doi:10.6041/j.issn.1000-1298.2024.05.039

面向预制食品溯源的隐私数据加密共享方法研究

王少华[1,2]　孙传恒[2,3]　罗　娜[2,3]　徐大明[2,3]　张　航[1]　邢　斌[2,3]

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

摘要: 随着区块链技术在食品溯源领域的发展,预制食品的质量安全得到了有效保障。然而,预制食品上下游生产加工环节众多的产业特点,使溯源变得困难。在溯源的同时安全共享食谱、秘方等隐私数据,使供应链更好地协同生产则十分重要。为解决上述问题,提出了一种面向预制食品溯源的门限代理重加密(Threshold proxy re-encryption)隐私数据共享的方法,设计了一条预制食品溯源区块链和追溯生产批号关联相关溯源数据,确保数据的真实可信。使用门限代理重加密,预制食品生产商通过门限代理重加密将研发的食谱加密为初加密密文,同时在本地生成重加密密钥,将初加密密文与重加密密钥上传至预制食品溯源区块链中;第三方半诚实服务商将从区块链上获取的重加密材料进行重加密生成重加密密文,将重加密密文上传至区块链;监管部门等数据访问者则使用自身私钥将从区块链上获取的重加密密文进行重加密解密,实现隐私数据在溯源区块链上的安全共享。该方法基于 Hyperledger Fabric,搭建了一个预制食品溯源区块链原型系统进行测试。测试结果表明,所提出的面向预制食品溯源的隐私数据加密共享方法在隐私数据共享方面与常用的数据加密共享方法相比计算开销较低。数据上链、公开数据查询、隐私数据查询的平均时延分别为 1 473.8、63.9、59.9 ms,系统性能良好。实验结果表明,提出的方法达到了供应链隐私数据安全共享的目的,确保了商业机密和知识产权的安全共享,对预制食品行业发展和食品安全提升具有参考价值。

关键词: 预制食品; 区块链; 溯源; 隐私保护; 门限代理重加密

中图分类号: TP309.2; TS201.6　　**文献标识码**: A　　**文章编号**: 1000-1298(2024)05-0405-14　　**OSID**:

Privacy Data Encryption Sharing Method for Prepared Food Traceability

WANG Shaohua[1,2]　SUN Chuanheng[2,3]　LUO Na[2,3]　XU Daming[2,3]　ZHANG Hang[1]　XING Bin[2,3]

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

Abstract: With the development of blockchain technology in the field of food traceability, the quality and safety of prepared foods have been effectively guaranteed. However, the numerous industrial characteristics of the upstream and downstream production and processing links of prepared foods made traceability difficult. How to safely share recipes, secret recipes and other private data while tracing the source is very important to enable better collaborative production in the supply chain. In order to solve the above problems, a threshold proxy re-encryption privacy data sharing method for prepared food traceability was proposed, and prepared food traceability chain blocks were designed and the production batch number associated related traceability data was traced. Using the threshold proxy re-encryption, the prepared food manufacturer re-encrypted the recipes developed through the threshold proxy to encrypt the recipe to generate the initial encryption ciphertext. At the same time, the re-encryption key was generated locally, and the initial encryption ciphertext and the re-encryption key were generated locally and uploaded to the prepared food traceability blockchain; third-party semi-honest service providers would re-encrypt the re-encrypted materials obtained from the blockchain and upload the re-encrypted ciphertext to the blockchain; data visitors such as regulatory authorities used the own private key would re-encrypt

收稿日期: 2023-09-25　修回日期: 2024-02-18

基金项目: 国家重点研发计划项目(2022YFD2001804、2023YFD2001304)

作者简介: 王少华(1999—),男,硕士生,主要从事农产品追溯技术研究,E-mail: 2285780842@qq.com

通信作者: 邢斌(1983—),男,副研究员,主要从事农业信息化技术研究,E-mail: xingb@nercita.org.cn

and decrypt the re-encrypted ciphertext obtained from the blockchain to achieve safe sharing of private data on the traceable blockchain. This method was based on Hyperledger Fabric, and a blockchain prototype system for full-process traceability of the supply chain of prepared foods was constructed for testing. Test results showed that the threshold proxy re-encryption method proposed showed lower computational overhead compared with commonly used data encryption sharing methods in secure sharing of private data in prepared food traceability. The average delays of data uploading, public data query and private data query were 1 473.8 ms, 63.9 ms and 59.9 ms, respectively. The system performance was good. Experiments showed that the proposed method achieved the purpose of secure sharing of supply chain privacy data, ensured the safe sharing of business secrets and intellectual property rights, which was of great value to the development of the prepared food industry and the improvement of food safety.
Key words: prepared food; blockchain; traceability; privacy protection; threshold proxy re-encryption

0 引言

近年来,我国预制食品产业蓬勃发展[1]。这一行业不仅提供了大量就业机会,还促进了农产品转化和农村经济的繁荣。中央一号文件《关于做好2023 年全面推进乡村振兴重点工作的意见》提出培育乡村新产业新业态,强调提升预制食品产业的标准化和规范化水平[2]。预制食品产业为乡村产业振兴和农民增收致富提供了重要支持,助力实现共同富裕[3]。

目前预制食品行业存在规模化企业少、集中度低、产业链条长、自动化程度待提高等问题[4],同时面临制作不规范、添加剂滥用、原料不新鲜、预制食品品质难以实时监控等难题。因此,建立预制食品的品质监控体系和食品安全溯源系统,实现全链条的追溯与控制,具有重大意义[5]。

随着现代预制食品层级结构的多样化发展,预制食品的种类、加工方式、组合形式越来越繁杂,这也给食品安全管理带来了挑战。预制食品生产环节众多[6],当出现食品安全问题时,对问题根源的查找非常困难,隐私数据的安全性也得不到保证。基于以上问题,相关研究人员提出了一些溯源解决方案:文献[7]提出了基于密文策略属性加密(Ciphertext policy attribute based encryption, CP-ABE)技术的小麦区块链追溯系统分级监管模型,解决了小麦农产品溯源系统中监管过程的隐私数据泄露等问题。文献[8]设计了基于区块链多链架构的果蔬产品溯源框架,利用智能合约实现加密数据链上存储、链间授权访问、授权解密查询,减轻了区块链存储压力,实现上下游溯源企业之间的隐私数据共享。文献[9]结合非对称加密算法(Rivest-Shamir-Adleman, RSA)和美国信息交换标准代码(American standard code for information interchange, ASCⅡ)设计农产品原产地可信追溯系统。文献[10]设计的农产品区块链追溯系统信息存储模型将追溯明文信息存储在各节点本地数据库,上传MD5(Message-Digest algorithm 5)哈希加密后的摘要密文到区块链。文献[11]在基于区块链的粮食供应链追溯方案研究中,设计基于零知识证明算法的共识机制用以验证链上隐私数据的一致性和完整性。以上研究将区块链技术与对称加密、哈希加密、零知识证明等隐私保护技术相结合提升农产品溯源系统的数据安全性,通过链下加密的形式上传至区块链上,保证链上链下隐私数据的一致性,保障了农产品溯源系统隐私数据的安全性。其目的主要是应对监管部门在问题产品溯源时对于生产销售的隐私数据的调查要求,加密技术在监管溯源阶段产生作用,隐私数据安全共享的灵活性不足。农产品、食品供应链中存在生产资料共享以达到协同高效生产的需求,当前预制食品溯源系统在隐私保护方面的研究较少,溯源系统中采用的隐私数据加密方法导致供应链上下游环节隐私数据存在分享不通畅,无法达到隐私数据安全、灵活地分享给被授权的数据访问者的问题[12]。

区块链技术是一种分布式、去中心化的数据库技术,通过链式数据结构记录和验证交易信息,具有不可篡改和去中心化的特点[13]。近几年,区块链技术与数据加密、访问控制等技术结合紧密,文献[14]将大数据存储在公共分布式存储哈希表中,利用区块链解决数据的存储、访问和用户撤销中的信任问题。基于无证书密码体系实现区块链交易的签名和认证,而区块链则为物联网设备提供了公钥广播,从而克服了无证书密码系统的缺点。文献[15]提出了 Droplet,一种分散的数据访问控制服务。Droplet 使数据所有者能够安全、有选择地共享其加密数据,同时在未经授权的各方和受损数据服务器存在的情况下保证数据的机密性。文献[16]基于 Fabric 并采用对称密码加密医疗数据并将其存储在符合法律法规要求的云存储。文献[17]依据 Fabric 实现社交网络数据共享透明。文献[18]实现

不同利益相关者边缘设备上数据共享透明，并提出符合边缘设备应用的共识机制、交易类型和区块来适应边缘设备计算和存储能力。文献[19]基于属性签名和密文策略属性加密实现物联网数据共享。文献[20]设计密文策略属性加密实现数据共享，采用基于属性的访问控制(Attribute based access control，ABAC)模型，策略不会随用户数量呈指数增长，但需权衡问责与隐私保护。区块链与传统的访问控制、数据加密等技术相结合，可以使数据生产者控制自己的数据，实现数据的定向分享和隐私保护。上述研究依据区块链实现访问控制直接进行数据共享流通，可能会带来隐私泄露和数据滥用等问题，并且将策略和权限存储在区块链，很容易被攻击者找到漏洞，同时会泄露共享关系。

目前，区块链技术在预制食品溯源方面的研究较少[21]。预制食品相较于农产品具有更多生产加工环节[22]，对于隐私数据的保护要求更高。因此，如何在复杂生产环节和供应链合作关系不断变化的背景下实现数据共享、数据隐私和知识产权保护[23]是迫切需要研究的问题。针对上述问题，结合分析预制食品溯源过程中的关键环节及溯源数据，本文提出一种面向预制食品溯源的门限代理重加密(Threshold proxy re-encryption)[24]隐私数据共享的方法。设计一条预制食品的供应链全链条溯源区块链，采用 raft 共识机制[25]，多个节点维护一个分布式区块链账本，设计预制食品追溯生产批号关联相关溯源数据，确保数据的真实可信性。引入门限代理重加密技术满足数据共享的灵活性和适应性，以适应合作关系的动态变化。预制食品生产商通过第三方半诚实服务商对食谱秘方等隐私数据进行重加密，数据访问者可使用自身私钥进行解密以实现隐私数据共享的目的。最后，搭建区块链原型系统，通过实验验证本研究提出的面向预制食品溯源的隐私数据共享方法的可行性和测试分析各项性能。

1　预制食品全链条环节分析与网络模型

1.1　预制食品全链条溯源数据分析

预制食品是以农产品、禽类畜类产品、水产品等为主要原料，经过洗涤、切割、配制加工等过程后，可以直接烹饪的食品，也称预制菜、快手菜等。将预制食品供应链划分为原材料供应商、中央厨房(含初加工环节、烹饪加工环节、包装加工环节)、物流企业、经销商等 6 个环节部门，中央厨房生产环节流程如图 1 所示。由环境温湿度传感器、菌落检测传感器、全球定位系统(Global positioning system，GPS)等终端设备实时采集温湿度、生产环境菌落数、产品食源性致病菌、生产批次数量、位置等溯源信息，保证预制产品全链条溯源数据真实性[26]。

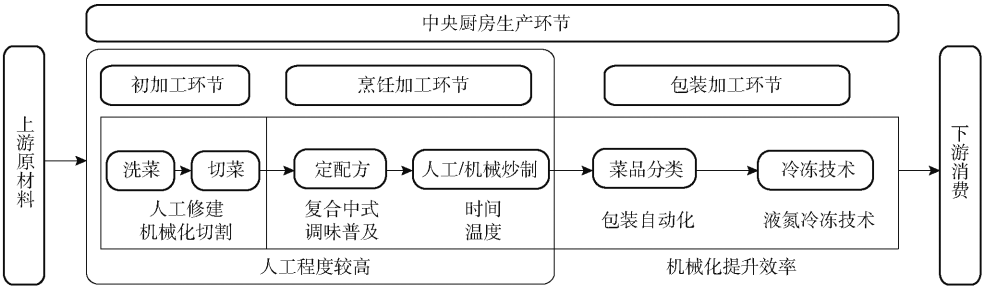


图 1　中央厨房生产环节流程

Fig. 1　Central kitchen production process

其中原材料供应商、初加工、烹饪加工、包装加工、物流企业、经销商 6 个环节上传相关环节生产运输公开信息，各环节将隐私数据进行加密处理。预制食品全链条溯源主要包括食品生产加工流程、地理位置、微生物检测等食品安全相关数据，本研究主要对于预制食品材料信息、加工流程信息、各环节食源性致病菌检测信息、温湿度信息、GPS 信息、批次规格数量等信息进行追溯，其中以食谱、秘方、加工工艺参数等作为商业隐私数据[27-30]。在预制食品溯源领域，监管机构具有重要作用，预制食品生产全链条关键数据组成应由企业与监管部门协商并达成分级授权共识。本研究将预制食品溯源信息根据隐私等级以及溯源中的作用分为三级公开溯源信息、二级隐私信息、一级隐私信息，具体如表 1 所示。预制食品生产销售全链条关键数据应全部对具有公信力的监管部门开放，监管部门调查审核时公开数据通过溯源区块链网络即可查询相关信息，二级和一级隐私数据则由中央厨房等数据拥有者通过隐私数据共享方式传输给监管部门。消费者仅可见其关心的原材料数据、生产运输日期、抽检结果等三级公开数据，二级和一级隐私数据对消费者不可见。对于供应链中其他企业，三级公开数据可通过溯源区块链查询，二级隐私数据通过隐私数据共享方式共享给链上所有企业，以此达到高效协同生产的作用。一级隐私数据主要为生产环节各企业原材料进价、秘方等数据，具有较高的保密要求，对应环节的一级

表 1 预制食品生产销售全链条关键数据

Tab. 1 Key data of whole chain of prepared food production and sales

数据类别	原材料提供商	中央厨房			物流运输	经销商
		初加工	烹饪加工	包装加工		
三级公开数据	原材料提供商名称、原材料名称、原材料属地	初加工生产线编号、生产批号、原材料提供商信息、进货日期、抽检人员、抽检日期、抽检方法、抽检结果	烹饪环节生产线编号、生产批号、加工日期、车间操作人员、抽检人员、抽检日期、抽检方法、抽检结果	生产批号、包装日期、车间操作人员、抽检人员、抽检日期、抽检方法、抽检结果、食品生产厂家名称	冷链运输企业名称、生产批号、运输方式、环境条件、运输人员、出发时间、到达时间	经销商企业名称、生产批号、出厂产品名称、产品规格数量、生产日期、检验合格单、销售单价
二级隐私数据	原材料仓储信息	原材料采购数量	加工工艺流程	包装工艺参数	运输产品批次及数量、订单信息	进货数量、销售数量
一级隐私数据	原材料成本	原材料进价成本	加工工艺参数	食谱、秘方	运输成本	进货价格

隐私数据拥有者通过隐私数据共享方式分享给必要的已被授权的数据访问者,对于其他未授权用户则不可见。

1.2 预制食品溯源网络模型

目前,预制食品供应链溯源存在一些缺陷。首先,现有的溯源方式通常集中于中心化的数据管理和控制,这容易导致数据的可信度不高,容易受到篡改和伪造的威胁。其次,信息的透明度和可追溯性有限,消费者对食品的生产过程和来源了解有限,难以获取全面的信息。此外,信息的共享和互操作性也存在问题,供应链中各方之间的数据交流和协同合作不够顺畅,导致信息孤立和协作困难。

预制食品溯源与区块链结合具有明显优势:确保数据真实性和防篡改性,提高食品信息可信度;去中心化和分布式存储减少单点故障,促进信息共享;智能合约实现自动化验证和交易执行,提高效率和准确性;不可变性和公开透明性增强消费者信任,追溯整个供应链,获得更多生产和质量信息。本研究通过开源的企业级分布式账本平台 Hyperledger Fabric 使预制食品全链条中的各个环节存在于一个通道中,映射为通道中的组织;所有组织共同维护一个分布式区块链账本,组织中包含环节的节点和客户端,每个节点上部署预制食品溯源智能合约,各环节节点通过 Hyperledger Fabric 平台客户端 client 调用智能合约进行溯源数据的相关操作,消费者和监管机构可以通过区块链网络调用智能合约完成预制食品正向信息流传递与逆向溯源全流程。预制食品溯源区块链网络数据溯源模型如图 2 所示。

预制食品溯源区块链将原材料提供商组织、初加工组织、烹饪加工组织、包装加工组织、冷链运输组织、经销商组织映射为链上组织节点。原材料提供商通过区块链网络上传原材料提供商名称、原材料名称、原材料属地等关键溯源数据,在中央厨房接收到原材料提供商提供的原材料并在区块链网络中查询到对应信息后进行初加工、烹饪加工、包装加工操作并将关键溯源信息上传至区块链网络。生产批号作为关键的溯源信息,由中央厨房 3 大环节中的初始生产批号、各环节不同生产线编号、加工时间进行区分。由于经销商销售节点众多,本研究提出销售环节 4 阶段分级编码,首先根据经销商所在地级市的邮政编码进行第 1 级划分;经销商下辖小型批发商通过字母编码定位到区县进行第 2 级划分;经销商和批发商代理的预制食品种类进行第 3 级编码划分(1 表示水果,2 表示肉类,3 表示面食等);最后根据渠道进行第 4 级编码划分(线上销售为 1,线下门店销售为 2,批发销售为 3 等),达到每批预制食品溯源生产批号拥有唯一的编号,确保正向信息流传递与逆向溯源的精确性。将消费者和第三方溯源研究机构如监管机构等映射为外部组织,通过组织节点调用智能合约进行相关溯源查询。例如,经销商销售环节批号 A001 - A - 1 - B - 2 - 100000 - A - 1 -1,其表示 A001 货物经过初加工环节 A 生产线、烹饪加工环节一号生产线、包装加工环节 B 生产线、物流运输环节第二批次运输、北京地区东城区某水果类预制食品批发商代理产品进行线上销售。

2 预制食品隐私数据共享方法设计

预制食品产业具有众多环节,各企业之间具有灵活的合作关系,供应链上下游企业之间协调合作的难度大,将食谱、秘方等需要保护的生产资料适当共享将有利于各方之间高效的协同生产。门限代理重加密具有二次加密、灵活授权、无私钥泄露风险等特点,运用在预制食品溯源区块链中可以保护预制食品产业生产资料的隐私安全,以避免敏感数据泄露或被未经授权的用户访问,帮助预制食品企业建立更加灵活、高效的数据共享权限管理机制,实现更加安全、高效、可控制的数据共享和管理,解决预制食品产业需要保护的生产资料无法安全、灵活的共

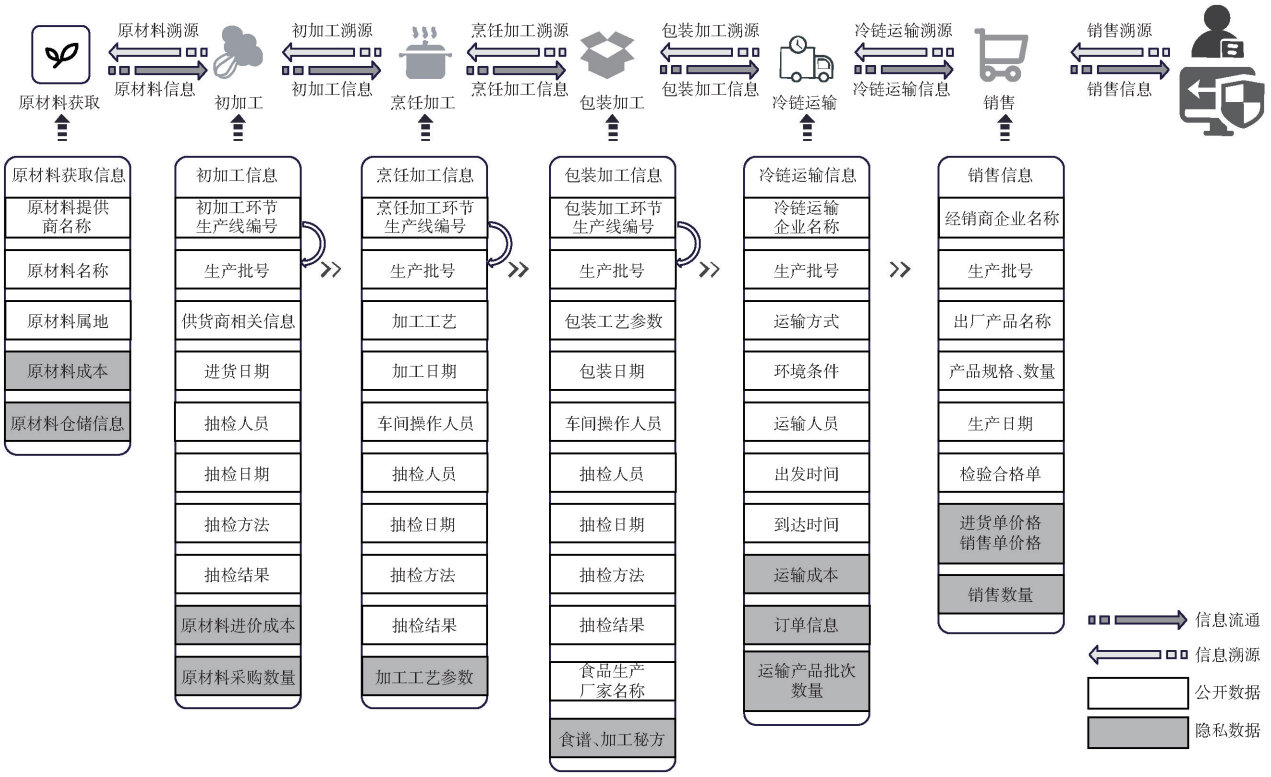


图 2　预制食品区块链网络数据溯源模型

Fig. 2　Data traceability model of prepared food blockchain network

享而导致的生产活动效率低的问题。

代理重加密(Proxy re-encryption, PRE)技术允许一个实体(称为代理)将一个密文转换为另一个密文,而无需获取原始的明文内容[31]。目前,代理重加密主要是与云存储、云计算等技术相结合,在数据共享方面应用较广,文献[32]提出一种基于代理重加密的 CP-ABE 方案,并对密钥的生成方法进行了改进;文献[33]将密钥隔离机制扩展到基于属性的代理重加密系统中,最终实现数据安全共享;文献[34]提出一种利用代理重加密的电子病历数据共享方案,将智能合约与属性访问控制方法相结合,确保使用代理重加密隐私数据的细粒度访问和提高系统安全。代理重加密流程中的参与者主要分为数据拥有者、数据访问者、第三方代理。

数据拥有者:此参与者是使用代理重加密委托其解密权限的参与者。为此,创建了一个重加密密钥,并将其发送给代理。

数据访问者:数据访问者被授予解密密文的权利,虽然最初不是为其准备的,但在数据拥有者的许可下进行重新加密密文即可拥有解密密文的权利。

代理:主要处理重新加密的过程。代理将数据拥有者公钥加密的密文转换为数据访问者可以使用的私钥解密的密文。代理在此过程中使用重加密密钥加密密文,并且不用学习任何其他信息。代理重加密流程如图 3 所示。

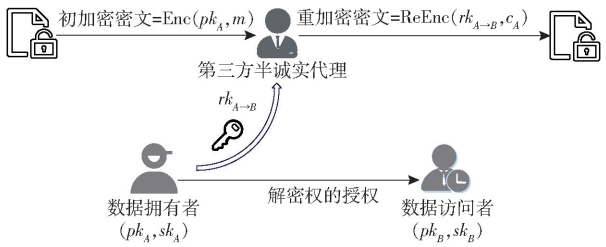


图 3　代理重加密流程

Fig. 3　Proxy re-encryption process

在此过程中,数据拥有者完成初次加密,代理根据初加密密文进行重新加密密文的操作以供不同的共享用户解密。数据所有者在共享数据时不需要重复加密操作,并且重加密工作将移交给代理服务器,由此减少了工作负载。根据密文的转换方向,可以将代理重加密技术分为单向代理重加密和双向代理重加密。单向代理重新加密只能实现从数据拥有者到数据访问者的密文转换。

传统代理重加密技术存在单一点故障风险,其代理重加密过程中的加解密材料存放于中心化的云服务器中,带来了巨大的数据泄露和恶意节点篡改材料的风险。使用初加密时数据拥有者的公钥对密文进行非对称加密,导致开销大。为解决预制食品溯源过程中隐私数据的安全性和灵活共享的问题,引入门限代理重加密技术。它允许持有者将密文委托给多个代理,代理完成重加密环节后,数据访问者搜集到足够的重加密密文碎片即可解密。使用对称

密钥进行初加密和最终解密,节省时间开销。门限代理重加密技术通过设定门限值、控制代理协同进行重加密、动态调整门限值和代理数量等操作保护数据隐私和安全性,提高数据共享的灵活性,适用于预制食品溯源中共享隐私数据的需求。本研究使用的门限代理重加密基于 secp256k1 椭圆曲线公钥加密体系,其曲线公式为

$$y^2 = x^3 + 7 \tag{1}$$

其中 x 和 y 表示在二维平面上的坐标点,x 轴表示横坐标,y 轴表示纵坐标。对于任意一点 $P(x,y)$,当且仅当它满足 $y^2 = x^3 + 7$ 时,就在该椭圆曲线上。门限代理重加密的加密解密过程如图 4 所示。

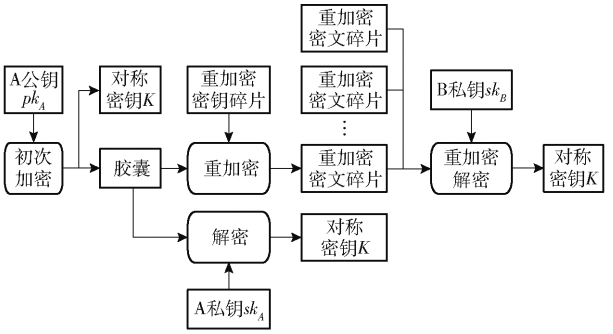


图 4 门限代理重加密算法流程

Fig. 4 Process of threshold proxy re-encryption algorithm

2.1 公共参数设置

设置算法首先根据安全参数 sec 确定一个素数阶 q 的循环群 G。设 $g, U \in G$。设 $H_2: G^2 \rightarrow Z_q$, $H_3: G^3 \rightarrow Z_q$ 和 $H_4: G^3 \times Z_q \rightarrow Z_q$。设 $\mathrm{KDF}: G \rightarrow \{0,1\}^{\prime}$ 是一个作为随机预言机模型的密钥派生函数,其中 $\prime$ 根据安全参数 sec 设定。H 为随机域的哈希函数,Z_q 表示一个循环群 G 的素数 q 阶,用于表示群 G 中的元素取值范围。全局公共参数用元组表示为

$$params = \{G, g, U, H_2, H_3, H_4, KDF\} \tag{2}$$

2.2 密钥生成算法

密钥生成算法 KeyGen 均匀随机地选择 $a \in Z_q$,输出一对公钥和密钥(pk_A、sk_A) = (g^a, a)。输入密钥 $sk_A = a$ 以及被授权 $pk_B = g^b$ 的公钥、片段数 N 和阈值 t,重加密密钥生成算法 ReKeyGen 计算 A 和 B 之间的重加密密钥的 N 个片段,每个片段命名为 KFrag。

计算过程如下:

(1)随机选择 $x_A \in Z_q$ 并计算 $X_A = g^{x_A}$。x_A 为临时私钥,由发送方 A 生成;X_A 为临时公钥。

(2)计算 $d = H_3(X_A, pk_B, (pk_B)^{x_A})$。$d$ 是 B 的密钥对和本阶段密钥对(x_A, X_A)之间的非交互式 Diffie - Hellman 密钥交换的结果,使用共享秘密使本研究的重新加密密钥具有非交互式特性。

(3)随即选择 $t-1$ 个元素 $f_i \in Z_q$,其中 $1 \leqslant i \leqslant t-1$,计算 $f_0 = ad^{-1} \bmod q$。f_i 为随机选择的元素,用于构造多项式 $f(x)$。f_0 为多项式 $f(x)$ 的常数项。

(4)构造一个度为 $t-1$ 的多项式 $f(x) \in Z_q[x]$,例如 $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{t-1} x^{t-1}$,用于计算重加密密钥片段。

(5)计算 $D = H_6(pk_A, pk_B, pk_B^a)$,$D$ 为根据发送方 A 和接收方 B 的公钥以及接收方 B 的临时公钥 pk_B^a 计算得出的哈希值。

(6)初始化 $KF = \varnothing$,重复 N 次:随机选择 y,$id \in Z_q$;计算 $s_x = H_5(id, D)$ 和 $Y = g^y$;计算 $rk = f(s_x)$;计算 $U_1 = U^{rk}$;计算 $z_1 = H_4(Y, id, pk_A, pk_B, U_1, X_A)$ 和 $z_2 = y - az_1$;将一个重加密的密钥碎片 KF 定义为元组($id, rk, X_A, U_1, z_1, z_2$);$KF = KF \cup \{kFrag\}$。其中,$KF$ 为重加密密钥片段集合,id 为随机选择的标识符,y 为随机选择的值。s_x 为根据 id 和 D 计算得出的哈希值。rk 为重加密密钥片段的一部分,通过多项式 $f(x)$ 计算得出。U_1 为重加密密钥片段的一部分。z_1 和 z_2 用于计算重加密密钥片段的一部分。

(7)输出一组重新加密的密钥片段 KF。

2.3 封装与解封装算法

在输入公钥 pk_A 和消息 M 时,加密算法首先计算(K, capsule)。encData 将关联数据认证加密(Authenticated encryption with associated data, AEAD)应用于对称密钥为 K 的加密消息 M 的结果,以胶囊作为相关数据。最后,输出密文 C = (capsule, encData)。

输入密钥 sk_A 和密文 C = (capsule, encDate) 时,Decapsulate 算法解密计算密钥 K = Decapsulate(sk_A, capsule),并使用以对称密钥 K 和 capsule 作为关联数据的 AEAD 解密功能解密数据,如果解密正确,则得到消息 M,否则为 $\perp$。最后,输出消息 M(如果解密无效则输出 $\perp$)。

2.4 重加密算法

在输入重新加密密钥片段 KFrag 和密文 C = (capsule, encData) 时,重加密算法 ReEncapsulate( ) 使用 capsule 与 KFrag 重新加密封装以获取 cFrag,并输出重加密的密文 C = (cFrag, encData)。

2.5 解密算法

输入 B 的密钥 sk_B,一组重加密密文 C_i = (cFrag, encData)。首先,片段解密算法 DecryptFrags( ) 解密碎片 cFrags;其次,解密算法 DecapsulateFrags(sk_B, $\{cFrag_i\}_{i=1}^{t}$) 需要判断是否具有足够的门限数量的 cFrags,才能产生对称密钥 K 和使用 AEAD 的解密功能解密密文,以密钥 K 和胶囊作为关联数据

进行解密，如果解密正确，则得到消息 M，否则为 ⊥。最后，输出消息 M（如果解密无效则输出 ⊥）。对称加密的密文封装对相同密文 C 的所有重加密的 Data 是相同的。

3　预制食品隐私数据共享溯源模型实现

3.1　预制食品隐私数据加密共享模型

在预制食品全链条溯源流程中，多方合作和供应链的动态变化是常见情况。参与方之间需要共享食谱秘方、供应链信息及销售数据等，以促进生产协调；供应链复杂，数据流动需平衡保密性；动态变化需要灵活方案适应合作关系的变动。预制食品区块链溯源的同时保障食谱、秘方等隐私数据的安全性和灵活共享是本研究的主要问题。本研究以中央厨房食谱、秘方等隐私数据通过门限代理重加密技术实现安全共享为例。

本研究主要分为两部分：第 1 部分为数据拥有者向数据请求者共享隐私数据流程，分为 4 个环节：环节 1 为中央厨房加密密文、密钥；环节 2 为中央厨房加密自验证；环节 3 为半诚实代理节点（服务器）重加密；环节 4 为供应链第三方机构解密。第 2 部分为数据请求者授权更新流程。

隐私数据共享流程：首先，数据拥有者（以下称为中央厨房）由公钥基础设施（Public key infrastructure，PKI）获得公钥 a、私钥 a；数据访问者（供应链第三方机构）由 PKI 公钥基础设施获得公钥 b、私钥 b。中央厨房使用 Encrypt( ) 将公钥 a 加密为对称密钥 K 和 capsule（胶囊），将食谱、秘方等明文通过对称密钥 K 加密为密文，密文与胶囊封装为加密密文 C 并上传至区块链中。其次，供应链第三方机构通过链下获得隐私数据访问许可后，中央厨房以自身私钥 a 与供应链第三方机构公钥 b 通过 ReKeyGen( ) 生成重加密密钥 RK 并设置分片数以及阈值后上传至区块链中。以单个半诚实服务器为例：服务器收到供应链第三方机构的隐私数据重加密请求后，从区块链中获得加密密文 C 以及重加密密钥碎片，通过 ReEncrypt( ) 算法将密文 C 重加密为 C_i 片段，并上传至区块链中。供应链第三方机构从区块链中获取重加密密文碎片 C_i，通过 DecapsulateFrags( ) 算法输入供应链第三方机构私钥 b 后，将重加密密文 C_i 解封装为对称密钥和胶囊，使用对称密钥和胶囊即可解密密文。如果搜集的碎片数达到提前设置的阈值即可成功解密密文获得明文，反之则无法解密成功。中央厨房门限代理重加密隐私数据共享流程如图 5 所示。

数据访问者授权更新流程：溯源区块链网络中的半诚实代理服务器节点获取数据请求者许可，根据中央厨房的要求来更新为哪些数据请求者进行门限代理重加密。中央厨房向区块链上传并存储原始食谱、秘方等交易密文和门限代理重加密密钥，根据数据访问者链下发起的数据请求，中央厨房决定是否对交易密文进行重加密密钥的生成以此共享给数

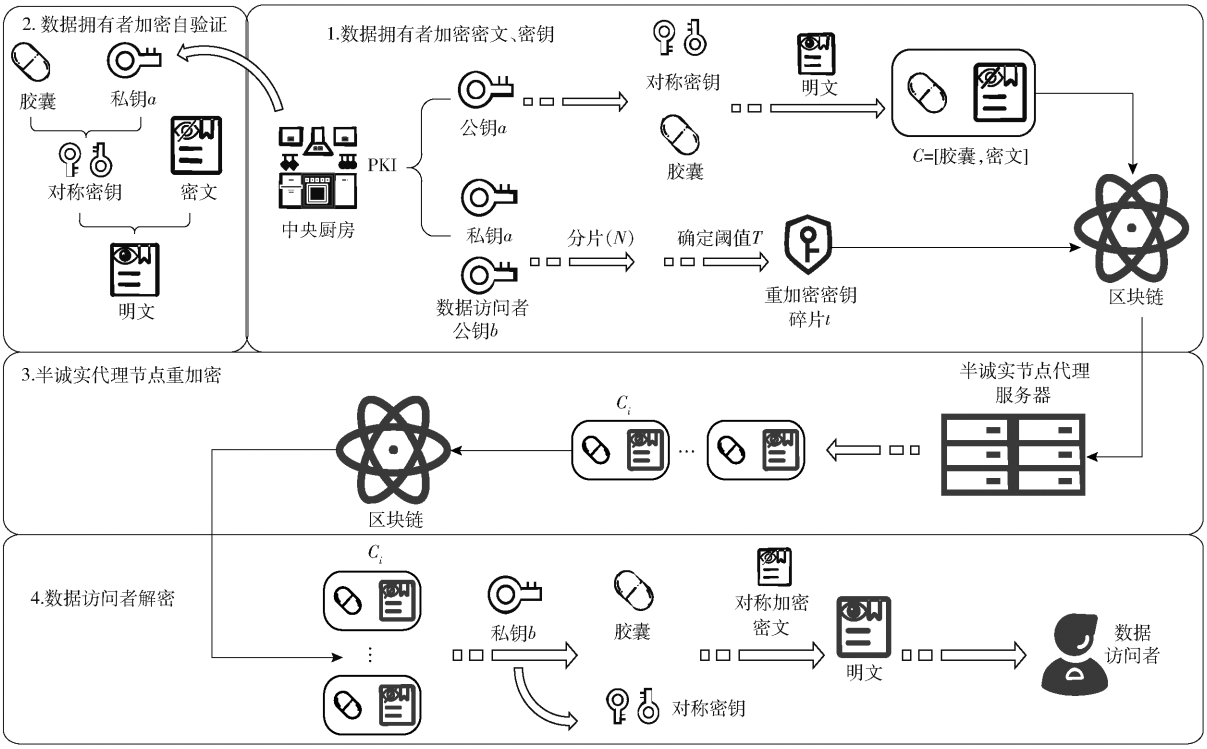


图 5　门限代理重加密隐私数据共享流程

Fig. 5　Threshold proxy re-encryption private data sharing process

据请求者。中央厨房与区块链网络中的半诚实代理服务器交互并撤消数据请求者对数据记录的访问权限,通过更新重加密密钥来授予数据请求者新的访问权限。

为了进一步具体描述区块链交易数据共享的隐私保护需求,本研究抽象一个区块链系统数据共享平台,如图 6 所示;初始化 4 个参与方 A、B、C、D,定义交易数据的隐私保护需求,如表 1 所示。在本研究中,交易数据分为公开溯源基础数据和隐私敏感数据两类。隐私数据只有中央厨房和授权的访问者可见,未授权的参与方只能看到密文。当中央厨房要授权将敏感数据分享给参与方 D 时,它会生成一个重加密密钥 $rk_{A\to D}$,并广播给区块链网络和半诚实代理服务器。代理服务器通过区块链系统获得密钥后,将密文代理重加密,并上传至区块链网络。参与方 D 使用私钥解密重加密密文,获取隐私数据。新参与方 E 的权限更新过程与参与方 D 相同。通过这种方式,区块链系统实现了安全的数据共享和隐私保护。

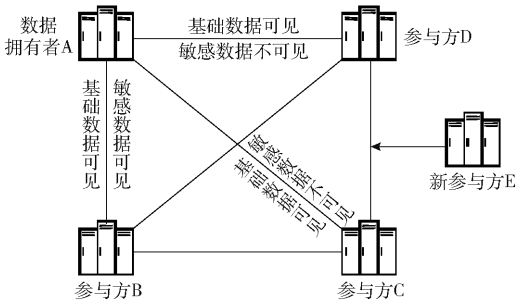


图 6 区块链系统数据共享平台

Fig. 6 Blockchain system data sharing platform

在以上授权更新过程中,数据拥有者在对交易数据进行初始加密后,后续更新访问权限不用再对数据进行重复加密,只需构造新的重加密密钥广播到区块链网络即可。

3.2 预制食品隐私数据共享溯源模型

在预制食品溯源中,区块链与门限代理重加密技术的结合可以构建一个安全、可追溯的溯源系统。区块链作为一个去中心化的分布式账本,不可篡改和公开透明地记录预制食品供应链各环节信息。门限代理重加密技术用于保护数据隐私和控制数据访问权限,确保只有授权的用户可以解密和查看敏感数据。

首先,门限代理重加密技术为预制食品溯源系统提供了强大的数据保护能力。通过生成密钥对和设置合适的门限值,该技术可以对生产、流通和销售等关键数据进行加密,从而保护数据的机密性和完整性。即使区块链中的数据被公开展示,没有获得相应权限的用户无法解密和获取敏感信息,有效地防止了数据泄露和非法访问。其次,区块链技术为预制食品溯源系统提供了可信的数据存储和验证机制,区块链中记录的溯源数据可以与门限代理重加密技术相结合,实现可控的数据共享和访问授权,只有获得合法权限的用户才能解密特定的数据,根据其权限和授权查看生产、流通和销售等环节的信息,通过门限代理重加密过程所生成的初加密密秘文、重加密密钥、重加密密文等加密材料被完整地保存在区块链系统上。由此,可将由门限代理重加密链下环节众多、隐私保护责任主体不明确、中心化特性风险进行有效降低。

将区块链技术和门限代理重加密引入预制食品全链条溯源系统中,通过正向供应链各环节信息流传递,预制食品溯源区块链中存储了各环节溯源信息,当正常商品开始生产和流入市场后供应链各环节合作方可以通过溯源区块链系统获得预制食品全链条供应链数据信息。中央厨房会根据前期市场调研、计划、食品研发团队等各环节确定食谱、秘方等隐私数据内容,通过预制食品区块链溯源模型中的门限代理重加密技术中封装的 PKI 生成自身的公私钥,中央厨房使用门限代理重加密环节中的对称加密进行密文的初加密,将自身私钥和数据访问者公钥进行重加密密钥的生成,此过程参考图 7 代理重加密流程步骤 1 ~ 3。生成的初加密密文 C 和重加密密钥上传至预制食品溯源区块链上,半诚实代理服务器从区块链上获取生成的重加密密文以及重加密密钥使用代理重加密进行重加密操作,生成重加密密文 C_i,将重加密密文 C_i 上传至区块链中,此过程参考图 7 代理重加密流程步骤 4 ~ 7。数据访问者根据中央厨房预先设定的门限将链上的重加密密文进行搜集,使用自身私钥进行重加密密文的解密,此过程参考图 7 代理重加密流程步骤 8 ~ 10。通过将隐私数据分享给第三方数据访问者如行业组织、学术机构或政府监管机构部门等,由此进行溯源监管或相关研究活动,以达到正向信息流传递的目的。正常产品流入市场后,消费者可以通过预制食品溯源区块链系统逆向查询预制食品供应链全链条溯源信息。问题产品流入市场后,监管部门迅速介入,通过预制食品隐私数据共享溯源区块链获得相关溯源隐私数据和溯源公开数据,立刻展开确定问题产品批次行动,链下截断问题产品继续流入市场以减少其对消费者和市场造成的不良影响。

3.3 智能合约设计

本研究基于 Hyperledger Fabric 平台,结合预制食品产业相关资料、预制食品生产环节的实际情况等制订相关的智能合约规则。智能合约业务逻辑设计如表 2 所示。

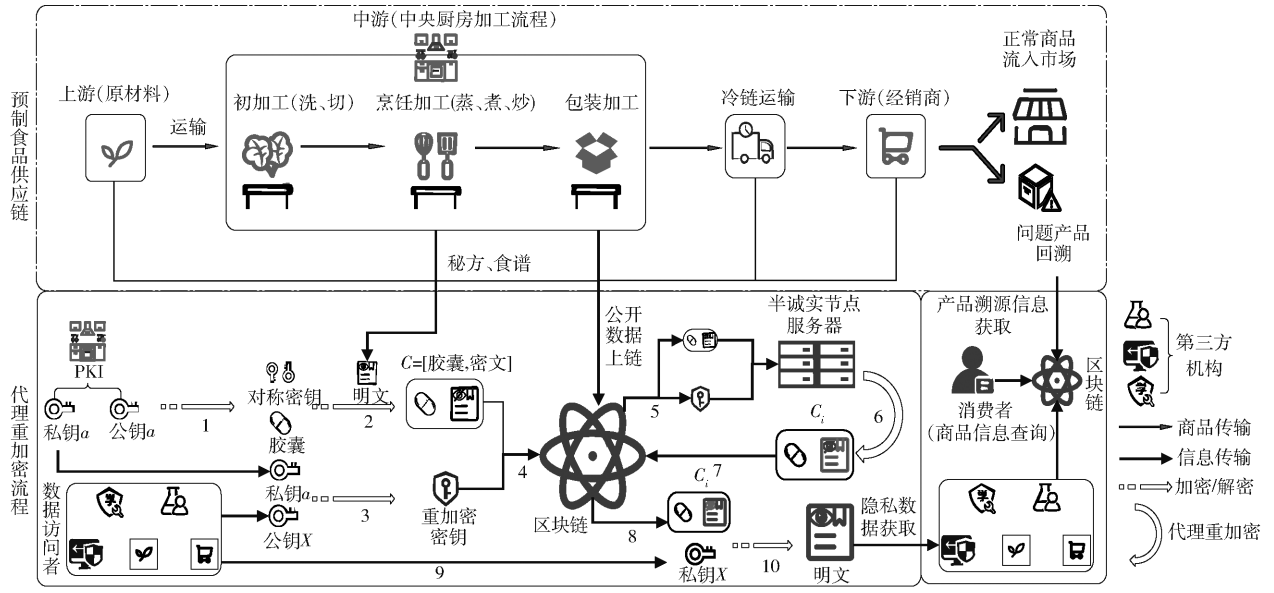


图 7　预制食品隐私数据共享溯源模型

Fig. 7　Shared traceability model of prepared food privacy data

表 2　智能合约设计

Tab. 2　Smart contract design

合约功能	合约方法	描述	输入	输出
数据上链	Recordpreconditioning( )	将初加工环节基本信息写入区块链	初加工环节基本信息	True/False
	RecordCooking( )	将烹饪加工环节基本信息写入区块链	烹饪加工环节基本信息	True/False
	RecordPackage( )	将包装加工环节基本信息写入区块链,并把中央厨房通过门限代理重加密生成的加密材料写入区块链	包装加工环节基本信息/加密材料	True/False
	RecordTransport( )	将物流运输环节基本信息写入区块链	物流运输基本信息	True/False
	RecordSale( )	将经销商环节基本信息写入区块链	经销商基本信息	True/False
	Updataencrypt( )	将半诚实代理服务器重加密后的加密数据写入链上	加密数据	True/False
数据查询	getRecordByID( )	通过批次号查询溯源信息	产品批次号	对应批次号溯源基本信息/加密材料
	getRecordByName( )	通过名称查询溯源信息	产品名称	对应产品名称溯源基本信息/加密材料

将预制食品各生产销售环节的溯源信息写入区块链均由智能合约实现。以预处理环节为示例,具体算法为:

Input: 预处理生产线编号、生产批号、原材料提供商信息、进货日期等溯源信息

Output: True/False

//区块链中的预处理环节对应 peer 节点发起 invoke 上链请求

function Recordpreconditioning( )

　if len(args) then //判断请求中的数组长度是否符合规定长度标准

　return shim. Error //数组长度不符合标准,上链失败,返回具体错误原因

　end if

　uploadData ← preconditioning //将参数填入数据结构中

　m ← json. M arshal(uploadData) //将对象序列化成数组存储

　err ← stub. P utState(uploadData. ID, m) //根据 ID,创建索引

　err ← stub. P utState(uploadData. Name, m) //根据 Name,创建索引

　if err then //判断上链请求是否成功

　return shim. Error //上链失败,返回具体错误原因

　end if

end function

4　测试与分析

4.1　实验架构

该实验基于 Hyperledger Fabric 设计预制食品

溯源区块链网络,实验搭建一条区块链,区块链网络中涉及 5 个组织,第 1 个组织为预制食品原材料组织(上游),包括一个原材料供应商节点;第 2 个组织为中央厨房(中游),主要有食品研发团队、初加工、烹饪加工、包装加工 4 个节点;第 3 个组织为运输销售组织(下游),有物流企业和经销商 2 个节点;第 4 个组织为供应链外部数据获取组织,主要有消费者、监管机构、学术机构 3 个节点;第 5 个组织为服务器组织,其中设置了两台服务器节点。本研究在主机配置为 4.60 GHz、i5 - 12400F CPU、32 GB RAM、系统为 Windows 10 下进行实验。实验架构如图 8 所示。

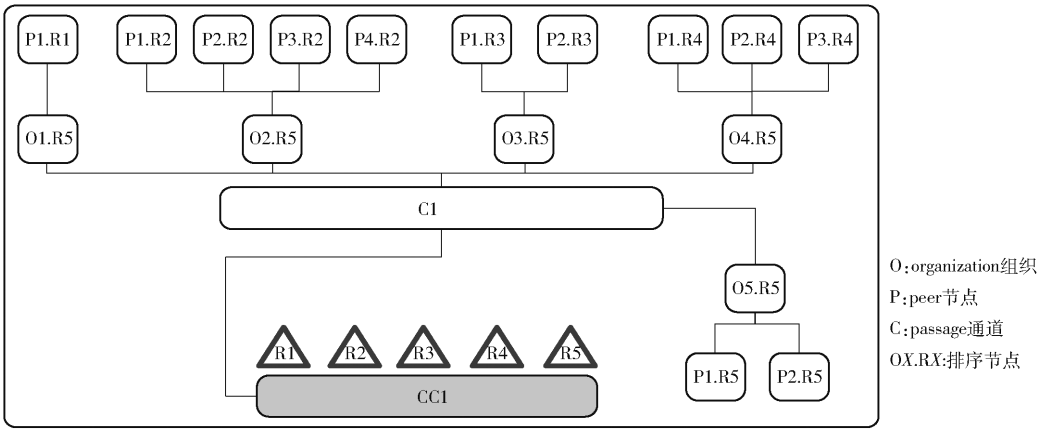


图 8 预制食品溯源区块链结构配置

Fig. 8 Prepared food traceability blockchain structure configuration

本研究的测试环境基于 Hyperledger Fabric 2.4、Hyperledger Explorer 1.1.8 搭建,使用虚拟机系统版本为 Ubuntu 16.04 LTS。性能测试将智能合约通过 balance - transfer 接口进行封装,使用测试工具 Hyperledger Caliper 进行 30 轮次的测试。硬件配置为:4 GB 内存、8 核处理器、40 GB 硬盘。区块链通过 12 个节点存储预制食品生产销售全链条溯源数据,其中包含原材料供应商节点、中央厨房初加工节点、中央厨房烹饪加工节点、中央厨房包装加工节点、物流运输节点、经销商节点、中央厨房隐私数据上传节点各 1 个,供应链外部溯源消费者节点和监管机构节点以及第三方研究机构节点各 1 个,半诚实代理服务器节点 2 个。预制食品溯源区块链中的所有节点均采用状态数据库 CouchDB 存储上链数据,通过 key - value 键值对检索状态数据库查询相应数据。具体测试环境配置如表 3 所示。

表 3 区块链配置信息

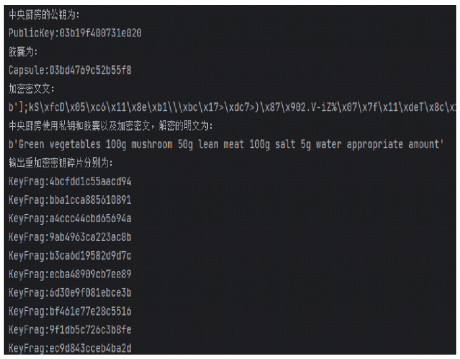
Tab. 3 Blockchain configuration information

区块链配置	数值	描述
链条	1	预制食品生产销售 3 个组织和供应链外数据溯源机构以及代理服务器共同维护一条区块链
组织数量	5	原材料供应商、中央厨房、物流运输、经销商、供应链外部数据溯源机构
节点数量	12	原材料供应商节点、中央厨房初加工节点、中央厨房烹饪加工节点、中央厨房包装加工节点、物流运输节点、经销商节点、中央厨房隐私数据上传节点、供应链外部溯源消费者节点、监管机构节点、第三方研究机构节点、2 个半诚实代理服务器节点
数据库	CouchDB	整个区块链采用 CouchDB 状态数据库存储上链数据
共识机制	Raft	采用 Raft 共识机制使区块链中的所有节点共同维护账本一致性
出块时间	2 s	发布交易并打包生成区块的时间
区块最大交易数量	100	每个区块中所包含的最大交易数量
区块最大容量/MB	100	每个区块中存储数的最大容量
每条交易最大占据存储空间/KB	512	每条交易存储量最大为 512 KB

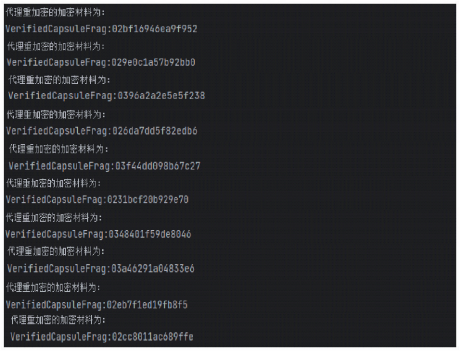
4.2 预制食品隐私数据共享功能测试

测试以中央厨房为数据拥有者,监管部门为数据访问者为例。如图 9a 所示,中央厨房使用 PKI 公钥系统生成自身公钥,利用自身公钥将明文生成初加密密文,通过区块链获取监管机构公钥生成重加密密钥碎片并上传至预制食品溯源区块链,交易 id 为 c3189581c881afa572f08109585936a1e2361ece1dbd56e 3b3b7444cfea8a16f,调用链码为 sacc2 等区块链交易信息,如图 10a 所示,写入账本的 key 值为预制食品 01#A001A、value 值为重加密密钥碎片信息,如

图 10b 所示。代理重加密服务器节点将初加密密文和重加密密钥碎片通过重加密生成代理重加密密文碎片，如图 9b 所示，上传至区块链。



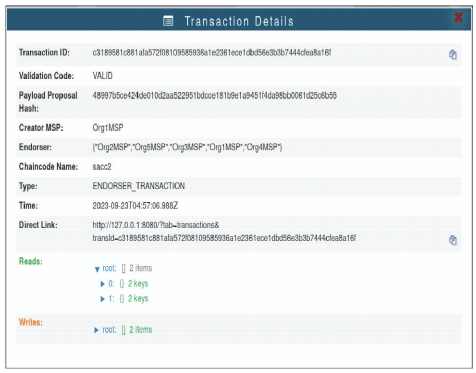
(a) 门限代理重加密——中央厨房端



(b) 门限代理重加密——代理服务器端

图 9　门限代理重加密过程

Fig. 9　Threshold indicated re-encryption process of proxy



(a) 重加密密钥碎片区块交易信息



(b) 链上存储的重加密密钥碎片

图 10　预制食品溯源区块链链上加密材料数据

Fig. 10　Prepared foods traced to encrypted material data on blockchain chain

监管机构通过区块链查询获取足够的重加密密文碎片后，使用自身私钥进行重加密密文解密以获得明文，如图 11 所示。

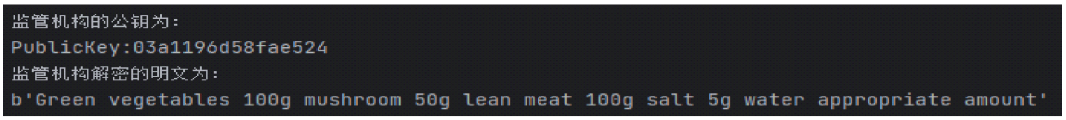


图 11　监管机构解密密文

Fig. 11　Regulator declassified ciphertext

4.3　门限代理重加密性能

4.3.1　加密方式

文献[35]提出了基于环签名的保密交易方案，通过环签名的方式隐藏交易金额、保护交易隐私和身份隐私。文献[36]基于属性加密提出区块链数据溯源算法，设计适用于区块链的策略更新算法，实现了交易隐私的动态保护。文献[37]将分层属性加密与线性秘密共享相结合，提出了一种基于可搜索属性加密的区块链数据隐私保护控制方案，对没有访问权限的节点隐藏交易信息，有权限的区块链节点可通过陷门关键字查询到交易的有效信息，解决了传统区块链交易中的隐私暴露问题。文献[38]提出了一种区块链保护隐私数据的模型，使用区块链智能合约判断用户的访问权限，利用对称或非对称的方式加密存储数据，只能进行一对一的数据安全传输。文献[39]提出了一种基于区块链技术的数据共享方案，提出了一种区块链双链结构，结合代理重加密技术，实现了安全可靠的数据共享。本研究采用的门限代理重加密技术，对产生的重加密密钥分割管理，在重加密密钥的确定性更新下，对预制食品溯源领域隐私数据访问权限动态更新，实现了预制食品产业链溯源中隐私数据的受控共享。将本研究与现有研究方案中的加密方式进行功能特性对比，结果如表 4 所示。

表 4　加密方式对比

Tab. 4　Comparison of encryption modes

加密方式	密文访问控制	抗共谋攻击	重加密	可追溯
文献[35]	×	√	×	√
文献[36]	√	×	×	√
文献[37]	√	√	×	√
文献[38]	√	×	×	×
文献[39]	√	×	√	√
本研究	√	√	√	√

注：√表示具备此特性，×表示不具备此特性。

4.3.2 实验

通过仿真实验对本研究各阶段包括密钥产生、加密算法以及数据上链查询等操作的时间消耗进行测试，根据实验结果对本研究性能效率进行评估。

本研究使用 Python 3.7.4 实现门限代理重加密算法模拟。在本研究中，整个隐私数据链下共享分为初加密密文、生成重加密密钥、代理重加密、解密 4 个阶段。对于 4 个阶段的计算效率进行分析比较，分别在 64、128、256、512、1 024 B 的数据明文大小下进行对比，并取算法运行 30 次的平均值作为实验结果。如图 12a 所示，代理重加密各环节在不同明文大小的情况下消耗时长基本稳定，初次加密明文时长基本稳定在 2.5 ms，在门限值固定的情况下生成重加密密钥时长大致为 13 ms，生成重加密密文时长为 17.5 ~ 20 ms，解密密文为 13 ms 左右；如图 12b 所示，设定不同门限值时，生成重加密密钥时间与门限值大小呈正相关关系，当门限值设定为 25 时，生成重加密密钥碎片时长平均值为 33 ms。因此，门限代理重加密在预制食品溯源流程中的隐私数据安全共享的计算开销与重加密密钥碎片设定值即门限数量相关，且各环节计算开销较低，可以实现预制食品溯源隐私数据访问权限的动态调整，更好地满足中央厨房与第三方数据访问者机构间进行食谱、秘方等数据共享的实际需要。

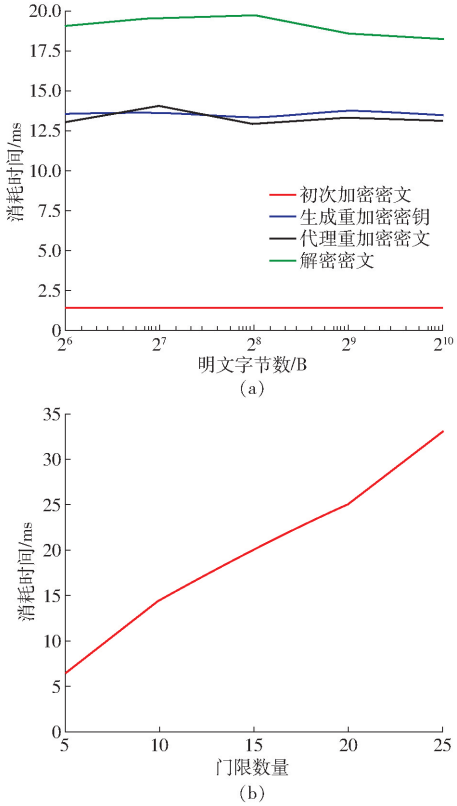


图 12 门限代理重加密性能测试

Fig. 12 Threshold proxy re-encryption performance test

目前，食品安全溯源领域对于隐私数据加密共享的主要方法为对称加密、非对称加密以及对称加密与非对称加密相结合等。本研究与高级加密标准(Advanced encryption standard，AES)算法、非对称加密 RSA 算法、AES + RSA 算法的加密与解密环节进行测试对比，实验结果取算法运行 30 次的平均值，结果如图 13 所示。本研究加密阶段包括初始加密密文和代理重加密部分，解密阶段表示对重加密密文的解密。在明文大小相同的情况下本研究在密文加密环节所消耗时长小于非对称加密、对称加密、非对称加密和对称加密相结合 3 种方案，消耗时长为 22 ms；解密环节消耗时长略大于其余 3 种方案，消耗时长为 13.34 ms。计算开销总体较小，具有一定优势，可以满足预制食品溯源场景中隐私数据安全共享的实际需求。

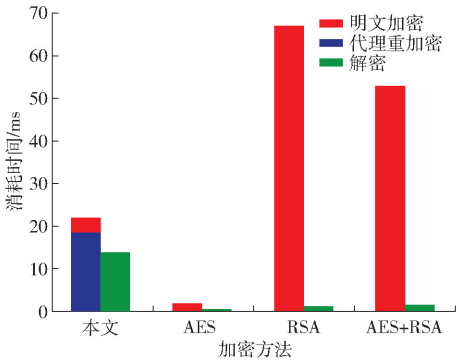


图 13 加密方法性能对比

Fig. 13 Performance comparison of encryption schemes

4.4 数据上链与查询性能

数据上链性能测试结果如图 14a 所示，预制食品生产溯源数据平均上链时间为 1 473.8 ms，能够满足预制食品生产全环节实时更新预制食品溯源数据的需求；数据查询性能测试结果如图 14b 所示，预

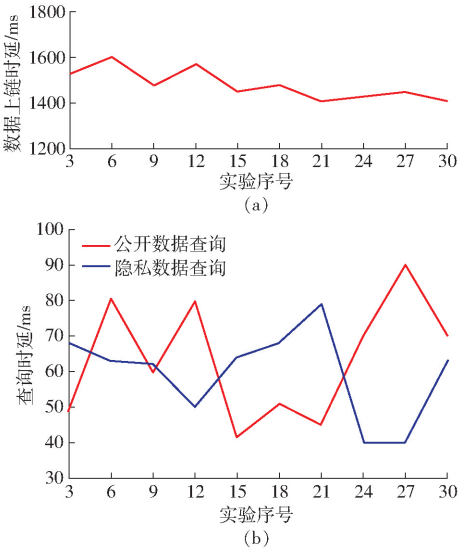


图 14 数据上链与查询性能测试

Fig. 14 Performance testing of data link and query

制食品生产公开溯源数据平均查询时间为 63.9 ms，预制食品生产隐私溯源数据平均查询时间为 59.9 ms，能够满足相关溯源用户快速查询预制食品生产溯源隐私数据的需求；由以上测试结果可以得出，该预制食品溯源区块链的数据上链和数据查询效率较高，可以满足各相关用户的日常需求。

5　结束语

提出了面向预制食品溯源的隐私数据加密共享方法，对预制食品供应链建立溯源区块链，各环节企业上传公开的溯源生产销售数据，共同维护一个区块链账本，保证了预制食品溯源的数据真实和不可篡改，通过门限代理重加密与预制食品溯源区块链联合解决生产销售溯源过程中隐私数据安全共享的问题，提高了预制食品溯源过程中生产资料共享的安全性以及灵活性。最后，搭建了预制食品溯源区块链原型系统进行测试，相关测试结果验证了门限代理重加密的方法性能，可以将食谱、秘方等隐私数据安全共享，证明了本方法模型的可行性，数据上链、公开数据查询、隐私数据查询平均时延分别为 1 473.8、63.9、59.9 ms，系统性能满足预制食品供应链溯源的需求，为预制食品供应链场景下区块链溯源系统中的隐私数据安全共享提供借鉴与参考。

参　考　文　献

[1] 张栎缘，周丰婕. 预制菜产业链现状与发展趋势研究[J]. 现代食品，2023，29(1)：15－18，38.
ZHANG Yueyuan，ZHOU Fengjie. Current situation and development trend of prepared food industry chain[J]. Modern Food，2023，29(1)：15－18，38.(in Chinese)

[2] YI B，XU H. Research and development status of prepared foods in China：a review[J]. Applied Sciences，2023，13(14)：7998.

[3] 王娟，高群玉，娄文勇. 我国预制菜行业的发展现状及趋势[J]. 现代食品科技，2023，39(2)：99－103.
WANG Juan，GAO Qunyu，LOU Wenyong. Development status and trend of prepared food industry in China[J]. Modern Food Science and Technology，2023，39(2)：99－103.(in Chinese)

[4] 张宇昊，陈海. 川渝预制菜产业现状与发展路径分析[J]. 中国食品学报，2022，22(10)：9－19.
ZHANG Yuhao，CHEN Hai. Analysis of the status quo and development path of Sichuan and Chongqing prepared vegetable industry[J]. Chinese Journal of Food Science，2022，22(10)：9－19.(in Chinese)

[5] 张德权，刘欢，孙祥祥，等. 预制菜肴工业化加工技术现状与趋势分析[J]. 中国食品学报，2022，22(10)：39－47.
ZHANG Dequan，LIU Huan，SUN Xiangxiang，et al. Current situation and trend analysis of industrialized processing technology of prepared dishes[J]. Chinese Journal of Food Science，2022，22(10)：39－47.(in Chinese)

[6] 赵超凡，陈树俊，李文兵，等. 预制菜产业发展问题分析[J]. 现代食品科技，2023，39(2)：104－109.
ZHAO Chaofan，CHEN Shujun，LI Wenbing，et al. Analysis on the development of prepared vegetable industry[J]. Modern Food Science and Technology，2023，39(2)：104－109.(in Chinese)

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

[8] 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. Research on fruit and vegetable blockchain traceability data storage method based on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery，2022，53(8)：361－370.(in Chinese)

[9] 马腾，孙传恒，李文勇，等. 基于 NB－IoT 的农产品原产地可信溯源系统设计与实现[J]. 中国农业科技导报，2019，21(12)：58－67.
MA Teng，SUN Chuanheng，LI Wenyong，et al. Design and implementation of agricultural product origin traceability system based on NB－IoT[J]. Journal of Agricultural Science and Technology of China，2019，21(12)：58－67.(in Chinese)

[10] 杨信廷，王明亭，徐大明，等. 基于区块链的农产品追溯系统信息存储模型与查询方法[J]. 农业工程学报，2019，35(22)：323－330.
YANG Xinting，WANG Mingting，XU Daming，et al. Data storage and query method of agricultural products traceability information based on blockchain[J]. Transactions of the CSAE，2019，35(22)：323－330.(in Chinese)

[11] 李佳潞. 基于区块链的粮食供应链溯源方案的研究[D]. 北京：北京邮电大学，2019.
LI Jialu. Research on traceability scheme of grain supply chain based on blockchain[D]. Beijing：Beijing University of Posts and Telecommunications，2019.(in Chinese)

[12] 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 technology：architecture and progress[J]. Journal of Computer，2018，41(5)：969－988.(in Chinese)

[13] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481－494.
YUAN Yong，WANG Feiyue. Development status and prospect of blockchain technology[J]. Acta Automatica Sinica，2016，42(4)：481－494.(in Chinese)

[14] 杨颜博，张嘉伟，马建峰. 一种使用区块链保护车联网数据隐私的方法[J]. 西安电子科技大学学报，2021，48(3)：21－30.
YANG Yanbo，ZHANG Jiawei，MA Jianfeng. A method to protect data privacy of vehicle networking using blockchain[J]. Journal of Xidian University，2021，48(3)：21－30.(in Chinese)

[15] HOSSEIN S,LUKAS B,SIMON D. Droplet:decentralized authorization for IoT data streams[J]. ArXiv,2018: 1806.02057.
[16] DUBOVITSKAYA A,XU Zhigang,RYU S,et al. Secure and trustable electronic medical records sharing using blockchain[J]. American Medical Informatics Association,2017,11(6):650 - 659.
[17] TRUONG N B, SUN K, LEE G M,et al. GDPR-compliant personal data management: a blockchain-based solution[J]. IEEE Transactions on Information Forensics and Security,2020, 15:1746 - 1761.
[18] XU Chenhan,WANG Kun,LI Peng,et al. Making big data open in edges:a resource-efficient blockchain-based approach[J]. IEEE Transactions on Parallel and Distributed Systems,2018,30(4):870 - 882.
[19] ZHANG Yunru,HE Debiao,KIM-KWANG R,et al. BaDS:blockchain-based architecture for data sharing with ABS and CP - ABE in IoT[J]. Wireless Communications and Mobile Computing,2018,2783658:1 - 9.
[20] YUAN Chao,XU Mixue,SI Xueming,et al. Blockchain with accountable CP - ABE:how to effectively protect the electronic documents[C]//Proc. of the 23rd Int. Conf. on Parallel and Distributed Systems. Piscataway,NJ:IEEE,2017:800 - 803.
[21] 曾新安,曹诗林,马骥,等. 预制食品供应链品质监控与区块链溯源技术研究进展[J]. 中国食品学报,2022,22(10):48 - 57.
ZENG Xin'an, CAO Shilin, MA Ji, et al. Research progress on quality monitoring and blockchain traceability technology of prepared food supply chain[J]. Journal of Chinese Food Science, 2022, 22(10): 48 - 57. (in Chinese)
[22] 韦佩贝,戚穗坚. 疫情全球化常态化趋势下中国预制调理食品市场发展现状[J]. 食品与机械,2020,36(9):18 - 25.
WEI Peibei, QI Suijian. Development status of China's prepared prepared food market under the normalization trend of epidemic globalization[J]. Food and Machinery, 2020, 36(9): 18 - 25. (in Chinese)
[23] HUANG J, ZHANG M, FANG Z. Perspectives on novel technologies of processing and monitoring the safety and quality of prepared food products[J]. Foods,2023,12(16):3052.
[24] GE C, SUSILO W, LIU A, et al. Secure keyword search and data sharing mechanism for cloud computing[J]. IEEE Transactions on Dependable and Secure Computing,2020,18(6): 2787 - 2800.
[25] LI Linhui, SHI Peichang, FU Xiang, et al. Three-dimensional tradeoffs for consensus algorithms: a review[J]. IEEE Transactions on Network and Service Management,2022,19(2): 1216 - 1228.
[26] 黄卉,陈胜军,赵永强,等. 水产品预制菜加工与质量安全控制技术研究进展[J]. 南方水产科学,2022,18(6):152 - 160.
HUANG Hui, CHEN Shengjun, ZHAO Yongqiang, et al. Research progress on aquatic product prepared vegetable processing and quality safety control technology[J]. Southern Fisheries Science, 2022, 18(6): 152 - 160. (in Chinese)
[27] YU Q, ZHANG M, JU R,et al. Advances in prepared dish processing using efficient physical fields: a review[J]. Crit. Rev. Food Sci. Nutr. ,2022,27:1 - 15.
[28] DE MEDICI D, RODRIGUEZ-LAZARO D, COOK N. Editorial: new advances in identification and quantification of foodborne pathogens[J]. Front Microbiol. , 2021,12:783406.
[29] 吴晓娟,许东,董界,等. 方便米饭安全生产关键监管数据标准化方法的研究[J]. 食品与机械,2020,36(9):91 - 96,107.
WU Xiaojuan, XU Dong, DONG Jie, et al. Research on standardization method of key supervision data for safe production of instant rice[J]. Food and Machinery, 2020, 36(9):91 - 96,107. (in Chinese)
[30] 吴晓蒙,饶雷,张洪超,等. 新型食品加工技术提升预制菜肴质量与安全[J]. 食品科学技术学报,2022,40(5):1 - 13.
WU Xiaomeng, RAO Lei, ZHANG Hongchao, et al. New food processing technology improves the quality and safety of prepared dishes[J]. Journal of Food Science and Technology, 2022, 40(5): 1 - 13. (in Chinese)
[31] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]// Advances in Cryptology-EUROCRYPT'98, International Conference on the Theory and Application of Cryptographic Techniques. Proceeding Springer, Berlin, Heidelberg, 1998.
[32] 王海勇,彭垚,郭凯璇. 云存储中基于代理重加密的 CP - ABE 访问控制方案[J]. 计算机应用,2019,39(9):2611 - 2616.
WANG Haiyong, PENG Yao, GUO Kaixuan. CP - ABE access control scheme based on proxy re-encryption in cloud storage [J]. Computer Applications, 2019, 39(9): 2611 - 2616. (in Chinese)
[33] 刘艳,段茹,琚名扬. 支持密钥隔离的属性代理重加密方案[J]. 小型微型计算机系统,2020,41(3):598 - 602.
LIU Yan, DUAN Ru, JU Mingyang. Attribute proxy re-encryption scheme supporting key isolation[J]. Small Microcomputer Systems, 2020, 41(3): 598 - 602. (in Chinese)
[34] CHEN W, ZHU S, LI J,et al. Authorized shared electronic medical record system with proxy re-encryption and blockchain technology[J]. Sensors,2021,21(22):7765.
[35] 洪璇,袁梦玲. 基于多变量公钥密码系统的环机密交易协议[J]. 计算机科学,2023,50(增刊 1):756 - 761.
HONG Xuan, YUAN Mengling. Ring secret transaction protocol based on multivariable public key cryptosystem[J]. Computer Science, 2019,50(Supp. 1):756 - 761. (in Chinese)
[36] 田有亮,杨科迪,王缵,等. 基于属性加密的区块链数据溯源算法[J]. 通信学报,2019,40(11):101 - 111.
TIAN Youliang, YANG Kedi, WANG Zuan, et al. Blockchain data traceability algorithm based on attribute encryption[J]. Journal of Communications, 2019, 40(11): 101 - 111. (in Chinese)
[37] FENG T, PEI H, MA R, et al. Blockchain data privacy access control based on searchable attribute encryption[J]. Computers, Materials & Continua,2021,66(1):871 - 890.
[38] ZYSKIND G, ZEKRIFA D M S, ALEX P,et al. Decentralizing privacy: using blockchain to protect personal data[C]//IEEE Security & Privacy Workshops. IEEE, 2015.
[39] WANG Z, TIAN Y, ZHU J . Data sharing and tracing scheme based on blockchain[C]// International Conference on Logistics, Informatics and Service Sciences (LISS),2018.