软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(5):1547−1564 [doi: 10.13328/j.cnki.jos.006011]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种基于区块链的域间访问控制模型*

张建标[1,2], 张兆乾[1,2], 徐万山[1,2], 吴 娜[1,2]

[1](北京工业大学 信息学部,北京 100124)

[2](可信计算北京市重点实验室(北京工业大学),北京 100124)

通讯作者: 张建标, E-mail: zjb@bjut.edu.cn

摘 要: 云计算、物联网和移动互联网等新型计算模式的出现,使得域间相互访问以及数据共享的需求不断扩大,而目前“中心化”的传统访问控制技术所显现出的访问控制策略执行不透明、动态数据管理不灵活、资源拥有者自主性差,使其难以满足海量、动态和分布的新型计算模式.提出了一种以 ABAC 模型为基础、以区块链为交互方式的域间访问控制模型.介绍了 ABAC 模型和区块链的技术原理、特点、研究现状,详细阐述了模型框架,对 ABAC 模型进行了形式化定义;同时,对模型中的智能合约进行了具体描述,给出了本模型在具体场景中的应用和具体的访问控制流程;最后对比了现有的研究方案.该模型可以为域间访问提供标准化的安全、便捷、自主且细粒度的访问控制.

关键词: 区块链;ABAC;跨域;访问控制;数据共享

中图法分类号: TP393

中文引用格式: 张建标,张兆乾,徐万山,吴娜.一种基于区块链的域间访问控制模型.软件学报,2021,32(5):1547−1564. http://www. jos.org.cn/1000-9825/6011.htm

英文引用格式: Zhang JB, Zhang ZQ, Xu WS, Wu N. Inter-domain access control model based on blockchain. Ruan Jian Xue Bao/Journal of Software, 2021,32(5):1547−1564 (in Chinese). http://www.jos.org.cn/1000-9825/6011.htm

Inter-domain Access Control Model Based on Blockchain

ZHANG Jian-Biao[1,2], ZHANG Zhao-Qian[1,2], XU Wan-Shan[1,2], WU Na[1,2]

[1](Faculty of InformationTechnology, Beijing University of Technology, Beijing 100124, China)

[2](Beijing Key Laboratory of Trusted Computing (Beijing University of Technology), Beijing 100124, China)

Abstract: The emergence of new computing paradigms such as cloud computing, the Internet of Things, and the mobile Internet has increased the need for inter-domain access and data sharing, while at present the “centralized” traditional access control technology have showed opaque of access control policy execution, inflexibility of dynamic data management, low-autonomy of resource owners, these shortcomings make it difficult to satisfy the requirements of access control for new computing paradigms with massive, dynamic, and distributed features, an inter-domain access control model based on ABAC model and blockchain interaction is proposed. This paper introduces the technical principle, characteristics and research status of the ABAC model and blockchain, elaborates the model framework, defines the definition of the ABAC model. At the same time, the smart contract in the model is described in detail, and the application in the specific scenario and the specific access control flow are given. Finally, compared with the existing research solution, this model can provide standardized security, convenient, autonomous, and fine-grained access control for inter-domain access.

Key words: blockchain; ABAC; cross-domain; access control; data sharing

随着互联网的迅猛发展,数据成为网络时代最重要的资源.各种安全域之间的数据交换共享变得必不可少,

* 基金项目: 北京市自然科学基金(M21039); 北京工业大学国际种子基金(2018A01)

Foundation item: Natural Science Foundation of Beijing Municipality (M21039); International Research Cooperation Seed Fund of Beijing University of Technology (2018A01)

收稿时间: 2019-08-10; 修改时间: 2019-10-19; 采用时间: 2019-12-19

但是网络安全形势错综复杂、十分严峻,如何保障域间数据安全共享,成为当下信息安全研究的重点[1].对“信息孤岛[2]”问题,有的解决方案提出用集中式的数据平台来整合各个安全域的数据资源,虽然在一定程度上解决了该问题,但是这种传统的“中心化”也面临一些安全隐患[3],例如中心服务器易被攻击、数据易被篡改、面临宕机风险、权限判决不透明、无法判断中心化的判决是否真实地执行了策略制定者的意图[4]等等.

同时,因为各个安全域会按照自身的安全需求制定自己的访问控制策略,当一个终端用户或者安全域需要请求不同安全域的同一类型资源时,就需要针对不同安全域提出不同的请求,不便于用户访问或者域间数据共享;而对于被访问的安全域来说,拥有对资源的授权自主性也十分必要.另外,云计算、物联网等新型计算模式的出现,形成了当前动态的计算环境[5],这就使得各安全域之间数据交换共享的安全需求变的更为复杂.面对新型计算模式带来的安全挑战,传统的访问控制无法及时、有效地对其进行控制管理[5,6].

为了解决上述问题,本文提出一种基于区块链的域间访问控制模型,以基于属性的访问控制模型(attribute-based access control,简称 ABAC)为基础,使用统一的属性标准描述各域的访问控制策略,达到动态管理数据、方便系统管理、便于用户访问的目的;以区块链网络为交互媒介,以智能合约为驱动,达到策略判定自动化,策略执行真实、可信、透明且可追溯、可审计的目的;安全域可以选择使用非对称加密技术对敏感信息进行处理,达到保护隐私的目的;同时,各域根据属性标准制定满足自身安全需求的访问控制策略并维护,并根据访问控制策略执行结果自主授权,实现域间数据自主可控共享、访问控制策略自主定制、数据资源灵活管理的域间数据安全共享.

1 相关技术及研究

1.1 基于属性的访问控制模型ABAC

访问控制[7]作为保护数据资源的一种重要手段,一直都是安全方面研究的重点.传统的访问控制,包括自主访问控制(discretionary access control,简称 DAC)、强制访问控制(mandatory access control,简称 MAC)、基于角色的访问控制(role-based access control,简称 RBAC),均在不同场景发挥着相应的作用,见表 1.

Table 1 Traditional access control technology

表 1 传统访问控制技术

名称	作用	优点	缺点
DAC	主体对客体的访问权限进行自主管理,主体决定是否将客体的全部或部分访问权限授予其他主体,可应用于许多系统环境	比较灵活,具有一定的可扩展性	安全性差 开销大,效率低 静态分配权限
MAC	系统强制主体服从访问控制规则,主体和客体都被系统分配一个固定的安全属性(安全等级),利用安全属性(安全等级)决定一个主体能否访问某个客体,应用于强调机密等级的应用领域如军事、金融等	增强信息的机密性,安全性较高	灵活性差 静态分配权限
RBAC	权限和角色关联,通过为主体分配适当的角色,使其能够获得相应角色的权限,应用较为广泛	简化策略管理,明确责任和授权,安全性高,灵活性、可扩展性较高	较粗粒度 静态分配权限

随着云计算、物联网、移动互联网等新型计算模式的日新月异,这些新型计算模式所具有的一些特点给访问控制技术带来了相当大的挑战.

(1) 海量性.新型计算模式中,终端和用户数量呈现海量性特点.以物联网为例,终端节点的数量会随着物联网的发展变得十分庞大,而且终端节点的种类和数据格式繁多.面对海量的终端和权限,传统访问控制技术使用静态的方式管理用户和权限,随着数据的增长,往往需要构建和维护庞大的访问控制列表,不仅极大地增加系统开销,而且降低了访问控制效率.

(2) 动态性.新型计算模式中,节点、用户以及数据呈现动态性特点.在移动互联网中,终端节点以及用户不断移动;在云计算中,用户变动频繁,节点动态接入,数据对象实时变化.这些均体现出很强的动态性.传统的静态访问控制技术无法在动态环境下提前预知用户信息,无法准确了解用户和权限结构,更无法提前设定用户与权限的对应关系.同时,动态性使得静态的访问控制策略的更新更加复杂敏感.

(3) 分布式.新型计算模式中,不同域间的资源共享和信息互访需求增多,但不同的域是相互独立的,各自拥有自己的访问控制策略,一个域中的用户所具有的权限在另一个域中往往会失效.而传统访问控制技术更多应用在封闭环境下,面对新型计算环境下分布式特点,传统访问控制技术无法支持各域统一访问控制策略标准,并且若采用单一授权机构进行管理,海量用户和数据的频繁变动,会带来非常大的管理以及运算负担.

由于具有以上特点,传统的访问控制技术难以满足新型计算环境对访问控制的需求[8].因此,面对新型计算环境,基于主体、资源、操作和环境所提出的基于属性的细粒度访问控制应运而生.

ABAC[9]将主体和客体的属性作为基本决策要素,使用属性或属性集合[10]来描述实体,基于属性的逻辑语义描述访问控制策略,将策略管理和权限判定解耦.通过更加细粒度的属性或属性集合,从多个角度描述实体,并加入了环境实体作为另一种约束,从而可以针对实际情况对策略进行更改[11],具有相当程度的灵活性.

由于属性是实体固有的特性,通过实体属性发现机制,可以挖掘出独立、完备的实体属性集合,不需要事先手动分配,根据请求者以及访问资源所需求的属性进行授权,使得 ABAC 管理相对简单;并且在 ABAC 模型中,策略随用户和资源的增多呈线性增长[12],面对海量的用户和数据,系统开销较小并且可以有效解决动态性问题;同时,ABAC 所具有的细粒度性以及低复杂度且表达丰富的策略描述语言,可以使其恰当地应用在分布式环境中,并具有良好的可扩展性,是一种理想的访问控制模型.因此,ABAC 已经发展成为国防和情报界以及政府在内的许多机构的首选逻辑访问控制方法.

1.2 区块链相关技术

自中本聪 2008 年提出比特币[13]以来,区块链技术随着比特币等数字加密货币的兴起而引起各个行业的广泛关注.由于区块链技术所具有的去中心化、时序数据、集体维护、可编程和安全可信等优势,在单链上的节点间无须互相信任就可以实现基于去中心化信用的点对点交易,相互协调合作,数据共享,从而为解决中心化机构所存在的不安全的数据存储提供了解决方案[14].区块链技术在本质上是一个状态机副本协议[15,16],通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案[17].区块链数据不断增长,一经上链则无法修改或删除.通过这样的方式增加被攻击难度,参与维护的各节点可以通过区块链网络同步链上的所有数据而成为全节点.区块链的核心技术包括分布式账本技术、非对称加密算法以及智能合约等,具有去中心化共识机制、可追溯性以及高度信任等特征.正是由于比特币拥有诸多这些其他技术不可比拟的优势,使得区块链技术在现在社会系统中可以有着更加广泛的应用前景.

目前,随着区块链技术的发展,已经从区块链 1.0 比特币时代经过区块链 2.0 的智能合约时代发展到了如今的区块链 3.0 时代[18].智能合约[19]在区块链中的应用,使得区块链技术不再局限于金融方面,而是扩展了区块链的应用场景,进一步延伸到任何有需求的领域.智能合约本质上讲是由事件驱动的、具备状态的、部署于可共享的分布式数据库上的计算机程序,这些自动化程序一旦部署,就能实现自我执行和自我验证.同时,区块链除了公有链之外,私有链、联盟链逐渐成为当下研究热点,尤其是联盟链得到产学界的广泛关注.联盟链介于公有链和私有链之间,具有弱中心化、交易效率高、成本低、具备一定程度的访问限制等特点,参与者通过授权加入网络,参与维护联盟链的正常运行.相比公有链和私有链,联盟链具有更加广泛的应用场景和需求.

1.3 相关研究

近些年来,域间数据共享和访问控制在权限判定方面的研究大部分都侧重于集中式的权限判定,结构如图 1 所示,各域首先必须信任“中心化”第三方去执行授权操作.例如,江泽涛等人[20]提到的“异域控制模式”中,访问控制决策需要由一个可信的第三方域执行;张帅等人[21]提出一种基于 RBAC 的跨多企业服务组合访问控制模型,其中,用户需求经过中心引擎构建组合服务流程 CS 提交给各域后,会被“中心化”的面向服务授权框架中的策略执行点(policy enforcement point,简称 PEP)截获后进行处理;Joshi 等人[22]针对松耦合的多域环境提出一种“中心式”的扩展 RBAC 模型架构,通过中心化的“系统管理员”设置多域环境中的用户分配角色.虽然“中心化”的访问控制可以有效地解决域间互操作的问题,但同样面临“中心化”所带来的安全风险,例如权限判定不透明、

策略容易被篡改、单点故障等等.

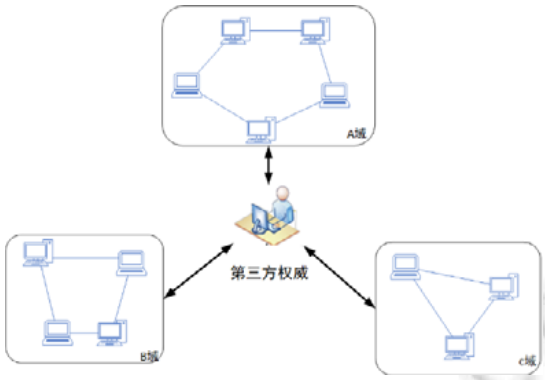

Fig.1 Centralized structure

图 1 集中式结构

随着区块链技术热度的提升,越来越多的研究将区块链技术应用于数据共享和访问控制,将区块链委托第三方进行维护,结构如图 2 所示.例如,Zyskind 等人[23]通过区块链存储包含访问控制策略的个人数据,以解决用户无法撤销对其私人数据的授权访问问题,其中的区块链系统委托第三方节点维护;Ding 等人[24]针对传统的访问控制技术不适用于物联网复杂和大规模的网络结构问题,提出一种基于属性的物联网系统访问控制方案,使用区块链技术来记录属性的分布,以避免单点故障和数据篡改,其中的区块链系统同样经由第三方权威维护;Alansari 等人[25,26]以云计算为背景,使用区块链存储访问控制策略和用户属性,区块链作为第三方仅用于防止数据被篡改.这种以区块链作为第三方提供“去中心化”服务的架构虽然可以有效地避免“中心化”所带来的风险,但对于多域环境来说,仍然存在恶意节点作弊、用户自主性差的问题.

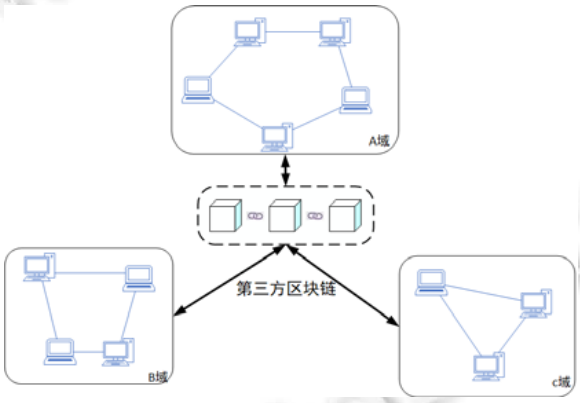

Fig.2 Entrust blockchain structure

图 2 委托区块链结构

当然,也有一部分研究提出了区块链由各参与方共同维护的访问控制框架,其结构如图 3 所示.例如,Ekblaw 等人[27]提出了“MedRec”框架,将智能合约与访问控制相结合进行自动化的权限管理,实现不同组织间医疗数据的整合和权限管理;薛腾飞等人[28]以医疗大数据为背景,提出一种基于区块链的医疗数据共享模型,利用区块链的特点,保障医疗数据在共享过程中的安全可信,在其中使用基于密码学的代理重加密(proxy reencryption)机制实现对数据的访问控制,但不具备细粒度性和可扩展性;刘敖迪等人[11]以大数据为背景,提出一种基于区块链的访问控制机制,结合 ABAC,实现了对分布式大数据资源的访问控制,但并未给出具体的访问控制流程,若请求者请求多个大数据资源权限时,需要按照不同资源拥有者的策略提出相应的访问请求,不便于用户访问.使用区块

链服务的用户同时参与维护区块链的运行,无需委托可信权威,区块链数据对用户更加透明,具有更强的真实性和可审计性,更加符合区块链技术“去信任”的本质特点.

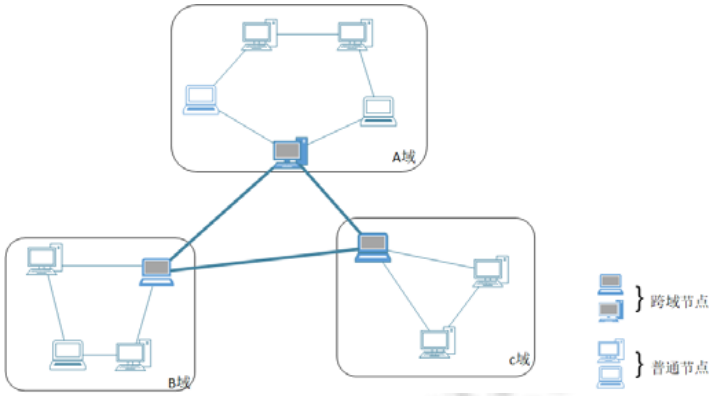

Fig.3 Inter-domain network structure

图 3 域间网络结构

2 域间访问控制模型

2.1 模型架构

(1) 域间网络结构

区块链由各个安全域共同维护.如上图 3 所示,该区块链由 *A* 域、*B* 域、*C* 域中的某一个域内节点作为跨域节点,所有安全域的跨域节点共同组成区块链中的网络节点,共同维护域间区块链的正常运行,其中,

- 跨域节点既是安全域中的网络节点,又是域间区块链的网络节点,主要负责本域和其他域的通信联系,维护区块链服务的正常运行.安全域中,跨域节点最多只有 1 个.
- 普通节点是安全域中的普通网络节点,主要负责维护本域中的数据.某一个普通节点由安全域指定为本域的跨域节点,若跨域节点宕机,则由新指定的跨域节点通过区块链网络进行同步获得链上数据.

因为各域是分布式位于不同位置,由各域的某些节点共同组成区块链并对其进行维护,符合资源的分布式特点,各域对于资源请求的授权与否都由各域独自决定而无需增加“资源汇聚机制”,这令各安全域在资源共享过程中更加自主.

(2) 模型架构

本文所述模型分为 3 层,自下而上分别为提供数据存储的数据层、提供区块链服务的服务层、提供各种功能的应用层,其架构如图 4 所示.

1) 数据层:各安全域存储的数据资源和区块链存储的访问控制策略、属性和属性关系、智能合约以及数据请求或响应操作等,这些数据在区块链中都以事务的形式存储.

2) 服务层:各安全域共同组成并维护的区块链,为域间交互提供访问控制服务.

- 网络服务:为域间交互提供 P2P 网络、数据广播以及数据验证机制服务.域间数据资源请求或者响应,属性和策略的创建、更新、撤销等操作,均通过区块链网络在域间广播.链上各节点负责验证这些消息的合法性,合法继续传播,否则停止.
- 共识机制:通过各种共识算法保证区块链节点间各类数据的一致性和可信性,以此在各域间达到稳定共识.
- 智能合约:ABAC 所需要的访问控制模块,在区块链中使用智能合约替代这些模块进行逻辑功能操作,包括:PIP Contract,用于查询实体属性和属性关系;PDP Contract,用于访问控制请求判断;PAP Contract,用于访问控制策略管理.

3) 应用层:主要提供各种功能应用,比如查询操作,请求数据资源和响应请求操作,属性和属性关系、访问控制策略的发布、更新、撤销等操作.

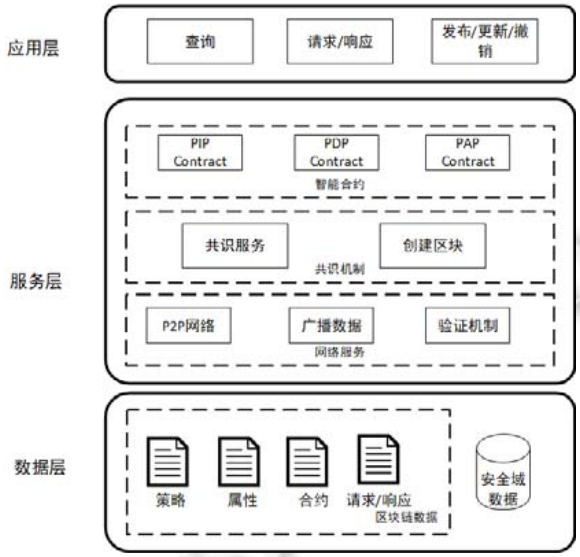

Fig.4 Model architecture

图 4 模型架构

2.2 访问控制框架

本模型将区块链和 ABAC 访问控制模型结合,对 ABAC 进行一定的改造,其框架如图 5 所示.

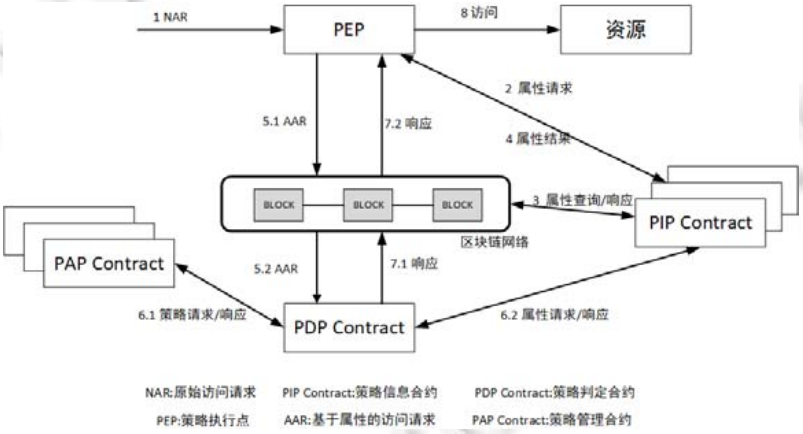

Fig.5 Inter-domain access control framework

图 5 域间访问控制框架

在 ABAC 中,主要由 PEP、属性权威(attribute authority,简称 AA)、策略管理点(point administration point,简称 PAP)、策略决策点(policy decision point,简称 PDP)以及策略信息点(policy information point,简称 PIP)这 5 个核心部分组成.在本文框架中,AA 由区块链替代,属性信息在区块链中存储,保证属性信息的真实可信;PAP,PDP,PIP 分别由 PAP Contract,PDP Contract,PIP Contract 这 3 种智能合约替代,智能合约由区块链存储,区块链中的节点可以调用合约来实现相应的功能;各安全域的跨域节点作为 PEP,接收访问请求并执行策略判定结果.

具体来讲,PEP 接收原始访问请求 NAR,然后根据 NAR 调用 PIP Contract 查询在区块链中存储的相关属性信息,用来构建一个基于属性的访问请求(AAR),AAR 描述了主体、资源、操作和环境属性,如果不希望公开请求,那么 PEP 会将 AAR 用资源拥有域的公钥加密封装成请求事务,然后通过区块链网络广播,区块链网络中的节点负责验证该事务的合法性并将其继续传播,资源拥有域收到该事务后调用 PDP Contract,PDP Contract 会分别调用 PAP Contract,PIP Contract,通过 PAP Contract 和 PIP Contract 获取策略集和属性信息,对 AAR 进行判定,并将判定结果和资源访问地址用请求域的公钥加密后封装成响应事务,通过区块链网络广播.PEP 收到响应事务后执行此访问,判定结果.

访问控制策略存储在区块链中,防止中心化策略判决不透明,保证策略按照资源拥有域的意图判定,即策略信息以及策略执行结果对于区块链中的各个安全域是公开透明、可验证、可追溯、不可篡改的.如果未进行加密处理,那么维护区块链的所有安全域均可以对策略信息和策略执行结果进行公开验证;如果对 AAR 进行了加密处理,那么请求域(作为请求方的安全域)可以对策略信息和策略执行结果进行公开验证,保障访问控制过程和结果的可信性.使用区块链网络作为各种事务的传播方式,对于请求域来说,区块链服务处理过程是完全透明的,请求域可以使用资源拥有域的公钥对请求进行加密处理,在充分利用区块链网络特点的同时,有效地防止请求域隐私泄露,保障在公开的域间区块链网络中的隐私安全.

2.3 区块链服务

1) 数据存储结构

各类数据以事务形式存储在区块中,区块链将各种事务经过分类组成事务数据集,并将它们打包成区块进行存储,区块格式如图 6 所示.数据区块由区块头和区块体构成:区块头封装了前一区块哈希、Merkle 根以及时间戳等信息;区块体包括当前区块的事务数量以及经过验证的、区块创建过程中生成的所有事务数据,主要包括智能合约、属性和属性关系、访问控制策略以及请求/响应,这些事务经过 Merkle 树的哈希过程生成唯一的 Merkle 根并计入区块头.Merkle 根可以快速归纳和校验区块数据的存在性和完整性,极大地提高了区块链的运行效率和可扩展性.

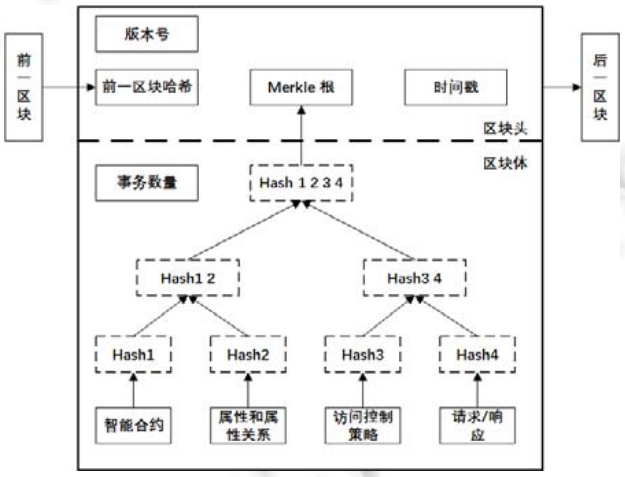

Fig.6 Block structure

图 6 区块结构

2) 事务的数据格式

各类非合约事务数据在区块链中的数据格式如图 7 所示,其中,ID 表示事务的编号;Transaction_Type 表示事务的类型,具体包括属性事务类型 *A*、访问控制策略事务类型 *P*、数据请求/响应事务类型 *R*;Publisher_PK 表示发布者的公钥地址,在数据请求/响应事务中用于加密;Operation_Type 表示操作类型,具体包括创建操作 *C*、更新操作 *U*、撤销操作 *D*.数据请求/响应事务类型在操作域统一填入创建操作 *C*;Transaction_Data 表示事务的

具体信息,不同的事务数据类型在 Transaction_Data 域有不同的格式;Timestamp 表示事务创建时时间戳;Signature 表示发布者的签名.

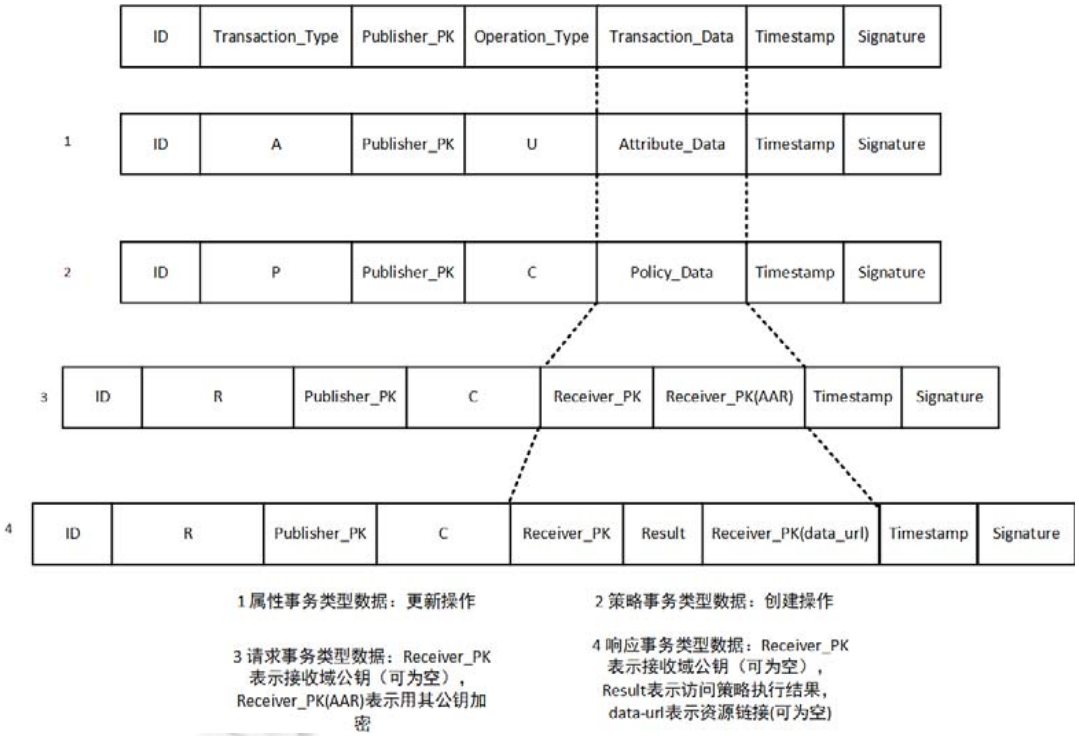

Fig.7 Data format

图 7 数据格式

各类非合约型事务经由图 7 所示数据格式打包进区块中进行存储,这些事务一旦被打包进区块就无法被更改或删除,这样可以便于日后审计.事务具有 3 种操作类型,其中,创建操作 *C* 只能进行一次;更新操作 *U* 可以进行若干次,直到该事务被撤销;同样,撤销操作 *D* 也只能进行一次.事务的操作类型作为系统判断该事务是否合法的依据,判断方法如下.

(1) 检查事务的数据格式是否正确:正确,则进行下一步.

(2) 使用发布者公钥(Publisher_PK)检查事务签名是否有效:有效,则进行下一步.

(3) ① 对于操作类型为 *C* 的事务:(a) 检查其 ID,若存在,则不合法;(b) 对于事务类型为 *A* 的事务,检查其发布的属性是否已存在,若存在,则不合法(对于事务类型为 P 的事务,无需检查该策略是否存在,因为策略是由各安全域根据自身需要定制的).

② 对于操作类型为 *U* 或 *D* 的事务,检查其 ID:若不存在,则不合法;若存在,则检查原事务和更新后事务的公钥是否相同,若不同,则不合法(防止策略状态被非法篡改,例如 *A* 域非法更改 *B* 域策略状态).

由于事务可能会被更新或撤销,且旧事务仍会存在于区块链中,所以系统在进行相关事务查询时,需要根据其操作类型进行筛选.当一个事务被撤销后,无法被添加进结果集中,当一个事务被多次更新后,系统将选择时间戳最新的事务添加进结果集中.

3) 区块链网络的工作流程

(1) 各种数据经过发布者按照上述的数据格式封装成事务后,经由区块链网络广播至全网节点.

(2) 链上节点对该事务进行验证:如果合法,则继续向附近节点广播;否则,停止传播.

(3) 网络中担任共识节点功能的网络节点收到该事务后,将其放入事务等待队列中,队列中的各种

事务按照类型分类排序,各类型数据达到一定数量后将其封装到一个区块中.

(4) 共识节点在全网广播该区块,其他网络节点验证该区块的合法性:如果合法,则将该区块加入到本地区块链的尾部;否则,停止传播.

通过以上流程,经过封装成事务的数据存储在区块链网络中,使数据有迹可循,达到透明可信、可追溯、可验证的目的.

2.4 智能合约

本文所述模型使用智能合约作为代理,为系统提供相关属性及策略的查询或判定服务,其中,PIP Contract 提供属性查询服务,PAP Contract 提供策略查询服务,PDP Contract 提供策略判定服务.数据在使用区块链存储后,因为在区块链中区块的数量是不断增加的,所以区块链系统的数据查询效率是当前区块链面临的一个重要问题[29].为了提高查询效率,本文使用布隆过滤器(Bloom filter)[30]配合智能合约进行查询.布隆过滤器是一种利用空间效率较高的随机数据结构,主要用于迅速判断某一元素是否存在于集合中.下面简单介绍其原理.

存在一个集合 $S=\{x_1,x_2,\ldots,x_n\}$、m 位二进制向量 $BF=\{B_0,B_1,\ldots,B_{m-1}\}$以及 k 个相互独立的哈希函数 $H=\{h_0,h_1,\ldots,h_{k-1}\}$,且哈希函数的值域均为$[0,m-1]$.首先,将 BF 中所有位的初始值置为 0,然后将集合 S 中的元素 x_i 令 $BF[h_j(x_i)]=1$,其中,$i\in[1,n]$,$j\in[0,m-1]$,这样就可以得到集合所对应的布隆过滤器 BF_S.当判断某一元素 E 是否存在于集合 S 中时,只需计算 $h_j(E)$,$j\in[0,m-1]$,然后检查 $BF[h_j(E)]$是否全部为 1:如果不全为 1,$E\notin S$;否则 $E\in S$.但是,布隆过滤器存在一定概率的误判(false positive),误判率为

$$P=\left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^k\approx\left(1-\mathrm{e}^{\frac{-kn}{m}}\right)^k.$$

若给定 m,n,则当 $k=\frac{m}{n}\ln 2$ 时,误判率最小值:

$$P=\left(\frac{1}{2}\right)^k\approx 0.6185^{\frac{m}{n}}.$$

虽然布隆过滤器存在一定概率的误判,但是不会将存在于该集合内的某元素判断为不存在.也就是说,若 $E\in S$,布隆过滤器给出的结果为 $E\in S$;若 $E\notin S$,布隆过滤器可能给出 $E\in S$ 的结果.但正是因为布隆过滤器具有较高的查询效率,且其误判率相比较其效率而言是可以容忍的,因此被应用于当前主流区块链系统[31].下面给出智能合约中布隆过滤器相关算法.

算法 1.

输入:待查询元素(*E*),待查询集合(*S*).

输出:查询结果标志(*Result_flag*).

```
Begin
//获取待查询集合 S 的布隆过滤器 BF,并将 Result_flag 置为 1
BF=getBF(S), Result_flag=1;
for (i=1; i<hashfunction.length; i++){
  bit_key=Hash[i](E);
//判断 BF 的二进制向量 bit_key 位置上是否是 1
  if (BF[bit_key]!=1){
    Result_flag=0;
    break;
    }//end if
}//end for
return Result_flag;
}
```

End

(1) 策略信息合约 PIP Contract

在 ABAC 模型中,策略信息点 PIP 用于提供实体的各种属性和属性关系.在本文所描述的模型中,属性和属性关系用区块链进行存储,以此来保障属性和属性关系的可信性.而 PIP Contract 主要作用为 PEP,PDP 提供属性查询功能.为方便表示,做如下定义:

定义 1. 属性(Attr)是具有指定数据类型和值域的变量,本文使用 $xAttr,x\in\{s,r,a,e\}$分别表示主体属性、资源属性、操作属性、环境属性;用 $xAttr_Set,x\in\{s,r,a,e\}$分别表示主体、资源、操作、环境属性集.用 $xAttrVp=\langle xAttr\propto attrValue\rangle,x\in\{s,r,a,e\},\propto\in\{>,<,=,\geqslant,\leqslant,\neq,\text{in,not in,between}\}$表示属性名和属性值之间的关系,称为属性名值对.用 $xAttrVp_Set,,x\in\{s,r,a,e\}$分别表示主体、资源、操作、环境属性名值对集合.

PIP Contract 伪代码如下所示:

算法 2.

输入:属性查询请求(*attributeRequest*).

输出:属性结果集(*Attribute_ResultSet*).

```
Begin
xAttr_Set=attributeRequest.xAttr_Set;
//创世块序号为 0,从序号为 1 的区块开始查询
for (i=1; i<blocks.length; i++){
//判断属性结果集中的属性是否包含请求属性集中的所有元素:若包含,则说明属性均已找到
if (attribute_ResultSet.contain(xAttr_Set))
     break;
//使用布隆过滤器判断该属性是否可能在此区块中
flag=bloomfilter(xAttr_Set,currentBlock);
if (flag=1){
//从当前区块中序号为 0 的事务数据开始查询
  for (j=0; j<blocks[i].trans_Data_Length; j++){
  if (blocks[i].trans_Data[j].Transaction_Type='A'){
       if (xAttr_Set.contain(blocks[i].trans_Data[j].Transaction_Data)){
           attribute_ResultSet.add(blocks[i].trans_Data[j]);
       }else continue;
  }else continue;
  }//end for
 } else continue;
}//end for
return Attribute_ResultSet;
End
```

(2) 策略管理合约 PAP Contract

在 ABAC 模型中,策略管理点 PAP 用于对访问控制策略的管理和整合.PAP 根据 PDP 所提供的 AAR 查询符合要求的访问控制策略,并将这些访问控制策略整合为策略集发送回 PDP 进行策略判决.在本文所述模型中,访问控制策略由各安全域根据各自的安全需求,使用标准化、统一的细粒度属性信息进行描述,按照访问控制策略事务数据格式封装后,发布到区块链中,由区块链进行存储,以此来保障策略的公开性和可信性.而 PAP Contract 为 PDP Contract 提供策略查询功能.为方便描述,做如下定义:

定义 2. 属性的访问请求(AAR)由主体、资源、操作、环境的属性名值对集合构成,用四元组表示如下:

$$AAR=\langle sAttrVp\_Set,rAttrVp\_Set,aAttrVp\_Set,eAttrVp\_Set\rangle.$$

四元组中,*sAttrVp_Set* 表示主体属性名值对集合,*rAttrVp_Set* 表示资源属性名值对集合,*aAttrVp_Set* 表示操作属性名值对集合,*eAttrVp_Set* 表示环境属性名值对集合.

AAR 的含义为:“属性为 *sAttrVp_Set* 的主体在环境属性 *eAttrVp_Set* 条件下,对资源 *rAttrVp_Set* 进行 *aAttrVp_ Set* 的操作请求”.

定义 3. 访问控制策略(Policy)定义了对资源进行特定操作所需要的属性集合.用三元组表示如下:

$$Policy\leftarrow\langle pAttr\_Set,Rule,CombiningAlgorithm\rangle.$$

三元组中,*pAttr_Set* 表示策略的属性集合,*Rule* 表示规则集合,*CombiningAlgorithm* 表示合并算法.

pAttr_Set 用四元组表示如下:

$$pAttr\_Set=\langle sAttr\_Set,rAttr\_Set,aAttr\_Set,eAttr\_Set\rangle.$$

四元组中,*sAttr_Set* 表示主体属性集合;*rAttr_Set* 表示资源属性集合;*aAttr_Set* 表示操作属性集合; *eAttr_Set* 表示环境属性集合,用来判断该策略是否满足请求.

Rule 表示规则集合:*Rule*={*rule*_1,*rule*_2,…,*rule_n*},其中,*rule_n* 表示第 *n* 条规则.*rule* 用四元组表示如下:

$$rule=Result\leftarrow\langle sAttrVp\_Set,rAttrVp\_Set,aAttrVp\_Set,eAttrVp\_Set\rangle.$$

四元组中,*sAttrVp_Set* 表示主体属性名值对集合,*rAttrVp_Set* 表示资源属性名值对集合,*aAttrVp_Set* 表示操作属性名值对集合,*eAttrVp_Set* 表示环境属性名值对集合.*Result* 表示规则的判决结果,*Result*∈(*Permit*,*Deny*)

CombiningAlgorithm 为用来解决策略冲突的合并算法,用来解决规则集判定冲突问题.

PAP Contract 伪代码如下所示.

算法 3.

输入:*AAR*.

输出:策略结果集(*Policy_ResultSet*).

```
Begin
rAttrVp_Set=AAR.rAttrVp_Set;
//创世块序号为 0,从序号为 1 的区块开始查询
for (i=1; i<blocks.length; i++){
//使用布隆过滤器判断包含该属性的策略是否可能在此区块中
flag=bloomfilter(rAttrVp_Set,currentBlock);
if (flag=1){
//从当前区块中序号为 0 的事务记录开始查询
for (j=0; j<blocks[i].trans_Data_Length; j++){
  if (blocks[i].trans_Data[j].Transaction_Type='P'){
    if (rAttrVp_Set.contain(blocks[i].trans_Data[j].
      Transaction_Data(pAttr_Set.rAttr_Set))){
      Policy_ResultSet.add(blocks[i].trans_Data[j]);
        }else continue;
      }else continue;
    }//end for
  }else continue;
}//end for
return Policy_ResultSet;
End
```

(3) 策略判定合约 PDP Contract

策略判定点 PDP 用于对访问控制策略的判定,最终结果为允许访问 *Permit* 或者拒绝访问 *Deny*.当 *AAR* 中的属性和属性值分别满足某一策略中的属性和属性值的谓词或约束时,称此访问请求满足该策略,即属性相同且属性值符合策略谓词或约束条件,最终根据策略的判定结果为 *Permit* 或 *Deny*.否则,当 *AAR* 中所提供的属性信息不足或存在不满足策略中属性谓词或约束的,最终结果为 Unknown.在本文策略结果判定中,对判定为 Unknown 的请求最终以 *Deny* 为授权结果.PDP Contract 用于访问控制的判定.

PDP Contract 伪代码如下所示.

算法 4.

输入:*AAR*,*Policy*.

输出:策略判定结果(*result*).

```
Begin
Req_xAttrVp_Set=AAR.xAttrVp_Set, Rule=Policy.Rule;
//判断请求属性是否包含策略属性
if (Policy.pAttr_Set(xAttr_Set)⊆Req_xAttrVp_Set.xAttr_Set){
//判断请求是否满足策略规则
   for (i=0; i<Rule.length; i++){
   if (Req_xAttrVp_Set.xAttr==Rule[i].xAttrVp_Set.xAttrVp.xAttr
&& Req_xAttrVp_Set.attrValue∝Rule[i].xAttrVp_Set.xAttrVp.attrValue)
results[i]=Rule[i].Result;
   }//end for
//合并策略集结果
   result=Conbining(results[·],CombiningAlgorithm);
   return result;
}
else
   return null;
End
```

3 实例分析

本节以某零售行业供应链中各机构交互作为实例进行分析.在零售行业内,各机构处于不同地理位置,且存在协作关系,这就需要各机构之间进行频繁的数据共享和信息交互,但每个机构由于在供应链的分工不同而无法共享所有数据,因此,各机构需要根据自己的安全需求制定访问控制策略.同时,行业内数据具有一定的通用性,并且数据的爆炸增长所带来的海量性和动态性,均使本文所述模型可以恰当地应用于此类场景,具体如下.

A,*B*,*C*,*D* 为同一零售行业内的 4 家机构,其中,*A* 为供应商,*B*,*C* 为中间商,*D* 为零售商,各机构将属性和访问控制策略存储在共同维护的区块链中.各机构供货关系如图 8 所示.

在同一行业内,各机构对实体的描述相似,因此在本系统中,各机构共同协商对实体的属性标准,但各机构在策略中对实体描述的属性集不相同,例如,*A* 作为供应商,使用如下属性集对策略中的实体进行描述:

$$\{s\_ID,s\_Role,s\_Name,r\_Name,r\_Level,a,e\_Time\},$$

其中,*s_ID* 表示主体 ID,*s_Role* 表示主体角色,*s_Name* 表示主体名,*r_Name* 表示资源名,*r_Level* 表示资源等级,*a* 表示操作,*e_Time* 表示访问时间.

B,*C* 作为中间商,对访问该资源的主体要求提供更多的属性,例如,*B* 在上述属性集合基础上增加了环境属性约束 *e_Location*(访问地点);*C* 在上述属性集合基础上增加了主体属性 *s_Level*(主体等级),而对于新增加的数

据,可以及时地使用已经被写入区块链且合适的属性对其进行描述.虽然各机构所使用的是同一套属性标准,但更加细化的属性对实体的描述也更加丰富,策略也可以根据需求自行制定.例如,*C* 的一条策略规则可以为

Permit←⟨{*s_ID*≠*NULL*,*s_Role*=*retailer*,*s_Level*≥3,*s_Name*≠*NULL*},{*r_Name*=“*product*”,*r_Level*≤*private*},{*a*=*read*},{*e_Time* between (9:00,17:30)}⟩.

其中,*s_ID*,*s_Name* 由主体提供且不能为空;*s_Role* 为 *retailer*,*r_Name* 为“*product*”;*s_Level* 大于等于 3(3 级以上零售商);*r_Level* 小于等于 *private*(private 或 public);操作为“*read*”; *e_Time* 在 9:00~17:30 区间内.如果访问请求满足以上条件,那么授权为 *Permit*.

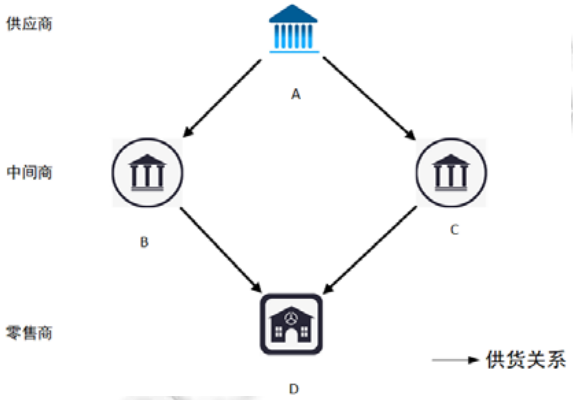

Fig.8 Relationship of supply chain institutions

图 8 供应链各机构关系

当 *D* 想要比较名为“*product*”的产品在 *B*,*C* 两家中间商的定价时,经过以下步骤获取资源访问权限.

步骤 1. *D* 机构用户发送跨域原始请求 NAR 给 *D* 机构的 PEP;

步骤 2. *D* 机构 PEP 调用 PIP Contract 请求属性结果集.

步骤 3. PIP Contract 以请求为输入在区块链中查询属性结果集.

步骤 4. PIP Contract 将查询到的属性结果集作为输出返回给 *D* 机构 PEP;

步骤 5. PEP 首先根据属性结果集将 NAR 构造为 *AAR* 如下:

AAR=⟨{*s_ID*=2,*s_Role*=*retailer*,*s_Level*=4,*s_Name*=‘*D*’},{*r_Name*=“*product*”,*r_Level*=*private*},{*a*=*read*},{*e_Time*=12:00,*e_Location*=“London”}⟩.

如果 *D* 不希望公开请求,那么分别使用 *B* 机构、*C* 机构的公钥对 *AAR* 进行加密如下.

- B:$Transaction\_Data(PK_B,PK_B(AAR_D))$.
- C:$Transaction\_Data(PK_C,PK_C(AAR_D))$.

最后,按照请求类型事务格式将两个加密后的 *AAR* 封装为请求类型事务,先后经区块链网络广播.

区块链中的网络节点负责验证并转发该事务,共识节点负责将该事务打包进区块后广播;

步骤 6. *B*,*C* 机构跨域节点收到该事务,解析出 *AAR*,调用 PDP Contract,PDP Contract 会调用 PAP Contract,PIP Contract 获得策略结果集和属性结果集进行访问控制判定并返回判定结果;

步骤 7. *B*,*C* 机构跨域节点根据判定结果进行数据封装,如果结果是 *Permit*,则将 *D* 机构所请求的资源 *url* 链接用 *D* 的公钥加密,连同访问控制结果和 *D* 的公钥一并封装为响应事务的 *Transaction_Data*,如下所示.

- B:$Transaction\_Data(PK_D,Permit,PK_D(url_B))$.
- C:$Transaction\_Data(PK_D,Permit,PK_D(url_C))$.

最后,将所有数据封装为响应类型事务,经区块链网络广播;如果结果为 *Deny*,资源 *url* 为空.

区块链中的网络节点负责验证并转发该事务,共识节点负责将该事务打包进区块后广播;

步骤 8. *D* 机构 PEP 收到该响应后,解析得到访问控制结果和资源 *url* 密文,解密后进行资源访问;

经过以上步骤,*D* 机构可以获得相应的访问权限进行资源访问,以查看其请求资源的相关信息,比如产品价格、配置信息等等.当然,*D* 机构也可能因为提交的属性不满足 *B* 或 *C* 的策略要求而导致访问失败.

D 作为访问主体所具有的属性是其本身所具有的,无需系统预先为 *D* 分配权限,*D* 能否获得某资源的访问权限,首先取决于 *D* 所具有的属性能否满足其所访问资源的属性要求.对于不断变化的数据,使用不断扩展的属性对其恰当描述.随着对某一实体的属性描述增加,ABAC 策略数目呈线性增长.例如在上文给出的 *C* 机构策略中,主体等级大于等于 3(*s_Level*≥3)即可访问资源等级为 *private* 或 *public* 的商品(*r_Level*≤*private*),一条策略即可满足要求.如果使用 RBAC,除了需要预先为不同的主体分配明确的角色外,还需要根据主体的角色制定相应的策略,见表 2,等级为 3 级的零售商的权限需要指定两条策略.权限列表会随着零售商角色的增多呈指数增长.

Table 2 Relationship between RBAC role and permissions

表 2 RBAC 角色和权限对应关系

角色 Roles	权限 Permissions
1 级零售商	可以访问资源等级为 *public* 的商品
2 级零售商	可以访问资源等级为 *public* 的商品
3 级零售商	可以访问资源等级为 *public* 的商品 可以访问资源等级为 *private* 的商品

请求域可以选择将具体请求使用资源拥有域的公钥加密处理,若请求多个安全域同类型资源的访问权限时,则需要分别用他们的公钥加密,封装成多个事务请求发送,有效保障安全域的隐私性;请求域也可以选择不加密,那么所有拥有该资源的安全域均可以响应该请求,如果均同意授权,请求域可以获得所有该资源相关的访问权限.资源 *url* 由资源拥有域自主决定是否授予请求域,一旦发现区块链网络中有恶意节点根据属性构造恶意请求时,被请求域可以拒绝分享资源 *url*,在访问控制策略由资源拥有域制定并维护的条件下,进一步提高安全域的自主性,有效保障资源安全.

综上所述,本文所提出的基于区块链的域间访问控制模型能够适应于很多以多域环境为背景的应用场景中,为域间数据共享提供了一种更安全、更主动、更灵活、更细粒度、扩展性更高的访问控制模型.

4 实验分析

本文基于 Hyperledger Fabric[32]实现了原型系统.Fabric 是一种商用区块链框架,它所具有的高度模块化、支持多种编程语言的智能合约、可插拔共识机制的特点令其应用的场景更加广泛.在上述实例场景中,各安全域通过 Fabric 提供的配置文件进行设置,以组织的形式加入同一个通道(channel)中,共同维护一条联盟链,非常符合本文模型应用的前提.在各安全域以联盟形式参与维护区块链后,通过链码(智能合约)为各域的访问控制提供属性、策略查询或策略判定服务.

本文实验环境具体为 64 位 Ubuntu 18.04 操作系统,4G 内存,Intel(R) Core(TM) i5-4590@3.30GHz 处理器,Hyperledger Fabric 版本为 1.40,Docker 版本为 19.03,go 版本为 1.12.9.本文分别测试策略数量为 1000,2000,3000,4000,6000 的查询效率和策略判定时间.需要说明的是:测试所用数据库为 CouchDB,且仅限于本文所述算法,对于如何提高底层数据库的查询效率并不是本文讨论的重点;同时,如何从底层方面提高整体查询效率需要进一步研究.

查询效率体现在查询时间的长短,重点在于和未使用布隆过滤器的查询方法进行对比.根据上文对于布隆过滤器相关内容可知:当 *m*/*n* 越大时,误判率越低,且哈希函数的个数对于误判率的影响会随着哈希函数的增加而降低.图 9 为哈希函数个数 *k* 和误判率的关系,可以看出:当 *k*>5 时,误判率下降极为缓慢且在可接受范围内,故本文使用 *k*=6 进行查询效率测试.图 10 为使用布隆过滤器和常规方法的查询时间比较.

策略判定时间体现在策略响应请求的平均时间长短.本文随机选择 20 条请求,每条请求中属性个数为 5,重点测试时间和策略数目的关系,重复 50 次实验取平均值.如图 11 所示.可以看出:随着策略数的增加,策略判定的平均时间增加,且增长率较快.

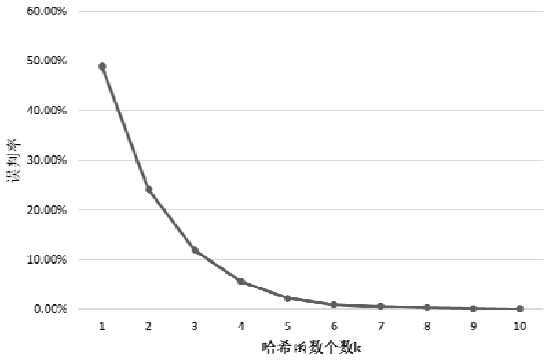

Fig.9 Relationship between k and false positive rate

图 9 k 与误判率关系

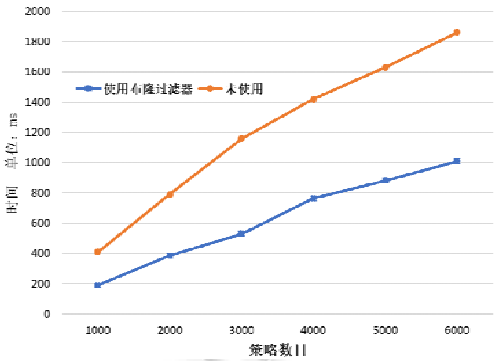

Fig.10 Query efficiency comparison

图 10 查询效率比较

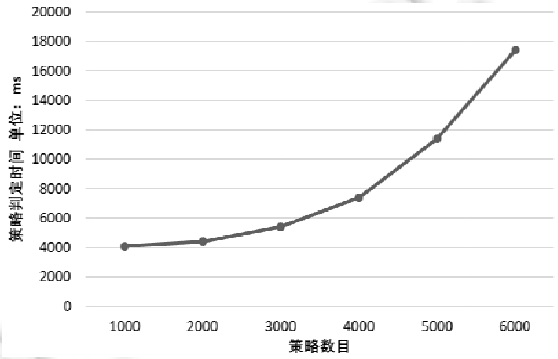

Fig.11 Policy decision time

图 11 策略判定时间

5 对比分析

通过对比分析来评估本文提出的访问控制模型:一方面,同传统访问控制模型进行对比(表 3),分析本文模型的优缺点;另一方面,同已有研究进行对比(见表 4),分析本文模型具有的优势.

本模型和传统访问控制模型以新型计算模式所具有的海量性、动态性、分布式的特点为角度进行对比,具体如表 3 所示.可以看出,本模型在面对新型计算模式所带来的特点具有一定的优势.

Table 3 Comparative analysis between the model and traditional access control model

表 3 本模型和传统访问控制模型对比分析

名称	海量性	动态性	分布式
传统访问控制模型	随着数据的增长,访问控制策略呈指数增长,系统开销极高且访问效率低下	静态分配权限,无法满足动态需求;粗粒度无法应对数据频繁变动	无法支持各域统一访问控制策略标准,不便于信息共享
本模型	随着数据的增长,访问控制策略呈线性增长,系统开销较小且访问效率较高	实体自带属性,不需要预先分配权限;细粒度可以及时管理动态数据	细粒度性和良好的灵活性可以支持各域统一访问控制策略标准,并使用区块链存储策略,方便信息共享

本文模型和目前已有的研究分别从是否基于区块链、是否基于 ABAC、是否具有细粒度性、安全机制、是否便于用户访问、是否自主授权、判决是否透明这 7 种角度进行对比.具体见表 4.

Table 4 Comparative analysis between the model and existing research programs

表 4 本模型和已有研究方案对比分析

模型	基于区块链	基于 ABAC	细粒度性	安全性	便于访问	自主授权	判决透明
BD-ABAC[33]	否	是	具备	访问控制机制	对不同的资源域需要发送不同请求,不便于访问	不具备	不具备
MDSM[28]	是	否	不具备	访问控制机制 非对称加密 锚定公链	同上, 不便于访问	不具备	不具备
BBAC-BD[11]	是	是	具备	访问控制机制 区块链	同上, 不便于访问	自主制定策略	具备
本模型	是	是	具备	访问控制机制 区块链 非对称加密	链上资源域统一访问控制标准,无需发送不同请求,便于访问	自主制定策略 自主授予资源 url	具备

结合表 4 可以看出,本文所述模型在多域环境下具有以下几个方面的优势.

(1) 细粒度性:细粒度的 ABAC 访问控制可以针对动态数据进行及时的管控,同时,本文提出了建立标准化的属性对访问控制策略进行描述,属性统一和策略定制相结合,既可以准确描述各域访问控制策略,又便于用户访问,易于系统管理.

(2) 安全性:本文模型通过改进 ABAC 访问控制模型实施访问控制;各域自行维护的区块链令数据更可信,区块链数据动态不断增长,攻击难度不断加大,有效防止恶意节点攻击、篡改;若请求域不希望公开具体访问信息,可采用非对称加密技术对隐私信息进行加密处理,从而保障隐私安全.

(3) 便于用户访问:若需要请求多个安全域资源,请求域只需根据需求发出一条原始请求即可.若对具体请求不作加密处理,则 PEP 封装成一个请求事务发出;若请求域不公开具体请求,根据标准的属性信息,同样只需要构造一条原始请求即可,然后 PEP 使用多个资源拥有域的公钥分别加密后,封装成多个请求事务发出,无需根据不同安全域的访问控制策略发出不同的原始请求.

(4) 自主授权:访问控制策略由安全域根据自身需求制定并维护;资源拥有域根据智能合约的自动化授权结果,自主决定是否授予访问资源 *url*,令资源拥有域具有更强的自主性.

(5) 判决透明:属性信息由区块链存储,保证属性的真实可信;策略信息包括策略执行过程和结果也存储在区块链中,保障信息真实可信的同时,有效防止中心化判定存在的判定不透明或越权行为的发生.

6 结束语

将区块链应用于访问控制,是当前区块链研究的一大趋势.本文模型将区块链和 ABAC 相结合,基于 Hyperledger Fabric 实现域间访问控制.一方面,充分发挥了区块链"共享"的特点;另一方面,通过细粒度的访问控制,对各域资源进行有效的控制管理.本文的核心思想是:使用区块链作为访问控制策略的载体,利用区块链的特点将"中心化"策略决策方式改为由智能合约自动化进行,策略执行过程和结果公开且可验证;区块链由各安全域维护,进一步提高策略执行的可信性,同时,策略由各域根据自身需要制定,且对权限授予与否拥有最终决定权,进一步提高资源拥有者的自主性,保障资源的访问权由资源拥有者决定;本文所述访问控制模型基于 ABAC 模型,并提出了对属性信息和访问控制策略标准化的概念,在更加准确地描述策略的同时,增加对整个动态系统管理的灵活性;使用非对称密钥对隐私信息进行加密处理,有效地保障各安全域的隐私安全.本文所述模型在新型计算环境下能有效地保障域间访问和数据的共享安全,同时增强了用户的自主性,提高了系统的灵活性、扩展性和可管理性.因此,本模型具有广泛的应用价值.

References:

[1] Feng DG, Zhang M, Li H. Big data security and privacy protection. Chinese Journal of Computers, 2014,37(1):246−258 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2014.00246]

[2] Wang JJ. Breaking out of information islands to achieve digital resource sharing. Journal of Academic Libraries, 2004,22(3):16−18 (in Chinese with English abstract).

[3] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract).

[4] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1): 71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[5] Fang L, Yin LH, Guo YC, Fang BX. A survey of key technologies in attribute-based access control scheme. Chinese Journal of Computers, 2017,40(7):1680−1698 (in Chinese with English abstract).

[6] Li XF, Feng DG, Chen CW, Fang ZH. Model for attribute based access control. Journal on Communications, 2008,29(4):90−98 (in Chinese with English abstract).

[7] Sandhu R. The future of access control: Attributes, automation and adaptation. In: Proc. of the IEEE Int'l Conf. on Information Reuse and Integration. 2013. xxiii−xxiv. [doi: 10.1109/IRI.2013.6642437]

[8] Wang XM, Fu H, Zhang LC. Research progress on attribute-based access control. Acta Electronica Sinica, 2010,38(7):1660−1667 (in Chinese with English abstract).

[9] Yuan E, Tong J. Attributed based access control (ABAC) for Web services. In: Proc. of the 2005 IEEE Int'l Conf. on Web Services (ICWS 2005). IEEE, 2005. 561−569. [doi: 10.1109/ICWS.2005.25]

[10] Li NH, Mitchell JC. Datalog with constraints: A foundation for trust-management languages. In: Proc. of the 5th Int'l Symp. on Practical Aspects of Declarative Languages (PADL 2003). New Orleans, 2003. 28−73.

[11] Liu AD, Du XH, Wang N, Li SZ. A blockchain-based access control mechanism for big data. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2636−2654 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

[12] Chen GK, Yin XL, Liu WL. Access control model applicability for big data. Authentication and Confidentiality, 2016,7(7):3−5 (in Chinese with English abstract).

[13] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[14] Han X, Yuan Y, Wang FY. Security problems on blockchain: The state of the art and future trends. Acta Automatica Sinica, 2019, 45(1):206−225 (in Chinese with English abstract).

[15] Eyal I, Gencer AE, Sirer EG, *et al*. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Conf. on Networked Systems Design and Implementation. USENIX Association Berkeley, 2015. 45−59.

[16] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: Proc. of the Int'l Workshop on Open Problems in Network Security. Springer Int'l Publishing, 2016. 112−125.

[17] Swan M. Blockchain: Blueprint for a New Economy. Sebastopol: O'Reilly Media, Inc., 2015.

[18] Ouyang LW, Wang S, Yuan Y, Ni XC, Wang FY. Blockchain-enabled smart contracts: Architecture, applications andfuture trends. Acta Automatica Sinica, 2019,45(3):445−457. (in Chinese with English abstract). https://doi.org/10.16383/j.aas.c180586

[19] Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 2016, 4: 2292-2303.

[20] Jiang ZT, Xie Z, Wang Q, Zhang WH. A cross-domain access control model for cloud computing environments. Microelectronics & Computer, 2017,34(3):65−69 (in Chinese with English abstract).

[21] Zhang S, Sun JL, Xu B, Huang C, Kavs AJ. RBAC based access control model for services compositions cross multiple enterprises. Journal of Zhejiang University (Engineering Science), 2012,46(11):2035−2043 (in Chinese with English abstract).

[22] Joshi JBD, Bhatti R, Bertino E, *et al*. Access-control language for multidomain environments. IEEE Internet Computing, 2004,8(6): 40−50.

[23] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the 2015 IEEE Security and Privacy Workshops (SPW). IEEE Computer Society, 2015. 180−184.

[24] Ding D, Cao J, Li C, Fan K, Li H. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access, 2019,7: 38431−38441. [doi: 10.1109/ACCESS.2019.2905846]

[25] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations. In: Proc. of the 2017 IEEE 37th Int'l Conf. on Distributed Computing Systems (ICDCS). IEEE, 2017. 2131−2136. [doi: 10.1109/ICDCS.2017.241]

[26] Alansari S, Paci F, Margheri A, Sassone V. Privacy-preserving access control in cloud federations. In: Proc. of the 2017 IEEE 10th Int'l Conf. on Cloud Computing (CLOUD). IEEE, 2017. 757−760. [doi: 10.1109/CLOUD.2017.108]

[27] Ekblaw A, Azaria A, Halamka JD, *et al*. A case study for blockchain in healthcare: MedRec prototype f rototype for electronic health records and medical research data. Technical Report, 5-56-ONC, Massachusetts Institute of Technology, 2016.

[28] Xue TF, Fu CQ, Wang Z, Wang XY. A medical data sharing model via blockchain. Acta Automatica Sinica, 2017,43(9):1555−1562 (in Chinese with English abstract).

[29] Wang QG, He P, Nie TZ, Shen DR, Yu G. Survey of data storage and query techniques in blockchain systems. Computer Science, 2018,45(12):12−18 (in Chinese with English abstract).

[30] Bloom BH. Space/Time trade-offs in hash coding with allowableerrors. Communications of the ACM, 1970,13(7):422−426.

[31] Yu G, Nie TZ, Li XH, Zhang YF, Shen DR, Bao YB. The challenge and prospect of distributed data management techniques in blockchain systems. Chinese Journal of Computers, 2021,44(1):28−54 (in Chinese with English abstract).

[32] Androulaki E, Barger A, Bortnikov V, *et al*. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proc. of the EuroSys Conf. Porto: ACM, 2018. 30:1−30:15. [doi: https://doi.org/10.1145/3190508.3190538]

[33] Wang JY, Fan Y, Yu WH, Han LF. Big data security protection method based on fine-grained access control. Computer Technology and Development, 2019,29(10):134−140 (in Chinese with English abstract).

附中文参考文献:

[1] 冯登国,张敏,李昊.大数据安全与隐私保护.计算机学报,2014,37(1):246−258. [doi: 10.3724/SP.J.1016.2014.00246]

[2] 王俊杰.冲出信息孤岛,实现数字资源共享.大学图书馆学报,2004,22(3):16−18.

[3] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494.

[4] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[5] 房梁,殷丽华,郭云川,方滨兴.基于属性的访问控制关键技术研究综述.计算机学报,2017,40(7):1680−1698.

[6] 李晓峰,冯登国,陈朝武,房子河.基于属性的访问控制模型.通信学报,2008,29(4):90−98.

[8] 王小明,付红,张立臣.基于属性的访问控制研究进展.电子学报,2010,38(7):1660−1667.

[11] 刘敖迪,杜学绘,王娜,李少卓.基于区块链的大数据访问控制机制.软件学报,2019,30(9):2636−2654. http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

[12] 陈垚坤,尹香兰,刘文丽.大数据环境下访问控制模型适用性研究.信息安全与技术,2016,7(7):3−5.

[14] 韩璇,袁勇,王飞跃.区块链安全问题:研究现状与展望.自动化学报,2019,45(1):206−225.

[18] 欧阳丽炜,王帅,袁勇,倪晓春,王飞跃.区块链智能合约的发展现状:架构、应用与发展趋势.自动化学报,2019,45(3):445−457. https://doi.org/10.16383/j.aas.c180586

[20] 江泽涛,谢朕,王琦,张文辉.一种适用于云计算环境的跨域访问控制模型.微电子学与计算机,2017,34(3):65−69.

[21] 张帅,孙建伶,徐斌,黄超,Kavs AJ.基于 RBAC 的跨多企业服务组合访问控制模型.浙江大学学报(工学版),2012,46(11):2035−2043.

[28] 薛腾飞,傅群超,王枞,王新宴.基于区块链的医疗数据共享模型研究.自动化学报,2017,43(9):1555−1562.

[29] 王千阁,何蒲,聂铁铮,申德荣,于戈.区块链系统的数据存储与查询技术综述.计算机科学,2018,45(12):12−18.

[31] 于戈,聂铁铮,李晓华,张岩峰,申德荣,鲍玉斌.区块链系统中的分布式数据管理技术——挑战与展望.计算机学报,2021,44(1):28−54.

[33] 王继业,范永,余文豪,韩丽芳.基于细粒度访问控制的大数据安全防护方法.计算机技术与发展,2019,29(10):134−140.

张建标(1969－),男,博士,教授,博士生导师,主要研究领域为可信计算,网络安全,区块链技术.

徐万山(1988－),男,博士生,主要研究领域为可信计算,网络安全,区块链技术.

张兆乾(1992－),男,博士生,主要研究领域为可信计算,区块链技术,访问控制.

吴娜(1997－),女,硕士生,主要研究领域为区块链技术,云计算安全.