

计算机集成制造系统  
*Computer Integrated Manufacturing Systems*  
ISSN 1006-5911, CN 11-5946/TP

## 《计算机集成制造系统》网络首发论文

题目：基于区块链的多部门数据共享访问控制流程建模  
作者：蒋家昊，张璇，邓宏镜，王杰，黄河祥  
收稿日期：2021-09-23  
网络首发日期：2021-12-16  
引用格式：蒋家昊，张璇，邓宏镜，王杰，黄河祥. 基于区块链的多部门数据共享访问控制流程建模[J/OL]. 计算机集成制造系统.  
<https://kns.cnki.net/kcms/detail/11.5946.tp.20211215.0943.002.html>



**网络首发：**在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

**出版确认：**纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

# 基于区块链的多部门数据共享访问控制流程建模

蒋家昊<sup>1</sup>，张璇<sup>1,2,3+</sup>，邓宏镜<sup>1</sup>，王杰<sup>1</sup>，黄河祥<sup>1</sup>

(1.云南大学 软件学院，云南 昆明 650000；2. 云南大学 云南省软件工程重点实验室，云南 昆明 650000；3. 云南大学 教育部跨境网络空间安全工程研究中心，云南 昆明 650000)

**摘要：**随着国际贸易的发展，诸多国际组织都提出了建立“单一窗口”通关模式的构想，希望实现各部门运政大数据平台的数据交换，提升多部门数据的自动资格审验能力。但是，目前主流的数据平台难以在多部门的情况下保证数据的一致性、真实性、完整性，也难以抵御对数据的恶意攻击。针对运政出入境信息共享流程，基于区块链技术，首次提出了一种混合属性访问控制和能力访问控制的数据共享访问控制模型的流程控制，同时，采用 IPFS 星际文件系统以链下的方式拓展区块链的可存储性。通过基于智能合约，以更细粒度的模式实现访问能力生成和委托，并对访问控制的框架和流程进行的详细的阐述和分析。最后，通过仿真实验验证了本区块链网络的性能和有效性，并对研究内容进行了总结和展望。

**关键词：**区块链；访问控制；基于属性的访问控制；基于能力的访问控制；智能合约；IPFS  
**文献标识码：**A

## Multi-department data sharing access control scheme on block chain

JIANG Jiahao<sup>1</sup>，ZHANG Xuan<sup>1,2,3+</sup>，DENG Hongjing<sup>1</sup>，WANG Jie<sup>1</sup>，HUANG Hexiang<sup>1</sup>

(1. School of Software, Yunnan University, Kunming 650000, China;

2. Key Laboratory of Software Engineering of Yunnan Province, Yunnan University, Kunming 650000, China; 3. Cross-border Cyberspace Security Engineering Research Center, Ministry of Education, Yunnan University, Kunming 650000, China)

**Abstract:** With the development of international trade, many international organizations have put forward the concept of establishing a "single window" customs clearance model, hoping that the data exchange of the big data platform of the operation and administration of various departments can be realized, and the ability of automatic qualification verification of multi-department data can be improved. However, the current mainstream data platforms cannot guarantee the consistency, authenticity, and integrity of data in a multi-departmental situation, and it is also difficult to resist malicious attacks on data. An access control scheme mixed with attribute-based and capability-based access control models on block chain for the cross-departmental border port entry and exit information sharing process was proposed for the first time in this article, at the same time, the IPFS interplanetary file system was used to expand the storability of the block chain in

收稿日期：2021-09-23；修订日期：2021-10-09。Received 23 Sep. 2021; accepted 09 Oct. 2021.

基金项目：国家自然科学基金资助项目（61862063，61502413，61262025）；国家社会科学基金资助项目（18BJL104）；云南省软件工程重点实验室开放基金资助项目（2020SE301）；云南省重大科技专项计划资助项目（202002AE090010，202002AD080002-5）；云南大学数据驱动的软件工程省科技创新团队资助项目（2017HC012）；云南省教育厅科学研究基金项目（2021Y020）。Foundation items: Project supported by the National Natural Science Foundation, China (No. 61862063, 61502413, 61262025), the National Social Science Foundation, China (No. 18BJL104), the Open Foundation of Yunnan Provincial Software Engineering Key Laboratory, China (No. 2020SE301), the Yunnan Provincial Key Science & Technology Plan, China (No. 202002AE090010, 202002AD080002-5), the Yunnan Provincial Data-Driven Software Project Foundation for Science & Technology Innovation Team, China (No. 2017HC012), and the Science Research Foundation of Yunnan Provincial Education Department, China (No. 2021Y020).

an off-chain manner. By the process access control based on smart contracts, the generation and delegation of access capabilities can be performed with a more detailed intensity. It also elaborated and analyzed the framework and process of access control in detail. Finally, the performance and effectiveness of the block chain network were verified through simulation experiments, and the research content is summarized and prospected.

**Keywords:** block chain; access control; attribute-based access control; capability-based access control; smart contract; IPFS

## 0 引言

目前,由于互联网通信技术以及物联网技术的快速发展,大数据已经渗透到生活中的许多角落。良好的数据交互方式为各部门、各企业提供了便捷的数据共享。企业或政府部门可以利用大数据技术挖掘海量数据中的潜在价值,更好地帮助自身提高服务质量、了解用户意愿、推动产业升级<sup>[1]</sup>。在实际应用中,部门与部门间往往可以通过云服务器、物联网等方法来进行数据交互,这些方式能够使存储和计算资源得到充分的利用。但是,这些访问方式仍然存在着不容忽视的安全隐患,集中式的管理方法无法确保数据的安全访问,可能会导致数据的泄露,安全性无法保障等问题。例如,在边境口岸的出入境业务流程中,面向国际贸易的出入境人员首先需要申请各种许可证书,而这些证书的申请往往需要在多个不同的部门间往返,例如公安局、海关部门、工商局、交管部门等等。因此这些部门间需要经常进行数据的共享与访问,如何确保数据的一致性、真实性、完整性和合法性就显得尤为重要。

然而目前面向多部门间的访问控制模型都是基于某个单一的访问控制技术,例如基于角色的访问控制(RBAC)、基于属性的访问控制(ABAC)等,但是这些技术各有弊端。例如,基于角色的访问控制缺乏最管理员授权操作的限制,容易导致角色权限的滥用、基于属性的访问控制容易造成敏感属性的暴露问题。为了提高多部门多企业间数据共享的安全性,改善现有访问控制模型的不足,在本文中,我们面向边境口岸的出入境信息共享业务,基于HyperledgerFabric 联盟链,混合基于属性、能力的访问控制技术,提出了 CABAC (Capability-AttributeBasedAccessControl):一种基于区块链的多部门数据共享访问控制方法。CABAC 模型在继承基于属性的访问控制模型的灵活性的基础上引入了能力令牌这一概念,首先通过不同角色各自具有的属性来分配相应的访问权限并生成相应的能力令牌,用户可以根据访问策略来将自身拥有的能力令牌进一步委派给其他用户,该用户在获得能力令牌后便能对访问对象执行相应的操作。相比现有的访问控制模型,该方案优化了繁琐重复的身份验证过程,能够允许具有相同属性的用户间的能力委派,具有更好的灵活性。同时,与其他基于能力的访问控制模型不同,本文中的能力令牌是以单个能力划分,一个用户可以同时拥有多个能力令牌,因此在权限委派上具有更细的粒度。

本文的主要贡献如下:

1. 首次提出了混合基于属性和能力访问控制模型的数据共享访问控制方案,目前尚未有相似的方案实现,通过开发链码在实施访问控制的前提下引入基于能力的访问控制以更细的粒度来进行访问能力的生成与委派。
2. 针对面向多部门的出入境场景提出了基于 HyperledgerFabric 联盟链和 IPFS 星际文件系统的无中心安全信息存储管理框架,对信息业务管理流程进行了建模、阐述和分析,提供了标准可信的业务操作流程,保证了多部门协同过程中的数据不可篡改,业务流程按照实现约定的顺序执行,更符合多部门间的数据共享要求。

# 1 相关工作

## 1.1 中心化的访问控制

访问控制技术最早可以追溯到 1960 年代提出的多级安全概念,由许多规则和法规组成,旨在对计算、存储、服务等资源的访问设置条件,确保对信息的安全访问。随着技术的发展出现了自主访问控制(Discretionary Access Control, DAC)和强制访问控制(Mandatory Access Control, MAC)。在这之后,基于角色的访问控制(Role-Based Access Control, RBAC<sup>[2], [3]</sup>)和基于属性的访问控制(Attribute-Based Access Control, ABAC<sup>[4]</sup>)产生了。RBAC 将用户映射到角色,通过角色享有许可,通过定义不同的角色与其之间的关系来规范用户的行为。但是在开放网络环境中, RBAC 模型无法适应复杂的环境,且存在角色爆炸问题。而 ABAC 针对复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题,将实体属性的概念联系在一起,通过对主体、客体、权限和环境统一建模来进行访问控制。Gusmeroli 于 2013 年提出了基于能力的访问控制(Capability-Based Access Control, CBAC<sup>[5]</sup>)模型,访问权限以令牌(Token)的形式存在,通过为实体赋予权限来实施访问控制,同时支持权限的委派和撤销。但是,以上的模型都是基于中心化的架构,用户无法得知自己的数据被使用的情况。随着云端技术与区块链技术的成熟,传统访问控制模型的弊端也显露出来。

## 1.2 基于区块链的访问控制

自从中本聪<sup>[6]</sup>于 2008 年提出首次比特币区块链的相关概念后,区块链技术就被广泛应用于金融、医疗、交通等领域。访问控制技术也可以很好的结合区块链技术,达到对共享数据、物联网设备和公共服务的访问控制。Cruz 等人<sup>[7]</sup>将基于角色的访问控制与以太坊智能合约结合,提出了 RBAC-SC 框架,使用智能合约来对用户角色进行创建和分配,同时提出了质询-响应协议来对角色的所有权、分配进行验证。Zhu 等人<sup>[8]</sup>通过集成 ABAC 和区块链技术,将基于事务的访问控制(Transaction-Based Access Control, TBAC)运用到数字资产管理服务中,开发了 DAM-Chain 数字资产管理平台,能够提供主体、对象的保存和发布,访问的请求和授权。为了解决物联网 IoT 设备分布广泛但资源有限,难以采用传统的方法来抵御恶意攻击的问题,Zhang 等人<sup>[9]</sup>同样提出了一种基于属性的访问控制方案。他们在区块链网络中将节点分为授权节点和公共节点,同时将 IoT 设备与区块链分开,引入授权节点来充当区块链客户端,授权节点可以查询部署过的链码来检索已经注册的访问凭证来验证请求者的身份以及访问策略的有效性。Nakamura 等人<sup>[10]</sup>以 CBAC 为基础,通过以单独的能力作为基本单位来定义能力令牌,将传统的能力令牌划分成多个单独的能力令牌,从而实现了更细粒度的访问控制和更灵活的令牌管理。Qi 等人<sup>[11]</sup>考虑到区块链分布式的基础架构,将物联网中产品信息直接存储在链上会导致数据管理的效率和隐私问题,开发了 Cpds 压缩数据共享框架。通过链下的方式在参与者将数据提交到区块链上之前对数据进行压缩和加密,用户使用时再根据策略进行解密,能够让大型工业系统通过安全有效的方式来存储和访问大量的产品数据。Zhang 等人<sup>[14]</sup>为了解决智能电网数据共享中的隐私保护和数据安全问题,提出了一种具有隐私保护的多权限属性加密方案。Lyu 等人<sup>[15]</sup>提出了一个基于区块链的安全访问控制框架,引入了基于区块链的访问令牌机制来实现对内容的共享、审核和撤销,同时还引入了布谷鸟过滤器来提高验证中令牌访问查询的效率。Yang 等人<sup>[16]</sup>提出了一种基于属性加密和区



区块链技术的医疗数据共享方案，该方案结合了基于属性的加密和基于属性的签名，实现了数据隐私和细粒度的访问控制机制。Ullah 等人<sup>[17]</sup>提出了一种基于区块链的数据共享和访问控制系统，用于物联网设备之间的通信。该系统通过访问控制智能合约实现了物联网中数据共享的信任、授权和认真。Xu 等人<sup>[18]</sup>提出了一种具有鲁棒性的基于身份的能力令牌管理策略，利用智能合约对访问控制进行注册、委派和撤销。Banerjee 等人<sup>[19]</sup>为了物联网环境中的数据使用提出了基于 CP-ABE 的多权限属性加密方案，具有恒定大小的密钥和密文。Liang 等人<sup>[20]</sup>为了解决集中式医疗服务系统中的信息孤岛问题，提出了一个基于轻量级信息共享的医疗区块链系统，使用交织编码器对原始电子病历进行加密。和已有工作不同的是，本文提出了一种混合访问控制框架，在 ABAC 的基础上结合 CBAC，能够以更细粒度的模式实现访问能力生成和委托，同时在数据存储上引入 IPFS 星际文件系统来减轻区块链的数据存储压力。

## 2 总体框架设计

本节介绍了提出的 CABAC 框架，模拟不同部门对边境口岸的出入境信息的访问控制流程，通过制定适当的访问策略和属性也可以将本框架拓展到其他领域。与现有工作不同的是，本文首次提出了一种混合访问控制框架，在基于属性的访问控制前提下引入了基于能力的访问控制，能够在实施访问控制的前提下以更细的粒度来进行访问能力的委派。

任何访问控制系统的目的都是谁（主体）可以对什么资源（对象）进行什么（操作或者权限）[5]，本文所设计的访问控制框架涉及如下元素：

$S = \{s_i\}$  系统中所有主体的集合，

$O = \{o_j\}$  系统中所有对象的集合，

$OP = \{op_k\}$  系统中声明的操作的集合（例如读，写，执行），

$C = \{c_l\}$  系统中所有环境上下文的集合（例如时间），

$CAP = \{cap_m\}$  系统中所有能力令牌的集合，

访问控制系统可以定义为：

$\sum_n(s_i, o_j, op_k, c_l, cap_m)$  where  $s_i \in S, o_j \in O, op_k \in OP, c_l \in C, cap_m \in CAP$  for some  $i, j, k, l, m$

该规则表示任意一个访问控制系统都能由连接了主体  $S$ 、对象  $O$ 、操作  $OP$ 、环境上下文  $C$  和能力令牌  $CAP$  的规则集  $\sum n$  所定义。

出入境人员及各部门人员可以通过智能手机或者个人电脑来访问区块链网络从而执行访问控制，如图 1 所示。在图 1 中，本文提出的框架由联盟区块链和 IPFS 组成，主要参与者有检疫部门、交管部门、海关部门和公安部门。由于在边境口岸出入境信息共享业务流程中会涉及海量的数据，包括图片类型的数据（例如许可证、车辆的照片等），区块链技术虽然可以提供数据共享查询的通道，但是也存在着缺陷。例如区块的大小限制了存储在区块链上的文件数量和类型，在比特币区块链中，每个区块的大小仅为 1M，能够存储的信息十分有限，因此本文使用了 IPFS 星际文件系统从链下存储的方式对区块链的可存储行进行了拓展。将图片文件存储在 IPFS 中，同时将其返回的 Hash 值存储到区块链上，检索时只需要对应文件的 Hash 值就能在 IPFS 中查询到相应的文件。访问控制部分主要涉及五个智能合约：属性管理合约（Attribute Management Contract, AMC）、策略管理合约（Policy Management Contract, PMC）、令牌生成合约（Token Generation Contract, TGC）、令牌管理合约（Token Management Contract, TMC）和访问控制合约（Access Control Contract, ACC）。在访问控制过程中，AMC 负责存储和管理主体以及对象的属性，PMC 负责存储和管理访问控制策略，

The diagram illustrates a Blockchain-based Access Control Architecture, showing the flow of data and control between various components.

**External Entities and Blockchain Interaction:**

- 检验检疫部门** (Inspection and Quarantine Department) and **海关部门** (Customs Department) are connected to the **区块链** (Blockchain) via **IPFS** (InterPlanetary File System).
- 交管部门** (Traffic Management Department) and **公安部门** (Public Security Department) are also connected to the **区块链** via **IPFS**.

**CBAC (Context-Based Access Control) Layer:**

- The **CBAC** layer is the central component for access control.
- It contains two main components: **TGC** (Target Group Component) and **TMC** (Target Member Component).
- Both **TGC** and **TMC** have **Read: True, 1** and **Write: Ture, 1** permissions.

**ABAC (Attribute-Based Access Control) Layer:**

- The **ABAC** layer is responsible for defining attributes and policies.
- It contains two main components: **AMC** (Attribute Master Component) and **PMC** (Policy Master Component).
- AMC** manages attributes for users, such as **Alice** and **Bob**, with their respective roles and departments.
- PMC** manages policies, including logical operations like **AND** and **OR**, and roles like **主管** (Manager), **税务室** (Tax Room), **会计** (Accountant), and **分析师** (Analyst).

**ACC (Attribute-based Access Control) Layer:**

- The **ACC** layer is the final component that enforces access control based on the attributes and policies defined in the **ABAC** layer.
- It contains a list of attributes: **Alice; 检验检疫部门; 食品检验处; {Read; Write}**.

## 2.1 实现访问控制的智能合约设计

1. **AMC** 负责对主体以及对象的属性进行存储和管理。**AMC** 由管理员部署，同时只有管理员有权限执行它。在本文所模拟的多部门系统中，主体可以为各个部门中的职员，管理员可以是各部门中的行政主管。如果主体是物联网中的设备，则管理员可以是其拥有者。为了区分不同的主体，每个主体都有唯一的标识符来指定其身份，对象同理。在本系统中，使用 **HyperledgerFabric** 中 **CA** 颁发的证书来作为身份标识信息，例如表 1 中的“**MI9ZT...**”。表 1 举例展示了主体属性和对象属性，例如主体[**MI9ZT...**]的名称为 **Alice**，所属部门为海关，所属科室为税务室，职位为主管等，同样对象[**FU1B3**]是名称为“**Lenovo1**”的物联网设备，所属部门为检疫部门，所属科室为食品检验处。**AMC** 还定义了 **SubjectGet()**、**SubjectAdd()**、**SubjectDel()**、**ObjectGet()**、**ObjectAdd()**、**ObjectDel()** 方法，分别用于获取、添加、删除主体和对象的属性。

表 1 主体、对象的属性

Subject[MI9ZT...]	Object[FU1B3...]
名称: “Alice”	名称: “Lenovo1”
部门: “海关”	部门: “检疫部门”
科室: “税务室”	科室: “食品检验处”
职位: “主管”	Others: “ ”
Others: “ ”	

2. PMC 负责存储和管理本文中定义的访问策略, 与 AMC 相同, 同样只能由管理员 (对象的拥有者) 执行。在本文中访问策略定义为一组主体属性 (SA)、一组对象属性 (OA)、一组访问能力 (Cap) 和一组环境上下文 (Cxt) 的组合。也就是说, 在环境上下文 Cxt 的前提下, 具有 SA 属性的主体可以对具有 OA 属性的对象进行 Cap 操作。在环境上下文 Cxt 中设置了一个参数 Parm, 如果 Parm 为 0, 则不运用动态访问控制, 如果为 1, 则需要再设置开始时间 StartTime 和结束时间 EndTime, 表示只有在这段时间内才能对该对象实施访问。表 2 举例说明了一个访问控制策略, 主体属性 SA={部门: 海关, 科室: 税务室, 职位: 主管}, 对象属性 OA = { 部门: 检疫部门, 科室: 食品检验处}, 访问能力 Cap = { Read, Write, Execute, Degelated }, 环境上下文 Cxt = { Parm: 1, StartTime: 1622505600, EndTime: 1625043600 }。其中 StartTime 和 EndTime 表示为 Unix 时间戳, 代表在北京时间 2021 年 6 月 1 日 8 时到 2021 年 6 月 30 日 17 时这段时间内, 海关部门的税务室主管可以对检疫部门的食品检验处的信息进行读、写和执行的操作, 同时可以将这些能力进一步委派给下一个主体。与文献[12]不同的是, 由于访问策略不是针对某个特定主体或对象的, 因此一个策略可以限定多个主体和对象之间的访问控制。这些策略都以表格的形式存储在 PMC 中, 同时该合约中还定义了 policyGet(), policyAdd(), policyDelete(), policyUpdate()方法, 可以对访问策略实施获取、增加、删除、和修改操作。

表 2 访问策略示例

主体属性	对象属性	能力	环境上下文
部门:海关	部门:检疫部门	Read:True, 1	Parm: 1
科室:税务室	科室:食品检验处	Write:True, 1	StartTime:1622505600
职位:主管	其他:	Execute: True, 1	EndTime:1625043600
其他:			

3. TGC 负责在 ACC 通过主体的访问请求后根据访问策略为其生成相应的能力令牌, 提供了 tokenGenerate() 方法, 用于生成能力令牌。本文参考了 Nakamura 等人<sup>[10]</sup>的工作, 将传统包含多个操作的能力令牌拆分为单独的能力令牌, 能力令牌不再以主体为单位对象, 而是以一个单一的授权能力作为单位, 也就是说不是像之前的基于能力的访问控制的方案中那样为每个主体颁发一个能力令牌, 而是为每一个授权的能力创建一个单独的令牌。能力令牌的结构定义如下:

$$CAPS_o[IDs][IDo][OP] = \{ID_p, \{ID_{ch}\}, Dep, DR\} \quad (1)$$

其中:  $ID_s$  为主体的 ID;  $ID_o$  为访问对象的 ID;  $OP$  为一系列操作的集合, 例如读取、写入、执行等, 如果为 NULL, 那么将不允许对资源进行操作;  $ID_p$  为给主体 S 赋予权限的父主体的 ID;  $ID_{ch}$  为主体 S 赋予权限的子主体的 ID;  $Dep$  为令牌在委托树中的深度;  $DR$  表示是否可以进一步委派权限。

以表 2 为示例, 如果 ACC 通过了主体的访问请求, TGC 就会为该主体生成相应的三个能力令牌: 读 (Read) 能力令牌, 写 (Write) 能力令牌和执行 (Execute) 能力令牌。





### 2.2.1 区块链/IPFS 存储数据流程

IPFS 与区块链的存储数据流程如图 3 所示。因为 IPFS 与 HyperledgerFabric 联盟链是彼此独立的,所以 HyperledgerFabric 的链码不能直接调用 IPFS,通过增加 OpenAPI(如 ipfsadd)允许外部系统间接操作 IPFS 网络,而不需要改变 Fabric 的代码和内部流程。首先将文件上传到 IPFS,再将返回的代表存储地址的哈希值以事务的形式提交到区块链中。

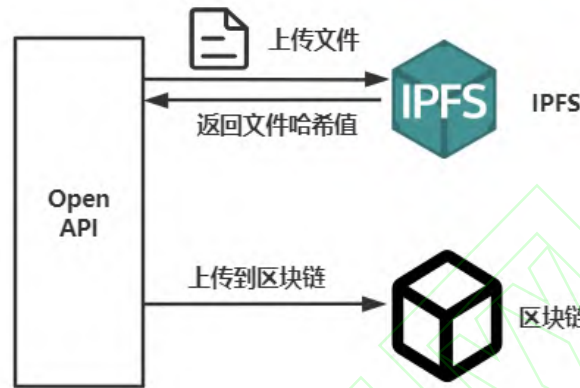


图 3 IPFS 与区块链交互流程

---

#### Algorithm 1 contentaddressedhash

---

**Require:** ImageFiles

//the file uploaded by the peers in the network

**1:**  $file \leftarrow \text{request.file}[\text{'upload'}]$

//initiated the IPFS distributed file storage

**2:**  $api \leftarrow \text{ipfsapi.connect}[\text{'localhost'}, 4200]$

//original file addition into IPFS storage

**3:**  $res \leftarrow \text{api.add}(file)$

//file to binary conversion

**4:**  $H_v \leftarrow \text{convert}(file, \text{binary})$

//create the hash message digest of the file

**5:**  $digest \leftarrow \text{ch}(\text{'sha256'}).update(file).digest()$

**6:**  $Mds \leftarrow (digest.bylength.toString(16), \text{'hex'})$

//combining binary conversion and salting message digest for content-addressed hash

**7:**  $content\_addressed \leftarrow \text{combine}(H_v, Mds, digest)$

**8:** return content addressed hash

---

各部门上传文件到 IPFS 见算法 1<sup>[21]</sup>, 算法描述如下: 文件由网络中的 peer 节点上传, 首先使用 ipfsapi.connect()方法建立与 IPFS 的连接,再调用 add()方法将图片文件存储到 IPFS 星际文件系统中,文件将会被切分为碎片,每一个不超过 256Kb,并使用 convert()方法转换为二进制格式,这些碎片会作为输入进行一次 SHA256 哈希运算<sup>[13]</sup>得到一个 digest 值,再将 digest 值转换为十六进制得到该文件的基于内容寻址的 hash 值。

### 2.2.2 访问控制流程

整个访问控制流程中各合约的交互过程如图 4 所示。首先,主体会将目标对象的访问

信息的以事务的方式发送给 ACC；ACC 在接收到来自主体的信息之后会从 AMC 中查询并获取主体以及对象的属性；接着，ACC 会从 PMC 中查询是否有相应的访问策略；如果没有查询到有关访问策略，那么 ACC 就会将禁止访问的结果返回给主体；在查询到相关访问策略后，ACC 会再从 TMC 中查询该主体是否拥有对于访问对象的能力令牌；如果主体之前就拥有对于该对象的能力令牌，那么就会将允许访问的结果返回给主体；如果主体未拥有能力令牌，那么 ACC 就会调用 TGC 为其生成相应的能力令牌；最后，ACC 会将响应结果返回给主体。

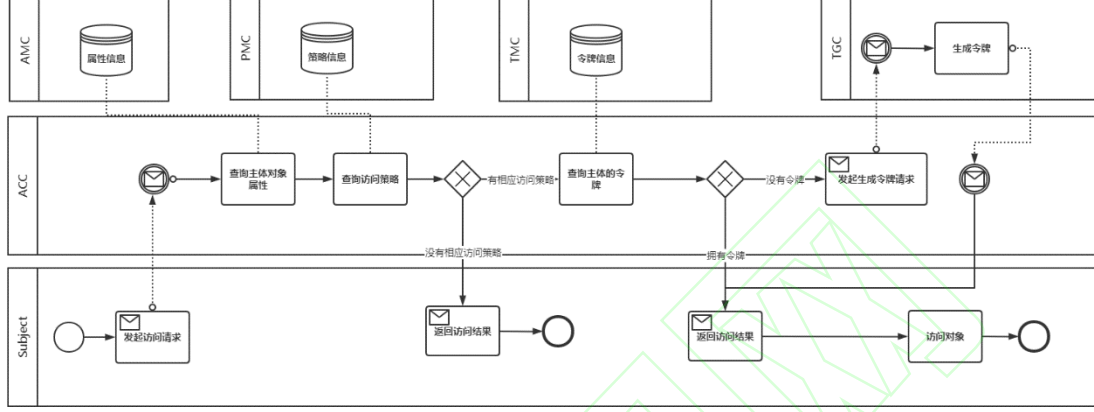


图 4 CABAC 的 BPMN 协作图

访问控制流程见算法 2:

---

**Algorithm 2** AccessControlProcess

---

**Require:** Subject\_ID, Object\_ID, Operations

//transaction contains request information send to accessControl ABI

**1: AccessRequest**  $\leftarrow$  Acc.accessControl(Subject\_ID, Object\_ID, Operations)

//AMC returns the attributes of subject and object

**2: Subject\_attributes**  $\leftarrow$  AMC.SubjectGet(Subject\_ID)

**3: Object\_attributes**  $\leftarrow$  AMC.ObjectGet(Object\_ID)

//PMC returns the matched access control policy

**4: AccessControlPolicy**  $\leftarrow$  PMC.policyGet(Subject\_attributes, Object\_attributes)

**5: if** AccessControlPolicy  $\neq$  “ ”

**6:   Allowed\_Capabilities**  $\leftarrow$  AccessControlPolicy.Capability

**7:endif**

//query the subject whether had capability tokens

**6: Subject.token**  $\leftarrow$  TMC.tokenGet(Subject\_ID)

**7: if** Subject.token  $==$  “ ”

**8:   Subject.token**  $\leftarrow$  TGC.tokenGenerate(Allowed\_Capabilities)

**9: end if**

**10: return** Subject.token

---

主体对对象发起的访问控制流程见算法 2，算法描述如下：主体首先调用 ACC 的 accessControl()方法，需要将自身的 ID、访问对象的 ID、对访问对象进行的操作作为输入，AMC 会调用 SubjectGet()和 ObjectGet()方法来获取主体与对象的属性，随后会调用 PMC 中的 policyGet()方法来获取相应的访问策略，如果访问策略不为空，那么 TMC 就会调用 tokenGet()方法查询主体是否之前就已经获得过对于对象的访问能力令牌，如果为空，那么

就会调用 tokenGenerate()方法为主体生成策略中定义的能力令牌,将结果返回给主体和对象。

---

**Algorithm 3** TokenDelegationProcess

---

**Require:** SubjectA\_ID, SubjectB\_ID, CapabilityToken

**1: DelegationRequest**

← TMC.tokenDelegate(SubjectA\_ID, SubjectB\_ID, CapabilityToken, 1,)

**2: SubjectA.token** ← TMC.tokenGet(SubjectA\_ID)

**3: if** CapabilityToken == SubjectA.token

**4:     if** SubjectA.token.DelegationRight == 1

**5:         SubjectB.token** ← TGC.tokenGenerate(SubjectA.token.Capability)

**6:         SubjectB.token.Parent** ← SubjectA\_ID

**7: SubjectB.token.Dep** += 1

**8:         SubjectB.token.DelegationRight** ← 1

**9:     endif**

**10: end if**

**10: return** SubjectB.token

---

主体间的令牌委派流程见算法 3, 算法描述如下: 主体 A 想要把自己的能力令牌 CapabilityToken 委派给主体 B, 使其拥有和自己同样的能力。首先主体 A 调用 TMC 中的 tokenDelegate()方法, 将自己的 ID、主体 B 的 ID、想要委派的能力令牌、是否允许进一步委派作为输入, TMC 就会调用 tokenGet()方法查询主体 A 是否拥有该能力令牌, 如果查询结果与 A 的能力令牌相匹配, 那么就会为 B 生成相同的能力令牌, 并逐一修改令牌中的参数 (父主体 Parent、委派深度 Dep、进一步委派权限 DelegationRight), 最后将能力令牌返回给主体 B。

### 3 CABAC 实验分析

通过仿真实验对本文所提出的 CABAC 框架的有效性进行了验证。实验环境如下: 操作系统为 Ubuntu18.04.5, CPU 为 Inter(R) Core(TM) i7-10700 CPU @ 2.90Ghz, 内存大小 16GB, HyperledgerFabric 版本为 1.4.0, node.js 版本为 10.13.0, npm 版本为 6.4.1。测试区块链网络运行在单台主机上, 包括两个 CA 和一个 Orderer 节点。

#### 3.1 访问控制实例

传统的基于属性的访问控制模型在访问过程中通过主体以及对象的属性来决定是否允许访问, 由于混合了基于能力的访问控制, 本方案相比基于单独机制的访问控制在整个访问流程中包含了有关能力令牌生成与委派的相关步骤。通过生成细化到单独操作的能力令牌, 例如 (read 操作), 能够以更细粒度的方式限制主体对访问对象进行的操作, 同时让权限的分配和管理更加灵活。

本小节模拟了一个访问控制过程实例: 部门数据管理员将文件上传到 IPFS 并获取哈希值 QmSyzwqkCnp8waXtx7BqUN15DWPAGg9gCWgYeHn81MnrFK, 如图 5 所示; 管理员为主体 A 添加主体属性, 如图 6 所示; 主体 A 对对象 B 发起访问请求, 获得能力令牌并将该

能力令牌委派给主体 C。首先，ACC 调用 TGC 中的 tokenGeneration()ABI 后会根据 PMC 中的访问策略为主体生成相应的能力令牌。图 7 展示了主体 A 的“read”能力令牌，该令牌表明了主体 A 可以对对象 B 进行 read 操作，因为是新生成的令牌，所以没有父主体，也没有子主体，相应的在委派树中的深度也为 0。DelegationRight 表明主体 A 可以将此令牌进一步进行委派。与 Nakamura 等人<sup>[10]</sup>的方案不同的是，本方案默认所有能力令牌的委派都是可以撤回的。


名称 ↑	大小
 出入境许可证.png Qm5y2wqkCnp8waXtx7BqUN150MPAg9gC4gYehN81MnrFK	283 KB

图 5 存入到 IPFS 中的文件及其哈希值

```
Successfully added subject'MIICAjCCAaigAwIBAgIUb9' attributes:
{'Org':'Customs','Dep':'Tax Office','Pos':'Executive'}
```

图 6 为主体添加属性

```
Caps[address A][address B][read]
Parent:
Children:
Depth:0
DelegationRight:True
```

图 7 新生成的能力令牌

当主体 A 将该“read”能力令牌委派给主体 C 之后，能力令牌的信息如图 8 所示。可以看到 Depth 从 0 变成了 1，表示该令牌在委派树中的深度为 1，也就是有过一次委派关系。

```
Caps[address A][address B][read] after delegation
Caps[address C][address B][read]
Parent:MIICAjCCAaigAwIBAgIUb9
Children:
Depth:1
DelegationRight:True
```

图 8 委派过后的能力令牌

最终 ACC 会返回访问请求信息，如图 9 所示。ACC 通过与其它几个合约的交互验证了主体 A 和对象 B 的属性，并根据匹配的访问策略赋予了主体 A “read”能力令牌，同时指定该“read”令牌是可以进一步委派的。

```
{'result':'Succeed','Subject':'MIICAjCCAaigAwIBAgIUb9','Object':'AUBgNVBAcTDVNhbiBGcHDAA'
'CapabilityTokens':'read,1'}
```

图 9 访问请求结果



## 3.2 区块链网络性能

### 3.2.1 存储空间性能

本文中使用的数据为云南省各口岸班车运营数据，包含 20 万条记录。

存储空间压缩比C的表达式如下：

$$C = \frac{H + iHash \times N}{H + \sum_{i=1}^N Tx_i} \quad (2)$$

其中， $H$ 代表区块链中每个区块链头的数据量大小， $iHash$ 表示事务在 IPFS 中哈希值的大小， $N$ 代表区块链中事务的数量， $Tx$  代表区块链中每个事物的数据量大小。区块头的大小为 80 字节，每个区块平均包含 500 个交易，每个交易的大小约为 250 字节。IPFS 返回的哈希值大小只占 46 个字节。由公式可以推出随着交易数量的增加，数据的压缩比明显增加。图 10、图 11 分别显示了数据压缩比随着数据量大小的变化以及区块链直接存储数据和存储 IPFS 文件哈希值的数据量大小对比。从图中可以看出，随着数据量的增大，源数据与返回的哈希值的占用存储空间比越来越大，使用 IPFS 进行链下存储的优势会愈发明显。

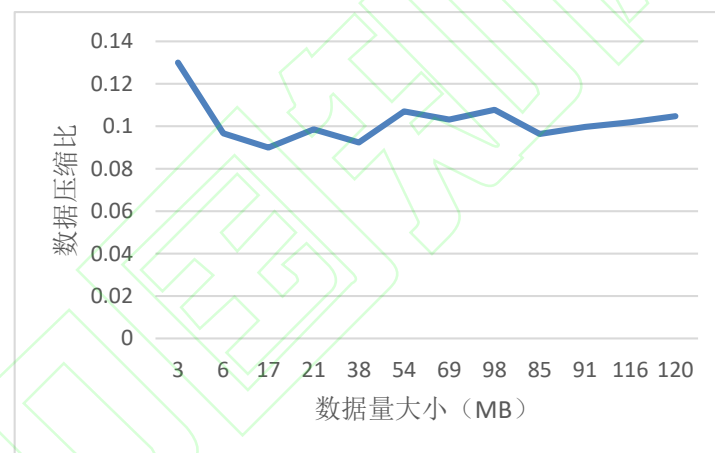


图 10 数据压缩比随数据量的变化

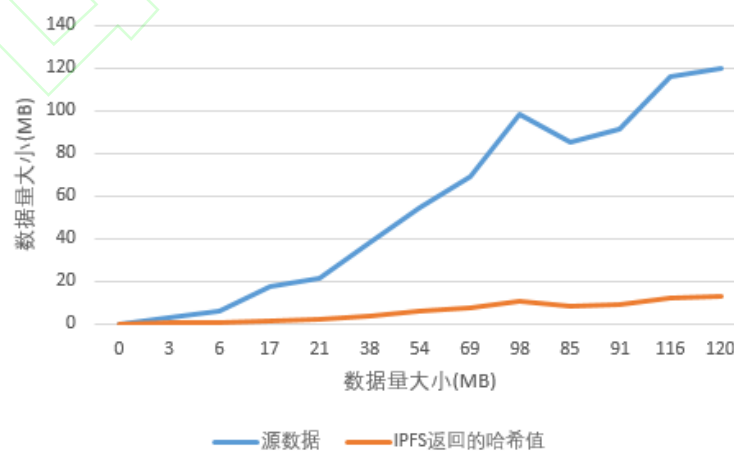


图 11 区块链存储源数据与 IPFS 哈希值数据量大小对比

### 3.2.2 访问控制流程性能

本文方案与其他文献方案在访问控制流程中的功能性比较：

表 3 访问控制方案对比

方案	基于属性	基于能力	数据加密	支持 IPFS
文献[9]ABAC	是	否	是	否
文献[10]CapBAC	否	是	否	否
本文方案 CABAC	是	是	否	是

如表 3 所示, Zhang 等人<sup>[9]</sup>提出了一种 ABAC 访问控制方案,他们在区块链网络中将节点分为授权节点 AN 和公共节点,AN 不仅为物联网设备分配属性,同时也对访问策略进行制定和决策,授权节点可以查询部署过的链码来检索已经注册的访问凭证来验证请求者的身份以及访问策略的有效性。而 Nakamura 等人<sup>[10]</sup>以 CBAC 为基础,通过以单独的能力作为基本单位来定义能力令牌,将传统的能力令牌划分成多个单独的能力令牌,从而实现了更细粒度的访问控制和更灵活的令牌管理。本文提出的方案结合了 ABAC 和 CBAC,既可以指定访问策略也能完成对能力令牌的划分,同时还支持区块链数据以链下方式存储。

在不同操作下, CABAC 方案中的不同操作的平均耗时如图 12 所示。横轴坐标表示操作名称,纵轴坐标表示平均耗时,单位 (ms)。从图中可以看出,本方案中的所有操作消耗的时间均在 450ms 之内,生成能力令牌操作和最后的返回访问结果操作相比获取属性和委派能力令牌操作需要花费更多的时间,但总体上还是可以接受的。

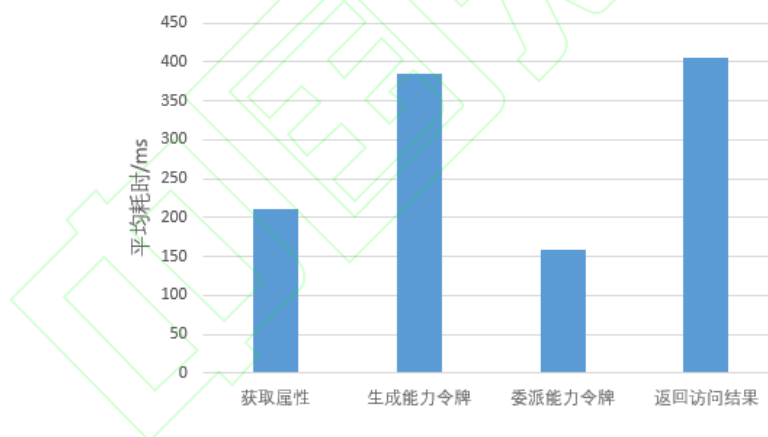


图 12 CABAC 中不同操作所花费的时间

## 4 结束语

为了实现部门与部门间的细粒度访问控制,本文首次提出了一种基于区块链的多部门数据共享混合访问控制方案,使用 HyperledgerFabric 联盟链作为区块链基础架构并编通过写链码来进行访问控制和权限的委派,同时利用 IPFS 以链下存储的方式拓展了区块链的可存储性,减轻了区块链的数据存储压力,最后通过仿真实验验证了该方案的可行性。与现有的基于区块链的访问控制方案相比,本方案提出了混合基于属性和能力的访问控制模型的数据共享访问控制方案,能够在实施访问控制的前提下以更细的粒度来进行访问能力的生成与委派。

但是，本方案未涉及基于属性的文件的加密，在数据安全性上有待提升。同时，本方案中的令牌委派过程没有对委派的对象设置限制，容易造成能力令牌的随意委派。针对以上问题，本文还需要进一步的研究来解决这些局限性。

## 参考文献：

- [1] 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). [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.]
- [2] D F Ferraiolo, D R Kuhn.Role-based access control [A] .In Proceedings of the 15th National Computer Security Conference [C] .Baltimore, USA, 1992,8.554-563.
- [3] R Sandhu, E Coyne, H Feinstein, et al. Role-based access control models [J] .IEEE Computer, 1996,2, 29(2) :38-47.
- [4] GoyalV, Pandya O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM conference on Computer and Communication Security. Alexandria, USA, 2006: 89-98.
- [5] Gusmeroli S , Piccione S , D Rotondi. A capability-based security approach to manage access control in the Internet of Things[J]. Mathematical & Computer Modelling, 2013, 58(5-6):1189-1205.
- [6] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: <https://bitcoin.org/bitcoin.pdf>, 2009.
- [7] Cruz J P , IEEE), Kaji Y , et al. RBAC-SC: Role-based Access Control using Smart Contract[J]. IEEE Access, 2018, 6:12240-12251.
- [8] Yan Z , Yao Q , Zhou Z , et al. Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control[C]// 2018 IEEE International Conference on Services Computing (SCC). IEEE, 2018.
- [9] Zhang Y , Li B , Liu B , et al. An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices[J]. Electronics, 2020, 9(2):285.
- [10] Nakamura Y, Zhang Y, Sasabe M, et al. Capability-based access control for the internet of things: An ethereum blockchain-based scheme[C]//2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019: 1-6.
- [11] Qi S , Lu Y , Zheng Y , et al. Cpbs: Enabling Compressed and Private Data Sharing for Industrial IoT over Blockchain[J]. IEEE Transactions on Industrial Informatics, 2020, PP(99):1-1.
- [12] Wang P , Yue Y , Sun W , et al. An Attribute-Based Distributed Access Control for Blockchain-enabled IoT[C]// 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2019.
- [13] Kumar A , Ghrera S P , Tyagi V . A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)[J]. Advances in Intelligent Systems & Computing, 2015, 337:401-408.
- [14] Zhang L , Ren J , Mu Y , et al. Privacy-Preserving Multi-Authority Attribute-Based Data Sharing Framework for Smart Grid[J]. IEEE Access, 2020, PP(99):1-1.
- [15] Lu Y , Huang X , Dai Y , et al. Blockchain and Federated Learning for Privacy-Preserved

- Data Sharing in Industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2019, PP(99):1-1.
- [16] Yang X , Li T , Pei X , et al. Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology[J]. IEEE Access, 2020, PP(99):1-1.
- [17] Ullah I , Sultana T , Javaid N . Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices[M]. 2020.
- [18] Xu R , Chen Y , Erik B , et al. BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT[J]. Computers, 2018, 7(3):39-.
- [19] Banerjee S , Roy S , Odelu V , et al. Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment[J]. Journal of Information Security and Applications, 2020, 53:102503.
- [20] Liang Y , Li Y , Shin B S . FairCs-Blockchain-Based Fair Crowdsensing Scheme using Trusted Execution Environment[J]. Sensors, 2020, 20(Sensors and Actuators for Personalized Medicine and Healthcare Applications).
- [21] Kumar R . Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain[C]// 2019 Fifth International Conference on Image Information Processing (ICIIP). 2020.

## 作者简介:

张璇 (1978—), 女, 江苏南京人, 教授, 博士, 博士生导师, 研究方向: 业务过程、知识工程、区块链, 网络空间安全, E-mail: zhxuan@ynu.edu.cn;

蒋家昊 (1996-), 男, 江苏镇江人, 硕士研究生, 研究方向: 区块链、访问控制;

邓宏镜 (1996-), 男, 湖北荆州人, 硕士研究生, 研究方向: 区块链、隐私保护;

王杰 (1997-), 男, 云南大理人, 硕士研究生, 研究方向: 区块链、联邦学习;

黄河祥 (1998-), 男, 贵州盘州人, 硕士研究生, 研究方向: 区块链、实证研究。