doi:10.6041/j.issn.1000-1298.2024.10.041

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

刘晓辉[1,2]　罗　娜[2,3]　邢　斌[2,3]　高官岳[2,3]　孙　梅[1,2]　孙传恒[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:区块链追溯对于保障食品安全、提升农产品品质、维护消费者权益至关重要。针对农产品供应链中隐私数据安全与保护需求,提出了一种基于属性的可搜索加密的农产品区块链追溯隐私数据访问控制方法,该方法允许追溯供应链数据拥有者利用基于属性的可搜索加密技术对访问控制中的访问控制策略进行加密处理,追溯供应链数据请求者通过生成陷门与加密策略进行匹配,以确保访问控制的安全性,有效抵御恶意节点伪造信息非法获取权限的行为,隐藏用户身份,避免策略信息泄露问题,确保了隐私数据的安全性。采用以太坊权威证明共识机制搭建私有链进行仿真实验,系统测试结果表明,可搜索密文生成时间为 2.5 ms,陷门生成时间为 39.8 ms,可搜索密文与陷门的匹配时间为 8.6 ms,同时密文生成时间不随属性数量增加而线性增长,具有稳定性特征。可搜索密文和陷门上传至区块链平均时间为 2 033 ms,查询匹配时间为 3.54 ms。因此,本研究提出的访问控制方法实现了访问控制策略隐藏,保障了追溯隐私数据的安全共享,适用于农产品区块链追溯环节中。

关键词:农产品溯源;区块链;基于属性的访问控制;基于属性的可搜索加密

中图分类号:TP311.11　　**文献标识码**:A　　**文章编号**:1000-1298(2024)10-0433-11　　**OSID**:

Attribute-based Searchable Encrypted Agricultural Blockchain Traceability Private Data Access Control Method

LIU Xiaohui[1,2]　LUO Na[2,3]　XING Bin[2,3]　GAO Guanyue[2,3]　SUN Mei[1,2]　SUN Chuanheng[2,3]

(1. *College of Computer and Information Engineering*, *Tianjin Agricultural University*, *Tianjin* 300384, *China*
2. *National Engineering Research Center of Traceability Technology and Application of Agricultural Product Quality and Safety*, *Beijing* 100097, *China*
3. *National Agricultural Informatization Engineering Technology Research Center*, *Beijing* 100097, *China*)

Abstract: Blockchain traceability is essential for ensuring food safety, improving the quality of agricultural products, and safeguarding consumer rights. Aiming at the security and protection needs of private data in the agricultural product supply chain, an attribute-based searchable encryption access control method for agricultural product blockchain traceability privacy data was proposed, which allowed the data owners of the traceability supply chain to encrypt access control policies in access control by using attribute-based searchable encryption technology. Traceability supply chain data requestors generated trap gates to match encryption policies to ensure the security of access control, effectively resisted the behavior of malicious nodes to forge information and illegally obtained permissions, hided user identities, avoided policy information leaks, and ensured the security of private data. Using ethereum proof of authority consensus mechanism to build a private chain for simulation experiments, the system test results showed that the generation time of searchable ciphertext was 2.5 ms, the generation time of trap gate was 39.8 ms, and the matching time of searchable ciphertext and trap gate was 8.6 ms. At the same time, the generation time of ciphertext did not increase linearly with the increase of number of attributes, and it had the characteristics of stability. The average time to upload searchable ciphertexts and traps to the blockchain was 2 033 ms, and the time to query for matches was 3.54 ms. Therefore, the

收稿日期:2024-05-29　修回日期:2024-07-10

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:刘晓辉(1996—),男,硕士生,主要从事区块链技术研究,E-mail:1594662635@qq.com

通信作者:孙传恒(1978—),男,研究员,主要从事区块链技术、物联网和大数据追溯技术研究,E-mail:sunch@nercita.org.cn

access control method proposed can realize the hiding of access control policies, ensure the safe sharing of traceability privacy data, which was suitable for agricultural blockchain traceability.

Key words: traceability of agricultural products; blockchain; attribute based access control; attribute-based searchable encryption

0 引言

农产品区块链追溯是利用区块链技术对农产品从育种到销售的全过程进行追溯的方法[1-3],它通过将农产品的关键信息以区块的形式进行记录,从而实现产品从田间到餐桌的全程可追溯和可验证[4-6]。这种追溯技术不仅有助于商家和监管部门及时发现问题,还能确保产品的安全和质量,提升供应链的透明度和信息互通,促进产业健康发展[7-9]。然而,供应链中存在价格、成本以及个人信息等追溯隐私数据,区块链的公开透明特性也带来了数据隐私保护的挑战[10-11]。为了解决这一问题,基于属性的访问控制技术(Attribute based access control, ABAC)被广泛应用于保障农产品供应链中的数据隐私[12-14]。ABAC 通过定义和管理用户的属性,实现对数据的细粒度访问控制,有效防止了未经授权的用户访问敏感信息[15-16]。

在隐私数据安全共享领域,众多学者进行了深入研究。文献[17]提出了结合基于属性的访问控制模型与区块链技术的数据共享方案,实现了物联网环境下的动态、分布式、可靠访问控制。针对 IoT 边缘节点与异构设备间的数据安全和管理挑战,文献[18]提出基于区块链与边缘计算的 IoT 访问控制模型 SC-ABAC。文献[19]为解决果蔬农产品供应链中的数据追溯差异化、细粒度共享难题及数据隐私保护问题,设计了一种支持异构多链的基于属性的果蔬跨链访问控制模型。文献[20]针对云边端协同结构中的数据安全问题,提出了一种基于智能合约的细粒度数据访问控制方法。

尽管 ABAC 在边缘计算与区块链交互中展现出细粒度访问控制的优势[21],但存储在区块链上的属性与策略信息的可见性,可能导致恶意节点伪造信息以获取权限,进而引发隐私数据泄露的风险[22]。在访问控制策略隐藏方面,研究人员探索了利用同态加密、属性基加密和零知识证明等方法以增强访问控制的隐私保护和安全性。文献[23]提出了 TrustAccess 方案,一种基于区块链的可信安全密文策略和属性隐藏访问控制方案,保障了策略和属性隐藏的同时实现可信访问。文献[24]采用属性基加密以及双线性映射技术,实现在不泄露访问控制策略的前提下,通过智能合约正确执行访问控制策略。文献[25]利用同态加密算法对属性和访问策略进行加密,并采用零知识证明确保解密结果的正确性。而文献[26]则利用智能合约和零知识证明实现了策略评估的透明性,同时保护了敏感属性数据。尽管同态加密和属性基加密增强了隐私数据的安全性,但这些方法的加密时间会随着属性数量的增加而线性增长。另一方面,零知识证明虽然在证明生成时间上保持恒定,但其生成和验证过程可能需要较大的计算资源和时间投入。因此,迫切需要一种既能有效隐藏访问控制策略,又能实现隐私数据稳定高效共享的访问控制方法。

本文针对农产品供应链中的数据隐私共享,提出一种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,实现访问控制策略的安全隐藏。该方法将基于属性的访问控制(ABAC)与基于属性的可搜索加密(Attribute-based searchable encryption, ABSE)技术相结合,利用 ABAC 策略确保数据访问权限的精确控制,保障只有授权用户才能访问特定数据,利用 ABSE 技术加密策略,提高策略信息的安全性,允许用户在策略保持加密状态下进行高效搜索。

1 农产品供应链隐私数据共享模型

1.1 农产品供应链关键信息

农产品供应链管理是一个涵盖育种、种植、加工、仓储、运输至销售等多个核心环节的复杂体系,各环节通过终端设备获取原始数据,再由边缘节点汇总上传至区块链[27]。鉴于边缘节点存储和计算能力上存在的差异性,为避免存储空间被海量物联网数据迅速耗尽,将边缘节点作为轻节点融入区块链架构中,并通过云端构建区块链,从而极大地优化数据处理效率,确保供应链数据流通既高效又稳定[28]。

在深入分析农产品供应链特点的基础上,终端设备能够从源头获取数据并根据不同的隐私级别进行精细分类,分别为公开数据、二级隐私数据、一级隐私数据[9,19,27]。公开数据无需进行额外的加密或哈希处理,直接用于供应链中的日常运作。二级隐私数据,涉及供应链各环节协作以及政府监管,虽具有一定的商业价值但并不属于核心隐私范畴,如产品数量、研发记录等。而一级隐私数据则承载着企

业的核心敏感信息，如成本价格、人员信息等，其隐私性极高，因此仅供企业自身或授予访问权限的企业或机构访问查看，一级隐私数据与二级隐私数据均由哈希函数分别进行哈希处理，以确保数据在区块链中的存储既节省空间又高度安全。终端设备将公开数据和隐私数据的哈希值传输给边缘节点，边缘节点作为轻节点将数据上传至区块链。本研究进一步细化了农产品供应链各环节的关键信息，为供应链的持续优化和管理提供了坚实的数据支撑，具体如表 1 所示。

表 1　供应链各环节关键信息

Tab.1　Key information of each link of supply chain

环节	公开数据	二级隐私数据	一级隐私数据
育种	农产品品种、育种企业、育种编号、生长周期、抗病性、品质特性、适应区域、专利信息	基因序列、遗传特性、种子资源、研发记录、性状数据、育种策略	田间试验数据、生长记录、育种人员信息、种子成本
种植	农产品品种、种植产地、种植编号、种植资质、播种时间、采收时间、农田地理信息	种植数量、温湿度、生物灭虫情况、农药和化肥使用情况、灌溉记录、气象条件、除草记录、生长周期、霉菌含量、土壤检测报告、农药残留检测	种植成本价格、农户种植人员信息
加工	农产品品种、加工企业、加工编号、加工资质、加工时间、加工方式、质检结果、包装信息、保质期时间	原料入场质检报告、加工数量、加工工艺、包装材料、杀菌消毒检测结果、真空包装检测结果、产品质检结果	加工设备状况监测、加工人员信息、加工成本、订单价格
仓储	农产品品种、仓储企业、仓储编号、仓储资质、仓储方式、仓储位置、仓储出入库时间	仓储库存状态、出入库记录、仓库温湿度、通风要求、霉菌毒素含量、质量检测结果	仓库成本、库存周转率、货损记录、仓储监控、仓库负责人员信息
运输	农产品品种、运输企业、运输编号、运输资质、运输路线、运输时间、运输方式	运输数量、运输车辆内有毒害物质检测、北斗定位追踪数据、运输货车温湿度、货物交接记录出入库	运输成本、运输合同、运输人员信息
销售	农产品品种、销售渠道、销售编号、销售资质、进货时间、销售时间	销售数量、销售地点、货物上架时间、订单信息	工作监控、销售人员信息、进货价格

1.2　农产品供应链隐私数据共享模型构建

农产品供应链隐私数据共享模型旨在使追溯过程中隐藏访问控制策略的前提下，又能实现隐私数据高效共享。在本研究中，假设数据拥有者和监管者为诚实可信节点，负责验证数据请求者的身份和权限。该模型由 3 个核心模块组成：认证模块、访问控制模块和隐私数据链下传输模块。将 ABAC 与 ABSE 结合为农产品供应链追溯模型的核心，访问控制模块作为隐私数据共享中重要的一环，农产品供应链隐私数据共享模型如图 1 所示。

隐私数据共享模型的第 1 个模块为认证模块，即供应链企业中参与的边缘设备与企业节点的注册与认证，在图 1 中过程为步骤 1 ~ 3，Kerberos 在认证通过后，认证双方便能利用共享会话密钥进行高效的加密通信[29]。用户向 Kerberos 进行注册，需要提供包括用户名、密码、企业 ID、角色、所处阶段等信息。注册完成后，将用户的信息存储在 Kerberos 的内置数据库中。Kerberos 协议认证首先用户向密钥分发系统 KDC 中的认证服务器（Authentication server，AS）传输用户信息，包括用户名和密码等凭证信息，进而在 AS 数据库中验证用户的身份信息，申请票据授予票据（Ticket granting tickets，TGT）。AS 返回使用用户密钥 SK_U 加密用户与票据授予服务器（Ticket granting server，TGS）之间的会话密钥 SK_U[会话密钥 SK_{U-TGS}]，并且返回包含用户信息的加密票据 SK_{U-TGS}[TGT]，该 TGT 包括用户的实体名、地址、时间戳、限制时间和会话密钥 SK_{U-TGS}。随后，用户收到信息后，用户发送请求使用会话密钥 SK_{U-TGS} 加密用户 ID 和时间戳，组成 SK_{U-TGS}[ID + 时间戳]，并附加接收到的加密票据 TGT，SK_{U-TGS}[TGT]和用户 ID 一同发送至 TGS 服务器。TGS 服务器验证该加密票据后，返回使用应用服务器密钥 SK_S 加密的用户信息 SK_S[TGT(用户信息)]，以及使用 SK_{U-TGS} 加密的用户与应用服务器之间的会话密钥（SK_{U-S}，SK_{U-TGS}[会话密钥 SK_{U-S}]）。其中用户信息包括客户端 ID、网络地址、有效期限、会话密钥 SK_{U-S}。最后，用户再次发送该加密的用户信息 SK_S[TGT(用户信息)]以及使用会话密钥 SK_{U-S} 加密的用户 ID 和时间戳 SK_{U-S}[ID + 时间戳]到应用服务器。应用服务器使用自身密钥解密加密票据得到用户与服务器之间的会话密钥，将其中的两个用户 ID 进行比较，匹配成功则继续发送消息，将时间戳使用 SK_{U-S} 加密 SK_{U-S}[时间戳]发送至用户，用户解密并检查该时间戳的正确性，于是便完成密钥交换，进而完成认证实现加密通讯。通过以上步骤完成 Kerberos 认证过程。Kerberos 认证流程图如图 2 所示。

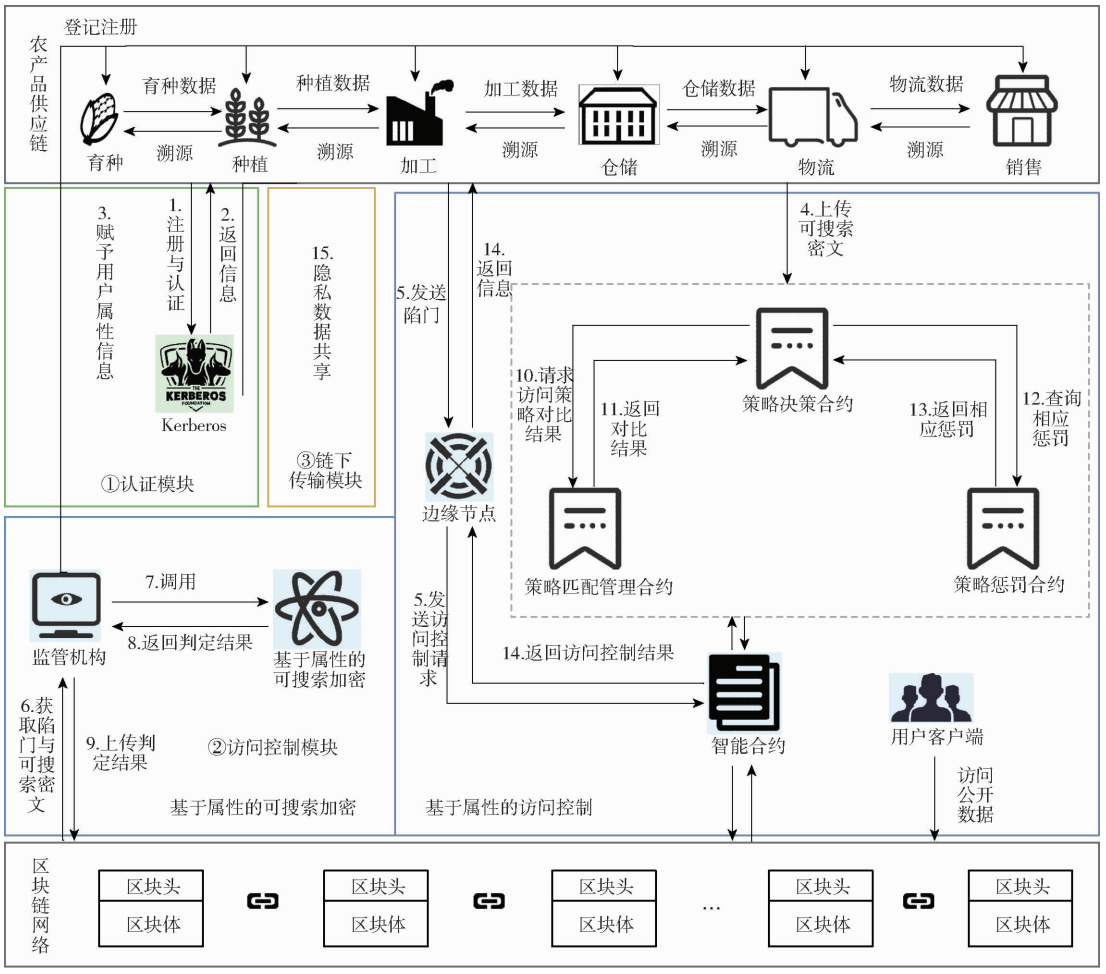

图 1 农产品供应链隐私数据共享模型

Fig. 1 Private data sharing model of fresh corn supply chain

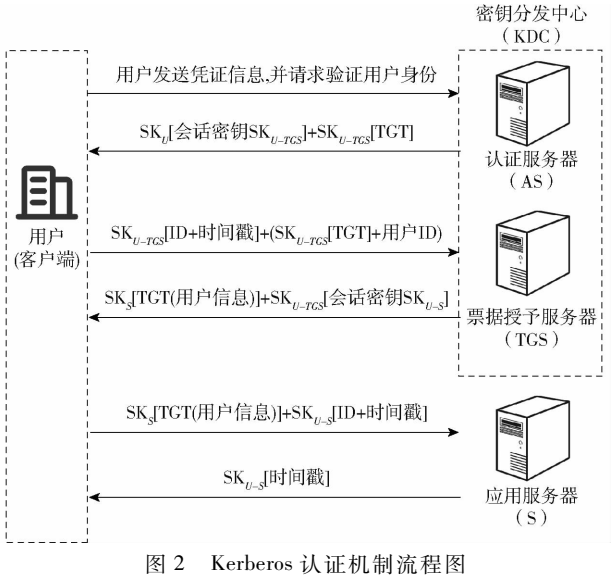

图 2 Kerberos 认证机制流程图

Fig. 2 Kerberos authentication mechanism flowchart

在 Kerberos 认证流程中,用户认证是通过票据和会话密钥来实现的。用户持有的 TGT 和从 TGS 获得的服务票据都包含用户身份信息和会话密钥,这些信息被加密并由 Kerberos 的服务器所验证。一旦服务票据被验证,用户与服务之间的通信就可以使用会话密钥进行加密通信,确保了隐私数据传输的安全性。由于用户属性信息在本场景下较为重要,于是由监管者根据其资质授予不同用户相应的属性信息。监管者运行 Kerberos 将用户的账户名上传至区块链中。

第 2 个模块为农产品隐私数据访问控制模块,在图 1 中为步骤 4 ~ 14,该阶段主要是以 ABAC 访问控制为基础,将 ABSE 对 ABAC 中的策略进行加密,并且可以通过可搜索密文与陷门匹配的方式完成策略对比,满足访问控制就可以实现农产品数据请求者请求访问农产品数据拥有者的隐私共享数据,数据拥有者将访问令牌通过属性基加密的方式保存于可搜索密文中,数据请求者与数据拥有者分别将陷门与可搜索密文上传至区块链,监管者通过区块链获取可搜索密文与陷门信息,监管者通过调用 ABSE 算法,可以得出匹配结果,满足可搜索加密的密文与陷门的对比,便会输出属性基加密的密文,将该匹配结果上传至区块链中。策略决策合约根据匹配结果选择调用策略惩罚合约对该访问 IP 地址做出惩罚。并将访问请求结果通过边缘节点返回给数据请求者。而边缘节点负责数据传输、访问控制格式转换、与区块链进行交互等操作。

第 3 个模块为链下隐私数据传输模块，在图 1 中为步骤 15，该阶段当数据请求者满足访问控制权限后，数据请求者通过属性私钥进行解密获得访问令牌。数据请求者通过将获取的访问令牌发送至数据拥有者进行通信，双方通过 Kerberos 进行共享会话密钥进行加密通信，将相应权限的农产品隐私数据通过加密通信进行数据传输，为了防止链下数据篡改，可以将获取到的农产品链下隐私数据进行哈希处理与链上隐私数据的哈希值进行对比，可以确保数据的真实与准确性，由此便完成了农产品供应链隐私数据共享。

2　基于属性可搜索加密的访问控制

对农产品供应链隐私数据共享中的基于属性可搜索加密的访问控制模型加以详细阐述，以加工环节向种植数据发出访问请求，查看种植环节中农产品的质检报告，以确认产品质量是否符合标准。由于 ABAC 中策略需要隐藏[30-31]，使用 ABSE 技术[32-33]对策略进行加密，可以实现通过可搜索密文上传至区块链后，多个用户可以根据属性运行相应算法，生成陷门进行匹配检索。于是本研究采用基于属性的可搜索加密方法对访问策略进行可搜索加密，既可以保证策略以密文形式展现，也可以对加密后的信息进行匹配检索。

2.1　基于属性的可搜索加密方法

定义 ABSE 技术中的参与者在农产品供应链中主要为：数据拥有者、数据请求者和监管机构。设计监管机构审核根据用户的身份信息为每位用户授予属性信息，图 3 为基于属性的可搜索加密流程图。

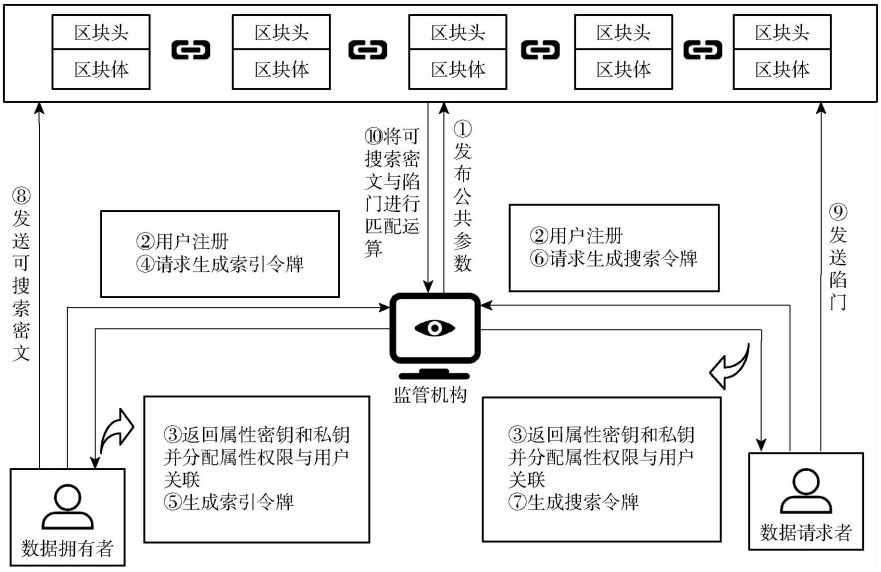

图 3　基于属性的可搜索加密流程图

Fig. 3　Searchable encryption flowchart based on attributes

图 3 中首先由监管机构运行初始化算法生成并发布公共参数至区块链，公共参数 CP 是系统中所有用户共享的，是用于后续加密和搜索操作的基础。数据拥有者与数据请求者向监管机构进行用户注册，监管机构返回属性密钥与私钥并分配属性权限与用户进行关联，然后数据拥有者向监管机构请求生成索引令牌，该索引令牌包含了访问策略和属性公钥列表，索引令牌确保数据可以按照特定的访问策略被检索，用于创建可搜索密文。数据请求者向监管机构请求生成搜索令牌，该搜索令牌确保只有符合拥有相应属性的用户才能检索到数据，用于创建陷门。最后数据拥有者生成可搜索密文并发送至区块链，数据请求者生成陷门并将陷门发送至区块链，监管者将区块链中的可搜索密文与陷门进行匹配，向数据请求者返回对比结果。

基于属性的可搜索加密由以下概率多项式算法组成：ABSE = (TSetup, AddUser, ASetup, AttG, PrdIT, PrdST, ABSE, TrpG, TEST)。

2.1.1　初始化

初始化算法 TSetup(δ)→(CP, UMK)：该算法运行建立系统发布公共参数，在图 3 中为步骤①。获取安全参数 δ，并输出公共参数 CP 和用户主密钥 UMK。

AddUser(CP, UMK)→(RK_i, SK_i)：该算法为用户向系统注册，在图 3 中为步骤②，输入公共参数 CP 和用户 i 的主密钥 UMK，可以输出一个用户 i 的公钥 RK_i，该密钥可以用于向监管机构进行注册。SK_i 是用户用来创建陷门的私钥。

ASetup(CP)→(AMK_j, APK_j)：该算法是用来设

置属性权限，在图 3 中为步骤③，通过输入公共参数 CP，输出关于属性 j 的主密钥 AMK_j 和属性公钥 APK_j，该属性主密钥对监管者保密，属性主密钥用于用户注册时创建用户属性私钥，属性公钥可以用于生成属性验证和陷门等功能。

$AttG(RK_i, AMK_j) \rightarrow ASK_{i,j}$：该算法用来运行对用户 i 进行属性关联，在图 3 中为步骤③，并输出属性私钥。输入用户 i 的公钥 RK_i 和属性 j 的主密钥 AMK_j，由此可以得出对于用户 i 拥有属性 j 的属性私钥 $ASK_{i,j}$。

2.1.2 生成令牌算法

$PrdIT(\Psi, AH) \rightarrow (IT_\Psi)$：该算法是由数据拥有者运行，可以用来创建索引令牌，在图 3 中为步骤④和步骤⑤。给定访问策略 Ψ，属性公钥列表 $AH = \{APK_Z\}_{Z=1}^{n}$。访问策略 Ψ 是指描述搜索条件和筛选条件的逻辑表达式，并通过逻辑运算符（如 AND、OR）组合多个属性值，以实现对加密数据的有效搜索和检索。属性公钥列表是指用于加密数据和生成陷门的属性相关的公钥集合。该算法生成将用于创建可搜索密文的索引令牌 IT_Ψ。

$PrdST(\vartheta, AP) \rightarrow (ST_\vartheta)$：该算法是由数据请求者运行用来创建搜索令牌，在图 3 中为步骤⑥和步骤⑦。给定请求访问策略 ϑ，属性公钥列表 $AP = \{APK_j\}_{j=1}^{m}$，该算法生成将用于创建陷门的搜索令牌 ST_ϑ，搜索令牌可以确保只有拥有相应属性的用户才能搜索到符合访问策略的密文。

2.1.3 生成可搜索密文算法

$ABSE(K, \Psi, D, IT_\Psi) \rightarrow E_{\Psi,K}$：由数据拥有者运行，在图 3 中为步骤⑧，生成可搜索密文算法参数包括关键字 K、访问策略 Ψ、数据密文 D 和可搜索密文的索引令牌 IT_Ψ，关键字 K 是指用于搜索加密数据的搜索词，数据密文 D 是指数据拥有者通过属性基加密的访问令牌，利用它可以创建可搜索密文 $E_{\Psi,K}$，并将该可搜索密文发送至区块链。

2.2 基于属性可搜索加密的访问控制方法

当加工节点向种植节点作为发起数据访问请求，其中基于属性的访问控制策略涵盖策略决策合约、策略匹配管理合约和策略惩罚合约。在该模型中，边缘节点负责与区块链进行交互，将访问请求进行格式转换，边缘节点还负责执行策略决策返回的决策结果。而策略匹配管理合约则负责管理用户构建的陷门与可搜索密文的匹配结果，策略惩罚合约负责管理该节点访问存在恶意攻击行为时做出惩罚，对恶意行为者将其 IP 地址加入黑名单禁止访问，有利于系统稳定。策略决策合约负责管理访问控制的决策过程，具体流程如图 4 所示。

访问控制主要分为访问控制策略生成及初始化和数据访问控制流程两个模块，其中数据访问控制流程按照图 4 步骤进行描述。

2.2.1 访问控制策略生成及初始化

在农产品供应链中，为了保证 Kerberos 服务的可用性，将其置于监管机构节点所处的云服务器

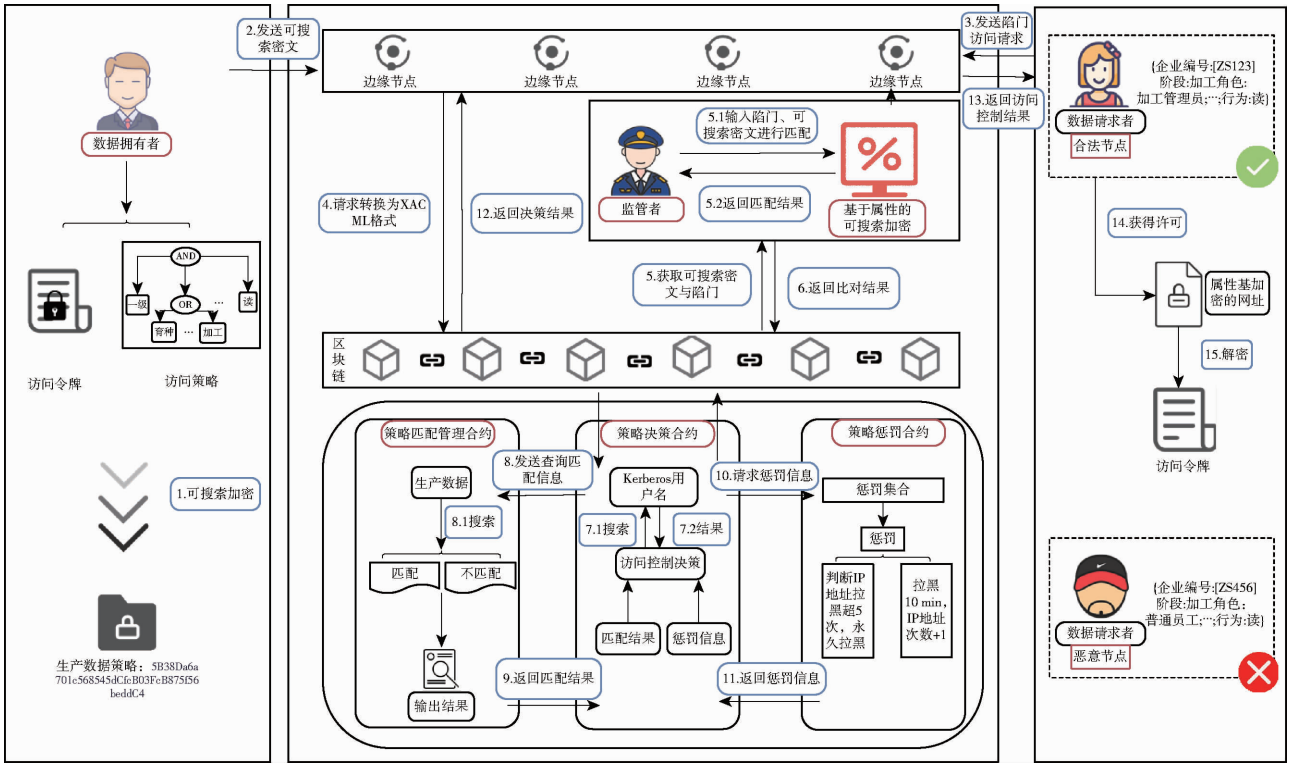

图 4 基于属性可搜索加密的访问控制模型

Fig. 4 Access control model for attribute-based searchable encryption

中，各参与方可以通过访问该云服务器上的 Kerberos 服务进行认证。Kerberos 注册后得到的账号是由系统管理员分配的，它们因为不同的组织、系统或身份提供者而有所不同。边缘节点与各环节节点采用设备的 MAC 地址作为唯一的标识符，向 Kerberos 进行注册，账号的用户名通常以 Principal 的形式表示，它包含了用户或服务的标识信息，例如部署在种植环节中的边缘节点表示为 EdgeNode/production@ EXAMPLE. COM。系统初始化节点由监管机构组织负责定义农产品供应链企业属性信息，这些属性包括主体属性、客体属性、环境属性和行为属性等。环境属性中包含请求来源地址、开始时间、结束时间等属性信息，行为属性中包括读取、写入、编辑、复制和删除等属性信息。数据拥有者定义访问策略，这些策略规定了用户根据其特有属性可以访问相应资源。为了便于描述基于属性的访问请求，访问控制策略含义为：主体属性在环境属性条件下，对客体属性进行行为属性的操作请求[19]。各环节拥有的相应主体与客体属性信息具体内容如表 2 所示。

表 2　各环节属性信息

Tab. 2　Attribute information of each link

环节	主体属性	客体属性
育种	企业编号：ID；角色：育种工作者、育种专家；阶段：育种环节；产品类别：农产品品种	产品类型：育种农产品名称；产品批次：育种的农产品批次编号；所处阶段：育种环节；数据敏感级别：一级隐私、二级隐私
种植	企业编号：ID；角色：种植者、农场管理员；阶段：种植环节；产品类别：农产品品种	产品类型：种植农产品名称；产品批次：种植的农产品批次编号；所处阶段：种植环节；数据敏感级别：一级隐私、二级隐私
加工	企业编号：ID；角色：加工工人、加工管理员；阶段：加工环节；产品类别：农产品品种	产品类型：生产农产品名称；产品批次：加工的农产品批次编号；所处阶段：加工环节；数据敏感级别：一级隐私、二级隐私
仓储	企业编号：ID；角色：仓库管理员、库管员；阶段：仓储环节；产品类别：农产品品种	产品类型：仓储农产品名称；产品批次：仓储的农产品批次编号；所处阶段：仓储环节；数据敏感级别：一级隐私、二级隐私
物流	企业编号：ID；角色：物流司机、物流管理员；阶段：物流环节；产品类别：农产品品种	产品类型：物流农产品名称；产品批次：运输的农产品批次编号；所处阶段：物流环节；数据敏感级别：一级隐私、二级隐私
销售	企业编号：ID；角色：销售员、超市管理员；阶段：销售环节；产品类别：农产品品种	产品类型：销售农产品名称；产品批次：销售的农产品批次编号；所处阶段：销售环节；数据敏感级别：一级隐私、二级隐私

种植节点作为策略制订者，根据属性信息制订访问控制策略，访问主体加工企业编号为[ZS123]、角色为加工管理员、阶段为加工环节、产品类型为鲜食玉米，访问客体产品类型为鲜食玉米、种植产品批次为 20240203A001、所处阶段为种植环节、数据敏感级别为二级隐私数据，在环境属性请求来源地址为北京，访问时间为 08:00—12:00，执行行为属性读取操作，满足以上策略信息即可满足访问控制。

2.2.2　数据访问控制流程

步骤 1、2：种植节点将使用属性基加密的访问令牌和访问策略等作为参数生成可搜索密文，上传至区块链中。

步骤 3、4：加工节点通过边缘节点向区块链发送请求。生成陷门算法是由加工节点运行 $\mathrm{TrpG}(W,\vartheta,\mathrm{ST}_{\vartheta},\mathrm{SK}_i,\mathrm{AS}_i)\rightarrow T_{\vartheta,W}$：在图 3 中为步骤⑨，给定关键字 W、访问策略 ϑ、搜索令牌 ST_{ϑ}、用户密钥 SK_i 和用户私有属性密钥 $\mathrm{AS}_i=\{\mathrm{ASK}_{i,j}\}_{j=1}^{m}$，输出陷门 $T_{\vartheta,W}$。加工节点运行该算法后，将陷门、Kerberos 用户名和 IP 地址以请求的方式向边缘节点发送原始访问请求，边缘节点将原始访问请求转换为 XACML 格式的访问请求，并将其转发至策略决策合约。

步骤 5、6：当加工节点上传陷门至区块链后，监管者通过关键字查询搜索陷门与可搜索密文，将获取后的陷门与可搜索密文通过基于属性的可搜索加密方法进行匹配验证，运行该算法 $\mathrm{TEST}(\mathrm{CP},E_{\Psi,K},T_{\vartheta,W})\rightarrow\{D,\mathrm{False}\}$：在图 3 中为步骤⑩，通过公共参数 CP，可搜索密文 $E_{\Psi,W}$ 和陷门 $T_{\vartheta,W}$，若加工节点满足访问策略则比对成功，输出数据密文 D，否则输出 False。将结果上传至区块链。

步骤 7：策略决策智能合约收到边缘节点信息后，先查询 Kerberos 用户名是否存在于区块链中，验证用户的身份信息，若搜索失败则直接输出 False

转至步骤 9。搜索成功后将查询策略匹配管理智能合约。

步骤 8:策略匹配管理智能合约通过搜索关键字来筛选出该陷门与可搜索密文,并将该对比结果发送至策略决策合约。

步骤 9:策略决策合约根据其密文匹配智能合约返回的信息,对访问请求进行评估和计算,判断加工环节是否允许在相应的环境下对种植节点一级隐私数据执行相关操作,若发现比对成功,则直接做出决策将密文 D 返回给加工节点。

步骤 10、11:如果输出为 False,策略决策合约向策略惩罚合约获取惩罚信息,判断该 IP 地址拉黑次数是否小于 5,若次数小于 5 则将其 IP 加入黑名单,10 min 内无法继续进行访问,并对该 IP 地址恶意访问次数进行累加。若大于等于 5 次将该 IP 地址直接加入黑名单,不再移除,该方法有效缓解非法访问,提高网络稳健性。

步骤 12、13:策略决策合约作出决策将结果通过边缘节点返回至加工节点。

步骤 14、15:加工节点通过属性私钥进行解密获得访问令牌。

2.3 智能合约设计

本文使用以太坊平台,开发 solidity 智能合约[34],针对农产品追溯实际情况,为了保护数据隐私安全问题,研究设计相关智能合约细节,如表 3 所示。

表 3 智能合约设计

Tab. 3 Smart contract design

调用者	合约方法	输入	输出	描述	合约功能
数据拥有者	addProduct( )	产品 Id/产品名称/公开数据/一级隐私数据/二级隐私数据/供应链阶段	True/False	添加农产品追溯数据	数据上链合约
	addEncryptedData( )	关键词/可搜索密文	True/False	添加可搜索密文	策略决策合约
数据拥有者、数据请求者、监管者	getProduct( )	产品 Id	产品数据集	获取农产品追溯数据	数据查询合约
数据请求者	addTrapdoor( )	关键词/陷门	True/False	添加陷门	策略决策合约
监管者	addResult( )	关键词/可搜索密文/陷门/判断结果/密文	True/False	将可搜索密文与陷门判定结果上传	策略匹配管理合约
	addToBlacklist( )	IP 地址	拉黑提醒	将 IP 地址加入黑名单,并设置黑名单截止时间为当前时间 + 黑名单持续时间	策略惩罚合约

在农产品数据共享中,当存在恶意节点进行访问时,发现本次访问不满足访问控制请求,则将对该 IP 地址进行访问控制策略惩罚,先判断该 IP 地址访问次数是否超过了预设的阈值,如果已经超过,将该地址永久加入黑名单,否则将该地址拉黑 10 min。具体算法内容为:

策略惩罚算法

输入:地址 addr

输出:黑名单截止时间为当前时间 + 黑名单持续时间

1. MAX_COUNT_BLACKLIST← 5
2. BLACKLIST_DURATION← 10
3. require(addr ! = address(0),"Invalid address") //判断该地址是否是合法地址
4. addressCount[addr]← addressCount[addr] + 1 //该地址次数 +1
5. if addressCount[addr] > = MAX_COUNT_BLACKLIST do //判断该地址非法访问次数
6. blacklistUntil[addr]← type(uint256).max //赋值该地址永久加入黑名单
7. else do
8. blacklistUntil[addr]← block.timestamp + BLACKLIST_DURATION //赋值该地址加入黑名单,但在 10 min 后自动移出

3 性能测试与分析

本文构建了一个基于属性可搜索加密的农产品隐私数据访问控制方法,旨在确保数据的隐私性和高效共享。为了全面评估该方法的性能和实用性,使用一台配置有 8GB RAM 的 Ubuntu 16.04 系统。运用 Solidity 编程语言编写智能合约,采用以太坊平台权威证明(Proof of authority,PoA)共识机制搭建私有链进行仿真实验。使用 Remix IDE 对智能合约进行模拟与调试。并使用 Metamask 钱包插件连接私链。为了自动化构建和部署流程,采用 Truffle 测试框架,测试数据上传至区块链的时间和数据查询时间,以确保系统性能和响应速度满足实际需求。

3.1　性能测试

本节通过仿真实验分别对可搜索密文与陷门的生成时间、可搜索密文与陷门的匹配时间和策略查询时间进行性能测试，图 5 为不同属性数量算法运行 100 次的平均值，可搜索密文生成时间为 2.5 ms，陷门生成时间为39.8 ms，可搜索密文与陷门的匹配时间为 8.6 ms。由图 5 可知可搜索密文与陷门的生成和匹配时间随着属性数量的增加波动变化较小，说明该算法较为稳定。本研究中随着属性数量的不断增加，可搜索密文与陷门生成的密文所占内存分别稳定在 24 byte 和 26 byte，由此可知本方法适合将访问控制策略进行隐藏并应用于追溯环节中。

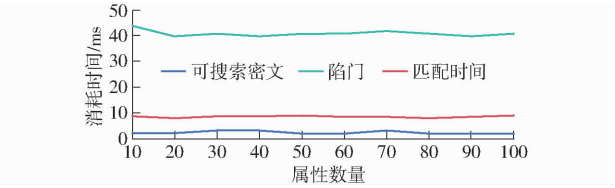

图 5　随着属性的增加性能测试结果

Fig. 5　Performance test results as properties increased

在本研究中，企业需要频繁地上传数据与可搜索密文，查询公开数据，监管者需要查询可搜索密文与陷门信息，上传可搜索密文与陷门的匹配信息。于是通过利用 Truffle 测试工具与基于 PoA 共识机制搭建的私有区块链进行连接，在轮转次数设定为 100 的情况下，将可搜索密文和陷门上传至区块链的平均时间为 2 033 ms，查询匹配时间为 3.54 ms。这一数据表明，尽管数据上传至区块链的过程相较于其他研究略显缓慢，但查询操作的高效性仍然非常显著。考虑到农产品追溯系统对实时性和准确性的要求，这一上传速度在实际应用中仍可接受，因此能够满足系统基本需求。具体如图 6 所示。

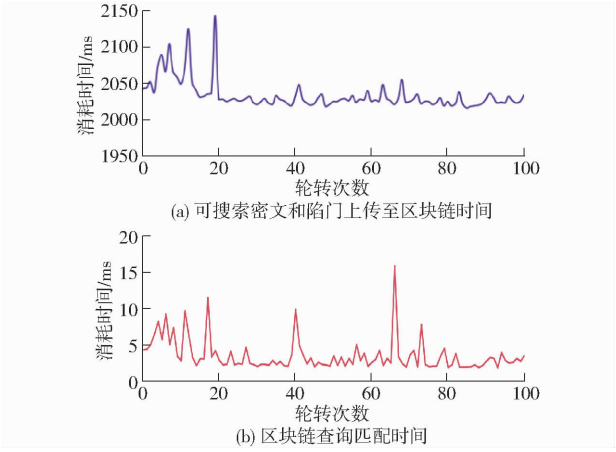

图 6　与区块链交互时间性能测试

Fig. 6　Performance test with blockchain interaction time

3.2　访问控制策略隐藏对比

通过与已有研究对比进行分析，文献[25]所提出的方法会根据属性数量的增加，所加密的时间会随着增加。文献[26]虽然加密时间是恒定的，但是每次生成证明的时间为 3 s，本方法中可搜索密文与陷门生成时间总和为 43 ms，由此可知本研究方法不仅随着属性的增加加密时间稳定，而且相比于其他加密方法耗时更短，具体如表 4 所示。图 7 展示了本研究与文献[25－26]在属性数量由 200 个增加至 1 000 个，不同属性数量加密时间对比，可以直观地看出本研究更适用于农产品追溯隐私数据共享中。

表 4　本模型与已有研究对比

Tab. 4　Comparison and analysis between proposed model and existing research schemes

研究	策略隐藏	策略表达方式	加密存储	安全性	是否可搜索	属性增加加密时间是否增加
文献[19]	×	AND-gates	×	基于属性的访问控制	否	是
文献[25]	√	访问控制树	√	基于属性的访问控制、同态加密、零知识证明	否	是
文献[26]	√	AND-gates	√	基于属性的访问控制、零知识证明	否	否
本研究	√	AND-gates	√	基于属性的访问控制 基于属性的可搜索加密	是	否

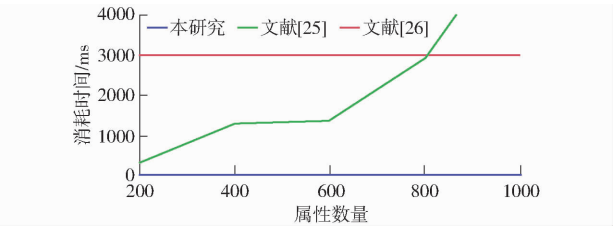

图 7　不同属性数量加密时间对比

Fig. 7　Comparison of encryption time of different attributes quantities

4　结论

(1)研究了区块链农产品追溯系统中的关键问题，如何在保障数据隐私的同时，实现高效的访问控制。提出了一种创新的访问控制策略隐藏方法，该方法融合了基于属性的可搜索加密(ABSE)和基于属性的访问控制(ABAC)技术，旨在强化访问控制策略的隐藏能力，并确保隐私数据的安全共享。首先分析了农产品供应链中的数据隐私和安全需求，

明确了现有区块链追溯系统在数据隐私保护方面的不足。针对这一挑战,该方法不仅能够有效地抵御恶意节点的攻击,保护用户身份和策略信息不被泄露,而且通过使用高效的可搜索加密技术,提高了策略检索效率和灵活性。

(2)系统测试结果展示了本方法的高性能和稳定性。利用以太坊平台 PoA 共识机制,实现了自动化的合约执行和管理,进一步提高了交易安全性、透明性和效率。可搜索密文的生成时间为 2.5 ms,陷门生成时间为 39.8 ms,匹配时间为 8.6 ms。即便在属性数量增加的情况下,系统性能依然稳定,内存占用保持不变。并利用 Truffle 测试工具,将可搜索密文和陷门上传至区块链的平均时间为 2 033 ms,查询匹配的时间为 3.54 ms,通过与现有研究对比分析,本文法在加密时间展现出显著优势。这些特性使得该方法适合应用于需要隐藏访问控制策略并确保数据隐私的追溯环节中,对于促进供应链管理产业的发展具有重要意义。

参 考 文 献

[1] 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 Huageng, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology [J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(1):1 - 13.

[2] SARANYA P, MAHESWARI R. Proof of transaction (PoTx) based traceability system for an agriculture supply chain[J]. IEEE Access, 2023, 11: 10623 - 10638.

[3] 弋伟国,何建国,刘贵珊,等. 区块链增强果蔬质量追溯可信度方法研究与系统实现[J]. 农业机械学报,2022,53(2):309 - 315,345.
YI Weiguo, HE Jianguo, LIU Guishan, et al. Development and implementation of blockchain to enhance traceability and reliability of fruit and vegetable quality [J]. Transactions of the Chinese Society for Agricultural Machinery,202,53(2):309 - 315,345. (in Chinese)

[4] GUAN S, WANG Z, CAO Y. A novel blockchain-based model for agricultural product traceability system [J]. IEEE Communications Magazine, 2023, 61(8): 124 - 129.

[5] SANTHIYA K. Agriculture basedfood supply chain traceability using blockchain[C]// 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE, 2023: 1 - 6.

[6] 刘双印,雷墨鹭兮,徐龙琴,等. 基于区块链的农产品质量安全可信溯源系统研究[J]. 农业机械学报,2022,53(6):327 - 337.
LIU Shuangyin, LEI Moyixi, XU Longqin, et al. Development of reliable traceability system for agricultural products quality and safety based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery,2022,53(6):327 - 337. (in Chinese)

[7] 孙传恒,杨晓虎,罗娜,等. 基于区块链的三文鱼冷链多链协同监管模型研究[J]. 农业机械学报,2024,55(1):360 - 370.
SUN Chuanheng, YANG Xiaohu, LUO Na, et al. Blockchain based salmon cold chain multi-chain collaborative supervision model [J]. Transactions of the Chinese Society for Agricultural Machinery,2024,55(1):360 - 370. (in Chinese)

[8] PATEL A S, BRAHMBHATT M N, BARIYA A R, et al. Blockchain technology in food safety and traceability concern to livestock products[J]. Heliyon, 2023,9(6):16526.

[9] 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)

[10] 杜瑞忠,张添赫,石朋亮. 基于区块链且支持数据共享的密文策略隐藏访问控制方案[J]. 通信学报,2022,43(6):168 - 178.
DU Ruizhong, ZHANG Tianhe, SHI Pengliang. Ciphertext policy hidden access control scheme based on blockchain and supporting data sharing[J]. Journal of Communications,2022,43(6):168 - 178. (in Chinese)

[11] THANGAMAYAN S, PRADHAN K, LOGANATHAN G B, et al. Blockchain-based secure traceable scheme for food supply chain[J]. Journal of Food Quality, 2023, 2023(1): 4728840.

[12] 叶进,庞承杰,李晓欢,等. 基于区块链的供应链数据分级访问控制机制[J]. 电子科技大学学报,2022,51(3):408 - 415.
YE Jin, PANG Chengjie, LI Xiaohuan, et al. Blockchain-based supply chain data hierarchical access control mechanism [J]. Journal of University of Electronic Science and Technology of China,2022,51(3):408 - 415. (in Chinese)

[13] NAMANE S, BEN DHAOU I. Blockchain-based access control techniques for IoT applications [J]. Electronics, 2022, 11(14): 2225.

[14] 谢绒娜,李晖,史国振,等. 基于区块链的可溯源访问控制机制[J]. 通信学报,2020,41(12):82 - 93.
XIE Rongna, LI Hui, SHI Guozhen, et al. Blockchain-based access control mechanism for data traceability,2020,41(12): 82 - 93. (in Chinese)

[15] CHEN Y, MENG L, ZHOU H, et al. A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection[J]. Wireless Communications and Mobile Computing, 2021, 2021: 1 - 12.

[16] ABDI A I, EASSA F E, JAMBI K, et al. Hierarchical blockchain-based multi-chaincode access control for securing IoT

systems[J]. Electronics, 2022, 11(5): 711.
[17] SONG L, LI M, ZHU Z, et al. Attribute-based access control using smart contracts for the internet of things[J]. Procedia Computer Science, 2020, 174: 231 – 242.
[18] 张杰,许姗姗,袁凌云. 基于区块链与边缘计算的物联网访问控制模型[J]. 计算机应用,2022,42(7):2104 – 2111.
ZHANG Jie, XU Shanshan, YUAN Lingyun. Internet of Things access control model based on blockchain and edge computing [J]. Journal of Computer Applications,2022,42(7):2104 – 2111. (in Chinese)
[19] 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)
[20] HE G, LI C, SHU Y, et al. Fine-grained access control policy in blockchain-enabled edge computing[J]. Journal of Network and Computer Applications, 2024, 221: 103706.
[21] 佟兴,张召,金澈清,等. 面向端边云协同架构的区块链技术综述[J]. 计算机学报,2021,44(12):2345 – 2366.
TONG Xing, ZHANG Zhao, JIN Cheqing, et al. Blockchain for end-edge-cloud architecture: a survey [J]. Journal of Computers,2021,44(12):2345 – 2366. (in Chinese)
[22] ZHU Y, YU R, MA D, et al. Cryptographic attribute-based access control (ABAC) for secure decision making of dynamic policy with multiauthority attribute tokens[J]. IEEE Transactions on Reliability, 2019, 68(4): 1330 – 1346.
[23] GAO S, PIAO G, ZHU J, et al. Trustaccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5784 – 5798.
[24] 林莉,储振兴,刘子萌,等. 基于区块链的策略隐藏大数据访问控制方法[J]. 自动化学报,2023,49(5):1031 – 1049.
LIN Li, CHU Zhenxing, LIU Zimeng, et al. A policy-hidden big data access control method based on blockchain[J]. Journal of Automation, 2023,49 (5) : 1031 – 1049. (in Chinese)
[25] WU N, XU L, ZHU L. A blockchain based access control scheme with hidden policy and attribute[J]. Future Generation Computer Systems, 2023, 141: 186 – 196.
[26] MAESA D D F, LISI A, MORI P, et al. Self sovereign and blockchain based access control: supporting attributes privacy with zero knowledge[J]. Journal of Network and Computer Applications, 2023, 212: 103577.
[27] 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)
[28] 殷昱煜,叶炳跃,梁婷婷,等. 边缘计算场景下的多层区块链网络模型研究[J]. 计算机学报,2022,45(1):115 – 134.
YIN Yuyu, YE Bingyue, LIANG Tingting, et al. Research on multi-layer blockchain network model in edge computing scenario[J]. Journal of Computers,2022,45(1):115 – 134. (in Chinese)
[29] CHEN J, XIAO H, ZHENG Y, et al. DKSM: a decentralized kerberos secure service-management protocol for internet of things[J]. Internet of Things, 2023, 23: 100871.
[30] ZAIDI S Y A, SHAH M A, KHATTAK H A, et al. An attribute-based access control for IoT using blockchain and smart contracts[J]. Sustainability, 2021, 13(19): 10556.
[31] ZHANG Y, WEI X, CAO J, et al. Blockchain-enabled decentralized attribute-based access control with policy hiding for smart healthcare[J]. Journal of King Saud University—Computer and Information Sciences, 2022, 34(10): 8350 – 8361.
[32] KHADER D. Attribute based search in encrypted data: ABSE[C]// Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, 2014: 31 – 40.
[33] ZHANG K, ZHANG Y, LI Y, et al. A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing[J]. IEEE Internet of Things Journal, 2023,11(1):1685 – 1697.
[34] 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)