. Schnorr-based conditional privacy-preserving authentication scheme with multisignature and batch verification in VANET[J]. Internet of Things, 2023,23: 100850.

[38] 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]. Jouenal of Computers, 2017, 40(7): 1680 - 1698. (in Chinese)

[39] 田秀霞, 杨明夷. 家庭物联网中基于智能合约的访问控制机制[J]. 计算机工程, 2023,49(3): 18 - 28.
TIAN Xiuxia, YANG Mingyi. Smart contract-based access control mechanism in home ioT[J]. Computer Engineering, 2023, 49(3): 18 - 28. (in Chinese)

(上接第 16 页)

[111] 孙传恒, 魏玉冉, 邢斌, 等. 基于智能合约和数字签名的马铃薯种薯防窜溯源研究[J]. 农业机械学报, 2023, 54(7): 392 - 403.
SUN Chuanheng, WEI Yuran, XING Bin, et al. Anti-channeling traceability of seed potatoes based on smart contracts and digital signatures[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(7): 392 - 403. (in Chinese)

[112] 孙传恒, 于华竟, 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 Huajing, LUO Na, et al. Blockchain traceability data storage method of fruit and vegetable foods supply chain based on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(8): 361 - 370. (in Chinese)

[113] 王少华, 孙传恒, 罗娜, 等. 面向预制食品溯源的隐私数据加密共享方法研究[J]. 农业机械学报, 2024, 55(5): 405 - 418.
WANG Shaohua, SUN Chuanheng, LUO Na, et al. Privacy data encryption sharing method for prepared food traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(5): 405 - 418. (in Chinese)

[114] 刘晓辉, 罗娜, 邢斌, 等. 基于属性可搜索加密的农产品区块链追溯隐私数据访问控制方法[J]. 农业机械学报, 2024, 55(10): 433 - 443.
LIU Xiaohui, LUO Na, XING Bin, et al. Attribute-based searchable encrypted agricultural blockchain traceability private data access control method[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(10): 433 - 443. (in Chinese)

[115] 孙传恒, 袁晟, 罗娜, 等. 基于区块链和边缘计算的水稻原产地溯源方法研究[J]. 农业机械学报, 2023, 54(5): 359 - 368.
SUN Chuanheng, YUAN Sheng, LUO Na, et al. Traceability method of rice origin based on blockchain and edge computing[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(5): 359 - 368. (in Chinese)