doi:10.6041/j.issn.1000-1298.2023.01.018

基于 PBFT 的猕猴桃溯源联盟链应用访问控制方案

景　旭　邢胜飞

（西北农林科技大学信息工程学院，陕西杨凌 712100）

摘要：针对基于属性的联盟链应用访问控制模型可能存在拜占庭节点而导致属性信息、访问控制策略查询结果不可信的问题，结合猕猴桃溯源场景的实际需求，提出了一种基于 PBFT 的联盟链应用访问控制方案。该方案使用属性权威作为联盟链实体组织的属性证书颁发机构以及 PBFT 的查询验证节点，对访问请求内容生成签名并验证；属性证书中存储主体与权限相关的属性信息；基于 PBFT 对用户属性、数据属性、访问控制策略查询验证，确保访问控制过程的可信性。基于 Hyperledger Fabric 原型系统测试表明，当记账节点中的拜占庭节点少于节点总数 1/3 时系统能够正常运行；当交易发送率在 100 ~ 1 500 TPS 之间变化时，交易吞吐量在交易发送率达到 300 TPS 后趋于稳定，平均时延在交易发送率达到 400 TPS 后趋于稳定，满足联盟链猕猴桃溯源的应用需求。

关键词：猕猴桃；溯源；联盟链；实用拜占庭容错算法；访问控制；属性证书

中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1000-1298(2023)01-0183-13　　**OSID**：

Access Control Scheme of Kiwifruit Traceability Consortium Blockchain Application Based on PBFT

JING Xu　XING Shengfei

(*College of Information Engineering*, *Northwest A&F University*, *Yangling*, *Shaanxi* 712100, *China*)

Abstract: Aiming at the problem that attribute information and access control policies might be untrustworthy due to the existence of Byzantine nodes in the attribute-based consortium blockchain application access control model, combined with the actual needs of the kiwifruit traceability scenario, an access control scheme of kiwifruit traceability application based on PBFT and consortium blockchain was proposed. The attribute authority was used as the attribute certificate authority of the consortium blockchain entity organization and the query verification node to generate signatures and verify the access request contents. The attribute information related to the subject and the authority was stored in the attribute certificate. The user attributes, data attributes and access control policies based on the PBFT were verified to ensure the credibility of the access control process. The tests based on the Hyperledger Fabric prototype system showed that the system could work normally when the number of Byzantine nodes in the accounting node was less than 1/3. The total number of transactions submitted to the blockchain was 1 000, 2 000, 3 000, and the transaction sending rate was 100 TPS, 200 TPS, …, 1 400 TPS and 1 500 TPS, the transaction throughput was stable when the transaction sending rate was 300 TPS, and the average latency was stable when the transaction sending rate was 400 TPS. The scheme met the requirements of the consortium blockchain kiwifruit traceability application.

Key words: kiwifruit; traceability; consortium blockchain; practical Byzantine fault tolerance; access control; attribute certificate

0　引言

目前，区块链以其公开透明、去中心化、不可篡改的特性，在银行、能源、物联网、健康、媒体等多个不同领域得到了应用[1]。根据不同的开放程度，区块链分为公有链、私有链和联盟链。公有链是一种

收稿日期：2022-02-07　修回日期：2022-04-28

基金项目：陕西省重点研发计划项目(2019ZDLNY07-02-01)、国家重点研发计划项目(2020YFD1100601)和上合组织成员国农业技术集成示范与标准化研究项目

作者简介：景旭(1971—)，男，副教授，博士，主要从事区块链技术、访问控制和信息系统安全研究，E-mail：jingxu@nwsuaf.edu.cn

完全开放的区块链,几乎没有保护交易隐私,需要消耗大量的算力维护分布式账本[2]。私有链是一个集中的区块链,链上数据的访问权限由单个组织控制,主要用于内部数据管理和特定组织的审计[3]。联盟链由多个机构组成的联盟构成,联盟指定的成员进行账本的生成、共识、维护,联盟链可以完全公开也可以仅有内部人员访问[4]。相比于公有链存在资源浪费、效率低下以及私有链存在中心化程度高的问题,联盟链具有易扩大规模、成本较低、吞吐量较高的优势[5],尤其是被广泛应用于供应链溯源领域。国内外学者已经从信息存储与查询[6]、隐私加密[7]、共识算法[8]、多链[9]、身份认证[10]、智能合约[11]等技术应用层面探讨了联盟链为供应链溯源带来的优势。文献[12 - 15]都涉及到将供应链环节数据存储到联盟链上,保证溯源信息的安全性、完整性,但是没有深入探讨溯源系统用户管理,增加了监管追责的难度,同时给数据的隐私性带来了巨大的挑战。访问控制技术是保障数据安全和隐私最常用的方法之一,能够很好地处理主体人员、客体数据以及业务流程之间的关系,因此研究联盟链应用的访问控制对于推动联盟链的推广和应用具有重要意义。

作为访问控制的重要模型之一,由于能满足联盟链环境中细粒度访问控制的需求,基于属性的访问控制(Attribute-based access control, ABAC)被广泛应用。ABAC 将主体和客体的属性作为基本的决策要素,灵活利用请求者所具有的属性集合决定是否赋予其访问权限,能够很好地将策略管理和权限判定相分离[16]。文献[17 - 23]以 ABAC 为基础,将属性信息以及访问控制策略以事务的方式存储到联盟链上;当主体发出访问请求时,联盟链记账节点执行查询处理,将权限相关信息返回到策略决策点;策略决策点决定是否允许主体执行操作。访问控制过程顺利执行的前提是联盟链环境真实可信。联盟链的准入机制表明节点的加入与退出需要满足一定的条件并得到许可,但是并不能保证节点行为的可信性。联盟链除了要面对由网络中断、机器宕机以及分布式拒绝服务攻击等因素造成节点失效的崩溃故障外,还可能存在恶意节点篡改数据、发送错误数据以及故意拒绝响应请求等拜占庭故障。拜占庭故障的常见原因是敌对影响,例如恶意软件注入和物理设备捕获[24]。发生拜占庭故障的节点称为拜占庭节点。相比崩溃故障,拜占庭故障更为严重。拜占庭节点可以将伪造的属性信息以及访问控制策略发送到策略决策点,导致策略决策点无法获取到真实的数据而做出错误的决策,影响用户访问授权操作。

实用拜占庭容错算法(Practical Byzantine fault tolerance, PBFT)是一种确保分布式系统与拜占庭故障节点一致性的通用解决方案[25],将传统拜占庭容错算法的时间复杂度从指数级降低到多项式级[26]。针对拜占庭节点的恶意行为,当系统中拜占庭节点的数量不超过节点总数 1/3 的前提条件下,利用 PBFT 解决此类问题有可行性。

本文以 ABAC 为基础,面向猕猴桃溯源,提出一种基于 PBFT 的猕猴桃溯源联盟链应用访问控制方案。访问控制策略和属性信息以交易的方式存储在联盟链上,确保权限的公开透明;用户发起访问请求后,基于 PBFT 对存储在链上的访问控制策略以及属性信息进行查询验证,确保查询结果的真实可信。以期提升猕猴桃溯源联盟链应用的容错率和可用性,推动联盟链在农产品溯源的广泛应用。

1 猕猴桃溯源联盟链应用架构

猕猴桃产业链各环节参与的企业主体众多,一般包括农资电商、生产合作社、加工企业、电商平台等组织。农资电商主要业务包括向农资生产商采购农资、存储、销售等。生产合作社主要的业务包括向农资电商采购农资、种植、打药、施肥、采摘、质检、存储、销售等。加工企业主要业务包括向生产合作社采购猕猴桃、加工、存储、销售等。电商平台主要业务包括向加工企业采购猕猴桃成品、存储以及销售等。除此之外,监管机构监察产业链的所有环节,保证猕猴桃产品的质量安全。各个组织相互独立、相互合作,构成联盟链中的联盟单位。组织间的数据共享通过联盟链实现。每个组织由多个部门组成,分别承担不同的业务。各部门分工明确,部门人员各司其职,保证猕猴桃产业链的生产有序。

联盟链的准入机制确保参与的多方实体存在一定的信任前提和利益约束,任何用户只有获取到联盟链证书颁发机构(Certificate authority, CA)颁发的公钥证书(Public key certificate, PKC)才具有与联盟链交互的权限[27]。以 Hyperledger Fabric 为例,该架构为客户端提供了 2 种角色,分别是普通用户和管理员,普通用户一般发起与应用有关的业务交易,管理员则发起与系统相关的配置交易[28]。联盟链提供的身份认证技术无法完全满足猕猴桃溯源场景中的复杂需求。

属性证书(Attribute certificate, AC)由属性权威(Attribute authority, AA)颁发,是一个包含序列号、发行人、持有人、有效期、属性信息以及属性权威数字签名等的证书文件[29]。它主要用于用户的权限管理,与 PKC 相关联,但认证方式、生存期不同[30],

生命周期比较短。因此，本文利用 AC 轻量、灵活、可验证的特点，存储与权限相关的用户属性，确保属性信息的真实、有效。权限更新时不会产生大量的证书撤销列表（Cerificate revocation list，CRL），减轻了证书管理的负担。猕猴桃溯源联盟链应用架构如图 1 所示。

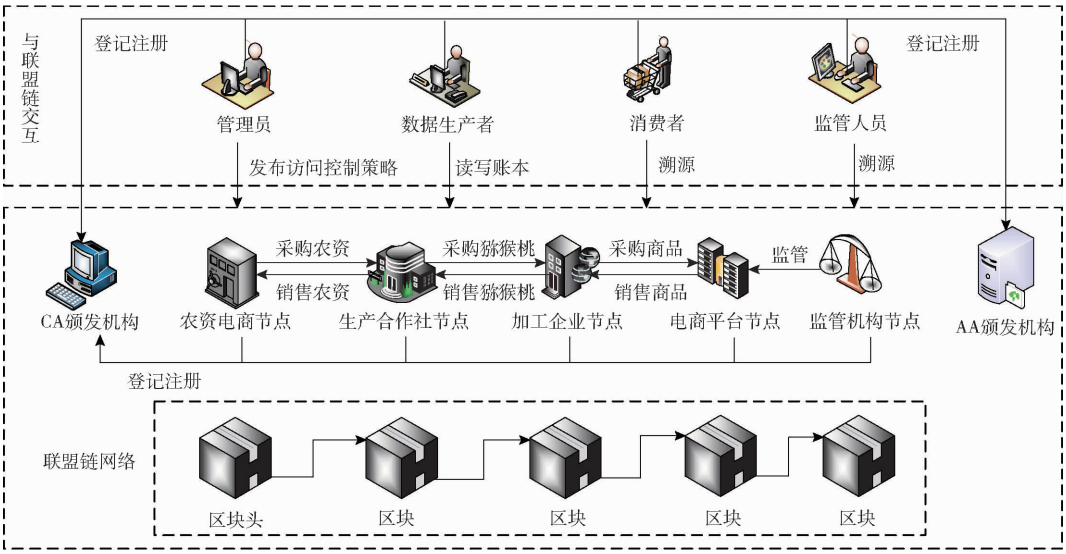


图 1　猕猴桃溯源联盟链应用架构

Fig. 1　Kiwifruit traceability consortium blockchain application architecture

在图 1 中，农资电商、生产合作社、加工企业、电商平台、监管机构等组织作为实体节点加入联盟链网络。组织内涉及到的用户如下：

（1）数据生产者：管理猕猴桃产业链各个环节的链上链下业务数据，实现上下游企业间的数据流通。

（2）监管人员：监督猕猴桃产业链各个生产环节，对出现质量问题的猕猴桃商品溯源与追责。

（3）管理员：负责权限以及证书管理，根据实际需求为数据制定相关访问控制策略，并发布到联盟链上。

（4）消费者：猕猴桃产业链的最终服务对象，可以从联盟链上查询猕猴桃商品的部分溯源信息。

猕猴桃溯源联盟链应用中的所有用户都需要向 CA、AA 登记注册 PKC 以及 AC。PKC 唯一标识用户在联盟链网络中的身份。AC 主要用于权限管理。用户访问系统资源时，需要满足访问控制策略。

2　猕猴桃溯源联盟链应用访问控制

2.1　访问控制设计思想

猕猴桃溯源联盟链应用访问控制的主要设计思想包括：

（1）基于公钥基础设施（Public key infrastructure，PKI）和特权管理设施（Privilege management infrastructure，PMI）的证书管理体系。猕猴桃溯源应用所使用的联盟链网络以 Hyperledger Fabric 为底层框架，通过成员服务提供者（Membership service provider，MSP）管理身份证书，通过 PMI 中的 AC 管理权限。管理流程包括：首先，为农资电商、生产合作社、加工企业、电商平台、监管机构等组织各部署一个 peer 节点，承担本组织记账节点角色；其次，为每个组织部署一个 CA，负责为本组织中的实体颁发身份证书；最后，为每个组织部署一个 AA，承担组织 AC 颁发机构以及查询验证节点角色。管理员将各组织 AA 的公钥存储到联盟链上，AA 节点需要从链上读取其它组织 AA 的公钥，形成节点索引表保存在本地。用户都向本组织 AA 节点申请 AC，并存储到联盟链上，以便于其它组织 AA 验证。AA 节点向本组织 CA 申请证书，获得向记账节点查询数据的权限。用户发出访问请求后，各组织 AA 在向本组织记账节点查询权限信息时进行可信验证。

（2）基于 PBFT 的猕猴桃溯源访问控制方案。组织用户访问溯源系统资源时，需要所有 AA 节点通过 PBFT 查询验证用户属性、数据属性、访问控制策略，确保访问控制的可信性；将查询验证结果作为执行用户请求的判定标准；验证结果中有超过节点总数 2/3 的节点允许用户执行操作，则命令系统执行该请求；否则，系统拒绝执行用户请求。

2.2　访问控制分层模型

在基于 PBFT 的猕猴桃溯源联盟链应用中，基于联盟链中的 PKC 作为用户身份凭证，以 ABAC 为基础，引入 AC 管理用户权限，基于 PBFT 提高访问控制过程的容错率，实现猕猴桃溯源的访问控制方案。实现该方案的智能合约主要包括身份证书管理合约（Public key certificate management contract，

PKCMC)、属性证书管理合约(Attribute certificate management contract, ACMC)、访问控制策略管理合约(Access control policy management contract, ACPMC)、数据属性管理合约(Date attribute management contract, DAMC)、访问控制合约(Access control policy, ACC)等。访问控制分层模型如图 2 所示。

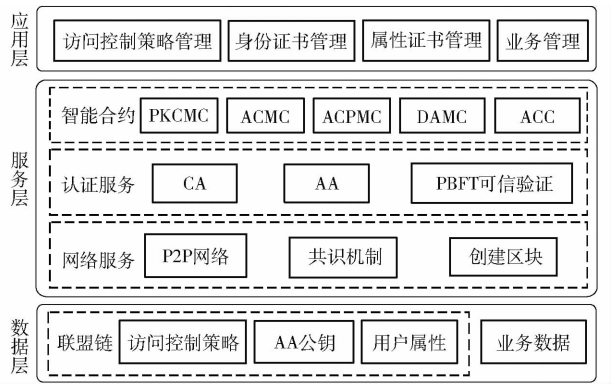


图 2 访问控制分层模型

Fig. 2 Access control hierarchical model

在图 2 中,模型从上至下分别为应用层、服务层、数据层,具体内容为:

(1)应用层:主要为猕猴桃溯源联盟链应用中的各类用户提供相应功能。

(2)服务层:是访问控制模型的核心层,提供联盟链服务以及联盟链可信查询服务,主要由网络服务、智能合约以及认证服务 3 部分组成。①网络服务:提供了 P2P 网络、共识机制、创建区块等服务。通过联盟链网络将用户 AC、数据、访问控制策略等发送到各节点;数据经过共识机制共识验证后,以交易的形式发布到联盟链上,保证各节点间数据的一致性。②智能合约:通过部署智能合约来实现逻辑功能,是实现溯源系统访问控制的工具。PKCMC 用来颁发和管理用户的身份证书。ACMC 用来颁发和管理用户的属性证书。ACPMC 用来存储和管理访问控制策略。DAMC 用来存储和管理数据的属性。ACC 用来响应用户对数据的访问请求。③认证服务:提供确保访问控制真实可信的手段。主要包括 CA、AA 的部署,以及组织 AA 基于 PBFT 查询验证属性信息、访问控制策略。

(3)数据层:主要提供数据存储服务。为降低联盟链的存储压力,所有业务数据存储在链下的数据服务器,链上只存储业务数据的唯一标识以及散列值。访问控制策略、用户属性、AA 公钥等非业务数据的数据量较少,而且数据状态较稳定,所以将原始数据直接存储在联盟链上。

2.3 访问控制建模

在猕猴桃溯源联盟链应用访问控制分层模型中,主要包括证书申请以及访问控制 2 个过程。

2.3.1 证书申请

猕猴桃产业链各组织用户都需要申请身份证书作为联盟链溯源系统的准入凭证,申请属性证书存储个人的权限信息。证书申请过程如图 3 所示。

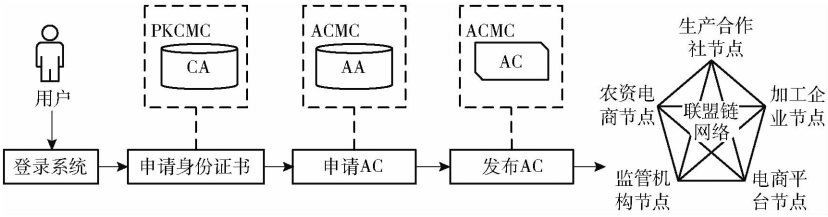


图 3 证书申请过程

Fig. 3 Certificate application process

在图 3 中,用户登录系统后,首先,将身份信息作为 PKCMC 的参数向 Fabric - CA 申请身份证书;其次,将身份证书的唯一标识以及其他属性信息作为 ACMC 的参数向 AA 申请 AC;最后,将 AC 以二进制的方式发布在联盟链上。组织内的管理员根据实际需求为数据制定相应的访问控制策略,并发布到联盟链。

2.3.2 访问控制

用户访问系统的任何资源都需要满足相应的访问控制策略。访问控制过程如图 4 所示。

在图 4 中,AA1、AA2、AA3、AA4、AA5 分别表示猕猴桃溯源联盟链中农资电商、生产合作社、加工企业、电商平台以及监管机构等组织的查询验证节点。当前视图的主节点为 AA1,从节点为 AA2、AA3、AA4、AA5。假设 AA5 是拜占庭节点,可以在看似正常情况下发生任意行为,本文用虚线箭头表示 AA5 篡改真实数据并向其他节点发送错误请求消息,即 $f=1$,f 表示联盟链网络中拜占庭节点的数量。依据 PBFT 的共识过程,主要包括 request(请求)、pre-prepare(预准备)、prepare(准备)、commit(确认)和 reply(响应)等 5 个阶段。主要步骤如下:

(1)request:用户通过与客户端交互,向 AA1 节点发送请求消息〈REQUEST, t, d, h, c〉,其中,t 为时间戳,d 为用户发送的请求内容,h 为 d 的消息摘

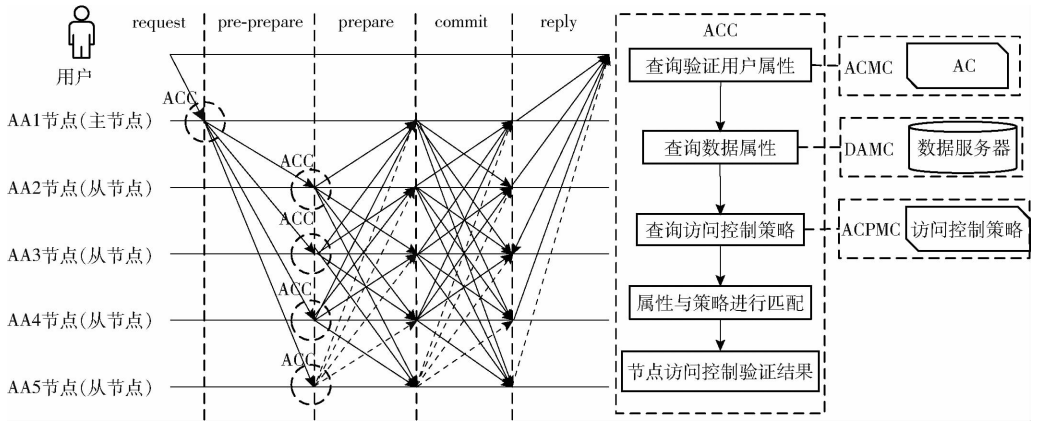


图 4　访问控制过程

Fig. 4　Access control process

要，c 为用户的身份信息。

(2) pre-prepare：AA1 节点接收到请求消息后，调用 ACC 为 d 分配一个编号 n，开始判决用户的访问请求。首先，根据 d 中的用户证书唯一标识调用 ACMC 查询存储在本组织记账节点中的用户 AC，根据 d 中的数据属性调用 DAMC 访问存储在数据服务器中的数据。其次，根据 c 获取 AC 对应 AA 的公钥以验证 AC。然后，根据用户属性、数据属性以及 d 调用 ACPMC 查询存储在本组织记账节点的访问控制策略，将访问控制策略、用户属性以及数据属性发送给 ACC 决策，生成访问控制结果。最后，向其它组织 AA 节点发送预准备消息〈PRE-PREPARE, v, n, d, h, c, u, o, p, r, i〉，其中，v 为当前视图编号，u 为用户属性，o 为数据属性，p 为访问控制策略，r 为访问控制结果，i 为当前节点的编号。

(3) prepare：AA2、AA3、AA4、AA5 收到 AA1 发送的预准备消息后，首先，对 d 重新生成摘要并与 h 比对，确保消息的完整性。其次，判决用户的访问请求，与 AA1 的判决过程相同。然后，向其它组织 AA 节点发送准备消息〈PREPARE, v, n, i, h, u, o, p, r〉。最后，收到来自非 AA1 的准备消息后，与 AA1 的预准备消息进行对比验证，验证的内容有 v、n、u、o、p、r、h。当有 $2f+1$ 个来自不同 AA 节点的准备消息与预准备消息一致时，进入确认阶段。

(4) commit：组织 AA 向其它节点发送确认消息〈COMMIT, v, n, i, $S(u, o, p, r)$〉，其中，$S(u, o, p, r)$ 为本节点对用户属性、数据属性、访问控制策略以及访问控制结果的签名。收到其它 AA 节点的确认消息后，通过 i 查找本地索引表中对应节点的公钥，验证确认消息的签名和 v、n、u、o、p、r。当有 $2f+1$ 个确认消息通过验证后，进入响应阶段；否则，可信查询失败。

(5) reply：组织 AA 节点向客户端发送响应消息〈REPLY, v, t, c, i, q, u, o〉，其中，q 为用户访问请求的验证结果。如果客户端接收到至少 $f+1$ 个相同的响应消息时，则根据 q 决定是否为用户授权；否则，可信查询失败。

2.4　访问控制管理函数

访问控制管理函数通过将数学符号以及实体符号相结合来形式化地描述访问控制流程，能够准确地管理访问控制过程[31]，为访问控制智能合约的设计提供了基础。管理员通过管理函数对数据进行有效管理，只有对各类数据做到高效和严格的管理，才能发挥最大的控制效能[32]。在猕猴桃溯源联盟链应用访问控制方案中，管理函数主要包括身份证书申请、属性证书申请、访问控制策略存储到联盟链、访问授权等。管理函数由实体、属性以及实体间关系组成。

实体是联盟链溯源应用中实际参与访问控制的集合，含义如表 1 所示。

表 1　实体描述

Tab. 1　Entity description

集合	实体及其含义
S	用户集合：$S=\{s_1, s_2, \cdots, s_i, \cdots, s_n\}$，$s_i$ 表示组织中的某一个用户
MKC	身份集合：$MKC=\{pkc_1, pkc_2, \cdots, pkc_i, \cdots, pkc_n\}$，$pkc_i$ 表示组织中某一个用户的身份证书
MAC	属性证书集合：$MAC=\{ac_1, ac_2, \cdots, ac_i, \cdots, ac_n\}$，$ac_i$ 表示组织中某一个用户的 AC
D	数据集合：$D=\{d_1, d_2, \cdots, d_i, \cdots, d_n\}$，$d_i$ 表示数据服务器中的某一数据
P	访问控制策略集合：$P=\{p_1, p_2, \cdots, p_i, \cdots, p_n\}$，$p_i$ 表示联盟链上的某一访问控制策略

属性指实体与访问控制相关的某些特征的集合。用户、数据、访问控制策略以及证书都有固有属性。实体的属性表示方法为：实体. $attr$，记为（属性名，运算符，属性值），如 $s.attr=(ino=20152586)$ 表示用户的唯一标识为 20152586。

实体间的关系是通过关系符号将各个实体集合连接起来,从而实现对实体属性的操作。各实体之间的关系如下:

(1)(S, MKC):表示一对一的用户与身份证书关系。如(s, pkc)∈(S, MKC)表示用户拥有组织 CA 颁发的身份证书。

(2)(S, MAC):表示一对一的用户与属性证书的关系。如(s, ac)∈(S, MAC)表示用户拥有组织 AA 颁发的 AC。

(3)($s.attr$, $d.attr$):表示用户属性与数据属性之间的关联关系。

关系符号还包括∧、∪、∀等。∧用于连接属性需同时满足的多个条件表达式。∪用于将单个实体合并到相应的实体集。∀用于取实体集中任何一个实体的属性。主要的管理函数定义如下:

(1)EnrollPKC(s, pkc):为用户颁发身份证书,ino 唯一标识用户。

条件:$s \in S$;

$s.attr = (ino \neq \varnothing \wedge ino \neq \forall\ s_i.ino)$;

操作:$MKC = MKC \cup pkc$, (s, pkc) ∈ (S, MKC).

(2)EnrollAC(s, ac):为用户颁发属性证书,age、dep、$role$ 表示用户的年龄、部门以及角色等。

条件:(s, pkc)∈(S, MKC);

$s.attr = (age, dep, role \neq \varnothing)$;

$s.attr = (ino \neq \varnothing \wedge ino \neq \forall\ s_i.ino)$;

操作:$MAC = MAC \cup ac$, (s, ac)∈(S, MAC).

(3)UploadPolicy(p, P):将访问控制策略存储在联盟链上,on 唯一标识访问控制策略,con 表示具体的访问控制策略。

条件:$p.attr(con \neq \varnothing)$;

$p.attr = (no \neq \varnothing \wedge no \neq \forall p_i.no)$;

操作:$P = P \cup p$.

(4)ManageDate(r, s):用户发出请求 r 操作数据服务器中的数据。verify(ac, pk)表示使用 AA 的公钥 pk 验证用户 ac。query(Arr, p)表示根据用户以及数据属性集 Arr 查询访问控制策略。如果满足访问控制策略,则访问数据 Operation(D)。

条件:(s, pkc)∈(S, MKC);

(s, ac)∈(S, MAC);

操作:$s.attr = (ino \neq \varnothing) => ac$;

$s.attr = (age, dep, role \neq \varnothing)$ (if verify(ac, pk));

$d.attr = (attr_1, attr_2, \cdots, attr_n \neq \varnothing)$;

$Arr = (s.attr, d.attr)$;

Operation(D)(if query(Arr, p)).

3 猕猴桃溯源联盟链应用访问控制智能合约

猕猴桃溯源联盟链访问控制方案中主要涉及 PKCMC、ACMC、ACPMC、DAMC、ACC 等 5 个智能合约。

(1)PKCMC 负责对用户身份证书的颁发和管理,只有组织管理员有权执行。使用 Hyperledger Fabric 中 CA 颁发的证书作为联盟链网络的准入凭证。PKCMC 主要定义的方法包括 PublishPKC()、RevokePKC()、ReenrollPKC(),分别为用户提供了颁发、撤销、重新颁发身份证书的功能。以 PublishPKC()为例,具体算法为:

```
PublishPKC(pkc.ino,pkc.pw, ca.name)
输入:(pkc.ino, pkc.pw, ca.name)
输出:( " Input Error/Register False/Enroll Success/Enroll Fail")
if (pkc.ino ! = null && pkc.pw ! = null && ca.name ! = null)
    then flag = Register(pkc.ino, pkc.pw, ca.name)//如果参数合法,开始身份证书登记
    else return "Input Error"//返回输入参数不合法的结果
    end if
    if (flag) then flag1 = Enroll(pkc.ino, pkc.pw)//如果身份证书登记成功,开始身份证书注册
    else return "Register False"//返回身份证书登记失败的结果
    end if
    if flag1 then reture "Enroll Success"//如果身份证书注册成功,返回注册成功的结果
    else return "Enroll Fail"//返回身份证书注册失败的结果
    end if
```

算法中,PublishPKC()由证书登记 Register()和证书注册 Enroll()两部分组成。pkc.ino、pkc.pw 以及 ca.name 分别表示申请证书所使用的用户标识、口令、CA 名称。Input Error、Register False、Enroll Success、Enroll Fail 是申请身份证书的 4 种不同结果,分别表示输入不合法、登记失败、注册成功、注册失败。

(2)ACMC 负责对用户的 AC 颁发和管理,只有组织管理员有权执行。ACMC 主要定义的方法包括 PublishAC()、RevokeAC()、ReenrollAC()、QueryAC()、ReadAC()、ValidateAC(),分别为用户提供了颁发、撤销、重新颁发、查询、读取以及验证 AC 的功能。以 PublishAC()为例,具体算法为

PublishAC(pkc.sk, pkc.pk, pkc.ino, s.a, aa.name)

输入：(pkc.sk, pkc.pk, pkc.ino, s.a, aa.name)

输出：("MesInput Error/PkcInput Error/Validate Error/Issue Success/Issue Fail")

if (pkc.ino ! = null && s.a ! = null && aa.name ! = null)

then reture R//如果参数合法,返回一个随机数

else return "MesInput Error"//返回属性信息输入不合法的结果

end if

if (pkc.sk ! = null && pkc.pk ! = null)//判断用户是否拥有身份证书

then Signature = Sign(R, pkc.sk)//用户用私钥对随机数签名

else return"PkcInput Error"//返回公私钥输入不合法的结果

end if

flag = Validate(Signature, pkc.pk)//属性权威验证用户的签名

if (flag) then flag1 = Issue(pkc.ino, s.a, aa.name)//如果验证通过,颁发属性证书

else return"Validate Error"//返回签名验证失败的结果

end if

if flag1 then UploadChain(pkc.ino, AC)//将属性证书写入联盟链

then reture "Issue Success"//返回属性证书签发成功的结果

else return "Issue Fail"//返回属性证书签发失败的结果

end if

算法中,PublishAC()包含用户身份认证和 AC 颁发两个过程。s.a、pkc.sk、pkc.pk 分别表示用户的属性信息、私钥、公钥。R 表示 AA 返回的随机数。aa.name 表示 AA 的名称。Signature 表示用户对 R 形成的签名信息。用户向 AA 提交个人属性信息以及对应 PKC 的标识,请求颁发 AC。AA 返回一个随机数,用户用私钥对该随机数签名,形成签名信息。AA 根据用户的公钥验证签名,若为真,则通过用户身份认证,AA 签发 AC,并把 AC 写入联盟链。MesInput Error、PkcInput Error、Validate Error、Issue Success、Issue Fail 是申请 AC 的 5 种不同结果,分别表示属性信息输入不合法、公私钥输入不合法、签名验证失败、签发成功、签发失败。

(3)ACPMC 负责存储和管理访问控制策略,只有组织管理员有权执行。访问控制策略存储在联盟上,确保权限的公开透明。ACPMC 主要定义的方法包括 UploadACP()、DownloadACP(),分别为管理员提供了向联盟链发布以及读取访问控制策略的功能。以 UploadACP()为例,具体算法为

UploadACP(acp)

输入：(acp)

输出：("Input Error/Upload False/Upload Success")

if (acp ! = null) then acphash = Hash(acp)//如果参数合法,将访问控制策略生成散列值

else return "Input Error"//返回参数输入不合法的结果

end if

txID = PutState(acphash, acp)//将访问控制策略以及散列值存储到联盟链

if (txID ! = null) then return "Upload Success"//如果交易 ID 不为空,返回写入账本成功的结果

else return "Upload False"//返回写入账本失败的结果

end if

算法中,UploadACP()主要由 HyperLedger Fabric SDK 提供的 PutState()方法实现。acp 表示访问控制策略,acphash 是访问控制策略的唯一标识,经过散列函数生成。Input Error、Upload False、Upload Success 是存储访问控制策略的 3 种不同结果,分别表示输入不合法、写入账本失败、写入账本成功。

(4)DAMC 用来存储和管理业务数据,只有非组织管理员有权执行。业务数据存储在链下的云服务器中,联盟链存储对应的散列值。DAMC 主要定义的方法包括 UploadDate()、DownloadDate()、AddDate()、UpdateDate()、QueryDate(),分别实现了业务数据的链上发布、链上查询、链下添加、链下更新、链下查询等功能。以 DownloadDate()为例,具体算法为

DownloadDate(Dateno)

输入：(Dateno)

输出：("Input Error/Download False/Download Success")

if (Dateno ! = null) then ChainHash = GetState(Dateno)//如果参数合法,从链上获取数据散列值

else return "Input Error"//返回参数输入不合

法的结果

end if

Date = QueryDate(Dateno) //查询链下数据服务器中的原始数据

DateHash = Hash(Date) //对链下原始数据生成散列值

if (ChainHash = = DateHash) then return "Download Success"

//如果链上散列值与链下散列值一致,返回查询成功的结果

else return "Download False" //返回查询失败的结果

end if

算法中,DownloadDate( ) 主要由 HyperLedger Fabric SDK 提供的 GetState( )方法实现。Dateno 表示数据唯一标识,ChainHash 是存储在联盟链上的数据散列值,Date 是存储在云服务器中的数据属性,DateHash 是 Date 的链下散列值。DateHash 与 ChainHash 的对比验证,保证链上链下数据的一致性。Input Error、Download False、Download Success 是查询链上业务数据的 3 种不同结果,分别表示输入不合法、查询失败、查询成功。

(5)ACC 用来响应用户对数据的访问请求,组织的任何用户都有权执行。ACC 定义的方法主要是 AccessControl( ),具体算法为

Grantaccess(Sno, Dateno, AAno)

输入:(Sno, Dateno, AAno)

输出:("MesInput Error/ResInput Error/ValidateAC Fail/Grant Success/Grant Fail")

if (Sno ! = null && Dateno ! = null && AAno ! = null)

then AC = ACMC. QueryAC(Sno) //如果参数合法,从链上查询属性证书

Date = DAMC. QueryDate(Dateno) //查询链下数据服务器中的原始数据

else return "MesInput Error" //返回参数输入不合法的结果

end if

if (Date! = null && AC ! = null)

then AAPK = QueryAAPK(AAno) //查询属性权威的公钥

flag = ACMC. ValidateAC(AC, AAPK) //验证用户属性证书

else return "ResInput Error" //返回属性证书或者原始数据查询失败的结果

end if

if (flag) then SubAttr = ACMC. ReadAC(AC) //如果属性证书验证通过,则读取用户属性

else return "ValidateAC Fail" //返回属性证书验证失败的结果

end if

Result = ACPMC. DownloadACP (SubAttr, ObjAttr) //查询链上的访问控制策略

If (Result) then reture "Grant Success" //如果查询到相应的访问控制策略,则允许用户访问

else return "Grant Fail" //返回拒绝访问的结果

end if

算法中,AccessControl( ) 主要由 ACMC. QueryAC( )、DAMC. QueryDate、QueryAAPK( )、ACMC. ValidateAC( )、ACMC. ReadAC( )、ACPMC. DownloadACP( )等方法组成。ACMC. QueryAC( )是智能合约 ACMC 提供的 AC 查询方法,可以查询用户存储在联盟链上的 AC。DAMC. QueryDate 是智能合约 DAMC 提供的原始数据查询方法,可以获取到存储在链下数据服务器中的原始数据。QueryAAPK( )提供了在本地索引表中查询 AA 公钥的功能。ACMC. ValidateAC( )智能合约 ACMC 提供的 AC 验证方法,利用 AA 公钥验证 AC 的合法性以及有效性。ACMC. ReadAC( )是智能合约 ACMC 提供的 AC 读取方法,用户 AC 验证通过后,解析读取 AC 中的属性信息。ACPMC. DownloadACP( )是智能合约 ACPMC 提供的访问控制策略查询方法,可以决策用户是否有相应的权限。Sno 表示主体唯一标识,Dateno 表示数据唯一标识,AAno 表示 AA 节点编号,AAPK 表示 AA 公钥,SubAttr 表示用户属性,Date 表示数据属性,Result 表示访问控制策略查询结果。MesInput Error、ResInput Error、ValidateAC Fail、Grant Success、Grant Fail 是判决访问请求的 5 种不同结果,分别表示请求内容不合法、AC 或者数据属性查询失败、AC 验证失败、允许访问、拒绝访问。

4 猕猴桃溯源联盟链应用访问控制测试与分析

本文选用农资电商、生产合作社、加工企业、电商平台等 4 个组织负责猕猴桃溯源“产购储加销”全产业链各个环节。为使得全链条溯源更为全面,将消费者权益组织加入联盟链网络,在保护消费者权益的同时,为消费者从组织记账节点查询猕猴桃产品溯源信息提供了便利。以包含 5 个组织的猕猴桃溯源全产业链为例,评测基于 PBFT 的猕猴桃溯源联盟链应用访问控制方案的功能与性能。

4.1　测试环境

(1)联盟链网络:选用 Hyperledger Fabric 1.4.0 搭建联盟链。Org_1. peer0、Org_2. peer0、Org_3. peer0、Org_4. peer0、Org_5. peer0 等 peer 节点充当组织记账节点,独立部署 1 个 order 节点和 5 个 CA 证书。状态数据库采用 levelDB。区块的最大交易数为 10 笔,最大打包时间间隔为 2s,最大字节数为 10MB。

(2)拜占庭共识算法:采用 corgi-kx 的 PBFT 算法 (https: // github. com/corgi-kx/blockchain_consensus_algorithm, 2019 - 12 - 1), AA1、AA2、AA3、AA4、AA5 充当查询验证节点。

(3)属性证书:遵循 X.509 v3 标准,签名算法选用 RSA。

(4)性能测试工具:Hyperledger Caliper。它是一个通用的区块链性能测试框架,允许用户使用自定义的用例测试不同的区块链解决方案,得到一组性能测试结果。

(5)系统环境:ubuntu 虚拟机 18.04,8 GB 内存,50 GB 存储磁盘,处理器内核总数为 2,带宽为 1 000 Mb/s。

4.2　功能测试

(1)访问控制策略的数据结构

访问控制策略 $P = \{U\_age, U\_dep, U\_role, D\_dep, D\_tem, D\_attr_1, D\_attr_2, \cdots, D\_attr_n, Operation\}$,其中,U_age、U_dep、U_role 分别表示管理员的年龄、所属部门以及角色;D_dep、D_tem 分别表示业务数据的来源以及类别;$D\_attr_1, \cdots, D\_attr_n$ 表示业务数据的属性;Operation 表示访问能力。

假设生产合作社某一条访问控制策略 $p_1 = \{$大于 25 岁,种植部门,业务管理员,幼苗培育部门,温室数据,日期,查询$\}$,表示年纪 25 岁以上的种植部门业务管理员有权查询某一个时间段的幼苗培育部门中的温室数据。

(2)访问控制可信决策过程

以生产合作社种植部门的业务管理员查询某一个时间段幼苗培育部门的温室数据为例。温室数据由物联网设备直接写入链下的数据库中,由幼苗培育部门的业务管理员存储到联盟链。本次查询是从链下的数据库中获取温室数据并进行防伪验证。业务管理员唯一标识为 20152586,用户属性集为$\{$大于 25 岁,种植部门,业务管理员$\}$,访问控制策略 p_1,用户发起访问请求的页面如图 5 所示。

在图 5 中,业务管理员选择数据的来源、类别以及时间范围,即数据属性集为$\{$幼苗培育部门,温室数据,2022 - 03 - 13 19:10_2022 - 03 - 14 21:10$\}$,访问能力为查询操作。业务管理员发出查询请求后,系统判决其是否具有相应权限,访问控制过程的可信决策如图 6 所示。

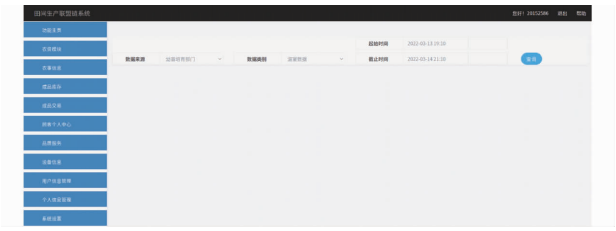
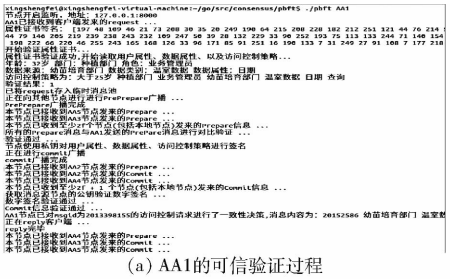
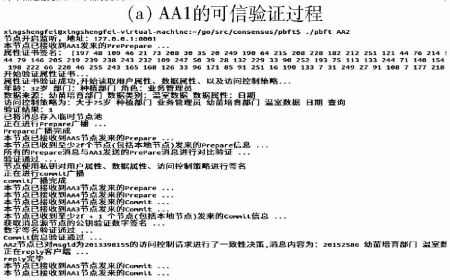


图 5　用户发起访问请求界面

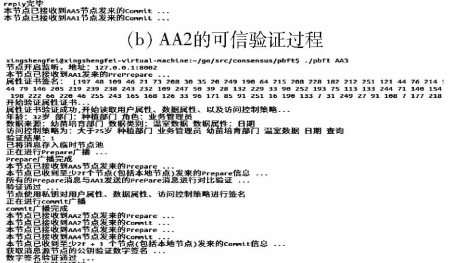
Fig. 5　User initiated an access request



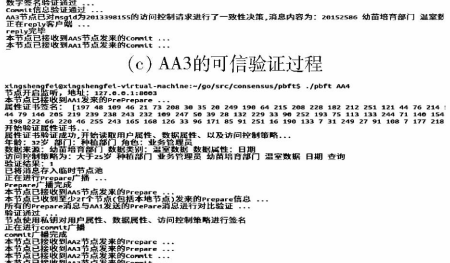
(a) AA1的可信验证过程



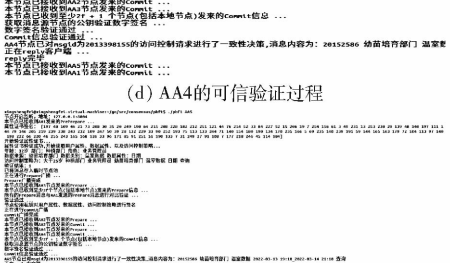
(b) AA2的可信验证过程



(c) AA3的可信验证过程



(d) AA4的可信验证过程



(e) AA5的可信验证过程

图 6　访问控制过程的可信决策

Fig. 6　Trusted decisions for access control processes

从图 6 可以看出,当种植部门的业务管理员发出访问控制请求后,联盟链各组织的的 AA 节点基

于 PBFT 对访问授权过程可信验证，客户端依据可信验证结果决定业务管理员的权限。访问控制请求内容由管理员唯一标识、数据类型、数据来源、日期、查询操作构成。主节点 AA1 收到客户端发来的请求消息后，执行过程如图 6a 所示。从节点 AA2、AA3、AA4、AA5 收到 AA1 发来的预准备消息后，执行过程如图 6b～6e 所示。各节点通过访问请求内容获取到的用户属性集为{32 岁，种植部门，业务管理员}，数据属性集为{幼苗培育部门，温室数据，2022－03－13 19:10_2022－03－14 21:10}，访问控制策略为{大于 25 岁，种植部门，业务管理员，幼苗培育部门，温室数据，日期，查询}。

基于 PBFT，各节点对用户属性、数据属性以及访问控制策略可信验证的具体工作流程如图 7 所示。

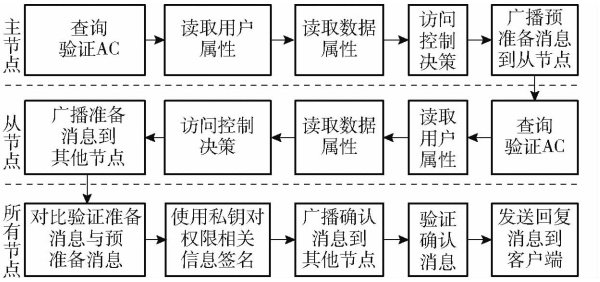


图 7 节点工作流程

Fig. 7 Node workflow

在图 7 中，首先，主从节点先后查询验证 AC、读取用户属性、读取数据属性以及决策访问控制请求，并分别广播预准备消息和准备消息到其他节点；其次，所有节点对比验证准备消息与预准备消息，验证通过后，使用私钥对权限相关信息签名，广播确认消息到其他节点；最后，各节点验证确认消息，根据确认结果，向客户端发送回复消息。

根据访问控制过程的可信决策结果可知，业务管理员拥有相应的操作权限，系统响应请求页面如图 8 所示。

图 8 系统响应请求页面

Fig. 8 System responded to request page

在图 8 中，页面显示的温室数据是从链下数据库中获取到的原始数据，种植部门的业务管理员需要执行防伪验证操作从联盟链上查询原始数据的散列值，与数据库中现有数据实时生成的散列值进行对比验证，确保原始数据的一致性。

以工作 ID 为 82 的温室数据为例，防伪验证的结果如图 9 所示。

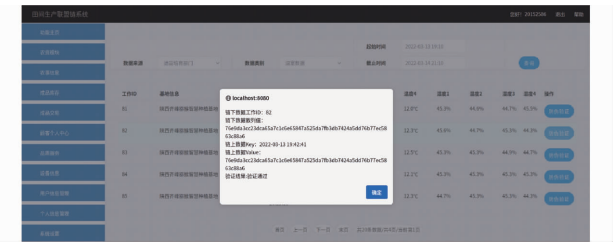


图 9 防伪验证

Fig. 9 Anti-counterfeiting verification

从图 9 可以看出，链上数据包含一个键值对(Key，Value)，其中，Key 为温室数据的记录时间，唯一标识该数据，Value 为数据的散列值。只有存储到联盟链上的数据才可以进行防伪验证，确保链下数据的完整性。由验证结果可知，链上数据的散列值与链下数据实时形成的散列值完全一致，说明该数据自上链以后未被篡改，查询结果真实可信。

(3)链码的核心操作

由访问控制可信决策过程可看出，主节点 AA1 以及从节点 AA2、AA3、AA4 分别在预准备阶段和准备阶段到各自组织的记账节点上查询管理员属性证书、链上的数据散列值以及访问控制策略。通过 Hyperledger Fabric 的命令行模式直接调用 ACMC. QueryAC( )、DAMC. DownloadDate( )以及 ACPMC. DownloadACP( )函数查询管理员属性证书、链上的数据散列值以及访问控制策略，查询结果与通过 HyperLedger Fabric SDK 调用链码查询出的结果保持一致，执行过程如图 10 所示。

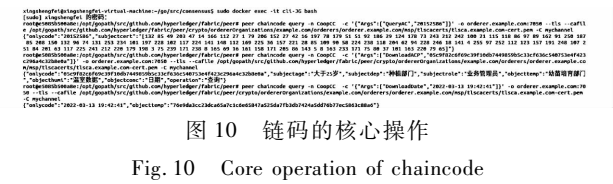


图 10 链码的核心操作

Fig. 10 Core operation of chaincode

由图 10 可以看出，联盟链账本上存储管理员属性证书的 Key 为 20152586，Value 为以字节形式表示的证书内容；账本上存储访问控制策略 p_1 的 Key 为 05c9f82c6f69c39f10db7449859b5c33cf636c5 40753e4f423c296a4c32b8e0a，Value 为{大于 25 岁，种植部门，业务管理员，幼苗培育部门，温室数据，日期，查询}；账本上存储温室数据的 Key 为 2022－03－13 19：42：41，Value 为 76e9da3cc23dca65a7c1c6e65847a525da7fb3db7424a5dd76b77ec5863c88a6。

4.3 性能测试

4.3.1 测试方案

通过模型共识过程可以看出，数据处理请求发

出到响应的时间主要由区块链查询时间决定，因此，主要测试不同交易总量、交易发送率条件下的访问控制策略链上查询效率。用交易吞吐量以及平均时延作为主要性能评估指标。通过设置相应的基准测试用例以及相关的配置文件来模拟测试不同条件下的网络性能。测试方案如下：

（1）基本参数为访问控制策略 p_1。

（2）交易总量分别为 1 000、2 000、3 000 条，对应测试方案 1、方案 2 和方案 3。

（3）交易发送率分别为 100、200、…、1 400、1 500 TPS，TPS 表示每秒向系统提交的并发交易量。

（4）每轮重复 10 次，取均值作为交易吞吐量和平均时延的最终结果。

4.3.2　测试与分析

（1）交易吞吐量是指区块链网络每秒成功处理的交易数，当一笔交易读写到区块链上，该交易处理成功。访问控制策略查询的交易吞吐量测试结果如图 11 所示。

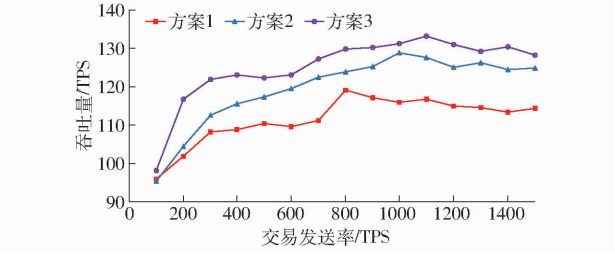


图 11　访问控制策略查询的交易吞吐量

Fig. 11　Transaction throughput for access control policy queries

由图 11 可以看出，3 种方案在交易发送率达到 300 TPS 前，交易吞吐量线性上升；在交易发送率达到 300 TPS 后，交易吞吐量总体趋于稳定。这是由于随着交易发送率越来越大，消息队列堵塞，磁盘读写速度变慢造成的。当交易发送率为 800、1 000、1 100 TPS时，3 种方案的交易吞吐量达到最高值。当交易发送率相同时，向联盟链提交交易总量越高，交易吞吐量越高。

（2）平均时延是指一笔交易从发起交易请求到收到交易处理结果所经历的时间间隔。访问控制策略查询的平均时延测试结果如图 12 所示。

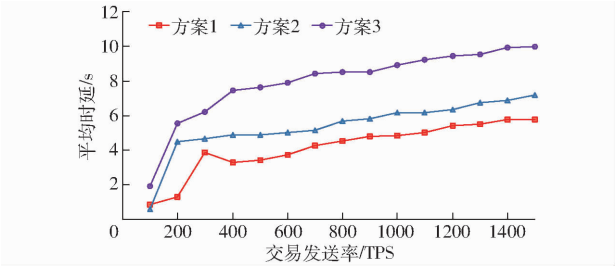


图 12　访问控制策略查询的平均时延

Fig. 12　Average latency for access control policy queries

由图 12 可看出，3 种方案在交易发送率 400 TPS 前平均时延波动较大；在交易发送率 400 TPS 后平均时延基本稳定。这是由于随着交易发送率增加，消息队列堵塞，导致磁盘读写速度变慢造成的。在相同交易发送率条件下，向联盟链提交交易总量越高，平均时延越高。

5　结论

（1）针对基于属性的联盟链应用访问控制模型可能存在拜占庭节点而导致属性信息、访问控制策略不可信的问题，以猕猴桃溯源为应用场景，利用属性证书真实、有效、可验证以及 PBFT 具备拜占庭容错能力的特点，提出了基于 PBFT 的猕猴桃溯源联盟链应用访问控制方案。所有用户申请 AC，存储与权限相关的属性。管理员将访问控制策略存储在联盟链上。用户发出访问请求后，组织 AA 调用智能合约查询链上的 AC、访问控制策略以及数据服务器中的数据属性，并基于 PBFT 查询验证用户属性、数据属性、访问控制策略的可信性，以决定是否为用户授权。

（2）基于 Hyperledger Fabric 猕猴桃溯源应用的测试结果可以看出，通过访问控制可信决策、核心链码测试表明方案合理、可行；通过不同交易总量、交易发送率条件下的访问控制策略链上查询性能测试表明交易吞吐量和平均时延均能达到稳定状态，交易吞吐量在交易发送率为 300 TPS 后趋于稳定，平均时延在交易发送率为 400 TPS 后趋于稳定，基本满足联盟链系统的应用需求。该方案具有良好的可用性和性能，保证了访问控制过程的可信性以及一致性，提高了猕猴桃溯源应用的安全性、容错性。

参　考　文　献

[1] BERDIK D, OTOUM S, SCHMIDT N, et al. A survey on blockchain for information systems management and security[J]. Information Processing and Management, 2021, 58(1): 102397.

[2] MORKUNAS V J, PASCHEN J, BOON E. How blockchain technologies impact your business model[J]. Business Horizons, 2019, 62(3): 295 - 306.

[3] YANG L. The blockchain: state-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15: 80 - 90.

[4] 刁一晴, 叶阿勇, 张娇美, 等. 基于群签名和同态加密的联盟链双重隐私保护方法[J]. 计算机研究与发展, 2022,

59(1): 172 - 181.
DIAO Yiqing, YE Ayong, ZHANG Jiaomei, et al. A dual privacy protection method based on group signature and homomorphic encryption for alliance blockchain[J]. Journal of Computer Research and Development, 2022, 59(1): 172 - 181. (in Chinese)
[5] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述:原理、进展与应用[J]. 通信学报, 2020, 41(1): 134 - 151.
ZENG Shiqin, HUO Ru, HUANG Tao, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134 - 151. (in Chinese)
[6] 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)
[7] 许继平, 王健, 张新, 等. 区块链驱动的稻米供应链信息监管模型研究[J]. 农业机械学报, 2021, 52(5): 202 - 211.
XU Jiping, WANG Jian, ZHANG Xin, et al. Information supervision modeling of rice supply chain driven by blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(5): 202 - 211. (in Chinese)
[8] 任守纲, 何自明, 周正己, 等. 基于 CSBFT 区块链的农作物全产业链信息溯源平台设计[J]. 农业工程学报, 2020, 36(3): 279 - 286.
REN Shougang, HE Ziming, ZHOU Zhengji, et al. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT - Blockchain[J]. Transactions of the CSAE, 2020, 36(3): 279 - 286. (in Chinese)
[9] 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.
YU Huajing, XU Daming, LUO Na,et al. Design of the blockchain multi-chain traceability supervision model for coarse cereal supply chain[J]. Transactions of the CSAE, 2021, 37(20): 323 - 332. (in Chinese)
[10] 杨信廷, 王杰伟, 邢斌, 等. 基于区块链的畜牧养殖资产监管身份认证研究[J]. 农业机械学报, 2021, 52(11): 170 - 180.
YANG Xinting, WANG Jiewei, XING Bin, et al. Identification of animal husbandry assets supervision based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(11): 170 - 180. (in Chinese)
[11] 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.
ZHANG Xin, PENG Xiangzhen, XU Jiping, et al. Dynamic supervision model of rice supply chain based on blockchain and smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(1): 370 - 382. (in Chinese)
[12] 葛艳, 黄朝良, 陈明, 等. 基于区块链的 HACCP 质量溯源模型及系统实现[J]. 农业机械学报, 2021, 52(6): 369 - 375.
GE Yan, HUANG Chaoliang, CHEN Ming, et al. HACCP quality traceability model and system implementation based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(6): 369 - 375. (in Chinese)
[13] GEORGE R V, HARSH H O, RAY P, et al. Food quality traceability prototype for restaurants using blockchain and food quality data index[J]. Journal of Cleaner Production, 2019, 240: 118021 - 118028.
[14] 许继平, 孙鹏程, 张新, 等. 基于区块链的粮油食品供应链信息安全管理原型系统[J]. 农业机械学报, 2020, 51(2): 341 - 349.
XU Jiping, SUN Pengcheng, ZHANG Xin, et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(2): 341 - 349. (in Chinese)
[15] 董云峰, 张新, 许继平, 等. 基于区块链的粮油食品供应链可信追溯模型[J]. 食品科学, 2020, 41(9): 30 - 36.
DONG Yunfeng, ZHANG Xin, XU Jiping, et al. Blockchain-based traceability model for grains and oils whole supply chain[J]. Food Science, 2020, 41(9): 30 - 36. (in Chinese)
[16] 房梁, 殷丽华, 郭云川, 等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报, 2017, 40(7): 1680 - 1698.
FANG Liang, YIN Lihua, GUO Yunchuan, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, 40(7): 1680 - 1698. (in Chinese)
[17] 张建标, 张兆乾, 徐万山, 等. 一种基于区块链的域间访问控制模型[J]. 软件学报, 2021, 32(5): 1547 - 1564.
ZHANG Jianbiao, ZHANG Zhaoqian, XU Wanshan, et al. Inter-domain access control model based on blockchain[J]. Journal of Software, 2021, 32(5): 1547 - 1564. (in Chinese)
[18] 杜瑞忠, 刘妍, 田俊峰. 物联网中基于智能合约的访问控制方法[J]. 计算机研究与发展, 2019, 56(10): 2287 - 2298.
DU Ruizhong, LIU Yan, TIAN Junfeng. An access control method using smart contract for internet of things[J]. Journal of Computer Research and Development, 2019, 56(10): 2287 - 2298. (in Chinese)
[19] MAlAMAS V, KOTZANIIOLAOU P, DASAKLIS T K, et al. A hierarchical multi blockchain for fine grained access to medical data[J]. IEEE Access, 2020, 8: 134393 - 134412.
[20] DING S, CAO J, LI C, et al. Anovel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019, 7: 38431 - 38441.
[21] ZHAGN Y, LI B, LIU B, et al. Anattribute-based collaborative access control scheme using blockchain for IoT devices[J]. Electronics, 2020, 9(2): 285.
[22] MAESA D D, MORI P, RICCI L. A blockchain based approach for the definition of auditable access control systems[J]. Computers & Security, 2019, 84: 93 - 119.
[23] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636 - 2654.

LIU Aodi, DU Xuehui, WANG Na, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636 – 2654. (in Chinese)

[24] XIAO Y, ZHANG N, LOU W J, et al. A survey of distributed consensus protocols for blockchain networks[J]. IEEE Commumications Surveys and Tutorials, 2020, 22(2): 1432 – 1465.

[25] WANG Y H, CAI S B, LIN C L, et al. Study of blockchains's consensus mechanism based on credit[J]. IEEE Access, 2019, 7: 10224 – 10231.

[26] WAN S H, LI M J, LIU G Y, et al. Recent advances in consensus protocols for blockchain: a survey[J]. Wireless Networks, 2020, 26(8): 5579 – 5593.

[27] 乔蕊, 曹琰, 王清贤. 基于联盟链的物联网动态数据溯源机制[J]. 软件学报, 2019, 30(6): 1614 – 1631.
QIAO Rui, CAO Yan, WANG Qingxian. Traceability mechanism of dynamic data in internet of things based on consortium blockchain[J]. Journal of Software, 2019, 30(6): 1614 – 1631. (in Chinese)

[28] 邵奇峰, 张召, 朱燕超,等. 企业级区块链技术综述[J]. 软件学报, 2019, 30(9): 2571 – 2592.
SHAO Qifeng, ZHANG Zhao, ZHU Yanchao, et al. Survey of enterprise blockchains[J]. Journal of Software, 2019, 30(9): 2571 – 2592. (in Chinese)

[29] VAIDYA B, MAKRAKIS D, MOUFTAH H T. Authentication and authorization mechanisms for substation automation in smart grid network[J]. Network IEEE, 2013, 27(1): 5 – 11.

[30] TOUCEDA D S, CAMARA J M S, ZEADALLY S, et al. Attribute-based authorization for structured peer-to-peer (p2p) networks[J]. Computer Standards & Interfaces, 2015, 42: 71 – 83.

[31] 李凤华, 陈天柱, 王震, 等. 复杂网络环境下跨网访问控制机制[J]. 通信学报, 2018, 39(2): 1 – 10.
LI Fenghua, CHEN Tianzhu, WANG Zhen, et al. Cross-network access control mechanism for complex network environment [J]. Journal on Communications, 2018, 39(2): 1 – 10. (in Chinese)

[32] 王于丁, 杨家海. 一种基于角色和属性的云计算数据访问控制模型[J]. 清华大学学报(自然科学版), 2017, 57(11): 1150 – 1158.
WANG Yuding, YANG Jiahai. Data access control model based on data's role and attributes for cloud computing[J]. Journal of Tsinghua University (Science and Technology), 2017, 57(11): 1150 – 1158. (in Chinese)

(上接第 182 页)

[21] 姜红花,牛成强,刘理民,等. 果园多风管风送喷雾机风量调控系统设计与试验[J]. 农业机械学报,2020,51(增刊 2): 298 – 307.
JIANG Honghua,NIU Chengqiang, LIU Limin,et al. Design and experiment of air volume control system of orchard multi-pipe air sprayer[J]. Transactions of the Chinese Society for Agricultural Machinery,2020,51(Supp. 2):298 – 307. (in Chinese)

[22] 郑永军,陈炳太,吕昊暾,等. 中国果园植保机械化技术与装备研究进展[J]. 农业工程学报,2020,36(20):110 – 124.
ZHENG Yongjun,CHEN Bingtai,LÜ Haotong,et al. Research progress of orchard plant protection mechanization technology and equipment in China[J]. Transactions of the CSAE,2020,36(20):110 – 124. (in Chinese)

[23] 王韦韦,谢进杰,陈黎卿,等. 3YZ – 80A 型履带自走式玉米行间喷雾机设计与试验[J]. 农业机械学报,2021,52(9):106 – 114.
WANG Weiwei,XIE Jinjie, CHEN Liqing, et al. Design and experiment of 3YZ – 80A crawler self-propelled corn interrow sprayer[J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(9):106 – 114. (in Chinese)

[24] 刘慧,龙友能,何思伟,等. 四轮独立电驱动高地隙喷雾机辅助转向系统设计与试验[J]. 农业工程学报,2021,37(13): 30 – 37.
LIU Hui,LONG Youneng,HE Siwei,et al. Design and experiment of the auxiliary steering system for a four-wheel independent electrically driven high clearance sprayer[J]. Transactions of CSAE,2021,37(13):30 – 37. (in Chinese)

[25] 刘国海,李持衡,沈跃,等. 同步转向高地隙喷雾机模糊自适应轨迹跟踪预测控制[J]. 农业机械学报,2021,52(9):389 – 399.
LIU Guohai,LI Chiheng,SHEN Yue,et al. Trajectory tracking and fuzzy adaptive model predictive control of high clearance synchronous-steering sprayer[J]. Transactions of the Chinese Society for Agricultural Machinery,2021,52(9):389 – 399. (in Chinese)

[26] 李遇春. 液体晃动动力学基础[M]. 北京:科学出版社,2017.

[27] 王照林,刘延柱. 充液系统动力学[M]. 北京:科学出版社,2002.

[28] 陈雨. 高地隙喷雾机独立式立轴空气悬架设计方法与特性研究[D]. 北京:中国农业大学,2017.
CHEN Yu. Research on design methods and characteristics of independent strut type air suspension system for high clearance sprayer[D]. Beijing:China Agricultural University,2017. (in Chinese)

[29] 陈雨,陈随英,杜岳峰,等. 基于摩擦阻尼的高地隙农机底盘悬架减振特性[J]. 农业工程学报,2016,32(7):51 – 57.
CHEN Yu, CHEN Suiying, DU Yuefeng, et al. Damping characteristics of chassis suspension system of high clearance agricultural machinery based on friction damper[J]. Transactions of the CSAE,2016,32(7):51 – 57. (in Chinese)