DOI：10.13666/j.cnki.jnlc.2019.0209

LibRSM：基于联盟链的数字图书馆信息资源安全共享模型*

沈凯旋　高　胜　朱建明

摘　要　当前，各机构的数字图书馆大都由各机构独立管理运行，由于建设标准、管理制度等的不一致难以实现馆间信息资源的有效共享，从而导致“信息孤岛”现象。基于联盟区块链技术的面向数字图书馆的信息资源安全共享模型 LibRSM，由用户模块、服务模块及数字图书馆联盟链模块组成，充分利用联盟链的分布式共识算法、统一的数据结构、非对称加密等技术特性保障模型的有效性和安全性，与现有的数字图书馆信息共享方案相比安全性更高、性能更好。在确保信息资源产权安全的情况下，LibRSM 能够增强馆间信息资源的协同处理和可信共享。图 4。表 1。参考文献 35。

关键词　数字图书馆　区块链　联盟链　可信共享　数据共享　信息孤岛

LibRSM: Digital Library Information Resources Security Sharing Model Based on Consortium Blockchain

Shen Kaixuan　Gao Sheng　Zhu Jianming

Abstract: At present, the digital libraries of various institutions are mostly managed and operated independently by various agencies. Due to the inconsistency between construction standards and management systems, it is difficult to realize the effective sharing of information resources between the libraries, resulting in the phenomenon of “information isolated islands”. LibRSM, an information resource security sharing model for digital libraries based on the consortium blockchain technology, consists of user modules, service modules and digital library consortium blockchain modules, using the distributed consensus algorithm, unified data structure, asymmetric encryption technology and other technical features of the consortium blockchain to ensure its effectiveness and security, and it has the characteristics of higher security and better performance compared with the existing digital library information sharing scheme. The LibRSM can enhance the collaborative processing and trusted sharing of information resources between libraries under the condition of ensuring the property rights of information resources. 4 figs. 1 tab. 35 refs.

Keywords: Digital Library; Blockchain; Consortium Blockchain; Trusted Sharing; Data Sharing; Information Isolated Islands

1　引言

当前，数字图书馆已成为数字基础设施的重要组成部分，推进其信息资源整合和开放共享，并保障数据安全已成为我国大数据战略中一项重要内容[1]。一般地，数字图书馆是指利用互联网和网络通信等技术为跨时空区域的用户提供数字资源存储、交换、流通等服务的知识网络系统[2]。当前，我国已建立多种类型的数字图书馆系统，国家层面的如国家数字图书馆、中国高等教育数字图书馆（如 CALIS、CADLIS、CADAL 等）等，企业层面的如中国知识基础设施工程（CNKI）、万方数据资源系统、超星数字图书馆等。但考虑到数字图书馆信息资源产权、管理制度等问题，目前大多数数字图书馆都由各机构独立建

* 本文系北京市社会科学基金项目“面向云计算环境北京数字图书馆信息资源安全共享保障体系研究”（项目编号：16XCC023）研究成果之一。

设管理,机构间缺乏协作,且制定的元数据、数据格式等标准仅适合自身,形成了数字图书馆间的“信息孤岛”现象。这种现象一方面会导致信息资源的重复建设,如 CNKI、万方数据资源系统等数字图书馆中存在大量的重复信息资源,浪费了不必要的人力资源,增加了建设成本;另一方面,数字图书馆的建设和服务机制(如数据存储格式、检索格式等)缺乏统一标准,使得数字图书馆之间难以实现互联互通[1,3]。因此,打破数字图书馆间的“信息孤岛”,实现数字图书馆信息资源的自由流通和安全共享成为当前我国数字图书馆发展中亟待解决的问题。

目前,我国数字图书馆信息资源的共享模型主要分为系统中心式和区域中心式两种[4-5]。两者的差别主要在于数字图书馆信息资源共享模型的建设主体及建设范围不同。系统中心式的信息资源共享模型由国家层面主导,互联全国的图书情报中心,典型的如 CALIS、NSTL、CSDL、EUDAT 等;而区域中心式的信息资源共享模型由地方政府主导,互联某地区的图书情报中心,典型的如上海市中心图书馆、东莞数字图书馆等。然而,这两种信息资源共享模型都是典型的集中式模型,中心节点容易成为攻击目标,并产生单点失效、性能瓶颈等问题;此外,各馆之间的信息不对称性使得信息资源产权得不到有效保护。

为解决数字图书馆信息资源共享模型的现有问题,本文将联盟区块链技术引入数字图书馆领域,解决信息资源自由流通和安全共享问题。联盟链是一种部分去中心化的区块链,其共识过程由一些预选节点控制,其他节点可参与交易,但不参与记账过程。本文基于联盟链构建数字图书馆信息资源安全共享模型 LibRSM,利用联盟成员节点共同维护数字图书馆信息资源的有效性和安全性,解决数字图书馆间的“信息孤岛”问题,同时利用区块链不易篡改、可追溯等特性保护信息资源产权,增强馆间信息资源共享的可信性。

2 相关研究概述

2.1 数字图书馆信息资源共享研究

数字图书馆信息资源共享的关键是解决异构资源的互操作性问题[6]。在国内,朱伟珠[7]在分析 OGSA-DAI 的基础上,利用网格技术设计数字图书馆动态联盟异构信息资源共享系统。赵捧未等[8]基于 P2P 和 Web Service 技术提出一种数字图书馆资源共享框架,解决数字图书馆异构资源的定位及互操作性问题。贾凤旭[9]利用 XML 技术在数据交互方面的优势构建数字图书馆资源共享平台。麦旭辉[10]指出利用跨系统图书馆联盟实现数字资源共建共享,重点在于数字资源的标准化整合。张鼐[11]、魏达贤和谢强[12]、陈宫和牛秦洲[13]均利用云计算技术整合数据资源,构建数字图书馆信息资源共享系统。在国外,Chauhan 等[14]介绍了印度数字图书馆联盟 UGC-Infonet,认为数字图书馆联盟的建设是实现信息资源共享的有效途径;Tripathi 等[15]提出在构建数字图书馆联盟时应注意版权、业务协作、数字资源互操作等内容。此外,国外的如世界数字图书馆(WDL)、美国公共数字图书馆(DPLA)、美国国家科学数字图书馆(NSDL)、欧洲数字图书馆等均通过构建数字图书馆联盟整合不同类型的数字资源,实现统一资源的共享。总体而言,这些数字图书馆信息资源共享方案通过中间层整合异构资源实现统一资源共享,本质上是一种集中式服务提供方式,容易产生单点失效、性能瓶颈等问题。

2.2 区块链信息共享研究

区块链是由参与节点共同维护一种分布式共享总账,综合了分布式账本、密码学、共识算法、智能合约等多项技术,具有分布式结构、透明可信、时序不可篡改等特点[16-17]。区块链作为多种技术的集成运用,在数据共享领域引起了学者们的高度关注。薛腾飞等[18]提出一个基于区块链的医疗数据共享模型,有效解决了不同医疗机构间数据共享难的问题。王继业等[19]提出的基于区块链的数据安全共享网络体系,解决了集中式数据部署访问受限、易窃取、易篡改等问题。董祥千等[20]提出一种基于区块链的数据共享模型,实现了数据共享的透明性、安全性以及高效性。黄

敏聪[21]从资源和服务两个维度探讨了区块链技术应用于图书馆领域的优势,指出其能够有效促进图书馆元数据系统建立、数据确权以及资源共享。余其凤等[22]提出一种基于区块链的数字资产管理方案,能够有效解决数字资产管理中的版权问题。Zhu 等[23]提出一种云环境下区块链数据管理模型(CBDM),确保数据共享的安全性。Wang 等[24]利用以太坊区块链和基于属性的加密(ABE)技术提出一种分布式资源存储共享框架,实现了对共享数据的访问控制。Xia 等[25]基于区块链提出一种医疗数据共享框架 BBDS,解决云数据存储的访问控制问题;随后,其进一步提出一种分布式、可撤销访问的 MeDShare 模型,解决不可信医疗机构间的医疗数据共享问题[26]。然而,数字图书馆信息资源共享既要保障安全性,更要保障共享的效率,这些模型并不适用于数字图书馆领域。

2.3 联盟链相关研究

区块链按照部署形式可分为公有链、联盟链和私有链[16]。其中,公有链是一种完全去中心化的区块链,所有节点都可匿名地随时进出区块链网络,在一定程度上这对于数字图书馆而言是不利于监管和追责的。而私有链适合机构或组织内部使用,适用于内部数据的访问和权限管理。联盟链则既具有公有链“去中心化”的特点,又保留了私有链的“隐私性”,是一种部分去中心化的区块链[16,17,27]。联盟链在组织机构间数据交互方面具有很大优势,相比以比特币为代表的公有链,联盟链节点数量较少,使得系统运行效率提高,并且只有被授权的节点才能加入联盟链网络,有助于监管和追责。相比私有链,联盟链具备较高的扩展性。在联盟链的具体应用方面,张超等[28]设计了一个基于 PBFT 算法的联盟式医疗区块链系统 Medical Chain ,解决了医疗数据易被篡改、泄露等问题。Brousmiche 等[29]提出了一个基于联盟链的车辆历史数据管理框架用于车辆生命周期管理,能够提高数据的透明性和协作能力。Xie 等[30]通过引入联盟区块链技术,解决了 B2B 交易平台的信用问题。Zhou 等[31]提出一种基于联盟链技术的模型 CSSP,提高了网络软件服务的可靠性。本文基于联盟链构建的数字图书馆信息资源安全共享模型 LibRSM 具有多中心化的特征,在易于控制用户权限的同时,又能实现馆间信息资源的安全高效流通。

3 LibRSM 概述

3.1 LibRSM 功能需求

目前,数字图书馆间信息资源共享的方式主要包括跨库检索、馆际互借、合作存储、联机编目以及业务合作等。然而,不同数字图书馆的异构性和馆间信任机制的缺失,使得数字图书馆信息资源产权得不到保障,成员馆之间的业务协作意愿较低。LibRSM 利用联盟链的分布式共识算法、统一的数据结构、非对称加密技术等一系列技术特性,打破了数据所有端和数据需求端之间的壁垒,同时建立起一种基于联盟链的信任机制,如图 1 所示(B 为数据区块)。这不仅促使用户积极参与馆间数据资源共享,也实现了信息资源从数据所有端到数据需求端的安全保护、版权保护、以及流通效率提升。

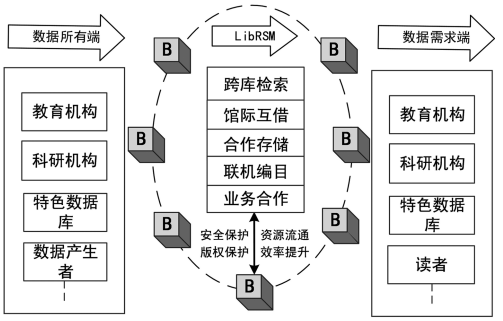

图 1 LibRSM 功能需求

3.2 LibRSM 基本结构

为实现数字图书馆信息资源的自由流通和安全共享,同时考虑到数字图书馆的异构性以及信息资源安全共享需求,本文将 LibRSM 划分为用户模块、服务模块、数字图书馆联盟链模块,如图 2 所示。在信息资源上传/下载、检索等服务模

块,用户既可以作为信息资源提供者,也可以作为信息资源消费者,从而扩大了数字图书馆资源的提供种类及服务范围;在数字图书馆联盟链模块,联盟节点共同维护数字图书馆信息资源,打破数字图书馆间的“信息孤岛”现象,促进数字图书馆间信息资源的自由流通与安全共享。

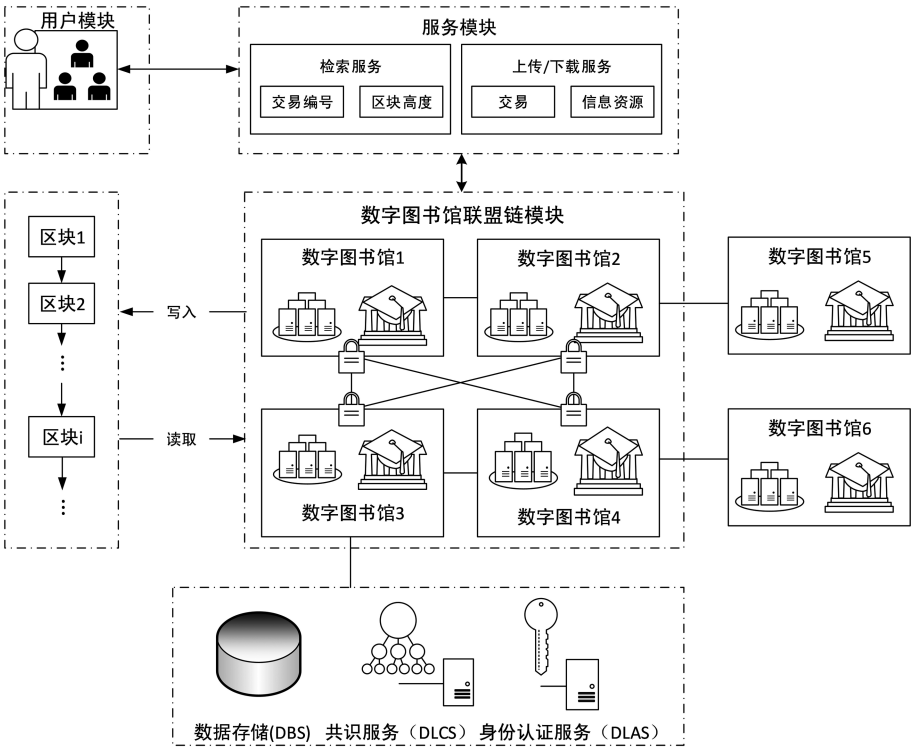

图 2　LibRSM 基本结构

(1)用户模块

用户模块主要包括信息资源的所有者和信息资源的需求者,如教育系统数字图书馆、医疗系统数字图书馆、特色数据库、个人数字图书馆等。

(2)服务模块

服务模块是用户与数字图书馆联盟链的交互中介,主要包括检索服务和上传/下载服务等,并提供不同的服务接口。由于联盟链网络中智能合约不能直接与联盟链网络之外的环境进行交互,该模块一方面可以将用户请求进行结构化处理,生成区块哈希值,使之可以与联盟链网络进行交互;另一方面能够使联盟链网络中的节点从底层数据库中提取所需的信息资源,并对其进行组织和处理后提供给用户。检索服务按照交易编号或区块高度查找信息资源,上传/下载服务以交易形式将信息资源提供给数字图书馆或用户。

(3)数字图书馆联盟链模块

数字图书馆联盟链由数字图书馆联盟成员共同维护和更新,并进行相应的写入和读取操作。每个联盟链网络由提供不同服务的数字图书馆组成(为表述方便,这里把联盟链网络节点抽象为数字图书馆,本质上它是数字图书馆内提供特定服务的服务器),主要包括数字图书馆身份认证服务器(Digital Library Authentication Servers, DLAS)、数字图书馆共识服务器(Digital Library Consensus Servers, DLCS)、数据库服务器(Database Server,DBS)等。这些数字图书馆联盟成员即 DLAS 和 DLCS 是由各数字图书馆根据一

定的机制选出的数字图书馆代表构成。考虑到我国目前尚未形成统一的数字图书馆评价体系，并结合当前数字图书馆信息资源服务能力的状况，LibRSM 将信息资源的内容（包括数据规范性、数量、权威性、重复性）、信息系统建设、以及用户使用情况（包括用户满意度、使用频率等）三个方面作为选择数字图书馆联盟成员的依据。DLAS 为用户提供身份认证服务，包括用户公私钥（PK/SK）生成、密钥存储管理以及用户真实身份到区块链地址映射关系维护等。考虑到 DLAS 分布式特性，可采用目前技术较为成熟的 PKI（公钥基础设施）和超级节点结合的策略[32]来保证身份认证的安全性。DLAS 将包括认证机构（CA）、注册机构（RA）、数字证书库等部分，同时选取信誉值最高的节点做超级节点，发挥中心服务器的作用。通过 PKI 的数字签名、公开密钥和安全认证协议等技术来确保认证的安全性。超级节点不仅使 DLAS 网络易于管理，而且能发挥其分散性和协作性优点。只有认证通过的用户才能加入该联盟链网络。DLCS 是该模型的核心，由认证通过的数字图书馆组成，为用户提供共识服务。其功能是在一定预设规则下，通过多方参与节点间的交互使得数据、行为等达成一致和有效。由于拜占庭容错算法（PBFT）在有限的节点中效率较为客观，且能够在≤[(n-1)/3]的故障节点下保证系统的安全性[33]，因此 DLCS 考虑用 PBFT 算法来保证分布式账本的一致性。其核心思想是节点执行一致性协议，通过点对点通信得知其他节点状态，通过类似投票的过程保证区块链数据的统一；同时，在一致性协议执行出现故障时，故障节点将会被替换（具体的共识算法应用在下文第 4 部分作详细阐述）。考虑到联盟链存储空间有限，DBS 作为模型底层的数据库，负责存储海量数字图书馆真实数据，联盟链中只存储真实数据的索引信息。

4 LibRSM 共享机制

下文以中国高等教育文献保障系统（CALIS）为例来阐述 LibRSM 共享机制。LibRSM 共享机制包括数字图书馆联盟区域代表选择以及不同区域代表间信息资源的共享过程两个方面。截至 2017 年底，全国参加 CALIS 项目的成员馆超过 1300 所[34]，LibRSM 数字图书馆联盟如果囊括所有成员馆，必然会造成数字图书馆联盟链运行效率的降低。因此可以通过选择代表的方式，来减少数字图书馆联盟成员数量，提高模型的运行效率。我们把 CALIS 成员馆依据地域分为不同的集群，每个集群选出区域代表，每个区域代表作为一个数据中心，一方面负责本区域所有数字图书馆信息资源的共享，另一方面负责与其他区域代表进行信息资源共享。

4.1 数字图书馆联盟的构建

考虑到联盟链运行的效率，LibRSM 采用委托权益证明算法（DPoS，Delegated Proof of Stake）[35]构建数字图书馆联盟。委托权益证明类似于“董事会决策”，通过投票来确认某段时间内的记账权限。数字图书馆联盟的构建过程具体如下：联盟链网络中每一个数字图书馆都享有投票权，它们会把票投给自己最信任的 3 个数字图书馆，然后统计联盟链网络中每一个数字图书馆获得的票数，得票最多的前 101 名机构代表组成 DLCS，负责轮流产生新区块。如果某个代表节点错失生成某区块，其他联盟节点将会收回投票，从而将该节点踢出 DLCS。得票数排在 101 名之后的 10 位成员馆组成 DLAS。为保证数据来源的真实性和可靠性，只有经过 DLAS 认证通过的数字图书馆才能加入 LibRSM 网络。DLAS 和 DLCS 一起组成数字图书馆联盟（如图 3 所示）。

4.2 数据共享

联盟链网络中包含两种用户类型，即数据所有者 $User_i$ 和数据需求者 $User_n$。不妨设 LibRSM 中数字图书馆 1（某一区域代表）作为 $User_n$，数字图书馆 2（另一区域代表）作为 $User_i$。数据共享是指数据所有者将元数据写入联盟链，并将真实数据加密存储在 DBS 中。数据需求者从联盟链获取所需元数据，并根据该元数据和密钥得到真

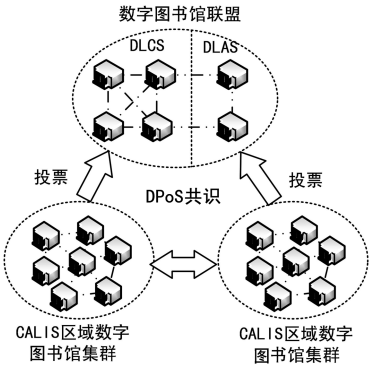

图3　数字图书馆联盟的构建

实数据在DBS中的位置信息和解密密钥,解密并访问所需真实数据。下面以 $User_i$ 和 $User_n$ 为例来说明异构数字图书馆间的数据共享,具体过程如图4所示。

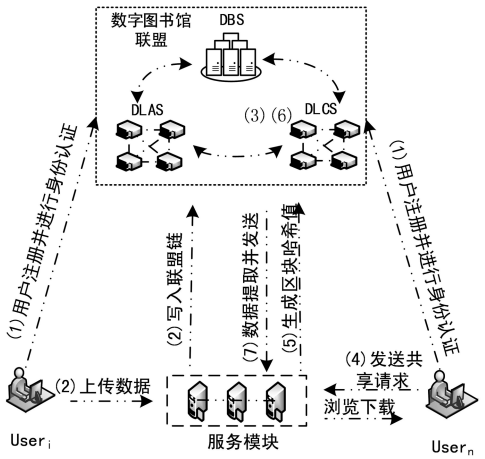

图4　数字图书馆间数据共享过程

(1)LibRSM用户即数据产生者 $User_i$ 和数据需求者 $User_n$ 进行注册和身份认证。该过程主要使用DLAS提供的身份认证服务来完成。

(2) $User_i$ 将元数据写入联盟链,并将真实数据加密存储在DBS中。写入联盟链的数据包括用户权限信息、数据摘要信息以及真实数据在联盟链上存储的位置信息等。

(3)生成主节点。DLCS中共识节点投票产生一个主节点,负责产生新区块,其余节点成为从节点,负责验证和审计主节点产生区块的合法性和正确性。

(4)产生并发送数据共享请求。$User_n$ 产生的数据共享请求Qrq包括所需数据RData的摘要信息RMetadata、PK_{User_i} 及、PK_{User_n},并经 SK_{User_n} 签名。根据数据共享请求的种类,将其转发给相应的服务接口:若用户有检索服务需求,则Qrq被转发给检索服务接口;若用户有上传/下载服务需求,则Qrq被转发给上传/下载服务接口。

(5)生成区块哈希值。LibRSM中服务模块根据 PK_{User_n} 解密Qrq,并根据Qrq中的信息生成区块哈希值并把结果发送给DLCS中的主节点 DL_n。

(6)响应请求。DLCS中主节点 DL_n 依据区块哈希值在联盟链中检索并解密出RData在DBS中存储的位置信息Location,生成响应结果Result。当联盟链上检索出的数据与RMetadata相似度低于一定阈值或者发现 $User_n$ 无此数据权限时,Result结果为空。否则,Result={Location; PK_{DL_n}}。DL_n 然后将Hash(Result)、时间戳信息(Timestamp)等,用 DL_n 的私钥 SK_{DL_n} 加密作为一个交易,之后 DL_n 把该段时间所有交易按时间排序并整合成数据区块Block。该Block中交易的数据结构可以表示为{RMetadata;Metaresult;Hash(Result); PK_{User_n}; PK_{User_i};Timestamp}。之后为保证响应结果的可信性,本文采用PBFT共识算法[27,33]保障结果的可信性,具体过程为: DL_n 向各个从节点广播该Block以待查验,从节点接收到Block后,按序模拟执行交易,验证该Block的合法性和正确性,并把它们的校验结果加上各自的数字签名广播给全网节点。全网中某一节点收集其他节点的校验结果后,与自身的校验结果进行对比,若有2f个(f为可容忍拜占庭节点数)其他节点的校验结果与自己相同,就向全网节点发送一个Commit消息。当一个节点收到2f+1个Commit消息后(包括自己),那么 DL_n 将把该Block链接到联盟链中。同时,经 SK_{User_n} 签名后记录信息经 SK_{DL_i} 加密后存入DBS。否则,该Block将被丢弃。

(7)数据提取和发送。DL_n 根据联盟链中信息从 DBS 中提取 RData。RData 提取成功后,进行有关质量控制。质量控制过程是为了满足信息资源需求者对资源质量的要求,质量控制通过后,RData 则经相应服务接口整合处理发送给 $User_n$,供其浏览或下载,从而实现数据的高效、安全、自由流通。

5 LibRSM 的特点

5.1 安全性

LibRSM 的安全性主要体现在数据的完整性、数据不可篡改、数据可追溯以及版权保护。首先,该模型是基于联盟区块链技术构建起来的,由于其采用分布式的存储技术,实现了数字图书馆数据的多重备份,从而极大地保证了数据的完整性。其次,该联盟链上的信息对联盟成员都是公开透明的,其产生交易、验证交易、记录交易信息等过程均是由建立在非对称加密算法之上的分布式共识机制完成,使得数据一旦被写入链中便不可篡改。而存储在 DBS 中的海量数字图书馆真实数据的访问或使用权限完全由联盟链控制,没有联盟链的授权信息将无法从 DBS 中提取出真实数据,从而保证了未上链数据的安全。另外,对于数字图书馆管理者而言,其可追溯性是指通过遍历联盟链中的所有区块,就能够获得所有的交易数据,并通过时间戳保证了数据的可追溯和可审计。最后,LibRSM 很好地解决了数字图书馆中的信息资源版权问题。第一,数字图书馆作为信息资源的提供方,其身份信息必须公开透明,以保证其真实性和可信度。联盟链上的所有信息都是公开透明的,且不可篡改,很好地保证了这一点。第二,LibRSM 中用户写入、读取数据等方面的权限管理完全由自己控制。联盟链中只包含加密后的数据在 DBS 中的位置信息、哈希值、访问权限等。没有用户的解密密钥无法解密出真实数据,只有被授权用户才可以获得解密密钥,查询真实数据,从而有效地保护数据版权。

5.2 互操作性

数字图书馆互操作性是指其利用自身机制屏蔽分布的、异构的数字图书馆之间的差别,充分消除“信息孤岛”,为用户提供一致的检索和服务功能。在 DLCS 和 DLAS 中存在着大量的哈希计算,其交易、区块都依靠哈希值进行标识,基于联盟链的数字资源的共享就是基于哈希值进行的。它能够统一不同的元数据描述体系,从而实现不同的元数据体系下的元数据交换。这使得异构数字图书馆在数据格式、数据类型、元数据规定等方面达成了统一标准,保证了数字图书馆间数据源的全面互操作。目前,区块链技术标准尚未完善,LibRSM 模型在实现数字图书馆间互操作方面将随区块链技术标准的完善而不断成熟。

5.3 性能

信息资源安全共享的性能主要指数据访问、流通、共享的效率以及数字图书馆用户参与度等。第一,LibRSM 是一种分布式共享方案,用户权限的审查、数据校验以及资源访问不再依赖第三方,解决了信用问题,减少了交易时间,节省了交易成本。第二,由于 LibRSM 联盟链中只存在交易数据的哈希值以及数据存储位置信息等,缩小了用户搜索空间,加快了资源检索及校验速度。第三,LibRSM 用户权限信息被写入联盟链,使得数据访问完全由用户自身控制,有效解决了数据共享和版权保护之间的矛盾。最后,LibRSM 不仅减少了用户对版权的担忧,还解决了信用问题,使得用户满意提高,从而有效提高了用户参与度。在未来应用中,区块链技术的一些固有局限性,如节点存储空间有限、计算成本较高等问题将会在一定程度上影响 LibRSM 节点的存储空间和计算速度,从而影响其性能。但随着区块链技术与云计算等技术的不断融合与发展,LibRSM 性能将会得到持续提高。

5.4 比较分析

本部分将 LibRSM 与目前一些主流信息资源共享方案在共享技术、安全性、一致性、易扩展性、版权保护、应用场景等方面进行对比,如表 1 所

示。与文献[8]提出的基于 P2P 和 Web Service 技术的数字图书馆资源共享模型相比,LibRSM 利用联盟区块链技术所具有的数据不可篡改、可追溯、易扩展等特点在数据共享安全性、可扩展性和版权保护等方面具有较大优势。与文献[11-13]所提基于云计算的数字图书馆资源共享模型相比,LibRSM 使用户能完全控制自己的数据,在安全性、隐私保护以及版权保护等方面优势较大。与文献[18]和文献[25-26]所提出的基于区块链的信息资源共享模型相比,LibRSM 是一种适用于数字图书馆领域的信息资源安全共享模型,利用 DPoS+PBFT 共识算法改进了共享流程,在保证信息资源产权情况下,提高了模型的可扩展性。

表 1　LibRSM 模型与现阶段主要共享方案的比较

	共享技术	安全性	一致性	可扩展性	共识机制	版权保护	应用场景
文献[8]	P2P 技术和 Web Service	×	×	√	-	×	数字图书馆
文献[11—13]	云计算	×	√	√	-	×	数字图书馆
文献[18]	区块链	√	√	√	改进 DPoS	-	数字医疗
文献[25—26]	区块链	√	√	×	PoW	-	数字医疗
LibRSM	联盟链	√	√	√	DPoS+PBFT	√	数字图书馆

6　总结

本文提出了一种基于联盟链的数字图书馆信息资源安全共享模型 LibRSM。LibRSM 利用联盟链的分布式存储、共识算法等保障数字图书馆信息资源的可信性,利用身份认证、访问控制等保障信息资源的安全性,利用统一化区块格式提升馆间信息资源的互操作性,利用交易可追溯、可审计等保障信息资源产权。通过 LibRSM 能突破数字图书馆间信息资源共享壁垒,实现信息资源自由流通。

目前,联盟区块链技术在数字图书馆领域的应用处于探索阶段,LibRSM 的应用也存在一定的不确定性:一是一些联盟链技术标准仍在研究阶段,各数字图书馆对区块链技术的认可度存在差异;二是区块链技术自身的局限性如存储空间有限、计算成本较高等导致其在数字图书馆领域应用的局限性。希望本文能够对联盟链技术在数字图书馆领域的应用研究提供一些启发与借鉴。

参考文献

1　李晓明,等.数字图书馆推广工程数字资源共建共享模式探析[J].国家图书馆学刊, 2012(5): 20-26.

2　Marshall C C. Annotation: from paper books to the digital library [C]//Proceedings of the second ACM international conference on Digital libraries. ACM, 1997: 131-140.

3　John Wilkin. 展望未来:数字图书馆技术的挑战和机遇[J].何欢欢,译.中国图书馆学报, 2008(4): 5-7.

4　李育嫦.数字图书馆信息资源共享现状及保障机制研究[J].图书馆学研究,2014(6): 75-77.

5　黄筱玲.我国信息资源共建共享模式之比较——系统中心和区域中心[J].图书馆, 2010(4): 82-84.

6　高胜,朱建明. 基于区块链技术的新型分层数字图书馆体系架构[J]. 图书情报工作, 2018(24): 57-64.

7　朱伟珠.基于 OGSA-DAI 的数字图书馆动态联盟资源共享[J].图书情报工作,2010(8): 123-126.

8　赵捧未,等.基于 P2P 和 Web Service 的数字图书馆资源共享框架研究[J].信息资源管理学报, 2011(2): 55-58.

9 贾凤旭.基于XML技术的数字图书馆资源共享平台构建[J].图书馆学刊,2013(9):110-111.

10 麦旭辉.跨系统图书馆联盟数字资源共建共享工作研究[J].四川图书馆学报,2017(4):2-5.

11 张鼐.云计算环境下信息资源共享模式研究[J].情报科学,2010(10):1476-1479.

12 魏达贤,谢强.基于云计算的国家数字图书馆基层"服务云"研究[J].国家图书馆学刊,2012(4):40-47.

13 陈宫,牛秦洲.基于云计算的数字图书馆信息服务平台[J].情报科学,2012(5):684-688.

14 S. K. Chauhan,P. Mahajan. Library consortia in India with special reference to UGC-Infonet digital library consortium[J]. International Information & Library Review, 2013, 45(3-4): 127-138.

15 A. Tripathi,J. Lal. Library Consortia[M]. Sawston: Chandos Publishing, 2017: 103-108.

16 马昂,等.区块链技术基础及应用研究综述[J].信息安全研究,2017(11):968-980.

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

18 薛腾飞,等.基于区块链的医疗数据共享模型研究[J].自动化学报,2017(9):1555-1562.

19 王继业,等.基于区块链的数据安全共享网络体系研究[J].计算机研究与发展,2017(4):742-749.

20 董祥千,等.一种高效安全的去中心化数据共享模型[J].计算机学报,2018(5):1021-1036.

21 黄敏聪.区块链技术及其对图书馆发展的变革性影响[J].图书情报工作,2018(13):11-18.

22 余其凤,等.区块链技术在图书馆数字资产管理中的应用探讨[J].数字图书馆论坛,2018(7):30-36.

23 L. Zhu, et al. Controllable and trustworthy blockchain-based cloud data management[J]. Future Generation Computer Systems, 2019, 91: 527-535.

24 S. Wang, et al. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018, 6: 38437-38450.

25 Q. Xia, et al. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments[J]. Information, 2017, 8(2): 44.

26 Q. Xia, et al. Medshare: Trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5(99): 14757-14767.

27 邵奇峰,等.区块链技术:架构及进展[J].计算机学报,2018(5):969-988.

28 张超,等. Medical Chain:联盟式医疗区块链系统[J].自动化学报,2019.

29 Brousmiche K L, et al. Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned[C]//2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018: 1-5.

30 X. Xie, et al. Design and Research on B2B Trading Platform Based on Consortium Blockchains[C]//International Conference on Cloud Computing and Security. Springer, Cham, 2018: 436-447.

31 L. Zhou, et al. Cssp: The consortium blockchain model for improving the trust worthiness of network software services[C]//2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC). IEEE, 2017: 101-107.

《2018 中国人读书报告》发布

2019 年 1 月 8 日,阿里巴巴发布基于天猫、淘宝、闲鱼、阿里文学等平台数据的《2018 中国人读书报告》。报告显示,在 2018 年:

• 中国的阅读人口与阅读总时长显著增加,阅读人口较 2017 年增长近 3000 万,上海阅读人口居全国第一;

• 80 后、90 后占阅读总人口的 75%,46%的电子书阅读者为 90 后;

• 人均购买纸质书 5.5 本,超过 50%的人同时选择纸质书和电子书阅读,在传统阅读领域,人们偏好儿童文学、教辅教材、绘本图书、期刊杂志等;在电子阅读领域,人们偏好小说、励志成功学、职场心理学等;

• 大量二手闲置图书通过转让、免费赠阅等形式从沿海省市流转到中西部省市,其中广东省以年人均交易 1.59 本闲置书为首,四川省流入图书最多。

资料来源

1 上线半年电子书订单超 2500 万单 天猫读书 APP 打造了一座移动图书馆[EB/OL].[2019-01-17]. http://www.xinhuanet.com/ent/2019-01/10/c_1123972440.htm.

2 阿里发布 2018 中国人读书报告“80 后”“90 后”为阅读主力[EB/OL].[2019-01-17].http://mil.chinanews.com/cul/2019/01-08/8723294.shtml.

(国家图书馆研究院 提供)

---

32 贺锋,王汝传.一种基于 PKI 的 P2P 身份认证技术[J].计算机技术与发展,2009(10):181-184,188.

33 M. Castro, B. Liskov. Proactive recovery in a byzantine-fault-tolerant system [C]//Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, 2000.

34 姚晓霞,陈凌.从共建共享到融合开放:培育高校图书馆资源共享的新生态——纪念中国高等教育文献保障体系(CALIS)启动建设 20 周年[J].大学图书馆学报,2018(6):44-48.

35 Zheng Z, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018(4): 352-375.

(沈凯旋 中央财经大学信息学院产业经济学专业 2017 级硕士研究生,高 胜 副教授 中央财经大学信息学院,朱建明 教授 中央财经大学信息学院院长)

收稿日期:2018-10-22