江苏农业学报(*Jiangsu J.of Agr.Sci.*),2024,40(4):740-752
http://jsnyxb.jaas.ac.cn

张德俊,饶　元. 农产品区块链多监管差分隐私共享模型设计[J]. 江苏农业学报,2024,40(4):740-752.
doi:10.3969/j.issn.1000-4440.2024.04.018

农产品区块链多监管差分隐私共享模型设计

张德俊[1,2,3]，　饶　元[1,2,3]
(1.安徽农业大学信息与计算机学院,安徽 合肥 230036；2.智慧农业技术与装备安徽省重点实验室,安徽 合肥 230036；3.农业农村部农业传感器重点实验室,安徽 合肥 230036)

摘要： 当前的农产品供应链系统,常由单个部门监管,存在单点故障、数据难以实时监管等问题,此外企业节点身份无明显区分,难以保证企业节点不会泄露企业隐私数据。本研究构建了农产品区块链多监管差分隐私共享架构,提出零知识证明身份验证算法,实现隐私数据对具有特定特征的监管部门的共享,降低了传统监管部门的压力。设计隐私数据分层规范,以基于密文策略的属性加密方案技术实现企业隐私数据差异化共享,降低了隐私数据泄露风险。在此基础上设计农产品区块链多监管差分隐私共享系统,并应用在某企业番茄供应链进行测试,测试结果表明,与现有监管模型相比,监管节点查询企业隐私数据时间缩短 7.1%,企业节点查询隐私数据时间缩短 23.9%。结果说明,本研究提出的方法能够在保证隐私安全的前提下提高监管效率。

关键词： 区块链；监管；零知识证明；密文策略属性基加密；隐私保护
中图分类号： TP309.2　　**文献标识码：** A　　**文章编号：** 1000-4440(2024)04-0740-13

Design of multi-regulation differential privacy sharing model for agricultural product blockchain

ZHANG De-jun[1,2,3]，　RAO Yuan[1,2,3]
(1.*School of Information and Computer Science*, *Anhui Agricultural University*, *Hefei* 230036, *China*; 2.*Anhui Provincial Key Laboratory of Smart Agricultural Technology and Equipment*, *Hefei* 230036, *China*; 3.*Key Laboratory of Agricultural Sensors*, *Ministry of Agriculture and Rural Affairs*, *Hefei* 230036, *China*)

Abstract: Current agricultural product supply chain system is often regulated by a single department, which leads to problems such as single point of failure and difficulties in real-time data supervision. Besides, the identities of enterprise nodes are not clearly distinguished, and it is difficult to ensure that enterprise nodes do not leak privacy data. To solve these challenges, a blockchain-based multi-supervisory differential privacy sharing architecture for agricultural products was developed. An identity verification algorithm using zero-knowledge proofs was proposed to share privacy data with specific supervisory departments, thereby reduced the pressure on traditional regulatory agencies. Privacy data were organized into hierarchical specifications, and enterprise privacy data differentiation sharing was achieved using ciphertext-policy attribute-based encryption (CP-ABE) technology, which effectively mitigated the risk of privacy data leakage. Based on the above work, a blockchain-based multi-supervisory differential privacy sharing system for agricultural products was designed and applied to a tomato supply chain of a certain company for test. Test results showed that compared to the existing regulatory model, the time for regulatory nodes to query enterprise privacy data reduced by 7.1%, and the time for enterprise nodes to query privacy data reduced by 23.9%. These findings demonstrate that the proposed

收稿日期:2023-04-01
基金项目:安徽省重点研发和开发计划项目(201904a06020056);安徽省自然科学基金项目(2008085MF203);安徽省财政农业科技成果转化项目(2022ZH014)
作者简介:张德俊(2001-),男,安徽阜阳人,本科,主要研究方向为农业物联网和区块链。(E-mail)2568446975@qq.com
通讯作者:饶　元,(E-mail) raoyuan@ahau.edu.cn

method can improve regulatory efficiency while ensuring privacy security.

Key words: blockchain; regulation; zero-knowledge proof; ciphertext policy attribute-based encryption; privacy protection

农产品是重要的食物来源,因此对其供应链各环节进行监管十分必要[1]。国家始终高度重视农产品质量安全问题[2],市场监管技术必不可少[3]。随着现代化农业的快速发展,农产品供应链已经由传统的单链式供应链拓展为集群式供应链。为适应实际监管需求,农产品供应链的监管应当由单链式供应链监管转变为集群式供应链监管[4]。当前时代背景下,隐私数据尤为重要,不论是个人还是企业,对保护隐私数据的需求都愈加强烈[5]。传统的农产品供应链系统中,企业链内部节点身份具有无差别性,可轻易获取企业隐私数据,企业无法保证链内节点不会获取隐私数据并泄露出去。因此,研究农产品区块链多监管差分隐私共享模型具有重要的现实意义。

近年来,国内外研究人员在农产品供应链监管与隐私保护方面开展了广泛的研究。于华竟等[4]、孙传恒等[6]在农产品供应链区块链上构造了单监督节点的监管模型。巫光福等[7]通过设计业务链和监管链的双链架构,以智能合约为基础,采用零知识证明方法分散监管节点权力,实现了可信监管。张新等[8]以智能合约为核心构建动态监管模型,使查验人员与监督部门相互监督,实现监管可信性。Azaria 等[9]利用区块链技术构造 MedRec(医疗记录)电子病历管理系统,以密钥作为隐私数据加密的手段。Zhang 等[10]为了提高隐私数据私密性,提出以身份为核心的隐私数据保护策略。刘彦松等[11]基于同态加密算法设计隐私数据保护方案,提高患者数据在链上的安全性。李莉等[12]、李雪莲等[13]基于区块链技术利用属性基加密、代理重加密等技术实现数据的隐私保护。然而,以上监管方式过于单一,未能根据农产品发展现状及需求作出多部门监管的改变,在隐私保护方面也没有考虑到不诚实节点获取隐私数据并泄露出去的风险,造成隐私泄露的问题。

本研究拟通过对农产品区块链业务流程以及流通过程中农产品关键数据进行分析,设计农产品区块链多监管差分隐私共享模型。对农产品业务流程进行分析后,提炼出企业公开数据与企业隐私数据,并对企业隐私数据进行分级加密存储,利用零知识证明身份验证算法实现企业隐私数据对相应特征的监管部门的共享,以降低传统监管部门的负担。利用基于密文策略的属性加密方案(CP-ABE)技术在企业链内部实现不同身份节点访问对应等级的企业隐私数据,降低企业隐私数据泄露的风险。以上述概念为基础,研发农产品区块链多监管差分隐私共享系统,并应用在某番茄供应链,最后对系统进行测试总结。

1 材料与方法

1.1 技术介绍

1.1.1 区块链 区块链是将不同区块按照时间顺序连接起来并可根据哈希指针逆向查询的链式数据结构,是由多方维护的分布式数据库,具有去中心化、不可篡改、可追溯的特点[14-16],确保了信息的安全性[17]。区块链内部以 Merkle 树作为交易数据的载体,使得交易具备防篡改性[18]。区块链上的各个节点按照规则和共识算法更新区块,实现多方监督,可有效降低交易成本[19]。

1.1.2 零知识证明 Goldwasser 等[20]提出了零知识交互式证明的概念。零知识证明指在证明方和验证方间相互交流,证明方在未得到外界任何信息提示的条件下,向验证方提供充足证据表明自己的确拥有某种权益,是一种具备较高安全性的密码学手段[21]。零知识证明具备 3 个性质:

(1)完备性。如果验证结果正确,验证者大概率接受证明者的结论。

(2)可靠性。如果验证结果不正确,验证者大概率放弃证明者的结论。

(3)零知识性。在证明过程中,证明者无法获取与结论相关的任何其他信息。

本研究中所使用的零知识证明身份的验证算法参数及含义如表 1 所示。

1.1.3 基于密文策略的属性加密方案 2005 年,在加密领域,Sahai 等[22]率先使用了模糊身份的概念,结合生物学特性,将其分解为多种身份信息,并与基于身份的加密策略相结合。Goyal 等[23]提出基于属

性的加密方案(Attribute-based encryption, ABE)。Bethencourt 等[24]在 ABE 基础上进一步提出了基于密文策略的属性加密方案。CP-ABE 采用一对多的加密方式[25],以属性描述用户特征,不同用户具备不同的属性特征,属性特征以访问结构作为载体,数据加密方具备制定密文访问结构的权力,当用户获取密文进行解密时,满足访问结构属性要求的用户才可解密密文[26-28]。

表 1 零知识证明身份的验证算法涉及的参数及含义

Table 1 Parameters and related meanings involved in the authentication algorithm based on zero knowledge proof

参数	含义
sk	根据 Merkle 树生成的监管部门标志
CPK	企业公钥
CSK	企业私钥
I	企业服务器节点数
R	企业服务器生成的随机数集合
T	企业服务器生成的向量集合
r_s	监管部门生成的随机数
p	根据 sk 和 r_s 生成的值
ER	加密后的 r_s
EP	加密后的 p
E	r_s 和 p 的哈希值
EM	根据 E、r_s 和 p 生成的密文
S_i	根据向量集 T 生成的向量集
$E_{i\alpha}$	验证向量

Waters[29]在 Bethencourt 等[24]的理论基础上提出一种 CP-ABE 访问控制方案,其过程包含以下 4 个步骤:

(1) 初始化算法 $(PK, MK) \leftarrow Setup(1\lambda)$:接受一个安全参数 λ。输出公钥(PK)和系统主密钥(MK)。

(2) 密钥生成算法 $SK \leftarrow KenGen(MK, S)$:输入主密钥($MK$)与用于标志密钥身份的属性集合 S,输出用户私钥(SK)。

(3) 加密算法 $CT \leftarrow Encrypt(PK, M, T)$:将公钥($PK$)、明文($M$)和明文访问结构($T$)作为输入参数,对明文($M$)进行加密,生成密文($CT$)。

(4) 解密算法 $M \leftarrow Decrypt(PK, CT, SK)$:密文($CT$)、公钥($PK$)以及私钥($SK$)作为输入参数。私钥($SK$)由属性集合 S 生成,若 S 能满足访问结构(T),则可成功解密 CT 并返回消息(M)。

本研究中使用的 CP-ABE 参数如表 2 所示。

表 2 基于密文策略的属性加密方案(CP-ABE)方案涉及的参数

Table 2 Parameters involved in ciphertext-policy attribute-based encryption (CP-ABE) scheme

参数	含义
λ	系统安全参数
p、q	随机大素数
g	生成元
e	双线性映射
MK	系统主密钥
PK	公钥
SK	用户私钥
S	用户属性集
M	原始数据
CT	加密密文
T	加密访问树
s	秘密值

CP-ABE:基于密文策略的属性加密。

1.2 农产品区块链多监管差分隐私共享模型

1.2.1 业务流程及关键信息分类 在整个农产品供应链中,参与主体包括种植个体户、仓储商、加工商、运输商、销售商、消费者。农产品从生产到销售的路线跨度长,参与角色多,使得农产品信息存在多源异构的特点,这些信息无法全部向外界暴露,因此需要划分公开数据、隐私数据的界限。企业上下游之间部分信息需要进行逆向回溯查询,然而企业之间缺乏统一的数据格式,导致上下游企业间存在信息壁垒,因此需要规范企业的数据。为了解决上述问题,保证农产品供应链企业信息隐私性,根据农产品供应链实际情况和需求,本研究将农产品供应链分为生产、仓储、加工、运输、销售五大环节,对上述环节进行数据分析后,提取出面向大众的公开数据和面向企业内部的隐私数据,分类如表 3 所示。

企业在运营的过程中,产生大量隐私数据,企业管理人员职位不同,相关人员对隐私数据的掌握程度也发生变化,根据私密程度,隐私数据可划分为不同的层次。本研究根据实际情况,将企业隐私数据划分为 3 个等级(表 4)。

1.2.2 农产品区块链多监管差分隐私架构 现有

的农产品供应链架构中,企业内部的区块链节点身份无特殊限制,使得企业隐私数据暴露在所有节点下,难以保证企业隐私数据不被泄露。在监管方面,传统供应链架构由单个监管部门监管企业链隐私数据,没有为监管节点划分具体的监管范围,容易出现单点故障、企业隐私数据泄露等问题[30]。为了解决上述问题,考虑到监管部门和企业隐私数据的安全性,并结合农产品的现实应用场景,以区块链技术为核心构建农产品区块链多监管差分隐私共享架构(图 1)。

表 3 农产品供应链关键信息分类

Table 3 Key information classification of agricultural product supply chain

数据类型	生产	仓储	加工	运输	销售
公开数据	产品名称、生产方式、生产时间、肥料使用数据、生产企业信息、灌溉量	产品入库时间、产品出库时间、仓储方式、仓储许可证、仓储环境数据	加工流程、加工市场、加工原料、加工设备、加工日期、加工负责人	运输时间、运输方式、运输路线、工具数量、运输环境数据、运输许可证	进货时间、销售价格、支付方式、销售许可证、产品批次号
隐私数据	员工身份信息、客户信息、财务信息、生产计划和进度、生产监控数据、生产设备信息、农产品生产数据、市场营销数据、农药使用情况、网络日志访问数据、生产地数据	员工身份信息、客户信息、财务信息、仓储计划和进度、仓储监控数据、仓储设备信息、仓储产品数据、产品质量检测数据、产品库存量、网络日志访问数据、仓储地数据	员工身份信息、客户信息、财务信息、加工计划和进度、加工监控数据、加工设备信息、农产品加工数据、市场营销数据、加工工序、网络日志访问数据、加工地数据	员工身份信息、客户信息、财务信息、运输计划和进度、运输车辆全球定位系统(GPS)数据、运输设备信息、运输货物信息、市场营销数据、运输环节信息、网络日志访问数据、运输地数据	员工身份信息、客户信息、顾客个人信息、财务信息、销售计划和进度、销售设备信息、农产品销售数据、市场营销数据、采购信息、网络日志访问数据、销售地数据

表 4 企业多级别隐私数据分类

Table 4 Multi-level privacy data classification for enterprise

私密等级	生产	仓储	加工	运输	销售
1	员工身份信息、客户信息、财务信息、生产计划和进度、生产监控数据	员工身份信息、客户信息、财务信息、仓储计划和进度、仓储监控数据	员工身份信息、客户信息、财务信息、加工计划和进度、加工监控数据	员工身份信息、客户信息、财务信息、运输计划和进度、运输车辆全球定位系统(GPS)数据	员工身份信息、客户信息、顾客个人信息、财务信息、销售计划和进度
2	生产设备信息、农产品生产数据、市场营销数据、农药使用情况	仓储设备信息、仓储产品数据、产品质量检测数据、产品库存量	加工设备信息、农产品加工数据、市场营销数据、加工工序	运输设备信息、运输货物信息、市场营销数据、运输环节信息	销售设备信息、农产品销售数据、市场营销数据、采购信息
3	网络日志访问数据、生产地数据	网络日志访问数据、仓储地数据	网络日志访问数据、加工地数据	网络日志访问数据、运输地数据	网络日志访问数据、销售地数据

在农产品区块链多监管差分隐私架构中,企业链在监管部门的监督批准下进行搭建,由监管部门共同构建监管区块链。各个企业完成相应的工作后,产生大量的原始数据,企业对数据进行整理后,根据企业客户端节点调用数据分离智能合约,得到隐私数据与公开数据,合约内部调用隐私数据分级加密合约,将分离后的隐私数据划分为多个级别并分别进行加密,随后对加密隐私数据执行上链操作,企业链节点通过 Raft 共识机制达成共识后,完成隐私数据上链操作,为压缩数据量,系统将公开数据上传至 IPFS(星际文件系统)并得到哈希值,随后将哈希值上传至企业公开链,最后同步更新区块链各节点的账本状态。企业私有链为每个参与节点设置身份属性,不同的身份属性可访问不同级别的隐私数据。监管部门设置负责人,负责人负责设置监管策略,企业可通过监管部门预先设置的接口,跨链获取对应监管部门的监管策略,企业按照相应策略对数据进行处理。数据上链后,监管部门人员依据监管策略对相应企业的公开数据、隐私数据进行审查,由于监管部门分散执行监管任务,因此在出现数据非法的情况下,能够更迅速地追溯到问题企业及部门,且多监管的形式避免了单点故障,减轻了传统架构中监管部门的负担,同时可降低企业隐私数据泄露的风险。

1.2.3 *基于 CP-ABE 的隐私数据访问* 为保证企业内部隐私数据的安全性,依据上述企业隐私数据等级划分标准,利用 CP-ABE 算法,实现不同企业管理角

色对不同等级隐私数据的共享。在算法执行过程中，由企业链的 CA（证书颁发机构）承担可信授权中心的角色，可信授权中心负责生成多种参数。系统主密钥（MK）和公钥（PK）由企业授权中心负责生成，上述过程完成后，企业授权中心将公钥发布到企业链，企业数据加密人员获取公钥后，结合公钥和访问控制树加密企业隐私数据，随后将加密数据上传到企业链。企业链内部 CP-ABE 算法包括如下四大流程：

（1）初始化算法：$(PK,MK)\leftarrow Setup(1^{\lambda})$。初始化算法的目的是生成系统所需的公钥（$PK$）与主密钥（$MK$），该过程由企业可信授权中心执行，算法以安全参数1λ作为输入参数。首先，随机选取 2 个大素数 p、q。G_0、G_1为 p 阶乘法循环群，Z_q^* 为 q 阶循环群，双线性映射 $e:G_0\times G_0\rightarrow G_1$，$g$ 为G_0的生成元。随机选取 2 个参数 α、β，$\alpha,\beta\in Z_q^*$，产生公钥（PK）和主密钥（MK）。

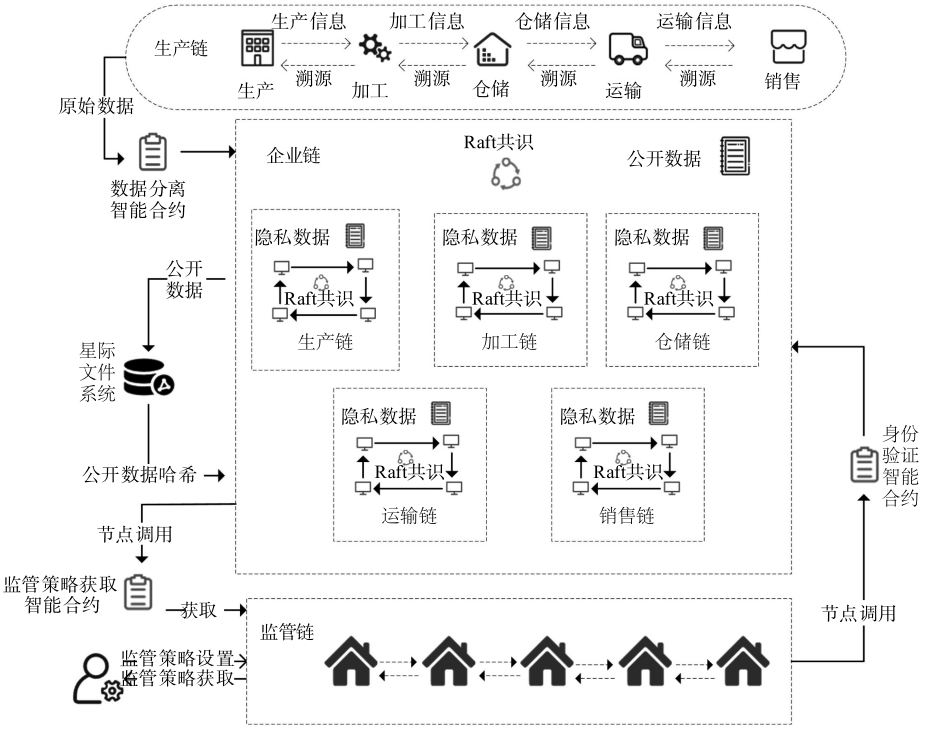


图 1 农产品区块链多监管差分隐私共享模型架构

Fig.1 Architecture of a multi-regulation differential privacy sharing model for agricultural product blockchain

$PK=[G_0,g,g^{\beta},e(g,g)^{\alpha}]$，$MK=(\beta,g^{\alpha})$

公钥（PK）向企业链内部节点公开，主密钥（MK）保存在企业可信授权中心。

（2）密钥生成：$SK\leftarrow KenGen(MK,PK,S)$。密钥生成过程由可信授权中心执行，企业节点可自主向可信授权中心申请密钥，该过程接收 3 个参数，分别为主密钥（MK）、公钥（PK）、企业管理人员属性集（$\boldsymbol{S}$），算法输出与管理人员属性集合相关联的私钥（SK）。算法具体流程为：

可信授权中心随机选取 $\gamma\in Z_q^*$，对于属性集中每个属性 $j\in S$ 选取 1 个随机数 $\gamma_j\in Z_q^*$，计算 SK：

$$SK=\{D=g^{(\alpha+\gamma)/\beta},\forall j\in S:D_j=g^{\gamma}\cdot H(j)^{\gamma_j},D'_j=g^{\gamma_j}\}$$

式中，D_j、D'_j为用户属性集合的生成参数，D 为用户身份验证参数。

（3）加密算法：$CT\leftarrow Encrypt(PK,M,T)$。企业链节点首先根据企业隐私数据访问策略生成满足访问策略的访问树（T）。首先为访问树（T）的每一个节点产生一个多项式 q_x，从访问树的根节点 R 开始由上而下为每一个节点选择多项式。阶数（d_x）和门限值（k_x）的关系定义为：$d_x=k_x-1$。然后从根节点 R 开始，选择随机数 s，$s\in Z_q^*$，s 为秘密值。针对根节点 R，有 $q_R(0)=s$，其余多项式 q_R 在其他 d_R 个点的值随机选取。对于继续向下的节点 x，有 $q_x(0)=q_{parent(x)}[index(x)]$，同样的，其他$d_x$个点的

值也是随机选取。

令 Y 为访问树 T 的所有叶子节点的集合,CT 为访问结构(T)的密文。算法如下:

$$CT=\left\{\begin{matrix}T,C'=M\cdot e(g,g)^{\alpha\cdot s},C=g^{\beta s},\\ \forall y\in Y:C_y=g^{q_y(0)},C'_y=H[attr(y)]^{q_y(0)}\end{matrix}\right\}$$

式中,C_y、C'_y为访问树节点生成参数,C'为明文加密参数,C 为加密辅助参数,m 为明文,y 为用户属性集合(Y)中的子属性。

(4) 解密算法:$M\leftarrow Decrypt(CT,SK)$。解密算法内嵌在智能合约供企业链节点调用,智能合约内部封装算法具体逻辑。节点将密文(CT) 和私钥(SK)作为输入参数, 若私钥(SK) 内嵌的属性集合满足访问树(T),则可进行解密运算。解密运算过程中不断递归调用 $DecryptNode(CT,SK,x)$,若 x 为叶子节点,则进行如下运算:

$$DecryptNode\ (\ CT,\ SK,\ x\ )=\frac{e[D_{att(x)},C_x]}{e(D_x,C_x)}=e(g,g)^{\gamma q_x(0)}$$

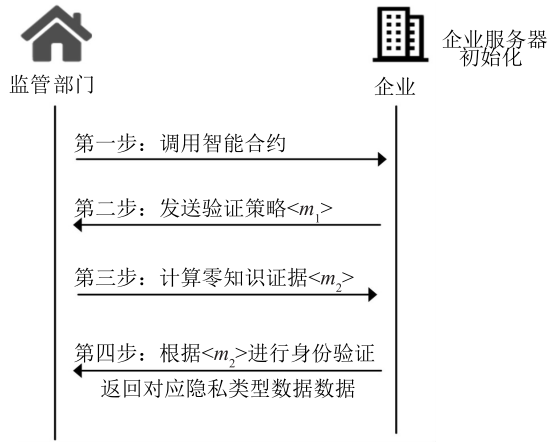
若不是叶子节点,则对其孩子节点(cd)递归调用函数 $DecryptNode(CT,SK,x)$,并返回F_{cd}。若用户属性集满足该节点,则可通过拉格朗日多项式对分发到节点 x 的秘密值进行重构,并得到返回值 $F_{cd}=e(g,g)^{rq_x(0)}$。

解密最后在根节点 R 开始调用函数 $DecryptNode(CT,SK,x)$,若用户属性集与访问树 T 匹配,函数返回值即为秘密值(s) ,获取秘密值(s)后,利用如下公式完成信息 M 的解密:

$$\frac{C'}{\left[\frac{e(C,D)}{e(g,g)^{\gamma s}}\right]}=\frac{Me(g,g)^{s}}{\frac{e[g^{\beta s},g^{\frac{(\alpha+\gamma)}{\beta}}]}{e(g,g)^{\gamma s}}}=M$$

1.2.4 基于零知识证明的监管部门身份验证 传统监管模式存在单点故障、企业隐私数据易泄露等问题,多监管模式则可以有效避免上述问题。为了实现多监管模式,在身份验证算法上需要作出相应的改进,本研究采用基于零知识证明的身份验证算法。

监管部门为企业制定监管策略,并以智能合约形式提供策略获取接口供企业调用。策略内容以默克尔树的形式呈现,且默克尔树的叶子节点包含 1 个时间戳,sk 为对应隐私数据监管属性的默克尔树的根的哈希值,用于标志监管者的身份,企业链节点可调用智能合约获取监管策略,并将监管策略进行链上存储,监管策略包括各隐私数据类型及对应的监管部门 sk 值。算法流程如图 2 所示。



m_1、m_2 为服务器生成的素数。

图 2 零知识证明身份验证算法流程

Fig.2 Flowchart of zero-knowledge proof identity authentication algorithm

首先,企业内部服务器生成素数对(m_1,n_1)、(m_2,n_2) ,计算$Num_1=m_1\times n_1$,$Num_2=m_2\times n_2$,随后企业服务器在本地产生公钥和私钥对,分别标记为 CPK 和 CSK。当监管部门需要查询企业隐私数据时,由监管部门调用企业提供的监管智能合约接口进行算法初始化,算法描述如下:

(1)随机数生成。假设企业内部含 I 个服务器节点,每个服务器节点生成 1 个 n 位的二进制随机数r_i,$r_i\in Z^*_{Num_1}$,$i\in I=\{1,2,3,\ldots,I\}$ 和向量 t_i,$t_i=[t_{i1},t_{i2},\ldots,t_{in}]$,$n$ 为向量的元素数,将所有的随机数和向量进行汇聚,构成$m_1=(R,T,CPK)$,随后返回m_1,其中 $R=\{r_1,r_2,r_3,\ldots,r_I\}$,$T=\{t_1,t_2,t_3,\ldots,t_I\}$。企业链节点将$m_1$返回给监督节点。

(2)零知识证据计算。监管部门节点获取m_1后,开始计算零知识证据。首先,监管部门生成随机数r_s,$r_s\in Z^*_{Num_2}$,根据公式:$p=sk\oplus r_s\oplus r_i(i\in[1,I])$计算出 1 个满足 $p\in Z^*_{Num_1}$条件的值。随后利用企业公钥 CPK 对r_s和 p 进行加密,得到 ER、EP。

$$ER=Encrypt(CPK,r_s)$$

$$EP=Encrypt(CPK,p)$$

加密完成后,对r_s、p 进行哈希值的计算:$E=H(r_s||p)$,并对 E 进行加密,加密后的结果为 EM ,加密公式为:

$$EM=(E^2\bmod Num_2)\oplus r_s\oplus p$$

获取企业服务器生成的向量 T 后,根据 T 内的

向量生成对应的向量集$S_i=[S_1,S_2,\dots,S_n]$,向量集 S 的元素和向量集 T 的元素关系为:

$$S_{i\alpha}=r_s pE^{t_{i\alpha}},i\in[1,I],\alpha\in[1,n]$$

运算结束后,把上述生成的向量汇集为向量集S_i。将有关数据生成为$m_2=(ER,EP,EM,S_i)$并最终返回给企业节点。

(3)身份验证。企业链节点根据监管节点传输来的消息(m_2)对监管节点身份进行验证。首先提取m_2中的数据 ER、EP ,利用企业的私钥完成解密,获取r_s、p。

$$r_s=Decode(CSK,ER)$$

$$p=Decode(CSK,EP)$$

随后,按照如下公式计算身份验证向量($E_{i\alpha}$),其中 $i\in[1,I]$,$\alpha\in[1,n]$。

$$E_{i\alpha}=(S_{i\alpha})^2 \bmod Num_2-r_s{}^2p^2(EM\oplus r_s\oplus p)^{t_{i\alpha}} \bmod Num_2$$

计算完成后,得到向量集 $\boldsymbol{E}=[\boldsymbol{E}_1,\boldsymbol{E}_2,\dots,\boldsymbol{E}_I]$,$i\in[1,I]$,随后对向量集进行判断,若监督部门身份合法,则向量集 $\boldsymbol{E}$ 的每个向量$\boldsymbol{E}_i$应当等于 0,否则说明监督节点的身份不合法。

完成监督节点的身份验证后,若身份合法,则利用公式 $sk=p\oplus r_s\oplus r_i(i\in[1,I])$计算出监督节点的 sk 值,由于最初企业链内获取并存储了监管策略的 sk 值,因此可在企业链上查找是否存在该 sk 值以及该 sk 值对应的监管部门所要监管的隐私数据类型,完成上述步骤后,最终将对应隐私数据返回给监督节点。

1.2.5 智能合约设计 智能合约可由区块链节点调用,在条件满足的情况下,智能合约可自动执行预先写入的业务逻辑,进而得到输出结果。本研究通过智能合约实现公开数据与隐私数据的划分、隐私数据上链、监管策略设置、监管策略获取、身份验证等功能。

智能合约主要功能及业务处理逻辑如表 5 所示。

农产品区块链多监管差分隐私共享模型包含多条企业链与一条监管链,企业链与监管链均设置智能合约,可通过调用智能合约接口实现企业链与监管链之间的数据交互。下面以加工环节为例介绍溯源数据加密上链的合约逻辑,以监管部门身份验证为例介绍身份验证的合约逻辑。

在加工环节,企业对产品进行处理时,产生大量原始数据,对于原始数据,需要将其划分为公开数据与隐私数据,公开数据上传至 IPFS(星际文件系统)获取哈希值,将哈希值上传至企业公开链,隐私数据则利用 CP-ABE 技术进行分级加密存储,数据处理流程如算法 1 所示:

算法 1:加工环节溯源数据写入算法。

输入:加工节点(processPeer),加工数据(processData),环节标志(ID)。

输出:操作结果(resultMsg),区块信息(blockMsg),错误信息(errorMsg)。

判断节点身份与环节(ID)的正确性:

If(isNodeIdLegal (processPeer) &&isLinkIdLegal (Id))

根据环节(ID)选择加工智能合约,判断数据类型和内容合法性:

If (isDataTypeLegal (processData) &&isDataContentLegal(processData))

划分公开数据与隐私数据:

For(item In processData)

If(isPrivateDataOfProcess(item))

privateDataArrayOfProcess.put(item)

Else

publicDataArrayOfProcess.put(item)

//调用隐私数据等级划分合约:

For(item In privateDataArrayOfProcess)

将隐私数据进行等级划分,利用 CP-ABE 对隐私数据分别加密上链。

//调用公开数据智能合约。

将公开数据上传至星际文件系统获取哈希值,并将哈希值上链,通知监管部门数据存储完成;

Return resultMsg, blockMsg;

Else

Return errorMsg;

Else

输出节点身份错误信息;

Return errorMsg;

监管部门身份验证算法在监管节点获取企业隐私数据时执行,算法以零知识证明为基础实现监管部门点对点获取企业隐私数据,并根据最终计算结果判断监管部门身份是否符合要求,身份验证流程如算法 2 所示:

算法 2:监管部门身份验证算法。

输入:监管节点(supervisoryPeer),消息(m_2)。

输出:消息(m_1),隐私数据(privateMsg),错误信息(errorMsg)。

判断身份节点合法性及消息m_2是否为空:

If (isNodeIdLegal (supervisoryPeer) &&isNull (m_2))

//说明此时节点第一次调用合约,进行算法初始化

企业服务器节点计算消息m_1;

Return m_1;

Else If(isNodeIdLegal (supervisoryPeer) && isNotNull(m_2))

//此时监管节点完成了零知识证据的计算

根据m_2计算向量集 $\boldsymbol{E}$

If(向量集 $\boldsymbol{E}$ 元素不为 0)

输出监督节点无查询对应隐私数据的资格。

Return errorMsg;

Else

计算 sk,链上查询 sk 对应的隐私数据类型,再查询对应类型的隐私数据。

Return privateMsg;

Else

输出节点身份异常;

Return errorMsg;

表 5 智能合约设计

Table 5 Design for smart contract

合约功能	合约名	业务逻辑描述
溯源数据写入	生产智能合约	判断生产节点身份的正确性,验证生产数据格式,划分公开数据与隐私数据
	加工智能合约	判断加工节点身份的正确性,验证加工数据格式,划分公开数据与隐私数据
	仓储智能合约	判断仓储节点身份的正确性,验证仓储数据格式,划分公开数据与隐私数据
	销售智能合约	判断销售节点身份的正确性,验证销售数据格式,划分公开数据与隐私数据
	运输智能合约	判断运输节点身份的正确性,验证运输数据格式,划分公开数据与隐私数据
	隐私数据智能合约	将隐私数据分级,分别加密存储上链
	公开数据智能合约	将公开数据存入星际文件系统,并将得到的哈希值存入企业链账本
监管节点身份验证	身份验证智能合约	由监管节点调用,合约内部通过零知识证明确定监管者身份
获取监管策略	策略获取智能合约	通过生成默克尔树的形式,返回监督部门对该企业的监督策略
设置监管策略	策略设置智能合约	监管部门管理员可以采用默克尔树的形式对监管策略进行设置

2 结果与分析

2.1 系统实现

本研究采用联盟链技术构建系统,在保障安全的前提下,以通道技术为基础建立多条企业链并结合加密算法保证隐私数据的安全性和访问权限,由智能合约保证监管策略的有效性和可控性,实现监管系统的数据安全。系统整体架构可分为 4 部分:应用层、接口层、服务层、存储层。具体结构如图 3 所示。

应用层通过传感器、摄像头、北斗定位装置等物联网设备进行数据采集,确保数据源头的真实性、可信性,并为企业提供将数据分离为公开数据和隐私数据等的功能。接口层为企业链提供数据写入、查询与监管策略获取操作接口,为监管链提供监管策略设置接口。服务层负责对数据类型进行逻辑判断处理以及数据加密、解密等操作,为接口层提供服务。存储层负责存储加密的隐私数据、企业节点获取的密钥以及企业公开数据,公开数据存储在星际文件系统中,其他数据存储在状态数据库 LevelDB 中,对于监管链,则主要存储监管策略以及各监管者的身份标志。

2.2 测试环境

农产品区块链多监管差分隐私系统以 Hyperledger Fabric 为基础进行构建。测试环境为 CenterOS7.5、Docker18.09、fabric-sdk-node2.2。虚拟机配置:内存大小为 64 G,处理器为 32 核,硬盘大小为 100 G,带宽为 150 Mb/s。本试验以番茄质量溯源平台为例,采用 Raft 共识机制完成共识,利用 IPFS、LevelDB 进行数据存储。

2.3 应用案例分析

将农产品区块链多监管差分隐私共享系统应用在安徽安庆某农产品公司的番茄供应链上,该番茄供应链包含生产、加工、仓储、运输、销售 5 个环节,供应链模式如图 4 所示。有关该番茄供应链的溯源环节和部分溯源信息如图 5、图 6 所示。如果采用

传统的溯源区块链架构,则容易出现隐私数据泄露、监管节点单点故障等问题,因此采用本研究系统针对上述问题进行优化。

企业可信授权中心的系统主密钥及公钥生成结果如图 7 所示。企业节点可将自身属性作为输入参数向可信授权中心申请与节点属性相关的私钥,以某企业人力资源部招聘与培训科的科长为例,对应的私钥生成情况如图 8 所示。

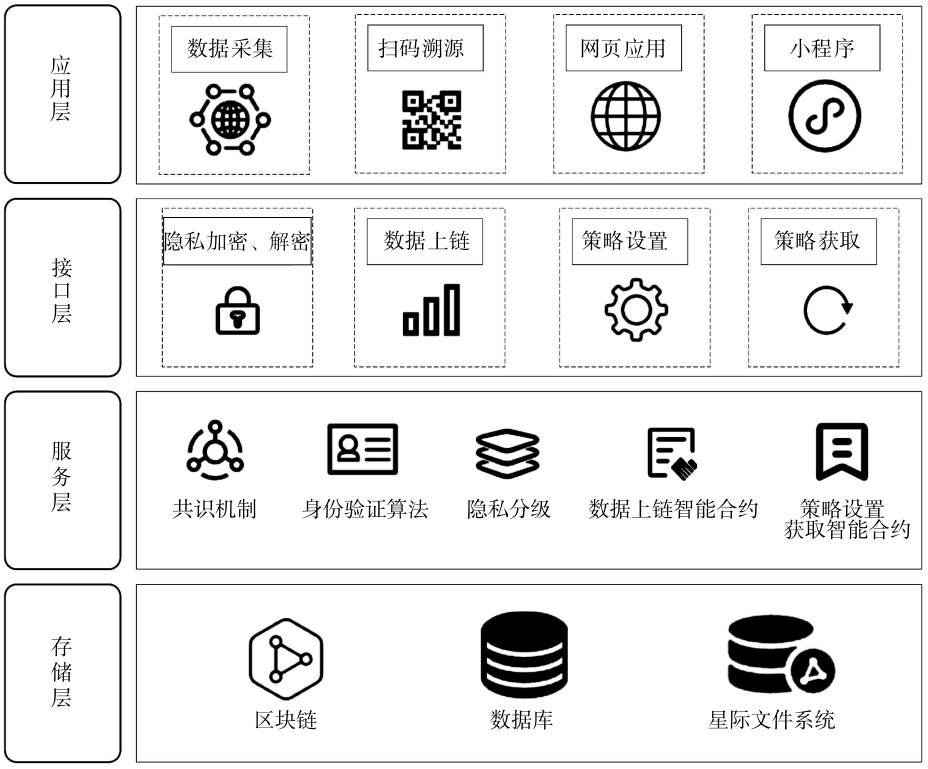


图 3 系统架构

Fig.3 System architecture diagram

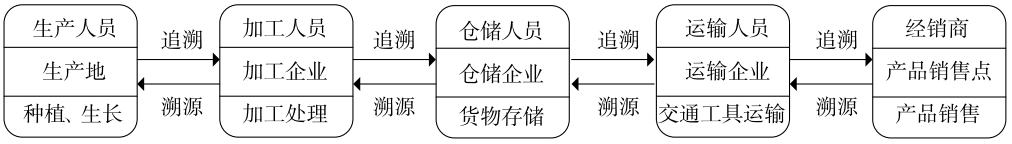


图 4 番茄供应链模式

Fig.4 Supply chain model for tomato

对于企业多级隐私数据,需要构造不同的访问树分别进行加密,以一级隐私数据为例,对访问树进行构建,如图 9 所示,ID 用于标志访问树的节点,Type 用于区分是否为叶子节点,若为叶子节点,则节点以 *attributeName* 标志叶子节点的属性值,*index* 为节点的索引值,*threshold* 表示访问树的阈值。当运输企业节点上传运输编号为 transport086 的隐私数据时,需要根据上述构建造的访问树对数据进行加密,随后执行上链操作,数据加密及上链结果如图 10 所示。在数据加密上链后,企业节点可将包含自身属性的私钥作为输入对加密数据进行解密,满足访问树结构且能达到阈值的条件才可成功解密密文,解密流程如图 11 所示。

2.4 区块链网络性能分析

农产品区块链多监管差分隐私共享模型利用 CP-ABE 技术实现企业不同隐私数据的差异化共享,使用零知识证明身份验证算法实现企业隐私数据对于具有特定特征的监管部门的共享,为验证模型的实际运行效率,采用性能测试软件 Caliper 对企业链公开数据与隐私数据的上传效率进行测试,对企业链节点、监管链节点查询企业隐私数据的效率进行测试。

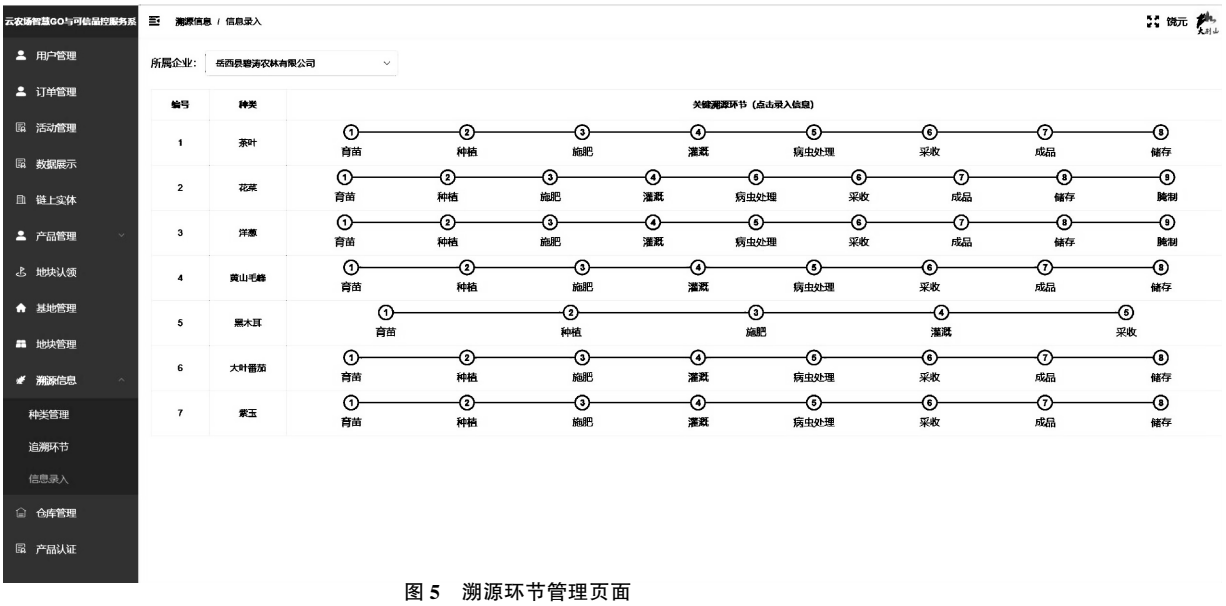


图 5 溯源环节管理页面

Fig.5 Management page for traceability link

图 6 溯源环节信息

Fig.6 Information of traceability link

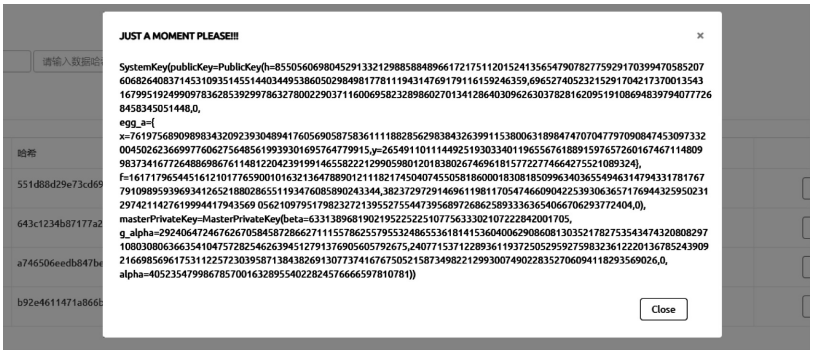


图 7 系统密钥生成结果

Fig.7 System key generation result

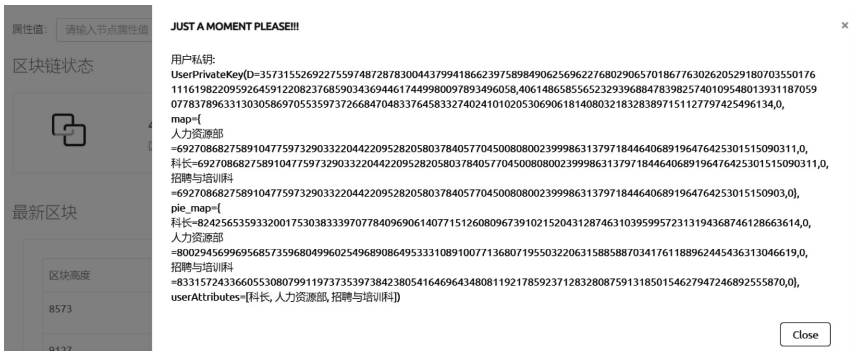


图 8 用户私钥生成结果

Fig.8 User private key generation result

图 9 访问树数据结构

Fig.9 Data structure for access tree

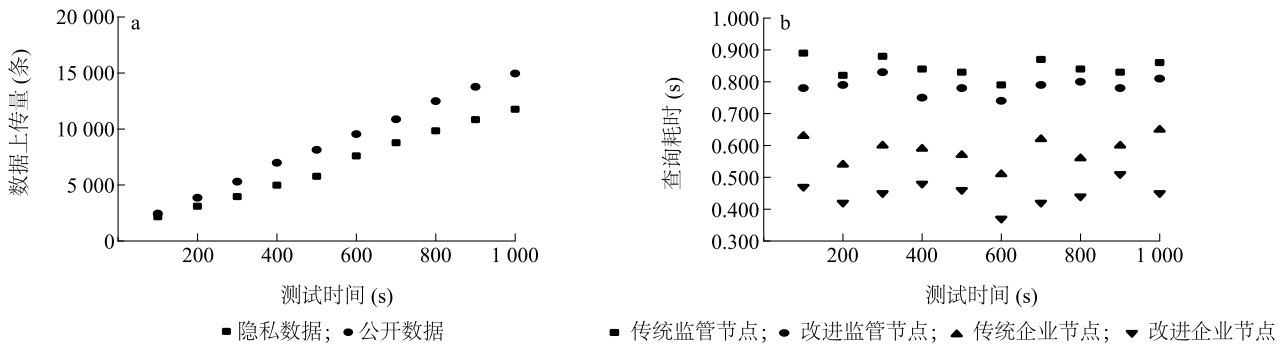
图 10 原始数据加密流程

Fig.10 Encryption process for original data

在试验过程中,在相同环境下执行相同的操作, 操作所需时间会在一定范围内上下浮动,为降低该

图 11 加密数据解密流程

Fig.11 Decryption process for encrypted data



a:写入效率;b:查询效率。

图 12 数据上传与查询效率测试

Fig.12 Data upload and query efficiency test

影响带来的误差,对每组数据各执行 10 次相同操作,取其平均值作为最终结果。通过上述方法对模型进行测试,并对试验结果进行相关性分析。

由图 12a 可见,随着测试时间的延长,企业公开数据与隐私数据的上传数据量基本呈线性增长,相同时间下,公开数据上传的数据量比隐私数据上传量大。

针对查询性能,为提高数据的准确性,采用 1 000次查询次数作为测试指标,同时为降低最终查询结果的误差,每测试 100 次对结果取平均值,将平均值作为最终结果进行展示。以监管节点查询企业隐私数据所消耗的时间作为分析指标,结果如图 12b 所示,传统监管节点的平均查询时间为 0.845 s,改进监管节点的平均查询时间为 0.785 s,传统企业节点的平均查询时间为 0.587 s,改进企业节点的平均查询时间为 0.447 s。与传统监管节点相比,改进监管节点查询隐私数据时间缩短 7.1%;与传统企业节点相比,改进企业节点查询隐私数据时间缩短 23.9%。试验结果表明,该系统能够适应农产品供应链使用效率方面的实际应用需求。

3 结 论

本研究以农产品区块链多监管差分隐私共享模型为基础,结合 Hyperledger Fabric(超级账本结构)构建农产品区块链多监管差分隐私共享系统,在某番茄供应链进行应用测试后,得出以下结论:

(1)在农产品区块链多监管差分隐私共享架构中,将数据源中公开数据与隐私数据分离,公开数据上传至星际文件系统,隐私数据则利用 CP-ABE 进行分级加密存储,使得企业内部节点差异化共享隐私数据,降低了传统区块链架构节点身份单一造成隐私数据泄露的风险。最终通过测试发现,相较于传统供应链系统,此模型企业节点查询隐私数据时间缩短 23.9%,能够满足企业的实际需求。

(2)设计企业隐私数据多监管机制,利用零知识证明身份验证算法,能够实现企业隐私数据对具有特

定特征的监管部门的共享,解决以往单部门监管存在的权力集中、单点故障等问题。最终测试结果表明,相较于传统区块链监管模型,此模型监管节点的隐私数据查询时间缩短 7.1%,监管效率明显提升。

(3) 将农产品区块链多监管差分隐私共享系统应用在某番茄供应链后发现,该系统可有效降低隐私数据易泄露的风险与监管部门的负担,提升了企业数据安全性,可为农产品供应链系统的设计提供参考。

参考文献:

[1] MIRABELLI G, SOLINA V. Blockchain and agricultural supply chains traceability: research trends and future challenges[J]. Procedia Manufacturing, 2020, 42: 414-421.

[2] VANGALA A, DAS A K, KUMAR N, et al. Smart secure sensing for IoT-based agriculture: blockchain perspective[J]. IEEE Sensors Journal, 2021, 21(16): 17591-17607.

[3] TENG Y, CHEN X L, YU Z G, et al. Research on the evolutionary Decision-Making behavior among the government, farmers, and consumers: based on the quality and safety of agricultural products [J]. IEEE Access, 2021, 9: 73747-73756.

[4] 于华竟,徐大明,罗 娜,等. 杂粮供应链区块链多链追溯监管模型设计[J]. 农业工程学报,2021,37(20):323-332.

[5] 钱文君,沈晴霓,吴鹏飞,等. 大数据计算环境下的隐私保护技术研究进展[J]. 计算机学报,2022,45(4):669-701.

[6] 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.

[7] 巫光福,余 攀,王柯柯. 双链式区块链交易监管研究[J]. 计算机工程与应用,2020,56(23):116-123.

[8] 张 新,彭祥贞,许继平,等. 基于区块链智能合约的稻米供应链动态监管模型[J]. 农业机械学报,2022,53(1):370-382.

[9] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management [C]. Vienna, Austria: IEEE, 2016: 25-30.

[10] ZHANG M, WANG S, ZHANG P, et al. Protecting data privacy for permissioned blockchains using identity-based encryption [C]. Chengdu, China: IEEE, 2019: 602-605.

[11] 刘彦松,夏 琦,李 柱,等. 基于区块链的链上数据安全共享体系研究[J]. 大数据,2020,6(5):92-105.

[12] 李 莉,曾庆贤,文义红,等. 基于区块链与代理重加密的数据共享方案[J]. 信息网络安全,2020(8):16-24.

[13] 李雪莲,张夏川,高军涛,等. 支持属性和代理重加密的区块链数据共享方案[J]. 西安电子科技大学学报(自然科学版),2022,49(1):1-16.

[14] 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.

[15] KASSANUK T, PHASINAM K. Design of blockchain based smart agriculture framework to ensure safety and security[J]. Materials Today: Proceedings, 2022, 51: 2313-2316.

[16] 钱建平,吴文斌,杨 鹏. 新一代信息技术对农产品追溯系统智能化影响的综述[J]. 农业工程学报,2020,36(5):182-191.

[17] 祝烈煌,董 慧,沈 蒙. 区块链交易数据隐私保护机制[J]. 大数据,2018,4(1):46-56.

[18] 祝烈煌,高 峰,沈 蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展,2017,54(10):2170-2186.

[19] 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.

[20] GOLDWASSER S, MICALI S. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989, 18(1): 186.

[21] BEN-SASSON E, CHIESA A, GENKIN D, et al. SNARKs for C: verifying program executions succinctly and in zero knowledge [C]. Berlin, Heidelberg: Springer, 2013: 90-108.

[22] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]. Berlin, Heidelberg: Springer, 2005: 457-473.

[23] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. New York, USA: ACM, 2006: 89-98.

[24] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]. Berkeley, CA, USA: IEEE, 2007: 321-334.

[25] 邱云翔,张红霞,曹 琪,等. 基于 CP-ABE 算法的区块链数据访问控制方案[J]. 网络与信息安全学报,2020,6(3):88-98.

[26] 孙国梓,董 宇,李 云. 基于 CP-ABE 算法的云存储数据访问控制[J]. 通信学报,2011,32(7):146-152.

[27] 芦效峰,付淞兵. 属性基加密和区块链结合的可信数据访问控制方案[J]. 信息网络安全,2021,21(3):7-14.

[28] 张兴兰,崔 遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报,2019,5(1):19-25.

[29] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]. Berlin, Heidelberg: Springer, 2011: 53-70.

[30] WANG Y, GOU G P, LIU C, et al. Survey of security supervision on blockchain from the perspective of technology[J]. Journal of Information Security and Applications, 2021, 60: 102859.

(责任编辑:陈海霞)