基于区块链的可溯源访问控制机制

谢绒娜[1,2]，李晖[2]，史国振[1]，郭云川[3]，张铭[2]，董秀则[1]

（1. 北京电子科技学院密码科学与技术系，北京 100070；2. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
3. 中国科学院信息工程研究所，北京 100093）

摘 要：为提高数据访问流转控制的透明性、访问流转的可溯源，提出了一种基于区块链的可溯源访问控制机制。所提机制将访问控制策略以智能合约的形式部署在区块链上，通过执行分布式的智能合约实现访问控制策略的评估，确保整个访问授权过程的无中心、透明性和可溯源；采用链下和链上相结合的方式，将客体存储在链下数据服务器，通过客体存储地址和摘要值等信息生成客体索引存储在客体区块链上；日志区块链详细记录了客体访问授权过程和访问过程，任何错误行为都不可修改地记录在区块链上。通过安全性分析，所提机制在保证客体资源隐私性的前提下，实现了访问授权无中心、透明性和可溯源。

关键词：区块链；访问控制；智能合约；无中心；可溯源

中图分类号：TP302

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020232

Blockchain-based access control mechanism for data traceability

XIE Rongna[1,2], LI Hui[2], SHI Guozhen[1], GUO Yunchuan[3], ZHANG Ming[2], DONG Xiuze[1]

1. Department of Cryptography and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. School of Cyber Engineering, Xidian University, Xi'an 710071, China
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: To improve the transparency and traceability of access control, a blockchain-based access control mechanism for data traceability and provenance was proposed. The proposed access control policy was transferred to the smart contract and deployed on the blockchain, and the access authorization evaluation was realized by executing the smart contract deployed on the blockchain to ensure the decentralization, transparency and traceability of the access control process. The manner of combining off-chain and on-chain was adopted, the object was stored in off-chain data server, and the object index was generated by the object storage address and hash value, and deployed on the object blockchain. The log of object access authorization and access were recorded in the log blockchain, any misbehavior was immutably recorded. The security analysis show that, the proposed mechanism achieve the properties of decentralization, transparency and traceability while ensuring the privacy of data.

Key words: blockchain, access control, smart contract, decentralized, traceability

1 引言

随着云计算、物联网、大数据等信息技术的发展，分布在不同域的各种不同系统、设备之间频繁地互联互通，相互之间数据的访问和流转成为一种趋势。在数据访问和流转中，数据的安全性和隐私性成为制约信息技术发展的瓶颈。访问控制技术为合法的主体在特定的访问环境下授予一定的访问

收稿日期：2020−06−22；**修回日期**：2020−08−12

通信作者：史国振，sgz1974@163.com

基金金项目：国家重点研发计划基金资助项目（No.2016QY06X1203, No.2017YFB0802705, No.2016QY06X1203）；国家自然科学基金资助项目（No.61932015）

Foundation Items: The National Key Research and Development Program of China (No.2016QY06X1203, No.2017YFB0802705, No.2016QY06X1203), The National Natural Science Foundation of China (No.61932015)

权限，成为保障数据安全和隐私的主要手段。

现有的基于角色的访问控制机制（RBAC, role based access control）基于主体的角色进行访问授权，基于属性的访问控制机制（ABAC, attribute based access control）基于主体属性、客体属性和环境属性进行访问授权。传统的访问控制机制大多通过集中授权点进行访问授权，存在单点失效导致整个控制系统失效以及性能瓶颈等问题，还存在访问过程不可追踪和溯源等缺点。如何实现访问控制过程的无中心、透明性、可溯源成为访问控制机制急需解决的问题。

区块链技术允许建立一个分布式、透明的、不可篡改的账本，因此受到越来越多的关注。自 2008 年被引入加密货币[1]以来，区块链技术被广泛应用于物联网、云计算、大数据等场景[2-5]。Maesa 等[6]将区块链技术引入访问控制中，通过区块链实现访问控制策略的存储和检索，而访问控制策略的评估通过传统的访问控制系统实现。文献[7]将基于属性的访问控制策略转化成智能合约（SC, smart contract）并部署在区块链上，通过智能合约实现访问控制策略的评估和属性管理。上述文献对于如何实现数据访问的可追踪和溯源没有给出很好的解决方案，同时存在一次授权多次访问的问题。

针对上述问题，本文利用区块链无中心、透明性和不可篡改等优点，以基于属性的访问控制机制为基础，提出了基于区块链的可溯源访问控制机制。该机制采用链上和链下相结合的方式，将客体资源存储在链下的数据服务器中，基于客体存储地址和摘要值生成客体索引存储在区块链上；将访问控制策略以智能合约的方式部署在客体区块链上，通过执行区块链上的智能合约实现访问控制过程的透明性，并将访问授权日志和访问日志记录在日志区块链上，在保障客体隐私性的前提下，实现访问过程无中心、透明性和可溯源。

本文主要贡献如下。

1) 提出了基于区块链的可溯源访问控制机制，把访问控制策略以智能合约的形式部署在区块链上，访问控制执行和评估通过执行区块链上分布式的智能合约实现，实现了访问授权的无中心和透明性，有效防止了策略执行点和策略决策点非法授权或者拒绝访问请求等问题，同时避免了集中授权造成的性能瓶颈。

2) 为保护客体资源的隐私性，采用链上和链下相结合的方式，客体资源采用链下的方式存储在数据服务器，基于客体存储地址及摘要值生成的客体索引存储在客体区块链上，提高了客体资源的安全性和隐私性。

3) 向授权访问主体分发访问凭据，并把访问凭据不可修改地记录在区块链上。主体在对客体访问时，通过区块链对主体访问凭据的有效性进行验证，实现细粒度的访问控制，有效避免了一次授权多次访问的问题。

4) 将区块链分为客体区块链和日志区块链，其中日志区块链详细记录了访问授权日志和客体访问日志，实现访问授权过程的可追踪和可溯源。

2　相关工作

区块链由于无中心、透明性、不可篡改等优点，被广泛应用在物联网、云计算、大数据等不同场景[2-5]，用来实现数据的安全性和隐私性。访问控制是保证数据安全的一种有效手段，传统的访问控制采用中心授权，存在单点失效以及性能瓶颈等问题，同时传统访问控制存在访问过程不透明、不可追踪和溯源等缺点，已有不少文献将区块链技术应用到访问控制中。Maesa 等[6]利用区块链技术实现访问控制，通过比特币协议实现访问控制策略的存储和检索，而访问控制策略的评估通过传统的访问控制系统实现。智能合约是部署在区块链上的计算机程序，当满足必要条件时，以无中心的方式自动执行某些功能。最近不少方案采用区块链和智能合约实现访问控制。文献[8]对文献[6]的方案进行改进，通过智能合约实现访问控制的主要功能。为提高访问控制策略评估的可审计性，文献[7]将基于属性的访问控制策略转化成智能合约并部署在区块链上，通过智能合约实现访问控制策略的评估和属性管理。针对大数据资源的特点以及集中式访问控制机制存在的问题，刘敖迪等[9]以 ABAC 模型为基础，提出一种基于区块链的大数据访问控制机制，该机制采用基于智能合约的访问控制方法实现对大数据资源透明、动态、自动化的访问控制。针对物联网中的特点，杜瑞忠等[10]提出一种基于层级区块链的物联网分布式体系架构，该架构以 ABAC 模型为基础，采用智能合约的方式实现对物联网设备基于属性的域内和跨域的动态、自动化访问控制。

数据安全保护是安全领域的一个研究热点。2018 年 5 月，通用数据保护条例（GDPR, general data

protection regulation）在所有的欧洲国家强制执行，通过委托授权服务提供者实现对个人数据的控制，并通过第三方监管机构验证服务提供者是否严格遵守 GDPR。如何验证服务提供者是否严格遵守 GDPR 是数据保护机制面临的挑战。针对上述问题，Truong 等[11]基于区块链和智能合约的优点，提出个人数据管理平台，利用区块链和智能合约实现数据授权的透明性，验证服务提供者是否遵守 GDPR，任何违反规则的行为都将被记录，通过给每个参与者颁发公私钥对进行身份管理，并采用非对称加密算法保护参与者身份和敏感信息。在策略部署和访问授权方面通过数字签名算法对相关信息进行验证，随着管理数据量的增加，该算法在密钥管理和访问控制效率等方面都面临巨大挑战。Wu 等[12]提出了采用公共区块链提供策略遵守的证据，并通过粘性策略的方式实现对跨域访问中策略遵守的监管。针对区块链数据的隐私性问题，Zyskind 等[13]结合区块链和链下的数据存储实现个人数据管理，但该方案仅考虑对用户数据的读操作，没有考虑其他访问操作。Kosba 等[14]提出一种去中心化的智能合约系统 Hawk，该系统以密文形式在区块链上存储交易，实现交易的隐私性。Hawk 能以直观的方式编写智能合约，编译器使用零知识证明等加密原语，自动生成有效的加密协议，使合同方与区块链进行交互。为提高智慧城市中数据的可用性、完整性和隐私性，Makhdoom 等[15]提出了基于区块链的隐私保护和数据共享方案 PrivySharing，该方案将区块链网络分成不同的通道，不同通道的数据相互隔离，每个通道包含有限个授权组织处理特定类型的数据。PrivySharing 通过在智能合约中嵌入访问控制规则实现对数据的访问控制。针对数据跨域共享存在的安全问题，Rahman[16]等提出了跨域的数据共享平台，并将数据共享平台部署在一个全局的云服务器中。当有跨域访问请求时，云服务器通过域内安全网关收集存储在本地的数据，并通过区块链记录数据转移。全局的云服务器通过区块链来检验完全网关的错误行为，但该方案通过一个全局云服务中心实现数据共享，存在单点失效造成的安全问题和性能问题。王秀利等[17]提出了一种应用区块链的数据访问控制与共享模型，利用属性基加密对数据进行访问控制与共享，达到细粒度访问控制和安全共享的目的。针对云存储电子病历（EMR, electronic medical record）共享的问题，牛淑芬等[18]提出了一种区块链上基于可搜索加密的 EMR 数据共享方案。该方案采用私有链和联盟链实现 EMR 的安全存储与共享，利用可搜索加密技术实现对联盟链上关键字的安全搜索，利用代理重加密技术实现 EMR 的共享。Neisse 等[19]利用部署在区块链上的公开审计合同提高数据访问、使用的透明度，实现记账能力和溯源追踪。

但是，上述文献对如何利用区块链和智能合约实现访问控制无中心、透明性、可追踪和溯源都没有给出完整的、详细的解决方案。

3 基于属性的访问控制机制及其面临的挑战

本节以基于属性的访问控制为例，介绍复杂网络环境下集中授权的访问控制机制及其面临的挑战。

3.1 基于属性的访问控制

基于属性的访问控制主要包括 3 个阶段，主要步骤如图 1 所示。

第一阶段为客体上传阶段，所有者将生成的客体上传到数据服务器，主要步骤如下。

Step1 数据所有者（DO, data owner），以下简称所有者，将生成的客体（O, object）上传到数据服务器（DS, data service）。

Step2 所有者针对客体生成对应的访问控制策略（P, policy）上传到策略管理点（PAP, policy administration point）。

第二阶段为访问授权阶段，访问控制系统对主体提出的访问请求进行授权判断，主要步骤如下。

Step3 主体（S, subject）生成访问请求（AR, access request）发送给策略执行点（PEP, policy enforcement point）。

Step4 策略执行点针对主体的访问请求生成访问决策请求（ADR, access decision request）发送给策略决策点（PDP, policy decision point）。

Step5 策略决策点针对访问决策请求生成策略查询请求（PQR, policy query request）发送给策略管理点，策略管理点查询访问控制策略库（PR, policy repository）得到对应的访问控制策略并发送给策略决策点。

Step6 策略决策点根据访问控制策略和访问决策请求生成属性查询请求（AQR, attribute query request）发送给策略信息点（PIP, policy information point），策略信息点查询相关主体属性、客体属性和环境属性，并将查询得到的属性发送给策略决策

点。

Step7　策略决策点根据访问控制策略和属性进行访问授权判断，生成访问控制结果（ACR, access control result）发送给策略执行点。

第三阶段为客体访问阶段，对于同意授权的访问请求，主体对客体进行访问操作，主要步骤如下。

Step8　对于同意授权的访问请求，策略执行点提出客体请求（OR, object request）发送给数据服务器。

Step9　数据服务器将客体发送给策略执行点。

Step10　策略执行点将客体发送给主体。

3.2　基于属性的访问控制面临的挑战

从上述访问授权过程可以看出，访问控制执行和决策过程依赖于策略执行点和策略决策点，这样的单一集中授权模式存在以下安全问题和性能问题。

1) 如果策略决策点或者策略执行点被收买或者攻击，对于同意授权访问控制结果，会返回一个否定的授权结果，反之亦然，甚至策略执行点直接拒绝主体的访问请求。

2) 访问控制过程不透明、不可追踪。从所有者角度来看，其不能发现自己创建的客体错误的肯定授权或过度授权，从而导致隐私泄露；同样，主体也无法发现错误的否定授权。

3) 所有访问控制的决策和执行都集中在策略决策点和策略执行点，造成性能瓶颈问题，甚至存在单点失效导致整个系统无法运行等问题。

4) 整个访问过程无法实现追踪和溯源，对于错误的访问控制授权和访问执行，无法找到相关的参与主体。

4　基于区块链的可溯源访问控制机制的设计原则与架构

针对基于属性的访问控制在实际应用中存在的问题，本节提出了基于区块链的可溯源访问控制机制。该机制把访问控制策略以智能合约的形式部署在区块链上，通过执行区块链上分布式智能合约对主体的访问请求进行评估，实现了无中心的访问授权管理。同时，利用区块链透明性和不可修改等优点，把访问授权过程记录在区块链上，实现访问控制过程透明性和可追踪。

4.1　基于区块链的可溯源访问控制机制设计原则

为保证基于区块链的可溯源访问控制机制的安全性，本文提出以下安全性假设条件。

条件 1　数据服务器半可信，它会准确执行每次访问，但存在非法篡改客体，或者把客体泄露给非法主体，或者拒绝合法主体对客体访问的可能。

条件 2　策略决策点或者执行点会被攻击或者被收买成为失效节点，从而生成错误访问决策或授权，或者拒绝主体对客体的访问。

针对基于属性的访问控制存在的问题，基于区块链的可溯源访问控制机制遵循以下原则。

1) 访问控制策略生成。访问控制策略采用细粒度、语义表达丰富的策略描述语言。所有者描述的

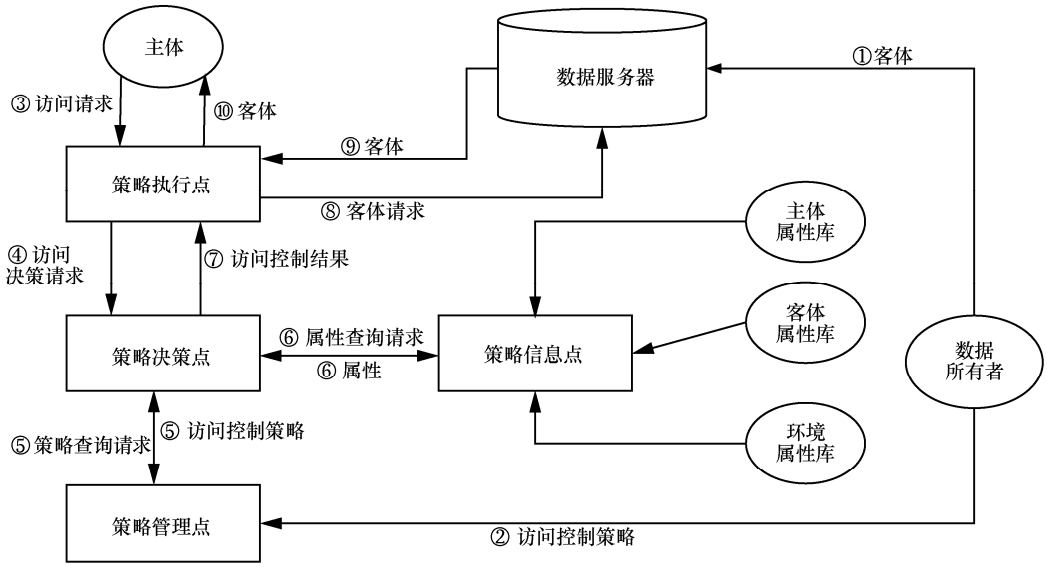

图 1　基于属性的访问控制机制

访问控制策略自动转化为智能合约并部署在区块链上。

2) 访问控制策略决策和执行。访问控制策略的决策和执行通过执行区块链上分布式的智能合约来实现，保证整个访问授权过程的透明性和可溯源。

3) 对于肯定的授权结果通过给主体颁发一个语义描述丰富的访问凭据（token）来表示，并记录在区块链上。主体访问客体时，通过区块链对访问凭据进行验证，防止一次授权无限制重复访问客体等安全问题。

4) 区块链分布式账本的设计。访问授权结果和访问结果都记录在区块链账本上。区块链账本上详细记录谁在什么时候对什么进行了什么操作，操作的原因是什么，操作的环境是什么。保证访问过程的透明性，实现访问过程可追踪和溯源。

5) 客体资源离线存储。数据采用传统的数据库管理系统，如 Oracle、Sybase，或者分布式存储系统，如 GFS（Google file system）等方式存储在链下的数据服务器上，保证客体资源的安全性和隐私性。如果客体直接存储在链上，客体的安全性和隐私性会受到威胁；如果采用密态方式存在链上，客体访问的灵活性和效率会大大降低，同时会大大增加账本维护成本。

6) 主体的安全性和隐私性。在数据访问过程中，主体属性属于个人隐私信息，所有主体相关属性信息存在链下的策略信息库中。

4.2 基于区块链的可溯源访问控制机制架构

基于区块链的可溯源访问控制机制架构如图 2 所示，包括客体上传、访问授权和客体访问 3 个阶段。在基于区块链的可溯源访问控制机制中，引入环境句柄（CH, context handler）执行访问授权和客体访问。根据不同的分工，把环境句柄细分为智能策略部署句柄（CHSPD, smart policy develop context handler）（简称策略部署句柄）、客体部署句柄（CHOD, object develop context handler）、智能策略执行句柄（CHPE, smart policy enforcement context handler）（简称策略执行句柄）、智能策略决策句柄（CHPD, smart policy decision context handler）（简称策略决策句柄）、访问凭据验证句柄（CHTV, token validation context handler）（简称凭据验证句柄）、日志记录句柄（CHL, log handler）。上述句柄为区块链的各个节点，实现智能合约的执行、客体上链前的验证和区块链账本的维护等。

第一阶段为客体上传阶段，主要步骤如下。

Step1 所有者将生成的客体上传到数据服务器，数据服务器将客体在数据服务器的地址和摘要值发送给所有者。

Step2 所有者针对客体生成对应的访问控制策略上传到策略管理点。

Step3 策略管理点将所有者上传的访问控制策略转化成智能合约的形式，生成智能访问控制策略（SP, smart policy）发送给 CHSPD，CHSPD 将 SP 部署在区块链上，部署成功后，CHSPD 将 SP 在区块链中的地址 SPA（smart policy address）发送给策略管理点进行存储。所有者根据客体地址和摘要值等生成客体索引发送给 CHOD，CHOD 将客体索引部署在区块链上。

第二阶段为访问授权阶段，主要步骤如下。

Step4 主体生成访问请求并发送给策略执

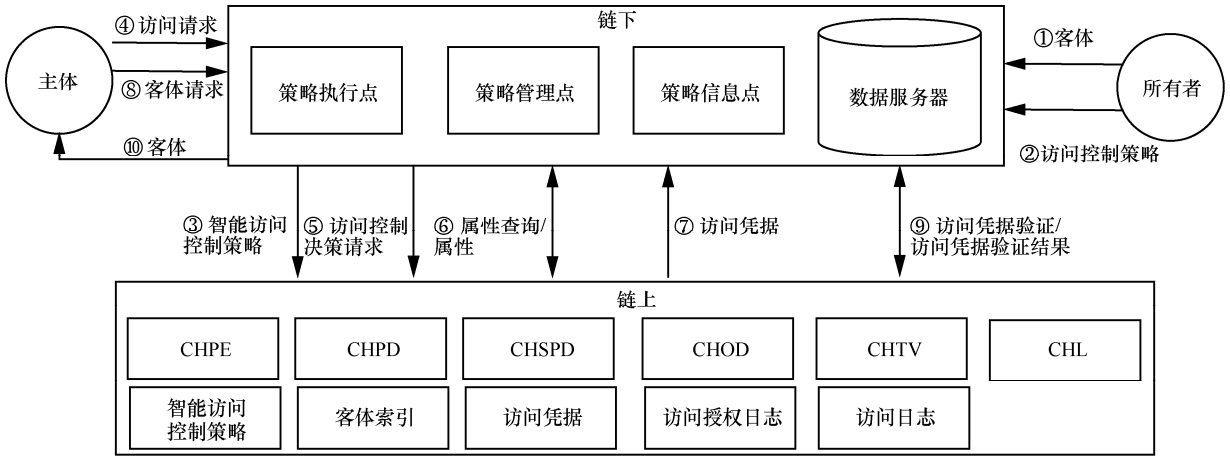

图 2 基于区块链的可溯源访问控制机制架构

行点。

Step5　策略执行点根据主体的访问请求从策略管理点查询智能访问控制策略地址，根据访问请求和策略地址生成访问决策请求，并发送给 CHPE。

Step6　CHPE 将访问决策请求发送给 CHPD。CHPD 根据访问决策请求中的策略地址调用对应的智能合约，智能合约生成属性查询请求发送给 PIP，PIP 将属性发送给智能合约，智能合约根据属性进行访问授权判断，生成访问控制结果。CHPD 将访问控制结果发送给 CHPE。

Step7　CHPE 根据访问控制结果生成访问授权日志和访问凭据，CHPE 和 CHL 分别将访问凭据和访问授权日志记录在区块链上，同时将访问凭据发送给主体。

第三阶段为客体访问阶段，主要步骤如下。

Step8　主体生成客体请求，并将客体请求发送给策略执行点，策略执行点将客体请求发送给数据服务器。

Step9　数据服务器将客体请求中主体的访问凭据发送给 CHTV，CHTV 对访问凭据有效性进行验证，并把验证结果发送给数据服务器，CHL 将访问日志记录在区块链上。

Step10　对于通过验证的访问凭据，数据服务器将客体发送给主体。

基于区块链的可溯源访问控制机制具有以下优势。

1) 利用区块链公开透明、无中心、不可篡改等优点，基于区块链的可溯源访问控制机制把访问控制策略、访问控制执行和策略决策过程记录在区块链中，有效防止了策略执行点和策略决策点被收买或者攻击造成的非法授权或者拒绝访问请求等安全问题，同时避免了集中授权造成的性能瓶颈问题。

2) 区块链中详细记录了访问授权日志、访问日志，访问请求主体可以通过区块链查看访问授权日志记录，确保自己没有被非法拒绝。

3) 所有者也可以通过区块链查看客体访问过程，保证自己的客体资源没有被非法授权或者过度授权。

4) 超级用户可以通过查看区块链访问授权和访问过程，实现整个过程的可追踪和溯源。

5) 策略决策点和策略执行点可以通过区块链证明自己诚实地执行访问控制策略。

5　基于区块链的可溯源访问控制机制原理

本节详细介绍基于区块链的可溯源访问控制机制如何进行客体上传、访问授权和客体访问。为提高访问控制和数据追踪溯源的效率，本文将区块链分成客体链 objectBlockChain 和日志区块链 logBlockChain。objectBlockChain 用于记录智能访问控制策略、客体索引、访问凭据，logBlockChain 用于记录访问授权日志和访问日志。客体上链时，多个节点通过实用拜占庭容错（PBFT, practical Byzantine fault tolerance）算法进行共识，各个节点调用函数 putData(data)将 data 上传到区块链上，同时调用函数 getData(data)得到区块链上的数据，data 可以为任意类型和结构的数据。

5.1　客体上传与策略部署

5.1.1　客体上传

所有者调用算法 1 进行客体上传。

算法 1　objectUpload(object, policy)

输入　待上传的客体 object 和对应的访问控制策略 policy

输出　客体部署结果 flag，flag=true 表示客体部署成功，flag=false 表示客体部署失败

```
flag=false;
objectReposit(object, DS, object_index);
policyTranslate(policy, policyID, smartpolicy);
flag = policyDevelop (smartpolicy, smartpolicy_Address);
if(flag)
{
policyReposit (policyID, smartpolicy_Address, policy);
flag=objectDevelop (object_index);
}
return flag;
```

客体上传协议如图 3 所示。在客体上传时，所有者调用函数 objectReposit( )将客体上传给数据服务器进行存储，得到客体地址 object_address，计算客体的摘要值 object_hash。所有者根据 object_address、object_hash、object_attribute 等信息生成客体索引 object_index。采用链下方式存储的客体具有以下优点：1) 区块链上仅存储客体索引而不是客体本身，提高了客体的安全性和隐私性；2) 在

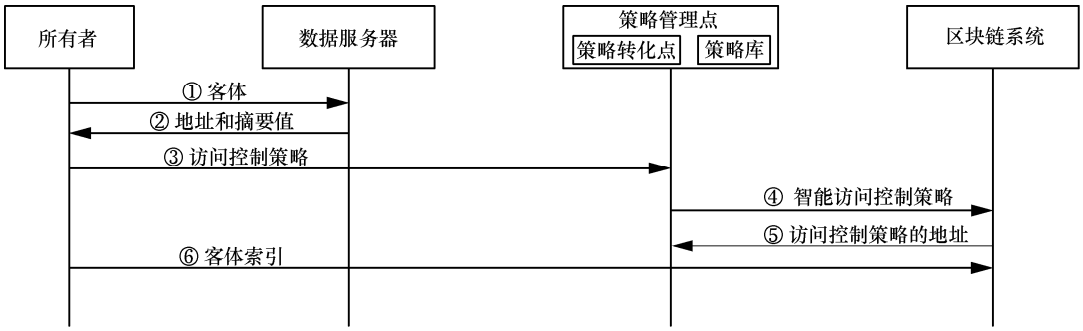

图3　客体上传协议

对客体访问时，通过对比摘要值对客体完整性进行验证，有效避免客体在存储和传输过程中被篡改的风险；3)通过客体地址可以快速找到待访问的客体，提高客体访问效率，如果客体为敏感的信息，所有者可以将客体以密态的形式存储在数据服务器中。

5.1.2　访问控制策略部署

为了提高访问控制策略转化效率，降低所有者的负担，本文将策略管理点分成策略转化点和策略库，其中策略转化点负责访问控制策略转化。策略转化点调用函数 policyTranslate( )为 policy 生成策略标识符 policyID，并将 policy 转化成智能合约的形式，得到智能策略 smartpolicy。策略转化成功后，CHSPD 调用函数 policyDevelop( )将 smartpolicy 部署在客体区块链上，并返回 smartpolicy 在客体区块链的地址 smartpolicy_Address。策略部署成功后，策略管理点调用函数 policyReposit( )将 policyID、smartpolicy_Address、policy 存储在策略库中，便于后续访问控制策略查询。

除了所有者针对客体制定的访问控制策略外，访问控制系统还会针对单个或多个客体制定系统访问控制策略。对于系统访问控制策略，同样按照上述方法进行策略部署和存储。

智能访问控制策略部署成功后，所有者将 object_index 发送给 CHOD，CHOD 将 object_index 部署在客体链上，完成客体及访问控制策略的部署。

CHSPD 和 CHOD 为客体区块链网络的节点，维护区块链账本和智能合约的运行。在客体上链和策略部署过程中，不同节点之间通过 PBFT 算法达成共识。

对于客体上链和访问控制策略的制定与部署，所有者可以委托可信第三方进行。

5.2　访问授权

在基于区块链的可溯源访问控制机制中，对于同意授权的访问请求生成 token，token 详细记录了访问客体时需要满足的时间、地点等属性信息。通过算法 2 对主体的 AR 进行授权评估，访问授权协议如图 4 所示。策略管理点调用函数 policyQuery( ) 根据 AR 在策略库中查找对应的 policy 及 smartpolicy_Address。策略执行点根据访问请求和策略地址生成访问控制请求发送给 CHPD。CHPD 根据 smartpolicy_Address 调用对应的智能合约对访问请求进行评估。在策略评估过程，根据需要从策略信息点查找策略评估需要的主体属性、客体属性和环境属性，生成访问控制结果 accessResult 和访问授权结果 flag。CHPD 将访问授权结果记录在客体区块链上。对于肯定授权，CHPE 调用函数 tokenGenerate( )生成 token，并将其记录在客体区块链上。CHPE 根据访问控制结果调用函数 authorizeLogGenerate() 生成访问授权日记 authorizeLog，并将其发送给 CHL，CHL 将访问授权日志记录在日志区块链上。日志区块链上详细记录了肯定授权日志和否定授权日志。

算法 2　accessAuthorize(AR)

输入　主体对客体访问请求 AR

输出　授权结果 flag 和访问凭据 token，flag=true 表示同意授权，flag=false 表示不同意授权

```
flag=false;
token=Null;
policyQuery(AR, smartpolicy_Address);
flag = policyDecision (smartpolicy_Address, accessResult);
authorizeLogGenerate (accessResult, authorizeLog);
putData(authorizeLog);
if(flag)
{
```

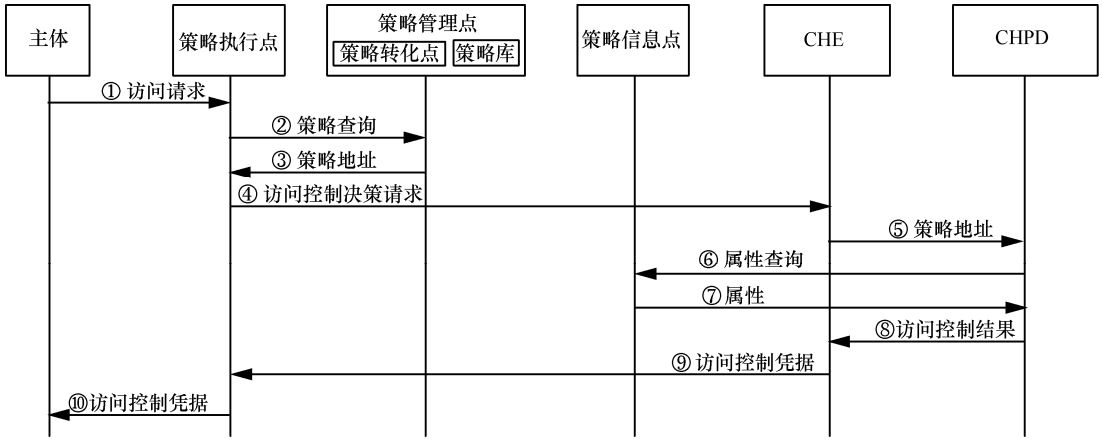

图 4　访问授权协议

tokenGenerate(accessResult,token);
putData(token);
}
return flag,token;

所有的访问控制结果不管是肯定授权还是否定授权都记录在日志区块链上，主体通过日志区块链可以查看访问请求是否被拒绝，同时可以对授权结果进行验证，防止策略执行点和策略决策点联合起来进行欺骗行为。通过访问授权日志对客体的访问请求进行追踪和溯源，防止恶意主体进行非法访问或者重放攻击等。在访问授权结束后，将 token 记录在客体区块链中，便于后续主体对客体访问时，对主体访问凭据的有效性进行验证，有效避免了一次授权，主体对客体无限次访问，同时可以杜绝主体将访问凭据泄露给其他非法主体等安全问题。

5.3　客体访问

在访问授权阶段，对于同意授权的 AR，CHPE 会给主体返回一个 token。主体在提出客体请求时，将 token 一起发送给策略执行点。客体访问协议如图 5 所示，通过算法 3 实现主体对客体的访问。策略执行点将主体的访问凭据发送给数据服务器 DS，CHTV 调用函数 tokenValidate( )对 token 的有效性进行验证，调用函数 accessLogGenerate( )生成访问日志 accessLog，并将访问日志 accessLog 发送给 CHL，CHL 将访问日志记录在日志区块链上。

算法 3　objectAccess(OR, flag, object)

输入　主体对客体请求 OR

输出　访问结果 flag，flag=true 表示访问凭据验证通过，并将客体 object 发送给主体 subject；flag=false 表示表示访问凭据验证没有通过

flag=false;
flag=tokenValidate(token);
accessLogGenerate(accessLog);
putData(accessLog);
if(flag)
{
send(object);
}
return flag;

在客体访问过程中，所有 token 及其验证结果都记录在区块链上，主体通过区块链可以查看访问凭据的验证结果，有效防止了数据服务器非法拒绝服务。同时日志记录句柄将访问日志 accesslog 记录

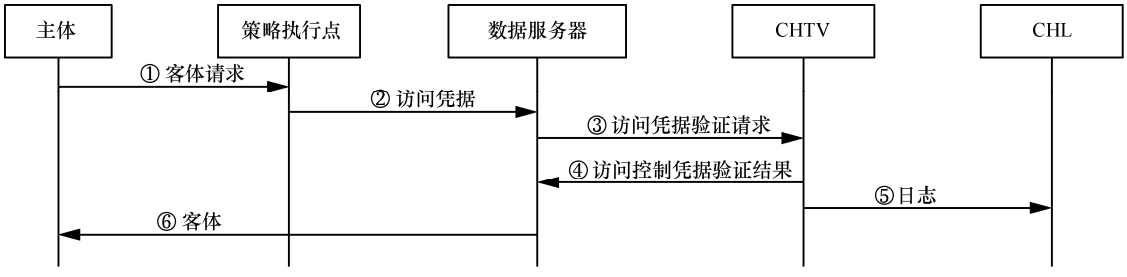

图 5　客体访问协议

在日志区块链上，后续可以通过日志区块链实现客体访问追踪和溯源。

5.4 访问凭据数据结构

token 是主体访问客体的唯一凭据，详细记录了主体访问客体时需要满足的各种条件。关键字−值（key-value）的方式是区块链中广泛采用的数据结构，本文采用关键字−值的方式设计访问凭据的数据结构。访问凭据关键字包括主体、所有者、客体地址。访问凭据记录了访问凭据 ID 值、访问凭据摘要值、随机数、策略地址、策略 ID 号、客体摘要值、客体允许操作的时间{time}、允许对客体进行的操作{op}、主体操作客体需要满足的环境属性{*e*}、客体属性、主体属性。{time}为允许操作的时间集合、{op}为主体可对客体进行的操作集合、{*e*}为主体对客体进行操作时需要满足的环境属性集合，包括对客体操作的位置属性、操作平台属性等。

token
{
key:
{
“Subject”:subject_account;
“Owner”:owner_account;
“Object Address”:object_Address;
}
value
{
“TokenID”:tokenID;
“Token”:randNumber;
“Token Hash”: token_Hash;
“Policy Address”: smartpolicy_Address;
“Policy ID”: policyID;
“Object Hash”: object_Hash;
“Object approved Access Time”: {time};
“Operator approved”:{op};
“Object approved Access Environment Attribute”: {e};
“Object Attribute”: Oattribute;
“Subject Attribute”: Sattribute;
}
}

访问凭据详细记录了主体对客体进行操作所必须满足的各种条件。通过访问凭据可以实现对客体细粒度的访问控制。

5.5 实用拜占庭共识机制

共识算法是区块链中的关键技术，实用拜占庭容错算法已经被广泛应用于各种场景。本文智能访问控制策略部署、客体部署、访问授权、访问授权日志记录、访问日志记录都通过 PBFT 共识算法将相关数据记录到客体区块链和日志区块链中。下面讲解如何利用 PBFT 算法将智能访问控制策略部署到客体区块链中。

本文通过策略部署句柄 CHSPD 将智能访问控制策略部署到客体区块链中。CHSPD 至少有 $3f+1$ 个，其中 f 为可能失效副本的最大个数，$f \geqslant 1$。本文根据 CHSPD 的信任度将 CHSPD 分为主节点 CHSPD_primary 和副节点 CHSPD_replica，主节点负责产生新的区块，共识过程如图 6 所示，包括以下几个主要步骤。

广播（broadcast）。PAP 生成智能访问控制策略部署请求，将 smartpolicy 发送给 CHSPD，CHSPD 验证请求的有效性，将策略部署消息发送给全网策略部署句柄。

预准备（pre-prepare）。主节点 CHSPD_primary 收到策略部署消息后，生成预准备消息 pre-prepare

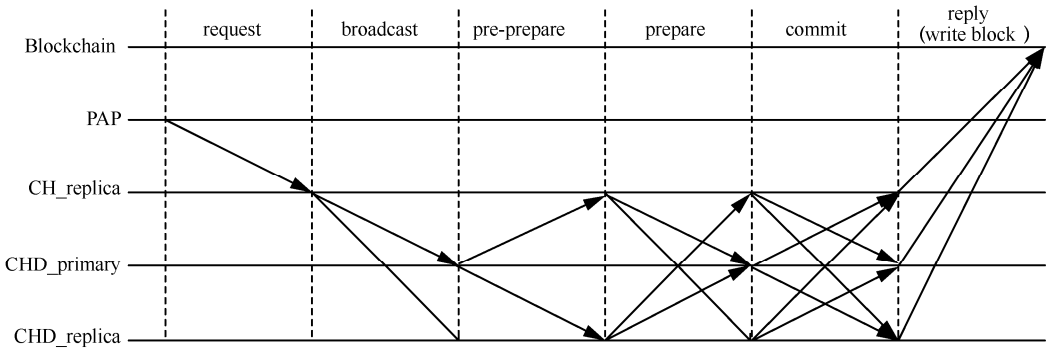

图 6 共识过程

message，并在全网公布预准备消息。

准备（prepare）。副节点 CHSPD_replica 收到预准备消息后，验证预准备消息的有效性，生成准备消息 prepare message，并将准备消息广播给全网其他节点。

确认（commit）。副节点 CHSPD_replica 收到其他节点发送的准备消息，验证其他节点发送的准备消息与主节点发送的预准备消息是否一致。当该副节点收到 $2f$ 个准备消息并验证通过时，生成确认消息，并在全网公布确认消息。

响应（reply）。一旦副节点 CHSPD_replica 收到 $2f+1$ 个确认消息（包括其自己），则认为策略部署达成了共识，并把执行结果发送给主节点和策略管理点。主节点不断收集策略部署，进行排序生成新的区块，并将新的区块添加到客体区块链上。达成共识后，记录在区块链上的智能访问控制策略就是永久的。

在智能策略部署过程中，主节点 CHSPD_primary 负责智能策略的收集并打包成块，达成共识后将新的区块增加到区块链上。主节点的选取根据各个节点的信任度进行选择，节点的信任度根据节点在共识过程的参与度进行动态评价，如果主节点存在区块记录失误，将取消该节点的主节点权限并降低该节点的信任度。

对于客体部署、访问授权、访问授权日志记录、访问凭据验证和访问日志记录等共识过程，采用类似的方法。策略部署节点、客体部署节点、策略执行节点、策略决策点等可以为同一个节点，也可以为不同的节点，可以根据访问控制系统的规模、节点的能力以及隐私程度进行选择。

接下来，从安全性和性能 2 个方面对本文提出的访问控制机制进行分析。

6　安全性和性能分析

6.1　安全性分析

本文提出的基于区块链的可溯源访问控制机制将访问控制策略、访问授权、客体访问过程都记录在区块链上，继承了区块链无中心、透明性、分布式和不可篡改等优点。

1) 无中心、透明性

本文提出的访问控制机制通过执行部署在客体区块链上分布式的智能合约进行访问评估，实现访问授权过程的无中心化和透明性。

2) 不可伪造性

利用区块链不可篡改的特点，将所有访问授权日志（包括肯定授权和否定授权）和访问日志（肯定访问和否定访问）都记录在日志区块链上，任何人或组织都不可以伪造错误的访问控制授权结果，有效杜绝了策略执行点和策略决策点被攻击或收买造成的安全问题；访问凭据和访问日志记录在区块链上，有效杜绝了数据服务器的非法拒绝访问等安全问题。

3) 可追踪溯源

所有的访问授权日志和客体访问日志都详细记录在日志区块链上，所有者（或者超级用户）可以通过区块链查看整个客体授权和访问过程，验证策略执行点、策略决策点、数据服务器是否按照访问控制策略对客体进行受控访问；所有者（或者超级用户）通过日志可以对客体访问和流转过程进行追踪和溯源，防止对客体进行错误的肯定授权或过度授权；主体可以通过区块链查看整个授权结果、授权日志和访问日志，防止策略执行点和策略决策点拒绝访问或者错误授权，防止数据服务器非法拒绝访问；数据服务器可以通过区块链证明自己按照访问控制策略对客体进行受控访问。

4) 隐私性和可信性

在客体访问过程中，将客体存储在第三方服务器，客体地址、摘要值等生成的客体索引存储在客体区块链上，保护了客体隐私性。同时客体索引中包含了客体摘要值，防止半可信数据服务器对客体篡改，保护客体的可信性和完整性。

6.2　性能评估

为测试本文提出的访问控制机制性能，本节搭建了联盟链实验环境。本次实验的硬件环境如下：处理器为 AMD 3600×1，内存为 3 GB，操作系统为 centos。在进行性能评估时，只测试链上的操作速度，比如客体索引上链、访问控制策略部署、智能访问控制策略评估、日志查看等，对于链下运行速度，比如客体索引生成、访问控制策略转化不予考虑。

在基于区块链的可溯源访问控制机制中，客体索引上链、访问控制策略部署等都属于写区块链，访问控制策略评估为执行区块链上的智能合约并将日志写入区块链，日志查看为读区块链的数据。下面通过测试读区块链、写区块链速度来对基于区块链的可溯源访问控制机制进行性能评估。

区块链的读写速度不仅与硬件环境有关，同时

与区块链网络中的节点个数也有很大关系。本文配置一个排序节点，peer 节点个数分别为 5 和 10，测试不同条件下读写区块链的速度。测试时，通过模拟以不同速度不断给区块链发送交易，这些交易包括读区块链和写区块链，测试不同环境下读写区块的速度和完成交易所花费的时间。

1) 读写区块链速度

配置 peer 节点个数为 5，读写区块链速度和时间分别如表 1 和表 2 所示。

表 1 5 个 peer 节点读写区块链速度

每秒发送交易次数	读区块链速度/(次·秒$^{-1}$)	写区块链速度/(次·秒$^{-1}$)
5	3.15	2.51
20	2.71	0.34
50	2.74	0.29
70	2.71	0.34

表 2 5 个 peer 节点读写区块链时间

每秒发送交易次数	读区块链的时间/ms	写区块链的时间/ms
1	314	399
20	7379	57 727
50	18 271	169 463
70	25 805	204 852

从表 1 和表 2 中可以看出，读区块速度大于写区块速度，读区块的时间小于写区块的时间。这是因为写操作涉及创建新的区块、公布账本等，包含的流程比读操作多。

2) 读写区块链速度与 peer 节点关系

将区块链 peer 节点个数配置为 10，分别测试读写区块链速度和时间，如表 3 所示。通过对比表 1 和表 3、表 2 和表 4 的数据发现，随着 peer 节点个数的增加，读和写的速度在降低。因为随着节点的增加，共识机制占用的时间增加，导致读写区块链速度下降。

表 3 10 个 peer 节点读写区块链的速度

每秒发送交易次数	读区块链速度/(次·秒$^{-1}$)	写区块链速度/(次·秒$^{-1}$)
5	2.90	2.39
20	2.63	0.30
50	2.56	0.28
70	2.58	0.26

从上述实验分析可以看出，基于区块链的可溯源访问控制机制效率与联盟链中节点个数有很大关系。节点个数影响访问控制系统的规模，应在保证访问控制规模和效率的前提下，选择合适的节点个数。此外，交易的长度和结构也影响读写区块链的效率，为提高访问控制系统效率，应尽可能优化各个交易的数据结构，降低交易时延。

表 4 10 个 peer 节点读写区块链时间

每秒发送交易次数	读区块链的时间/ms	写区块链的时间/ms
1	345	418
20	7 603	67 263
50	19 537	178 235
70	27 098	265 645

7 结束语

针对传统访问控制机制存在集中授权、访问过程不透明、不可追踪和溯源等缺点，充分利用区块链无中心、透明性、不可篡改等优点，提出了基于区块链的可溯源访问控制机制。所提机制将访问控制策略以智能合约的形式部署在区块链上，访问控制决策判断通过执行部署在区块链上的智能合约实现，保证整个访问授权过程的透明性；为保护客体资源的隐私性，提出采用链下和链上相结合的方式，客体资源存储在链下半可信的数据服务器，通过客体存储地址和摘要值等信息生成客体索引存储在客体区块链上，授权主体通过客体地址访问客体资源；对于授权主体颁发访问凭据，将访问凭据部署在区块链上，访问凭据详细记录访问权限以及需要满足的条件，主体访问客体时，通过区块链验证访问凭据的真实性和可信性，有效杜绝了一次授权多次访问的问题，同时实现了细粒度的访问控制；将访问授权日志和访问日志记录在日志区块链上，通过日志区块链实现访问授权和访问过程的可追踪和可溯源。通过对基于区块链的可溯源访问控制机制进行安全性分析发现，所提机制在保证客体资源隐私性的前提下，实现了访问过程透明性、无中心、可追踪和可溯源。

下一步将结合具体应用场景分析论证方案的可行性和适用性，并对方案性能进行分析，研究数据访问溯源机制。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. (2008)[2020-06-22].

[2] NOVO O. Blockchain meets IoT: an architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018, 5(2): 1184-1195.

[3] SUKHODOLSKIY I, ZAPECHNIKOV S. A blockchain-based access control system for cloud storage[C]//Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. Piscataway: IEEE Press, 2018: 1575-1578.

[4] ZHU Y, QIN Y, GAN G H, et al. TBAC: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization[C]//Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference. Piscataway: IEEE Press, 2018: 535-544.

[5] ES-SAMAALI H, OUTCHAKOUCHT A, LEROY J P. A blockchain-based access control for big data[J]. Journal of Computer Networks and Communications, 2017, 5(7): 137-147.

[6] MAESA D D F, MORI P, RICCI L. Blockchain based access control[C]//Proceedings of the IFIP International Conference on Distributed Applications and Interoperable Systems. Geneva: IFIP Newsletter, 2017: 206-220.

[7] MAESA D D F, MORI P, RICC L. A blockchain based approach for the definition of auditable access control system[J]. Computers & Security, 2019, 84 (7): 93-119.

[8] MAESA D D F, MORI P, RICCI L. Blockchain based access control services[C]//Proceedings of the IEEE International Symposium on Recent Advances on Blockchain and Its Applications (BlockchainApp). Piscataway: IEEE Press, 2018: 1379-1386.

[9] 刘敖迪, 杜学绘, 王娜, 等.基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[10] 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 R Z, LIU Y, TIAN J F. An access control method using smart contract for internet of things[J]. Journal of Computer Research and Development, 2019,56(10): 2287-2298.

[11] TRUONG N B, SUN K, LEE G M, et al. GDPR-compliant personal data management: a blockchain-based solution[J]. IEEE Transaction on Information Forensics and Security, 2019,15(10): 1746-1761 .

[12] WU Z, WILLIAMS A B, PEROULI D. Dependable public ledger for policy compliance, a blockchain based approach[C]//Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2019: 1891-1900.

[13] ZYSKIND G, NATHAN O. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of the Security and Privacy Workshops (SPW). Piscataway: IEEE Press, 2015: 180-184.

[14] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//Proceedings of IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 839-858.

[15] MAKHDOOM I, ZHOU I, ABOLHASAN M, et al. PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities[J]. Computers & Security, 2020, 88(1): 1-34.

[16] RAHMAN M S, OMAR A A, BHUIYAN M Z A, et al. Accountable cross-border data sharing using blockchain under relaxed trust assumption[J]. IEEE Transaction on engineering management, 2020, 67(4): 1476-1486.

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

[18] 牛淑芬, 刘文科, 陈俐霞, 等. 基于联盟链的可搜索加密电子病历数据共享方案[J]. 通信学报, 2020,41(8): 204-214.
NIU S F, LIU W K, CHEN L X, et al. Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain[J]. Journal on Communications, 2020, 41(8): 204-214.

[19] NEISSE R, STERI G, NAI-FOVINO I. A blockchain-based approach for data accountability and provenance tracking[C]//Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES'17). New York: ACM Press, 2017: 1-10.

[作者简介]

谢绒娜（1976− ），女，山西永济人，博士，北京电子科技学院副教授，主要研究方向为网络与系统安全、访问控制、密码工程。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码信息安全、信息论与编码理论。

史国振（1974− ），男，河南济源人，博士，北京电子科技学院教授级高级工程师、硕士生导师，主要研究方向为网络与系统安全、嵌入式安全。

郭云川（1977− ），男，四川营山人，博士，中国科学院研究员、博士生导师，主要研究方向为访问控制、形式化方法。

张铭（1997− ），男，浙江宁波人，西安电子科技大学硕士生，主要研究方向为区块链、数据共享和流转控制。

董秀则（1976− ），男，山东莒县人，北京电子科技学院副教授，主要研究方向为密码信息安全、密码工程。