• 计算机工程与应用 •

基于区块链的供应链数据分级访问控制机制

叶 进[1,2*]，庞承杰[1,2]，李晓欢[2]，张 鑫[3]，刘 亮[4]

(1. 广西大学计算机与电子信息学院 南宁 530004；2. 广西综合交通大数据研究院 南宁 530025；
3. 南宁威耀集采集配供应链管理有限公司 南宁 530201；4. 广西交通运输厅信息中心 南宁 530000)

【摘要】针对供应链企业与部门间存在数据共享程度低、访问透明性差以及隐私保护的问题，提出了一种基于区块链的供应链数据分级访问控制机制。设计了面向供应链场景的多链架构，实现供应链数据与访问控制信息的隔离存储；同时提出了基于分级属性和区块链的分级访问控制模型，及其智能合约的实现与部署，并针对某集采集配供应链业务进行了实例分析。实验表明该机制在大规模策略下，吞吐量仍维持在 90 tps 以上，策略判定时间开销平均为 26 ms。

关 键 词 访问控制； 区块链； 智能合约； 供应链
中图分类号 TP311 **文献标志码** A doi:10.12178/1001-0548.2021321

Blockchain-Based Supply Chain Data Hierarchical Access Control Mechanism

YE Jin[1,2*], PANG Chengjie[1,2], LI Xiaohuan[2], ZHANG Xin[3], and LIU Liang[4]

(1. School of Computer and Electronic Information, Guangxi University Nanning 530004;
2. Guangxi Research Institute of Integrated Transportation Big Data Nanning 530025;
3. Nanning Weiyao Procurement and Distribution Supply Chain Management Co., LTD Nanning 530201;
4. Information Centre of Department of Transport of Guangxi Nanning 530000)

Abstract To address the low sharing degree, poor access transparency, and privacy preserving problems between supply chain enterprises and departments, this paper proposes a blockchain-based supply chain data hierarchical access control mechanism. A multi-chain architecture oriented to supply chain scenarios is designed to segregate the storage of supply chain data and access control information. A hierarchical access control model based on blockchain and hierarchical attributes is proposed and implemented as smart contracts. The efficacy of proposed mechanism is demonstrated through a case study of procurement and distribution supply chain. The experiment results show that the throughput of the mechanism still maintains above 90 tps under the large-scale policies, and the average time cost of the policy decision is 26 ms.

Key words access control; blockchain; smart contract; supply chain

供应链是一种复杂的网链，由一系列不同类型的企业组成，每个企业作为数据源，在供应链各阶段不断产生海量、异构的数据，这些数据在供应链管理中具有重要价值。供应链网络中涉及企业和部门众多，不同企业间既存在合作关系，又存在竞争关系，给企业间数据共享带来挑战[1]。一方面，供应链各阶段迫切需要诸如生产信息、流转信息的透明化访问与共享，来解决上下游企业间的信息不对称问题，提高企业合作效率，减少成本。以农产品供应链溯源为例，企业间的信息共享能有效提高整体追溯的效率，从而保障农产品质量，减少伪劣产品的产生[2]。但另一方面，供应链核心企业间，如同级供应商之间存在竞争关系，企业出于对自身隐私的保护，不希望商业机密、财务信息等隐私数据被他人获取。这使得企业或部门间共享数据的积极性降低，供应链运转效率大打折扣。如何既保证企业间必要的数据透明化访问与共享，又实现部分隐私数据的保护，是供应链亟待解决的问题。

收稿日期：2021－11－03；修回日期：2022－01－29
基金项目：广西重点研发计划 (2021AB06002)
作者简介：叶进 (1970－)，女，博士，教授，主要从事网络协议设计、数据中心网络等方面的研究.
*通信作者：叶进，Email：yejin@gxu.edu.cn

为了实现数据的授权访问和隐私保护，学者们提出了一些解决方案，其中访问控制是保护数据安全的主要手段，通过对用户权限进行分配和管理，使得用户在授权后可以合法访问特定的数据。本文主要关注访问控制机制在供应链场景下的应用。现有的访问控制机制包括自主访问控制 (discretionary access control, DAC)、基于角色的访问控制 (role-based access control, RBAC)、基于属性的访问控制 (attribute-based access control, ABAC)等，其中 ABAC 将实体属性作为关键要素构造访问策略实现灵活的访问控制[3-4]。这些访问控制机制大多使用集中授权的方式实现授权访问，即通过一台中心服务器进行授权，这种授权过程缺乏透明性，存在性能瓶颈和单点故障问题。由于供应链参与方众多且分散，同时存在着复杂的访问需求，上述访问控制机制已不能很好地适用，不仅不符合供应链多方参与的场景，更难以实现授权过程的可靠追溯。

近年来，将区块链技术与访问控制技术相结合受到越来越多的关注，并在各领域得到应用[5-6]，区块链的共识机制能确保供应链参与方对访问授权结果的分布式一致性，实现授权过程的透明化。这为供应链数据访问与共享提供了新的思路[7]，但也还存在一些挑战。供应链各阶段产生多源异构的流转信息、溯源信息、存证信息等数据，其重要性或隐私程度不一，访问控制机制应当根据不同的数据等级制定访问与共享策略，实现更细粒度的访问控制。

1　相关工作

根据区块链在访问控制中的作用，将现有的访问控制架构分为以下 3 种。

1) 第三方维护的架构。将区块链作为第三方维护的可信分布式账本，而访问控制机制运行在中心化的授权服务器。文献 [8] 将区块链与 ABAC 访问控制模型结合，以区块链交易的方式实现了访问策略的创建、更新、撤销和权限转移等，区块链授权过程由链下服务器完成。文献 [9] 提出了一种区块链与 DAC 结合的物联网访问控制机制 BlendCAC，通过访问控制矩阵实现授权访问，区块链用于存储访问控制矩阵。这一类架构虽然在一定程度上解决了传统访问控制中访问授权的透明性问题，但仍然存在授权服务器的公正性和单点故障问题。

2) 参与方共同维护架构。由参与方来共同维护区块链，利用智能合约实现访问控制。文献 [10] 提出了物联网场景下的访问控制框架，设计了访问控制合约、注册合约和审判合约，其中，审判合约实现了对恶意访问行为的惩罚。文献 [11] 提出了 MedRec 框架应用于医疗数据的访问控制场景，将医疗服务提供者及患者接入区块链网络，通过智能合约实现数据安全访问与共享。文献 [12] 提出了一种基于环签名技术的医疗区块链隐私数据共享模型。文献 [13] 以 ABAC 为基础，提出了大数据场景下基于区块链的访问控制机制，使用智能合约实现访问控制并且改进了策略检索效率。文献 [14] 提出了一种域间访问控制模型，划分不同的安全域，通过跨域节点的智能合约实现细粒度和灵活的访问控制。文献 [15] 提出了物联网下的访问控制系统，设计了资源子系统存储数据，区块链子系统管理访问策略并处理访问事务。这类工作将授权服务器去中心化，利用区块链的智能合约和存储结构的特点，增强了授权过程的透明性与可审计性，但缺乏对访问控制数据的隔离存储与保护。

3) 多链架构访问控制机制[16-19]。文献 [18] 提出一种企业场景下的数据访问控制模型，包含企业区块链和行业区块链，行业区块链由企业区块链选出节点组成，负责实现各企业链之间的数据访问控制与共享，但尚未给出具体实现。文献 [19] 设计了一种协同链机制，用于物联网场景下多条异构链的数据访问控制和安全共享，协同链存储访问记录与待共享数据，根据数据等级决定共享操作。这种多链访问控制能够实现业务数据与访问控制数据的隔离与保护，但需要相对复杂的链间操作。

综上，基于区块链的访问控制研究在供应链场景中的应用仍处于起步阶段，现有工作的访问控制模型难以适应供应链多方参与的场景，缺乏对供应链数据本身重要性和隐私程度的关注，以及对数据进行分级以满足不同访问控制需求。因此，本文提出了一种基于区块链的供应链数据分级访问控制机制，将区块链技术与基于属性的访问控制模型结合，主要贡献如下。

1) 设计了面向供应链数据访问控制的多链架构。该架构由数据区块链与访问控制链组成，数据区块链托管存储供应链企业在各阶段产生的业务数据，实现供应链数据的隔离，以保护数据的安全和隐私性。访问控制链负责存储属性信息、访问策略、访问记录等信息，并实现链上策略管理以及用户对数据的访问控制功能。

2) 提出了基于区块链的分级访问控制模型。基于 ABAC 模型，在客体属性中引入分级属性描述数据等级，根据供应链数据的隐私和重要程度建立

访问策略，实现细粒度的访问控制。设计了策略管理合约、策略判定合约并部署到访问控制链，通过访问事件触发合约调用执行访问控制工作流程。访问控制过程去中心化、透明化、链上留痕可追溯。

3) 基于 Hyperledger Fabric 平台实现了本文的访问控制机制。通过实验分析表明该机制具有稳定的性能，有较好的可行性。

2 访问控制结构设计

供应链中包含供应商、物流企业、经销商、消费者、监管部门等实体，在访问控制机制中存在对应的用户角色。供应商负责生产和供货，通过物流企业将货物运输至经销商，经销商从仓储中取货，将产品销售给消费者。生产到销售中的各环节可能存在多个企业或部门。

2.1 访问控制架构

本文基于多链架构设计了基于区块链的供应链数据分级访问控制机制，总体架构由数据区块链和访问控制链两部分组成，其中包含普通节点、跨链节点、审计节点和共识节点，如图 1 所示。

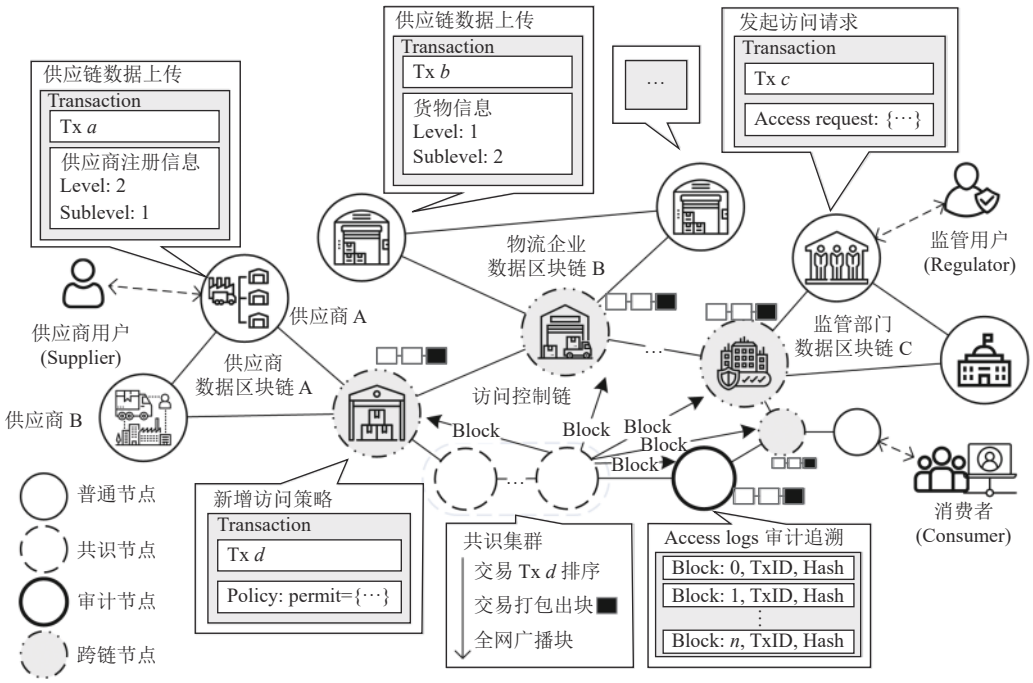

图 1 访问控制机制架构

数据区块链是由同类企业或部门组成的一条联盟链，链内包含若干普通节点。该链存储各企业或部门的业务数据，如生产信息、交易信息、物流信息和溯源存证等，实现数据的分布式安全存储。供应链中的供应商、物流企业、经销商和监管部门等实体分别构建并维护各自的数据区块链，各链之间数据隔离存储。

访问控制链作为供应链各方共同参与和维护的联盟链，由跨链节点、审计节点和共识节点组成。该链在网络中负责存储访问策略、属性信息、分级信息和授权访问记录等访问控制相关信息，通过链上节点及智能合约实现分级访问控制模型，为不同企业或部门提供数据访问控制服务。数据区块链和访问控制链中的 4 种类型节点功能具体如下。

1) 普通节点：代表单个企业或部门，与其他同类企业或部门的普通节点组成和维护数据区块链，用户通过客户端与之交互。部署并运行数据管理合约，负责向数据区块链上传、查询和下载数据，负责企业或部门内部分布式账本的存储。

2) 跨链节点：由数据区块链中的任一普通节点担任，并同时加入访问控制链，维护该链的账本。部署和运行分级访问控制模型的智能合约，处理来自普通节点的访问请求，实现企业或部门间的数据访问控制与共享。

3) 审计节点：负责访问控制链的管理，记录访问控制链的运行日志，为供应链监管用户提供历史授权访问记录的追溯和责任确权，减少非法授权行为的产生。

4) 共识节点：组成和维护访问控制链中的 Raft 共识集群，负责将访问控制过程的交易进行排序并

打包成区块，将区块广播到该链的其他节点，确保访问控制结果在区块链网络的分布式一致性。

2.2　存储结构

本文设计的访问控制链利用区块存储结构来存放访问控制所需信息，如图 2 所示。在访问控制链中，新增策略、更新策略以及授权访问等操作均通过智能合约以交易的形式执行。区块中 Merkle 树的叶子节点存储着交易数据，包括属性、访问策略、授权记录及发起访问时提交的交易，叶子节点的交易数据经过哈希函数运算后存储在其父节点中，递归直到生成唯一 Merkle 根哈希存储在区块头部。

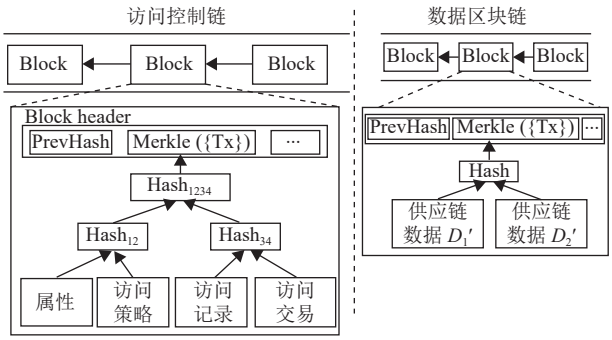

图 2　区块存储结构

通过区块头部的 Merkle 根哈希能够间接校验交易数据是否被篡改，实现交易数据的不可篡改和安全存储[17]。而访问控制链的共识机制保证链上各节点存储相同的分布式账本。

3　分级访问控制模型

3.1　访问控制模型

本文在 ABAC 模型基础上引入数据分级的思想，提出分级访问控制模型，根据供应链场景的需求来对数据客体进行分级。在分级访问控制模型中，属性与权限存在多对多的映射关系。定义 1 对分级访问控制模型进行形式化描述。

定义 1　分级访问控制模型形式化表示为：

$$\begin{aligned}&\text{result} \leftarrow f(P =< \text{SA}, \text{RA}^*, \text{EA}, \text{PA} >)\\&\text{SA} = \{\text{user}, \text{role}, \text{company}\}\\&\text{RA}^* = \{\text{data}, \text{level}, \text{sublevel}\}\\&\text{EA} = \{\text{time}, \text{location}\}\\&\text{PA} = \{R, W, X, U, D\}\end{aligned}$$

其中，P 为属性四元组组成的访问策略；SA 代表主体属性，包含用户、角色和所属企业；RA^*为客体属性，包含数据名称、数据分级和子分级，数据分级用于描述数据的重要或隐私程度，由数据拥有者根据供应链场景需求进行配置；EA 代表环境属性，如访问时间、用户位置等；PA 代表访问操作属性，其中包含读 (R)、写 (W)、执行 (X)、上传 (U) 和下载 (D) 等操作；f表示对访问策略进行判定，result = {permit, deny}表示判定结果，允许访问则返回 permit，拒绝访问则返回 deny。

在客体属性中，数据分级属性RA^*.level用于描述当前数据客体的等级，$\text{RA}^*.\text{level} \in [0, n]$，$n \geqslant 0$，当 level 取值 0 时，表示当前数据等级最低，即数据可以被公开访问，而取值 n 则表示等级上限。

面对供应链多源异构数据的累积，以及企业内部对数据分级的更细需求，通过配置客体属性中的数据子分级属性可实现更细粒度的数据分级访问策略。数据子分级RA^*.sublevel是对 level 的扩充和细分，其作用是在当前分级 level 的基础上再进行一层分级。其中，$\text{RA}^*.\text{sublevel} \in [0, s_i]$，$0 \leqslant s_i \leqslant m$，$s_i$表示当前 level 为 i 时，其对应的 sublevel 的等级上限。图 3 描述了供应链数据经过 level 及 sublevel 分级的过程。

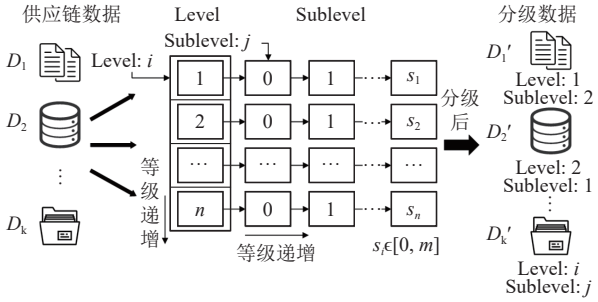

图 3　供应链数据分级

在分级访问控制机制中，主体角色属性与客体数据分级属性之间的对应关系通过分级表 LevelMap 进行记录，并托管到访问控制链进行存储。分级表 LevelMap 借助类哈希表存储结构，记录用户角色、每个角色所支持访问的数据分级以及对应的访问权限，用于访问授权过程中对角色与访问数据等级的比对和匹配，由访问控制链进行更新维护。

3.2　访问控制工作流程

在标准的 ABAC[20] 访问控制机制中，属性库、策略库分别是存储属性信息以及访问策略的数据库。策略信息点 (policy information point, PIP)、策略管理点 (policy administration point, PAP)、策略执行点 (policy enforcement point, PEP) 和策略决策点 (policy decision point, PDP) 分别用于访问策略的检索、管理、匹配与访问授权。本文的访问控制机制工作流程以标准 ABAC 授权过程为基础，并结合区块链技术实现。使用访问控制链作为属性库、

访问策略库，实现属性信息、分级信息和访问策略在区块链上的分布式记账存储。链上部署的策略管理合约 PolicySC 实现了 PIP 属性检索与 PAP 策略管理的功能，负责对访问策略进行全局管理。策略判定合约 AccessSC 整合了 PEP 和 PDP 的功能，通过合约调用实现分布式策略判定与访问授权。基于区块链的供应链数据分级访问控制机制工作流程如图 4 所示。

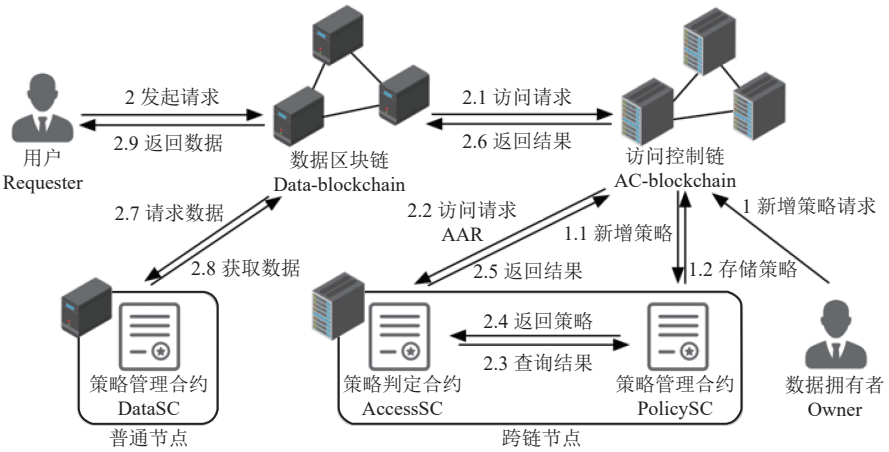

图 4 访问控制工作流程

数据拥有者是企业或部门中持有数据的用户，可以建立和新增数据的访问策略，通过与普通节点交互，发送请求到跨链节点，调用该节点部署的 PolicySC 发起新增策略交易。交易发起后，跨链节点收集访问控制链上的多数节点签名，提交至共识集群对交易排序，并将共识后的交易以区块形式打包分发至链内所有节点，链上各个节点验证该交易的背书签名以及版本号，之后将包含访问策略的区块追加到该链各个节点的分布式账本中。

供应链用户访问数据时，通过客户端与普通节点交互，发送访问请求至跨链节点。收到访问请求后，跨链节点调用 PolicySC 从访问控制链上查找相关属性并构造带属性的访问请求 (attribute access request, AAR)，由 AccessSC 执行访问策略判定。AccessSC 解析请求 AAR 后，跨合约调用 PolicySC 合约在链上查询与 AAR 相关的访问策略，匹配该策略中的属性并进行判定，决定是否对用户主体授权。

访问授权过程通过交易的形式产生区块，记录在访问控制链上，授权后跨链节点回调 DataSC 合约，将数据 URL 返回到用户所属的普通节点。

3.3 智能合约设计

智能合约是实现分级访问控制机制的核心，本文设计了数据管理合约 DataSC、策略管理合约 PolicySC 和策略判定合约 AccessSC。

1) DataSC 合约负责对供应链数据进行操作，包含数据的上传、查询和下载等。上传操作负责将数据上传到企业的数据区块链中进行存储，查询操作通过数据的键在链上查找数据并返回。

2) PolicySC 合约负责对存储在访问控制链上的访问策略进行管理，包含新增策略 AddPolicy()、查询策略 QueryPolicy()、更新策略 UpdatePolicy()、失效策略 InvalidPolicy() 以及属性解析 GetAttrs() 函数。通过该合约，数据拥有者可以新增访问策略到链上存储，更新已有策略和使某些策略失效，并查询链上存储的策略。

3) AccessSC 合约负责对接收到的访问请求进行访问策略的匹配、判定与授权访问。策略判定功能 f 通过函数 CheckAccess() 实现，详见算法 1。

算法 1 策略判定 CheckAccess
输入：属性访问请求 AAR
输出：判定结果 result
初始化：result = deny; timestamp; LevelMap;
Attrs = PolicySC.GetAttrs(AAR.AttrTuple);
PolicySet = PolicySC.QueryPolicy(Attrs);
for P in PolicySet do
  if Attrs.PA⊆P.PA and Attrs.EA⊆P.EA and
  Attrs.SA⊆P.SA and Attrs.RA⊆P.RA then
  RL = LevelMap[Attrs.SA.role];
    for k = 1 to RL.size do
      if P.RA.level∈RL_k and
      P.RA.sublevel∈RL_k then

result = permit;

PutACChain(AAR, result, timestamp);

return result;

算法流程描述：

1) 通过 GetAttrs() 函数解析 AAR 中的属性元组 Attrs；

2) 通过 QueryPolicy() 函数在链上查询与 Attrs 属性匹配的访问策略，存入策略集 PolicySet；

3) 遍历 PolicySet，查找与 Attrs 属性相匹配的访问策略 *P*；

4) 判定 Attrs 与访问策略 *P* 中的各个属性是否匹配，以及角色与访问策略 *P* 中的数据等级是否匹配；

5) 若匹配则返回 permit，否则返回 deny，并通过 PutACChain() 函数将访问控制过程上链存储。

4　实验与分析

基于 Hyperledger Fabric[21] 区块链平台实现分级访问控制机制，并利用 Fabric tape 工具进行性能测试。实验采用操作系统 macOS 11.5 64 位，处理器 Intel Core i5 2.7 GHz，内存 8 GB，Hyperledger Fabric 版本为 1.4.1，Golang 版本为 1.14，Docker 版本为 19.03。仿真实验利用 Fabric 多通道机制搭建区块链网络，设置 2 条数据区块链 (各包含 2 个普通节点) 和 1 条访问控制链 (包含 2 个跨链节点)，Raft 共识集群包含 5 个共识节点。

4.1　访问结果与分析

以南宁公立学校的食材集采集配供应链场景为例进行分析。实例的区块链网络中包含供应商 (链 A)、集采集配基地 (链 B)、监管部门 (链 C) 和消费者 (链 D) 这 4 条数据区块链及各方共同维护的访问控制链，分别使用 supplier、base、consumer 和 regulator 表示上述供应链实体中的用户角色。4 种角色分别对应上述 4 条数据区块链内的普通节点。在供应链中由基地向供应商采购订货，货物送达后经过质检进入基地存放，待基地分拣后出库，发车配送至各消费者。期间，具有资质的供应商产生采购信息、货物信息、发车信息和财务信息，基地则不断产生货物出入库信息、质检信息、分拣信息、车辆在途信息和配送签收信息。供应链从食材采购到配送的过程，需要各个实体进行一定程度的信息共享以实现协助配合。因此需要根据数据的重要程度，制定分级访问策略进行访问控制。

根据供应链场景需求，按照数据隐私程度将分级 level 设置为 0(公开)、1(限制)、2(隐私) 的等级，每个 level 下的 sublevel 可分为 1、2 等级，表 1 给出了分级示例。

表 1　供应链数据分级示例

level	sublevel	分级描述	数据
0	0	公开	配送签收信息、车辆在途信息
1	1	限制	出入库信息、分拣信息、发车信息
	2		质检信息、采购信息、货物信息
2	1	隐私	供应商注册信息、基地注册信息
	2		供应商财务信息、基地财务信息

同时，各企业数据拥有者与监管用户根据场景需求，共同确定角色与数据分级的对应关系及其访问权限，如表 2 所示，再共同制定对数据的访问策略。

表 2　角色与数据分级的访问权限关系

角色	level=0	level=1		level=2	
	0-0	1-1	1-2	2-1	2-2
supplier	R/U	R	R		
base	R/U	R/U	R/U		
regulator	R	R/D	R/D	R/D	R/D
consumer (school)	R	R			

由于供应商与基地存在供货关系，基地用户以角色 base 通过普通节点的 DataSC 合约对质检信息、入库信息等数据进行上传，以便供应商用户以 supplier 角色访问，保证食材供货信息畅通。出于溯源的需求，消费者以角色 consumer 通过跨链节点的 AccessSC 合约访问配送信息、车辆在途信息等溯源相关数据。监管用户以角色 regulator 对供应商的注册信息进行访问查看和下载存档，实现对供应商资质的审查和监督。

当监管部门履行对供应商的监督职责时，通过新增访问策略，实现监管用户对所有实体注册信息的访问和下载，同时阻止其他角色对该数据的非授权访问。该访问策略以 JSON 形式描述如下：

permit = {“SA”:{“user”: “zhangsan”, “role”: “regulator”, “company”: “CFDA”}, “RA”:{“data”: “*注册信息”, “level”: 2, “sublevel”: 1}, “EA”:{“time”: “any”, “location”: “any”}, “PA”:{R, D}}

通过 PolicySC 合约 AddPolicy() 函数新增该策略到访问控制链中。当监管用户对供应商的注册信息发起访问时，触发 AccessSC 中的 CheckAccess()

函数进行策略判定，只有满足上述访问策略属性的请求才能得到访问授权 permit。其他角色请求访问该数据时，CheckAccess() 判定访问请求与上述访问策略不匹配，则拒绝该访问请求。访问过程由访问控制链上所有节点分布式记账留痕以供审计。

4.2 策略分析

为验证本文机制在不同规模访问策略数量下的策略查询及判定效果，通过脚本生成策略数目为 500、1 000、1 500、2 000、2 500、3 000、3 500、4 000 的测试样本，测试在不同数量策略下发送单条交易及并发交易时，访问控制机制调用智能合约策略查询以及策略判定的响应时间。

实验设置不同分级下的策略查询和判定。不分级情况下，本文模型相当于 ABAC 模型在访问控制链上的实现，并将其与链下实现的 ABAC 模型对比。分级 1 代表该策略仅配置分级属性 level，并设置为 3 个等级，sublevel 设置为 0，策略判定时需要对角色与数据的等级进行匹配。分级 2 代表数据客体属性，同时设置分级属性 level 和子分级属性 sublevel，每个 level 下的 sublevel 设置 5 个等级，策略判定时需要先后匹配角色能否访问策略规定的 level 和 sublevel 等级的数据，因此，时间开销相应增加。实验多次测试取平均值后，结果如图 5 所示。

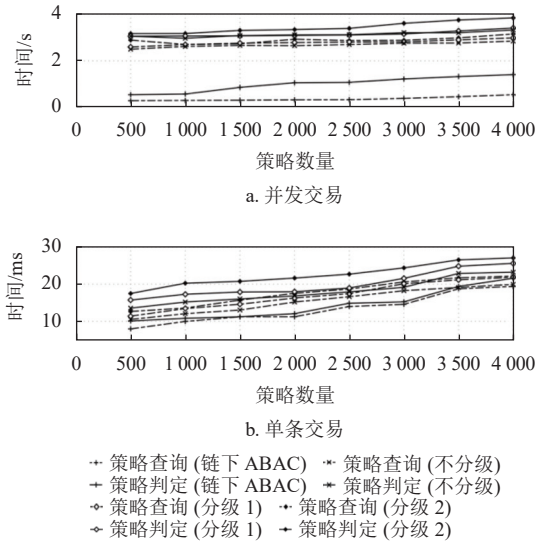

图 5 不同策略规模查询与判定时间比较

可以看出，随着策略规模增加，访问控制机制的策略查询及判定时间均有所上升。链下 ABAC 由于在单一服务器上实现访问控制，大部分情况下，其策略查询和判定时间开销相对最低。在发送单条交易且不分级时，策略查询与判定过程均能在较低的时间内完成，大部分情况下均维持在 20 ms 内。对数据分级后，策略判定的时间开销略微上升，且分级 2 情况下的策略判定时间开销相对最高。并发交易下，在策略数量达到 4 000 时，其响应时间能控制在 4 s 以内。可见本文机制的时间开销相比现有 ABAC 稍有增加，但仍能保证策略查询与判定的执行效率，在多条并发交易下，同样具有较为稳定的性能表现。

4.3 吞吐量测试

吞吐量在区块链性能测试中通常描述为 TPS (transactions per second)。为了测试访问控制机制中访问控制链的交易性能，实验使用 Fabric tape 生成不同数量的交易对吞吐量进行测试。本节设置每个节点连接 10 个客户端，客户端与节点的并发连接数分别设置为 10、20，观察分级和不同连接数下吞吐量的变化。实验结果如图 6 所示。

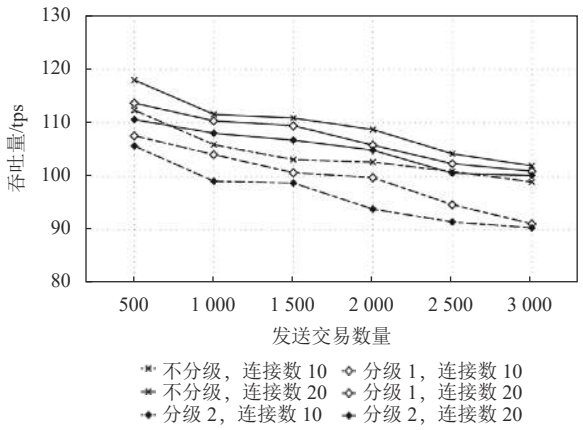

图 6 发送交易数量与吞吐量比较

当客户端与节点并发连接数从 10 增加到 20 时，访问控制链的吞吐量随之增加，随着发送交易数量的增加，访问控制链的吞吐量稍有下降，在发送交易数量达到 3 000 时，其吞吐量最低维持在 90 tps 以上。可以看出，访问控制机制性能较为平稳，即便在引入分级的情况下也能够保持相对稳定的吞吐量。

5 结 束 语

本文提出了一种基于区块链的供应链数据分级访问控制机制，面向供应链场景设计了数据区块链与访问控制链结合的多链架构。访问控制链负责存储供应链所有实体的属性信息、分级信息与访问策略等，通过链上部署访问控制合约进行分布式访问

授权，授权过程透明且可追溯。借助 Hyperledger Fabric 平台验证本文分级访问控制机制的可行性与有效性，实验表明本文所提机制在大规模策略数量的情况下仍具有相对平稳的性能，在供应链数据访问与共享的实际场景中具有可行性。

参 考 文 献

[1] WU H, CAO J, YANG Y, et al. Data management in supply chain using blockchain: Challenges and a case study[C]//2019 28th International Conference on Computer Communication and Networks (ICCCN). Valencia: IEEE, 2019: 1-8.

[2] 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 C H, YU H J, XU D M, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology[J]. Transactions of the Chinese Society of Agricultural Machinery, 2021, 52(1): 1-13.

[3] 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 L, YIN L H, GUO Y C, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, 40(7): 1680-1698.

[4] HU V C, KUHN D R, FERRAIOLO D F, et al. Attribute-based access control[J]. Computer, 2015, 48(2): 85-88.

[5] GHAFFARI F, BERTIN E, HATIN J, et al. Authentication and access control based on distributed ledger technology: A survey[C]//2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). Paris: IEEE, 2020: 79-86.

[6] ROUHANI S, DETERS R. Blockchain based access control systems: State of the art and challenges[C]//IEEE/WIC/ACM International Conference on Web Intelligence. Thessaloniki: IEEE, 2019: 423-428.

[7] HELO P, HAO Y. Blockchains in operations and supply chains: A model and reference implementation[J]. Computers & Industrial Engineering, 2019, 136: 242-251.

[8] MAESA D D F, MORI P, RICCI L. Blockchain based access control[C]//IFIP International Conference on Distributed Applications and Interoperable Systems. Neuchâtel: Springer, 2017: 206-220.

[9] XU R, CHEN Y, BLASCH E, et al. Blendcac: A blockchain-enabled decentralized capability-based access control for iots[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018: 1027-1034.

[10] ZHANG Y, KASAHARA S, SHEN Y, et al. Smart contract-based access control for the internet of things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605.

[11] AZARIA A, EKBLAW A, VIEIRA T, et al. Medrec: Using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data (OBD). Vienna: IEEE, 2016: 25-30.

[12] 王瑞锦, 余苏喆, 李悦, 等. 基于环签名的医疗区块链隐私数据共享模型[J]. 电子科技大学学报, 2019, 48(6): 886-892.
WANG R J, YU S Z, LI Y, et al. Medical blockchain of privacy data sharing model based on ring signature[J]. Journal of University of Electronic Science and Technology of China, 2019, 48(6): 886-892.

[13] 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 A D, DU X H, WANG N, et al. A blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[14] 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 J B, ZHANG Z Q, XU W S, et al. Inter-domain access control model based on blockchain[J]. Journal of Software, 2021, 32(5): 1547-1564.

[15] CHEN E, ZHU Y, ZHOU Z, et al. Policychain: A decentralized authorization service with script-driven policy on blockchain for internet of things[J]. IEEE Internet of Things Journal, 2022, 9(7): 5391-5409.

[16] 王瑞锦, 郭上铜, 邱玮鸿, 等. 基于信用投票共识的主从多链分层跨链模型[J]. 电子科技大学学报, 2021, 50(6): 907-914.
WANG R J, GUO S T, QIU H W, et al. A master-slave multi-chain hierarchical cross-chain model based on credit voting consensus[J]. Journal of University of Electronic Science and Technology of China, 2021, 50(6): 907-914.

[17] LI X, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[18] 王秀利, 江晓舟, 李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报, 2019, 30(6): 1661-1669.
WANG X L, JIANG X Z, LI Y. Model for data access control and sharing based on blockchain[J]. Journal of Software, 2019, 30(6): 1661-1669.

[19] CHANG J, NI J, XIAO J, et al. SynergyChain: A multichain-based data sharing framework with hierarchical access control[J]. IEEE Internet of Things Journal, 2021, DOI: 10.1109/JIOT.2021.3061687.

[20] HU V C, FERRAIOLO D, KUHN R, et al. Guide to attribute based access control (ABAC) definition and considerations[J]. NIST Special Publication, 2013, 800(162): 1-54.

[21] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains[C]//Proceedings of the 13th EuroSys Conference. Porto: ACM, 2018: 1-15.

编　辑　税　红