项目结题验收单

1 专家验收表（主持人所在单位组织 3-5 名专家对项目进行验收、自评。）

项目名称	基于区块链的图书馆信息安全技术研究				
主持人	程罗德	职务/职称	主任/实验师		
所在单位	（加盖公章）				
专家意见	2022 年 4 月 27 日，大连海洋大学图书馆组织 5 名专家，对 2021 年申报的 CALIS 课题研究项目进行了结题验收和自评。专家组听取了程罗德所承担的《基于区块链的图书馆信息安全技术研究》课题汇报，通过认真审阅课题研究报告，查看课题研究相关资料，经讨论，形成如下鉴定意见： 就如何解决新环境下数字图书馆信息安全问题，课题研究了联合体区块链的图书馆数据存储与共享安全模型，以解决图书馆数字资源存储共享链安全威胁，助推区块链技术在数字图书馆信息安全中深入应用。 课题在安全性方面区块链具有的技术安全优势及数字图书馆区块链上的智能合约虚拟机安全进行了深入的探讨。结合区块链平台相关组件设计了适用于图书馆网络传输信息安全技术框架，提出了采用区块链共识算法的一种网络传输信息安全和区块链结构安全网络数据保护方案。构建了图书馆数字证书管理过程可审计且扩展的高可信度用户身份认证机制和个人数据信息保护及基于区块链的数字图书馆数据共享、交换和云数据完整性保护模型。同时，给出了基于区块链的图书馆数字资源安全体系防护策略。 经过验收专家组评议，该课题研究选题立意较前沿，理论依据阐述充分，研究内容相当充实，研究方法运用具有科学性和创造性，较好的完成了申报计划规定的任务，达到了预期目标。课题研究基于区块链的数字图书馆信息安全，构建技术、机制、模式、人员、管理和服务立体综合性的图书馆信息安全防护体系，对提升其信息安全防护具有重要现实意义。经鉴定，该课题研究取得成果丰硕，提交的结题验收材料齐全，同意结题。				
专家签字					
职务/职称	教授	研究馆员	教授	副研究馆员	副研究馆员

项目编号：2021011

CALIS 全国农学文献信息中心研究项目
结题报告

项目名称：　基于区块链的图书馆信息安全技术研究

项目关键词：　区块链、图书馆、信息安全、智能合约

项目单位（盖章）：　大连海洋大学

通信地址:　辽宁省大连市沙河口区黑石礁街 52 号

大连海洋大学图书馆，邮编：116023

项目主持人：　程　罗　德

联系电话：　13604089923

电子邮件：　cld@dlou.edu.cn

提交日期：　2022 年 5 月 6 日

基于区块链的图书馆信息安全技术研究

（ 程罗德，大连海洋大学图书馆，项目编号2021011 ）

关键词：区块链、图书馆、信息安全、分布式、共识算法

1 课题研究背景、目的及意义

1.1 课题研究背景

区块链极具潜力，其应用已从最初的数字货币延伸至金融、物联网、智能制造等多个领域，为了推进区块链技术的研究和应用,我国工信部于 2016 年 10 月发布了《中国区块链技术与应用发展白皮书》，国务院在《“十三五” 国家信息化规划》中将区块链列入战略性前沿科技之一。

云计算、物联网及人工智能等技术的发展和应用，推动了图书馆向智能化、智慧化深层次信息服务发展。信息安全技术的不断升级，产生的安全威胁程度和破坏力已发生不可预测的变化，这给数字图书馆信息安全带来极大的挑战。

区块链技术应用到数字图书馆信息安全领域中，构建分布式系统，利用多节点共同作用，对信息进行管理，降低中心节点出现风险概率，提升图书馆信息安全防护能力。区块链技术作为又一项重要信息技术已引起人们极大的关注，图书情报领域（Library and Information Science, LIS）的相关人员也纷纷加入到区块链应用到数字图书馆建设的研究和实践中来。

1.2 课题研究目的

借助于区块链这一新兴技术在网络安全中构建分布式系统，利用多节点的共同作用，进行信息管理，降低中心点故障导致全系统障碍的风险，提升图书馆网络的安全防护能力，弥补图书馆专有网络固有的系统漏洞，促使其网络安全环境得到极大改善。

在数字图书馆建设中，有必要重视区块链技术的作用，发挥区块链技术的优势，推进区块链技术的应用，以充分保护图书馆读者个人信息的安全。

1.3 课题研究意义

课题研究联合体区块链的图书馆数据存储与共享安全模型，解决图书馆数字资源存储共享链安全威胁，助推区块链技术在数字图书馆信息安全中深入应用。

如何解决新环境下数字图书馆信息安全问题仍是数据建设、管理和服务中迫切需要解决的问题之一。区块链作为一种有效的分布式数据存储技术，在多个网络节点共同参与下，具有去中心化、防篡改和可追溯等优势，研究基于区块链的数字图书馆信息安全，构建技术、机制、模式、人员、管理和服务立体综合性的图书馆信息安全防护体系，对提升其信息安全防护具有重要现实意义。

基于区块链的云数据完整性保护技术应用于图书馆专业化数字资源建设安全保障体系的研究，可以对云端数据完整性进行监控和验证，保护用户数据的完整性，为完善图书馆数字资源安全，提供理论或实践方面的支持与借鉴，具有较高的学术研究价值和较强的实践意义。

2 课题研究思路及方法

2.1 课题研究思路

对图书馆信息安全和区块链技术相关基本概念进行阐述，并将其在国内外的研究现状和面临的关键问题进行总结。探讨基于区块链技术应用数字图书馆信息安全的特点和优势，得出对其深入研究的必要性。

在综合分析区块链技术的基础上，对利用该技术实现数字图书馆个人数据的保护及其适用性等内容进行研究。围绕数字图书馆个人数据安全保护问题、个人数据泄露途径和个人数据存在的安全威胁主要原因进行探讨和分析。指出区块链技术的数字图书馆个人数据保护优势和意义。

大数据和云计算技术解决了图书馆信息服务的针对性、有效性问题，而区块链技术解决了图书馆的信息收集多样性、存储的安全性及传播的广泛性。从数字图书馆馆藏资源安全保障现状进行分析，对区块链技术在数字图书馆资源安全保障体系中的应用特点进行梳理。指出区块链技术在数字图书馆观察资源安全存储中的应用优势和途径。

分析数字图书馆信息安全问题现状，阐释区块链技术的概念、特征和安全属性，探讨在安全性方面区块链具有的技术安全优势及数字图书馆区块链上的智能合约

虚拟机安全。

分析数字图书馆网络系统各层次的安全需求和所面临的安全威胁，结合区块链平台相关组件设计适用于图书馆网络传输信息安全技术框架，主要包括网络节点管理模块、传输消息结构设计、传输信息加密和身份认证模块以及 PBFT 共识模块等。针对数据传输过程中所面临的三种攻击威胁，提出采用区块链共识算法构建一种网络传输信息安全和区块链结构安全的网络数据保护方案。

针对传统身份管理与访问控制系统中心化造成的安全问题，运用区块链智能合约，构建数字图书馆多链的身份管理生态系统。

针对传统公钥 CA 认证中心操作记录难公开、不透明等问题，区块链技术结合分布式存储、数据加密技术及云数据多租户特征，提出图书馆数字证书管理过程可审计且扩展的高可信度用户身份认证机制和个人数据信息保护模型。

构建基于区块链的数字图书馆数据共享、交换和云数据完整性保护模型，提出的新的构建基于信任区块链的数字资源存储与共享安全架构，并从安全认证、可扩展的安全多方计算、完整性保护等方面，给出基于区块链的图书馆数字资源安全体系防护策略。

2.2 课题研究方法

在研究过程中，将综合运用文献研究、文献调查、实例分析研究、多学科研究等方法进行综合、系统的分析研究。

通过多种途径获取相关资源文献和实证资料，探讨基于区块链技术在图书馆信息安全应用中出现的特点、优势及存在的问题，在新信息环境下，满足用户应用需求与技术升级的要求，反映信息安全的作用和价值，凸显“创”与“新”技术、理念融合特质，关注图书馆信息安全需求的动态变化，进一步拓展数字图书馆信息安全的内涵和意义。为研究的展开和相关结论的提出，提供相应经验材料和实践指导参考。

3 课题研究具体内容

本课题研究内容主要利用区块链技术解决目前图书馆存储系统数据共享身份识别验证、数据操作记录追踪回溯等方面存在的问题和不足，探讨一种新的用户个

人数据的隐私保护方案，包括数据隐私保护协议、数据的上传和下载协议、区块链中的记录协议及交易隐私保护协议等内容。在应用过程中结合实际需求对区块链技术应用数据共享身份识别、访问控制和审计等数据安全性内容提出解决方案。

探索基于区块链技术在数字图书馆信息安全应用中出现的新特点和技术优势，对数字图书馆无中心网络身份认知技术进行研究，针对传统公钥基础设施中认证中心操作记录难公开、透明等问题，提出高可信度、数字证书管理过程可审计且扩展的身份认证机制。

基于 PBFT（拜占庭容错协议），设计一种区块链的图书馆无中心网络信任安全传输模式。应用区块链基础结构，设计立体式图书馆用户数据信息保护模型，引入智能合约块锁，使区块链对用户数据保护不再是指定的层级保护，而是实现立体式保护。

为解决图书馆云存储数据的机密性和身份验证问题，针对数字图书云数据的安全性，设计一种基于区块链的数据共享保护系统安全模型。

3.1 数字图书馆信息安全问题及现状

数字图书馆相比较传统图书馆来说，它以网络和数据库存储为基础平台，更多注重物联网和人机交互，完成与用户线上的交流和沟通，呈现出信息资源建设和管理网络化、数字化和共享化等特点。信息安全事关数字化图书馆能否正常开展线上、线下业务服务。

网络安全建设一般具有 P2P 网络的开放性，数字图书馆的资源建设、数据管理、价值服务都是在开放的网络环境下进行，面临着多种安全威胁，如遭受宽带攻击、协议攻击（包括 Smurf、UDP、ICMP、SYN、DNS、CGI 请求等）、软件漏洞攻击等 DDoS 攻击，攻击者通过大量僵尸节点向受害节点发送海量数据包以达到拒绝服务攻击。失效的身份认证和会话管理，与身份认证和会话管理相关的应用功能实现不正确，允许攻击者可以构造密码、密钥、会话令牌或利用信息系统功能缺陷，都会造成敏感数据泄露。功能级访问控制策略缺失，访问请求没有验证，攻击者构造请求，访问未授权的功能，对数据篡改、窃取。

如果安全访问级别设置偏低、缺少安全策略，存在系统漏洞等，容易受到攻击

或数据泄露。一旦网络入侵成功，可能引发系统性问题，造成整个联盟链节点受到牵连，给分布式共享参与主体带来损失。

当前图书馆网络建设和应用大多采用中心化架构，在这种网络结构体系中分布式或联盟链上的节点之间的数据传输需由核心服务器控制、分配来完成，在通信过程中数据容易受到非法获取、篡改、欺骗等。基于网络安全威胁，因中心化故障引发连锁反应，造成整个系统崩溃，中心化作用和地位已是整个系统的潜在安全威胁。

信息安全已成为数字图书馆建设重点内容，根据研究文献分析，国内外高校图书馆在信息安全方面的研究和应用各有侧重，一些专家学者从图书馆空间安全、智能识别、策略控制等物理安全层面进行了研究。图情领域相关技术人员对网络与设备安全、存储与系统安全、数据加密与共享等方面也进行了初步的探索。利用区块链技术驱动数字图书馆信息安全的研究和应用非常少，很难找到当前区块链技术应用于数字图书馆信息安全的实践案例。

因此，对区块链技术应用于数字图书馆进行深入的研究，需要对图书馆网络系统中各节点的身份进行管理和认证，构建技术、机制、模式、人员、管理和服务立体综合性的图书馆信息安全防护体系是非常有意义的。

3.2 区块链关键技术

区块链将 P2P 传输、分布式数据存储及智能合约等技术进行组合，结合数据加密、零知识证明等密码学技术，成为一种不断发展且防篡改的共享分布式账本和计算范式。2016 年 10 月，工信部发布《中国区块链技术与应用发展白皮书》，首次提出我国区块链标准化路线图。区块链技术具有公开性、去中心化、安全性和唯一性等特点。区块链技术为中心化的应用数据存储和信息共享中出现的信息网络安全威胁、用户数据泄露、云存储数据不可控等问题提供了解决方案。

3.2.1 区块和块链式数据结构

区块是链式存储结构中的数据元素，其中第一个区块被称为创始区块。区块作为区块链的基本结构单元，由记录当前区块的特征值区块头和实际数据的区块体构成。其中区块头包含了每个区块自身的身份识别信息、父区哈希值、时间戳等内容。区块体记录了所有的交易数据。

区块链由区块相互连接形成链式存储结构，它的数据结构含有父区哈希值、随机数、难度值和时间戳等信息，该结构将数据以区块为单位进行验证与存储，由于硬件或管理机构无中心特征，任意节点都是对等的，系统中具有维护功能的节点对链上数据库进行共同维护。

3.2.2 哈希算法

存储在区块链上的数据信息需经加密算法进行处理，只有授权合法用户才拥有访问和使用权限，保证数据的安全和个人隐私性问题。哈希算法，提供一个数据的摘要或者指纹，对数据进行完整性校验。哈希函数具有无冲突和不可逆的特点。

哈希算法有很多种，常见的哈希算法有 MD5、SHA-1 和 SHA-256 等，一般来讲，哈希越长的算法，安全性也越高。在区块链中通常采用 SHA-256 算法，该算法能生成 256 位，即 32 字节长度的哈希值，能够满足当前区块链利用哈希算法对交易数据生成交易摘要信息，最终得到 Merkle 根值的需求。

3.2.3 共识机制和智能合约

在一个去中心化的体系结构中，对等网络节点之间为了解决产生的决策分歧，维护系统及激励用户参与决策算法，遵守一个共同的规则，需要选择一个合理的共识。区块链网络系统中共识机制是 N 多个参与者对一个交易或提案是否将交易提交到账本及交易排序达成一致意见的过程。共识机制推动了更多用户参与到区块链网络的维护中来，增强了系统的稳定性。

使用的共识机制不同，区块链网络及其出现的特点、性能也会有所不同。在当前算法中，主要有工作量证明机制（Pow）、权益证明（Pos）、拜占庭容错协议（PBFT）和改进授权拜占庭容错协议（dBFT）等。

智能合约是部署在区块链网络中的一种服务程序，区块链网络使用智能合约，对分布式账本进行受控访问，支持信息一致性更新。智能合约的编码信息具有开放性，且不受硬件设备的制约。智能合约这种高效、安全的约定协议，可以促使参与用户能够在区块链上自觉履行所有承诺的协议内容。

3.3 数字图书馆区块链智能合约安全

3.3.1 虚拟机安全

在区块链的智能合约系统设计中，很少采用模拟完整操作系统模式，因为这种模式会消耗大量的资源并严重影响性能，对不同操作系统的架构也难以做到互相兼容。虚拟机安全可从智能合约运行的可确定性、停机问题、资源控制和资源隔离等几个维度进行分析。

数字图书馆区块链上的智能合约，一般要求其行为是可确定的，非确定性合约可能会破坏系统的一致性。使用非图灵完备、计价器或计时器等资源控制手段，通过对代码量设定上限，对运算资源进行计价或对执行时间设定上限等方法将智能合约占用的资源控制在合理的范围之内。在这个开放的数字图书馆区块链上，任何参与者都可以编写并上传智能合约，图灵完备的智能合约可以编写并执行任意的逻辑，其中包括病毒或故障合约。如果智能合约直接在区块链节点的宿主系统上运行，病毒就能自我复制，故障合约就可能破坏宿主系统的自身数据。

因此，智能合约须放在一个隔离的沙盒环境虚拟机中运行，以便合约和合约之间、合约和宿主系统之间进行有效的资源隔离，控制恶意或故障合约的影响范围。

3.3.2 身份管理与访问控制

身份管理与访问控制是数字图书馆信息系统安全的基石，区块链技术在解决图书馆身份管理与访问控制系统问题方法如表 1 所示，

传统身份管理与访问控制系统的问题	区块链技术的解决方法
身份碎片化	利用区块链技术，用户的数据不会存储在中心化的机构，而是存储在用户可以控制的终端。在区块链上可以存储相关信息的加密随机数，而不是数据本身。没有一个中心化的机构真正拥有用户的数据，对黑客来说，其攻击的代价会大大增加，用户数据得到有效保护。
口令的痛苦	区块链可利用公钥、私钥进行验证，也可以利用生物认证来摆脱口令
身份证明是一个人工操作的过程	利用区块链数据的不可篡改性，身份证明的结果可以用加密的方式发布到区块链上。
身份是静态的、不灵活	利用可以参数化的智能合约身份可以实现动态和灵活的身份管理。

图书馆许可链（包括私有链或联盟链）需对参与节点或用户身份进行验证和访问控制，Hyperledger Fabric 采用的是一个中心化的身份管理系统，与 Fabric CA 服务端的通信，都是通过 REST API 来实现。在访问控制上，Fabric 采用隔离区块链网络通道，通道内只允许被授权的参与节点使用通道 Chaincode 的数据。在通道内部，通过可见性设置对输入和输出数据的限制。将访问控制策略构建到 Chaincode 逻辑中，达到一定的基于角色的访问控制。这种模式利用 CA 集群提高了可用性，解决了单点的问题，但仍是一个中心化方案，可能成为黑客攻击的目标，从而导致整个数字图书馆网络和信息的不安全。

运用区块链智能合约，构建数字图书馆多链的身份管理生态系统如图 3-1 所示。

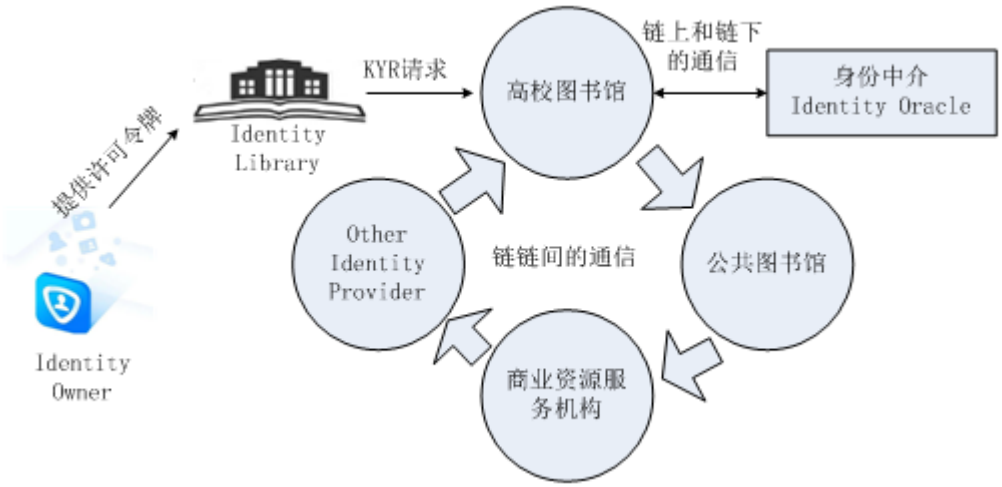


图 3-1 数字图书馆多链的身份管理生态系统

身份消费者，如一高校图书馆对读者有 KYR(Know Your Reader)的需求，必须获得身份拥有者的许可。许可可以用身份链的客户端产生一个许可令牌（Access Token），产生许可令牌前，用户必须进行指纹或虹膜扫描等生物认证的方式，以确保安全。身份消费者可以向多链的身份管理生态系统中某一条链发起 KYR 请求，请求满足，流程即可完成。如果当前请求链不能提供所有信息，可以转发给其他的身份链，获得用户信息数据。若需验证信息在所有的身份链上都无法完成，可以利用身份中介 Identity Oracle 获得可信的链下身份数据。Oracle 可提供诸如基础数据、资源数据、平台信息、规则条例等影响合约执行结果的任何信息，其所提供的信息是经过 Oracle 数字签名的，确保能够验证，且来源可靠。

数字图书馆公有链访问控制可以借助于修饰符（modifier）来实现对智能合约函数的访问控制，若某些系统功能函数不希望被非授权用户调用，可以创建一个修饰符并限制函数用法，设定多个不同角色，定义修饰符。对于图书馆联盟链上的访问控制，可以考虑建立节点准入条件，如操作系统类型、开放端口、关闭对区块链P2P通信无用账户、密码复杂度、CA根证书以及馆际联盟链成员间身份属性的映射规则和访问控制策略等。

3.4.区块链技术助推数字图书馆信息安全应用

3.4.1 区块链的图书馆无中心网络信任安全传输模式

区块链融合多维技术，发挥信任机制最大效果，需要与人工智能、物联网等技术结合，打造一个超级账本，进一步确保数据源头的真实、有效。图书馆无中心网络信任，需要做到去中心化网络以及对网络传输数据进行验证、审查。

在数据使用过程中，由于源头数据问题，造成网络异常，通过相关时间、日志和交易等线索，进行反向追溯，查找问题的根源，找到威胁发起者，对其追责。此外，引入惩罚、激励机制，通过区块链网络生态资源，阻止对数据的伪造行为，并对用户正向行为给与奖励。区块链技术确保数据在网络中的完整、有效、真实的对等传递，不受制于人的干扰或控制，在区块链的两端，做到人为与技术的结合，进一步最小化信任问题。

基于PBFT（拜占庭容错协议），设计一种区块链的图书馆无中心网络信任安全传输模式如图3-2所示。消息在网络传输模式中，采用信封结构对消息数据进行封装，以使其适应不同网络协议兼容性的要求，每一次节点之间的数据传输，不再发送至核心服务器，而是通过多节点集群共识模块对数据完整性检查，对消息内容的真实性和发送方身份进行验证。在该模式中传输数据加密、身份认证技术与共识模块结合应用，保障图书馆网络传输数据信息安全。

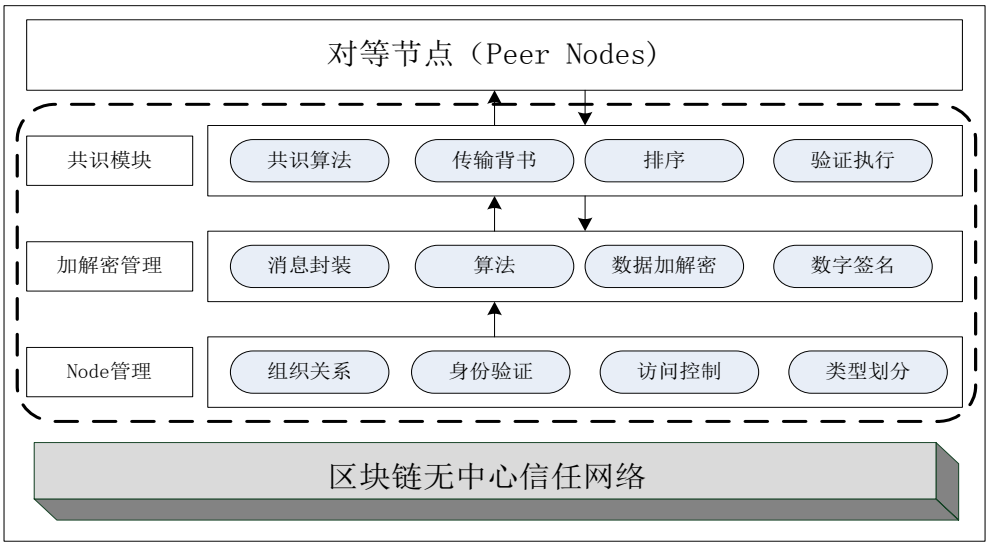


图 3-2 区块链的图书馆无中心网络信任安全传输模式

区块链网络节点管理模块主要对网络中的节点进行组织关系划分、信任身份验证、访问权限控制策略、Node 类型分类等功能管理。Client Node 发起消息传输请求，服务组件对节点划分组织关系，由组织节点选择加入到一个单独、专用的信息通道，所有 Node 的消息都要在组织通道里进行传输，其中 Anchor Node 负责与其他组织节点的通信。使用 Crypto Generator 工具，读取文件信息进行配置，快速生成证书和密钥，以用于对 Node 访问权限控制和管理。

为提高消息在网络中传输安全性，对信封信息进行处理和封装，使用这种信封结构无需考虑网连节点的具体通信方式或协议。采用非对称加密，数字签名的密钥对传输封装消息进行明文数据的加密或密文解密。在传输模式设计中，使用认证授权区块链作为根 CA，将其存储到区块链网络的创世区块中，为节点用户提供登记、事务调用等证书服务。TLS 证书保证用户或区块链组件之间通信的安全链接，以确保数据来源可靠，保护数据隐私。区块链无中心网络信任数据传输数据信息处理层，防止区块链网络数据传输安全遭到攻击。

智能合约共识层传输、排序和验证执行，实现网络数据的安全传输。 Client 用户发起信封结构且经过加密处理后的消息传输请求后，智能合约共识层 Primary node cluster 根据制定策略对发起的传输消息进行验证，若请求传输的消息被区块链网络中三分之二的节点投票通过，则把经过签名消息发给 Primary node 排序服

务节点，由其按时间戳来对传输消息进行排序，否则丢弃本次传输消息处理，并返回告警信息给发起 Client 用户。排序后的消息在信息传输通道内部送达接收 Executor node，由其对接收到的消息内容进行处理，消息一旦被正确处理完成，生成消息传输区块记录，对链上的所有节点发起广播，最后将消息传输的执行结果响应给发起端 Client 用户。

3.4.2 区块链的数字图书馆用户信息保护

利用区块链去信任化的特点，将其应用到图书馆用户信息保护中，引入新的管理机制，由目前的信息集中管理到无中心或弱中心化管理，这对于系统管理人员来说，从意识、操作、技能等方面，在很大程度上减少对接触用户数据信息的泄露机会。区块链对任何的交易行为和业务操作等都有时序记录，实现数字图书馆用户数据信息零信任、可追溯，防篡改的立体、全生命周期的保护。

应用区块链基础结构，设计立体式图书馆用户数据信息保护模型，引入智能合约块锁，使区块链对用户数据保护不再是指定的层级保护，而是实现立体式保护。图书馆用户数据信息的采集、存储、操作、销毁等全生命周期都会得到区块链技术的保护，确保用户数据信息的安全。区块链的立体式图书馆用户数据信息保护模型如图 3-3 所示。

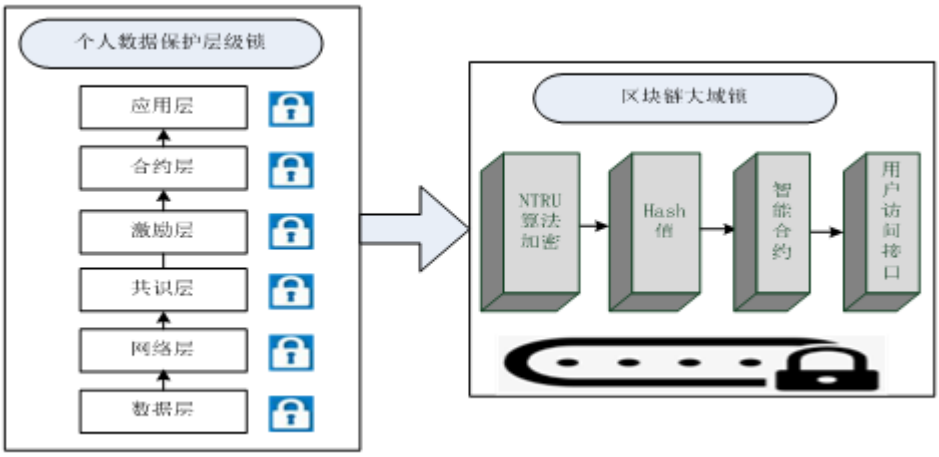


图 3-3 区块链的立体式图书馆用户数据信息保护模型图

采用（p,t）-门限 NTRU 算法对图书馆用户数据进行加密，保存 Hash 值，当需多租户使用共享密钥对数据解密时，私钥将被分成 p 份，某一个用户想要获取数

据，那么至少需要其他 t-1 个用户同意，共同解密才能完成，调用数据访问接口实现数据的请求和访问。即使是部分用户通过数据中心对密文 得到求和结果，也无法推导出每一个用户的私钥 Vk，Epk(Vk)不能被解密，该模型满足了机密性、防篡改性要求，达到了保护图书馆用户个人数据隐私性目的。

3.4.3 可信区块链的图书馆数字资源存储与共享保护

应用区块链技术组织图书馆链式数据资源结构，允许用户或平台管理人员参与数据库和安全存储的建设，提供资源数据的开放式服务，最大化利用数据资源。利用区块链技术的无中心网络信息安全传输和加密算法，结合数据聚合和深度挖掘、知识关联等，实现信息的安全认证，提升数据库安全水平，保证资源数据的安全存储。

在区块链数据管理中，信任数据被记录在区块链上，有效解决图书馆数字资源的共享存储、数据真实和安全等问题。可信任区块链的数字资源存储与共享安全架构如图 3-4 所示。

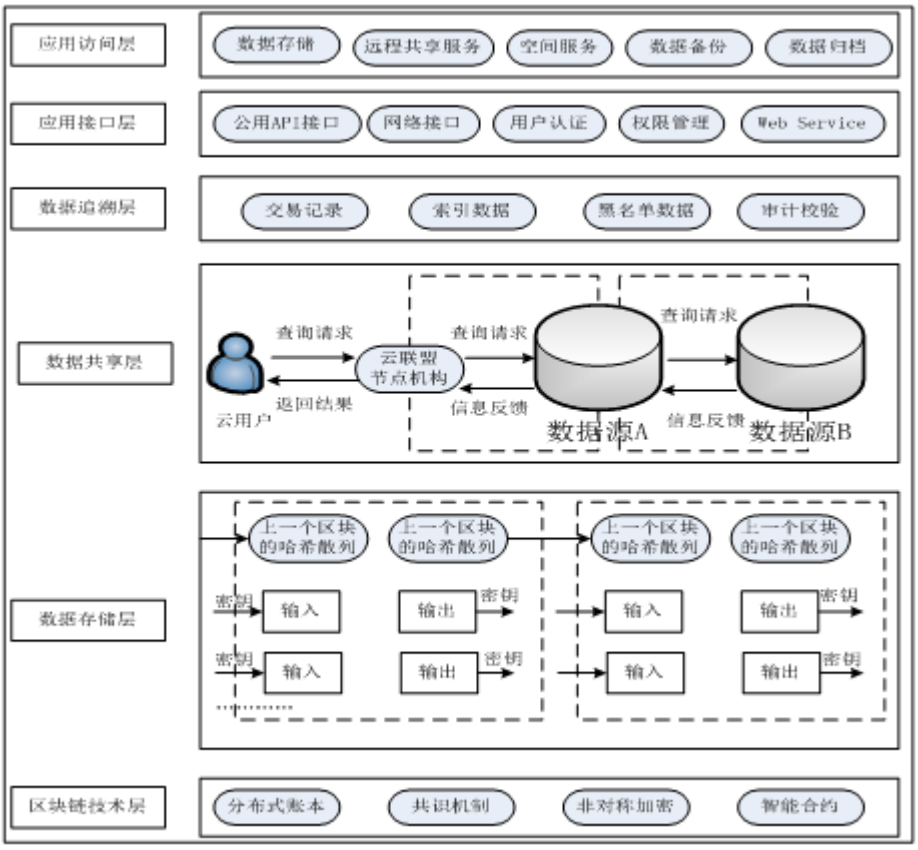


图 3-4 可信任区块链的数字资源存储与共享安全架构

数据存储层，索引数据存储在区块链中，元数据在各个参与主体的数据库中存储，程序记录海量数据信息，并将所有数据均存储在区块链网络计算机节点上，实时更新，使用无中心结构，实现链上的任意节点同步更新存储数据，增强数据库的安全性。

数据共享层，采用去中心化的机构联盟方式，各机构向区块链信任网络密文公布共享数据的索引，通过透明、可控的机制实现机构间（馆-馆-数据商）数据流动和交互。机构与数据源提供者之间，通过数据接口对接，不接触数据平台，所有的请求以匿名代码的形式发送。整个区块链信任网络中数据索引在区块链中存储，机构获得请求后向区块链上的各数据源进行查询，得到详细的数据。这种数据共享服务模式，在不共享源数据的情况下，实现联盟链多节点数据的共享。

数据追溯层，数据存储和共享的行动主体或行为都被记录到区块链上，节点的每一次交易信息被清晰、透明的组织起来，形成完整的交易明细清单。基于此，任何节点之间的交易都能查询和追溯，所有的交易需用一组公钥和私钥来进行加解密处理，增加到区块链上，永久不可改变。若出现对某个区块的值产生怀疑时，便可查看历史交易记录，判别该值的正确性，识别该值是否已被篡改或记录有误。

3.5. 区块链的图书馆数字资源安全体系构建策略

3.5.1 双链分离的安全认证

资源数据的存储模式主要有区块数据结构、非对称加密和记录数据结构等，为了提高认证的有效性，在安全认证时可将证书的分发链、撤销链进行分离，使用双链分离的数据存储结构。证书分发链和撤销链分别记录分发、审计和撤销等相应信息，撤销链根据接口提供的信息进行快速匹配，将认证结果向发起证书验证的用户反馈。

双链分离的安全认证模式，可在较小空间证书撤销链上实现高频次证书认证操作，提高认证效率，保障图书馆数字资源存储安全性和可靠性。

3.5.2 可扩展的安全多方计算

将共识机制应用于分布式节点共同计算，以达到对数据有效性最大化共识的结果，亦是一种可扩展性、安全多方计算模式（MPCM），可用于解决图书馆数字资源

安全体系在一致性及高时间复杂度等方面的问题，保证资源安全体系架构具有较强的可扩展性。

在 MPCM 模型中，参与任务计算的节点产生的特征数据通过协作，实现区块链的验证功能。各参与方只能获得与私密数据相应的输出数据，无法得到任何其他有效信息，自身数据信息也不会泄露其他参与计算节点。利用信息记录保证资源数据可查询和追溯，通过验证各节点存储的元数据一致性，满足图书馆数字资源安全防护模型具有可扩展、高效和安全性需求。

3.5.3 云数据验证及完整性保护

在网络系统中部署由多组数据库服务器构成的数据文件灾备体系，把服务器节点对资源数据的操作日志及源数据产生的审计验证作为元信息存储到区块链数据块中。当数据服务器对某个节点数据进行数据上传、修改等操作时，该操作所有发生的动作信息都会被审计和验证模块监控、记录，并生成一条包含操作类型和节点 ID、数据存储路径、时间戳等内容的事务信息，信息如验证通过，将新增到块链上，且对其不可篡改。为确保数据的完整性，将元数据信息进行加密处理之后，再将其添加到区块链中。

数据传输至云存储服务器时，节点用户使用私钥加密处理文件数据，通过 Hash 值，对数据文件进行身份证明和参数的完整性校验，以防止对数据的恶意篡改及对未授权数据读取或下载，导致数据信息的泄露或伪造。云服务器收到节点用户数据上传、提交请求，检索、分配存储空间资源，然后将请求存储的加密数据进行 Database Backup 多副本数据库备份。节点数据无论在传输过程中出现意外损坏，或是被遭到恶意的篡改，使用云存储的数据库备份副本，即可对损坏数据实施恢复。

4 课题研究结论与建议

4.1 课题研究结论

随着区块链技术逐步完善与成熟，研究区块链技术应用于数字图书馆的趋势将持续升温，区块链技术对于数字图书馆的变革已经逐步变为现实。

对于图书馆来讲，去中心性特征，变革了图书馆传统的“信息提供与保存”中

心的历史地位。数据可靠特征又使图书馆摆脱了传统的数据存储、提供与应用模式。

区块链网络作为一种共识机制、P2P 传输及分布式数据存储等新技术应用模式在 LIS 领域逐渐得到应用，使得节点之间 PoW 得到快速校验，数据高效传输，有效降低了单点数据故障所造成的影响。

图书馆数字资源存储和使用的高安全性，为用户提供更加高效、优质的资源信息服务，进一步提升图书馆信息安全水平和资源安全保障能力，推动图书馆数字资源建设健康、可持续发展。

4.2 课题研究中存在的问题及建议

当前区块链技术应用于图书馆信息安全的有关内容如采用区块链共识算法的网络安全传输、运用区块链智能合约的多链身份管理与访问控制、应用区块链基础架构的用户数据信息保护、可信区块链的数据存储与共享安全等实践案例非常少，数据库检索不到相关文献。

建议能给予课题研究基础保障基金支持，项目研究成果在期刊发表给予支持，更有利于项目研究成果的推广与应用。

在今后的研究中，要继续扩展研究的维度和深度，运用区块链点对点、去中心化、链式数据结构和密码学原理等有效预防运行故障和安全威胁，满足对数据监管和审计安全性要求，保障数据安全完整、可信和可审计，解决图书馆信息链中有关安全技术难题，实现图书馆多样性信息采集、安全性数据存储和广泛性资源共享。

5 课题研究成果

5.1 课题研究报告

5.2 发表文章及获奖

1.程罗德，利用区块链技术驱动高校图书馆数字资源建设研究，图书馆学刊：2021,43(07),50-54.

2. 区块链+图书馆:数字资源生态构建及应用研究，获 2021 年东北地区第十八次图书馆学科学讨论会征文三等奖。

6 参考文献

[1] 柳林子等. 区块链技术下图书馆读者个人信息保护研究[J]. 图书馆工作与研究, 2019,(05),96-101.

[2] 汪琼等. 区块链在图书馆著作权保护中的效用研究[J].数字图书馆论坛，2019,(03),69-72.

[3] 刘红. 区块链技术在高校图书馆馆藏资源安全存储中的应用[J].图书馆学刊，2018（5）：104-107.

[4] 徐俐华等.基于数字图书馆联盟链的信息资源安全共享模型构建[J].图书情报工作委，2020,64(03),53-58.

[5] 房永壮等. 基于大数据共享环境下图书馆“区块链”技术应用研究[J]. 现代情报,2018(5):120-124.

[6] 邵奇峰等.区块链技术:架构及进展[J]. 计算机学报, 2017:1-20.

[7] 中国区块链技术和产业发展论坛.中国区块链技术和应用发展白皮书(2016)[EB/OL].[2019-02-29].http://chainb.com/download/工信部-中国区块链技术和应用发展白皮书1014.pdf.

[8] 国务院.国务院关于印发“十三五”国家信息化规划的通知[EB/OL].[2019-07-29].http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm.

[9] 申屠青春. 区块链开发指南[M].北京: 机械工业出版社，2017.

[10] 谢辉，王健.区块链技术及其应用研究[J].信息网络安全,2016(9):192-195.

[11] 章宁等.基于区块链的个人隐私保护机制[J].计算机应用,2017,37(10):2787-2793.

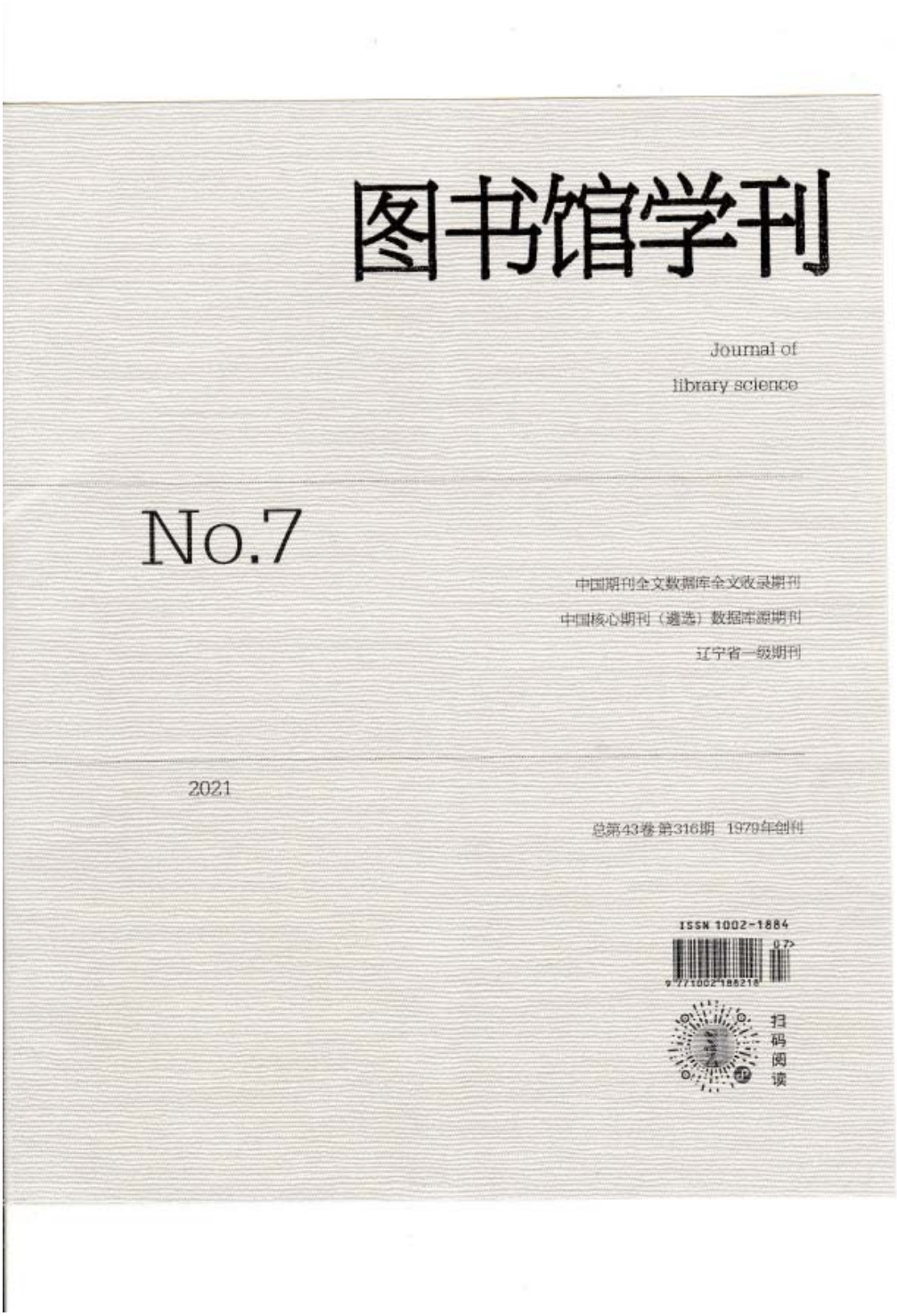
[12] 郝世博等.科学数据共享区块链模型及实现机理研究[J].情报理论与实践,2018,41(11):57-62..

[13] 秦志光等. 云存储服务中数据完整性审计方案综述[J]. 信息网络安全, 2014, 7: 1-6.

[14] 徐光伟等. 大数据存储中数据完整性验证结果的检测算法[J]. 计算机研究与发展, 2017, 54(11): 2487-2496.

附　件

1. 程罗德，利用区块链技术驱动高校图书馆数字资源建设研究，图书馆学刊：2021,43(07),50-54.



目 次

[illegible]

管理纵横

信息组织

服务经纬

利用区块链技术驱动高校图书馆数字资源建设研究*

程罗德

（大连海洋大学图书馆，辽宁 大连 116023）

[摘 要]针对新信息环境下高校图书馆数字资源建设面临的资源共建共享进程推进缓慢、大数据安全风险和资源生态不完善等方面的问题，运用区块链智能合约，构建数字图书馆多链的身份管理生态系统，设计馆内私有链、用户行为公有链和馆际联盟链的高校图书馆数字资源协同处理和可信共享架构。最后，提出了利用区块链技术驱动高校图书馆数字资源协同共建和可信共享、大数据资源安全防护、文献采购供应链价值、资源管理和服务等具体应用。

[关键词]区块链 高校图书馆 数字资源 可信共享 数据安全

[分类号]G250.7

目前，国内外LIS领域针对将区块链应用到图书馆数字化建设中进行了相关研究和探索。在国外，美国政府和图书馆支持的IMLS研究所将区块链技术应用于图书馆数字管理研究项目，以探索区块链技术在图书馆系统中的应用[1]。美国图书馆协会（ALA）也将区块链技术纳入到未来图书馆重要的革命性技术[2]。在国内，牛勇等[3]分析了区块链技术在图书馆资源建设和服务方面发挥的积极作用；徐川等[4]从馆、人不同维度设计了基于区块理论的高校图书馆资源共享服务模型，用以解决传统图书馆资源共享问题；汪琼等[5]基于区块链在图书馆著作权保护中的效用进行了研究，认为区块链技术在图书馆著作权保护中发挥的效用非常巨大。房永壮等[6]研究了大数据共享环境下区块链技术在图书馆信息服务中的应用，并提出保障数据共享中的信息安全问题。利用区块链技术数据加密、开放自治和去中心化等特点，将其应用于图书馆数据采集、管理和服务各阶段资源建设生态链中，为高校图书馆数字资源建设提供理论、技术和实践等方面的支持，驱动高校图书馆数字资源建设不断优化、创新和健康发展，具有重要的理论和实践意义。

1 区块链核心技术

区块链利用链式数据结构对数据进行验证和存储，运用分布式节点共识算法生产和更新数据，用加密算法保障数据传输和访问的安全性，用智能合约进行编程和数据操作的全新分布式基础架构与计算范式[7][8]。各个区块链采用的技术组合不同，形成的区块链特点也大不相同。在开放、共享环境中，将区块链应用于高校图书馆数据资源建设，可以确保资源数据的多样性、完整性和安全性，降低资源建设和管理的成本。

1.1 区块链数据库

区块链数据库具有公开可验证性，通过完整性和透明度来实现，用区块链查询、获取数据完成交易验证，用于以附加块形式向区块链添加更多数据，所有已存数据将被永久存储，且不可修改[9]。高校图书馆数字资源建设需要满足激增的大数据存储需求，这就要求网络传输、硬件架构、业务软件功能和数据库系统等具有高性能、高安全性，且保证资源数据的存储容量可动态、弹性扩展。利用区块链节点结构进行数据验证和存储，用共享机制保障数据的延续性，使用加密算法确

*本文系CALIS全国农学文献信息中心研究课题“基于区块链的图书馆信息安全技术研究”（项目编号：20211011）研究成果之一。

4.4　区块链拓展高校图书馆数字资源管理与服务

在区块链数据管理中，利用分布式账本、共识算法和链式数据存储结构等，消除用户、机构、特色数据库等数据需求端与数据生产者、机构和特色数据库所有端之间的壁垒。链上参与节点既是信息资源的提供者，又是信息资源的消费者，共同更新和维护数字图书馆信息资源。在数据跨库检索、馆际互借、合作存储、联机编目、特色库建设和业务合作等方面，可扩大高校图书馆数字资源种类和服务范围，进一步提升节点之间数据资源的共建、共享程度，保障数据安全和数字版权得到保护，促进馆际间的数字资源高效管理和流通共享。

基于区块链技术数据加密、可追溯和防篡改等优势[15]，高校图书馆除了资源自购、荐购和捐赠途径外，还允许成员节点用户将个人拥有的数字图书和学习笔记等资料上传到区块链上，提供给其他节点用户下载和学习，增加了图书馆资源建设来源的多样性。链上各成员节点之间无需受到传统资源借阅时空限制，根据用户自身对资源需求，通过共识和智能合约机制行为规范和约束，进行实时、动态的点对点资源借阅。这种点对点资源流通模式，极大提高了资源的流转量和使用率，资源的管理和服务也更加安全、高效。

5　结语

区块链技术为高校图书馆数字资源建设协同共建和开放共享、大数据安全、文献采购供应链、资源管理和服务等提供了新思路。利用区块链分布式存储、共识算法、智能合约等技术，可保障资源数据高效流通和互借，有效降低了传统应用中心化、数据异构及信息离散等所产生的影响。基于区块链技术的图书馆数字资源建设，会使参与主体增多，资源种类丰富，资源质量提高，存储规模扩大，共享程度提升，资源管理成本降低，资源安全升级，驱动高校图书馆为用户提供更加高效、优质、安全的资源信息服务。

参考文献：

[1] Linda. 区块链公共图书馆系统获美国政府10万美元资[EB/OL].(2017-09-05)[2018-12-13]. https://www.jinse.com/news/blockchain-business-news/63807.html.

[2] 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.

[3] 牛勇，等. 区块链与图书馆发展研究[J]. 图书馆学研究，2019(4)：41-45.

[4] 徐川，等. 基于区块链理论的高校图书馆资源共享服务模式建构研究[J]. 图书馆研究，2019(3)：56-62.

[5] 汪琼，等. 区块链在图书馆著作权保护中的效用研究[J]. 数字图书馆论坛，2019(3)：69-72.

[6] 房永壮，等. 基于大数据共享环境下图书馆“区块链”技术应用研究[J]. 现代情报，2018(5)：120-124.

[7] 邵奇峰，等. 区块链技术：架构及进展[J]. 计算机学报，2017：1-20.

[8] 乔蕊，等. 基于区块链技术的动态数据存储安全机制研究[J]. 计算机科学，2018(2)：57-62.

[9] 张炜，等. 以区块链促进协作保存网络环境下信息资源的可信性[J]. 国家图书馆学刊，2018(5)：89-98.

[10] 陈小平. 区块链技术在图书馆智慧服务中的应用研究[J]. 现代情报，2018(11)：66-71.

[11] 程罗德. 大数据环境下数字图书馆信息安全策略研究[J]. 图书馆学刊，2020(1)：74-79.

[12] 谢辉，等. 区块链技术及其应用研究[J]. 信息网络安全，2016(9)：192-195.

[13] 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.

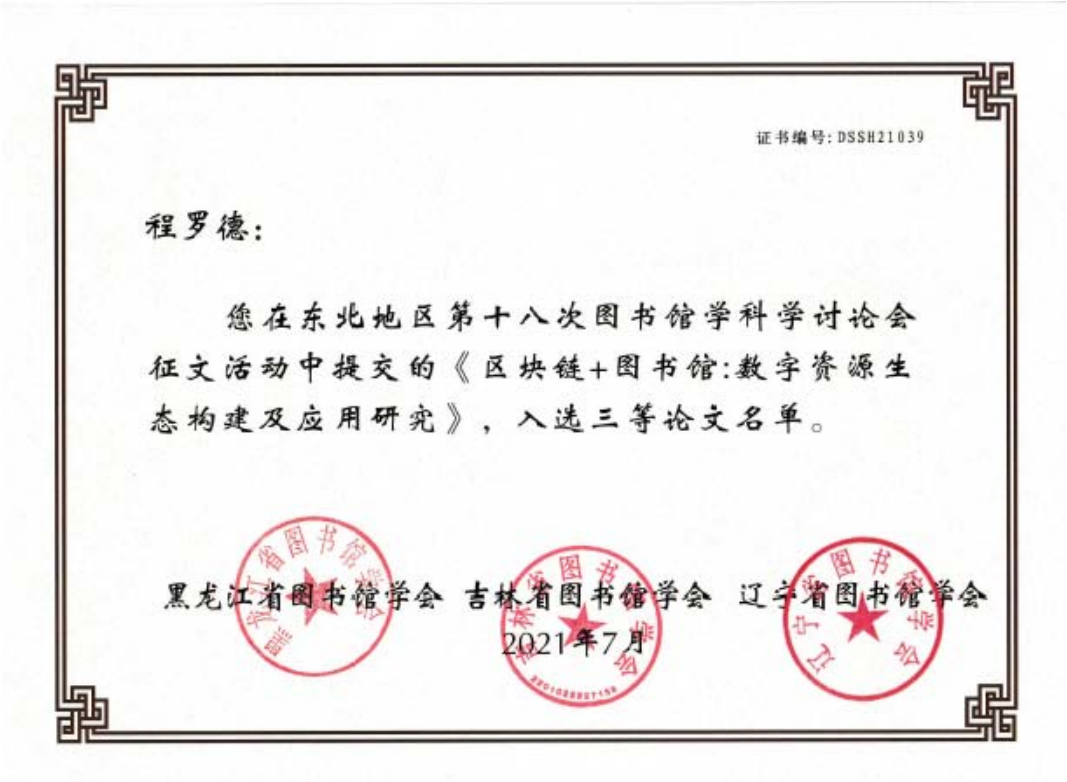
[14] 徐光伟等. 大数据存储中数据完整性验证结果的检测算法[J]. 计算机研究与发展，2017(11)：2487-2496.

[15] 赵伟娜. 区块链视阈下图书馆服务升级策略研究[J]. 图书馆建设，2019(4)：127-130，136.

程罗德　男，1982年生。硕士，实验师，技术服务部主任。研究方向：信息技术及数字图书馆建设。

（收稿日期：2021-01-26；责编：谷毓。）

2. 区块链+图书馆:数字资源生态构建及应用研究，获 2021 年东北地区第十八次图书馆学科学讨论会征文三等奖。



证书编号:DSSH21039

程罗德:

您在东北地区第十八次图书馆学科学讨论会征文活动中提交的《区块链+图书馆:数字资源生态构建及应用研究》，入选三等论文名单。

黑龙江省图书馆学会 吉林省图书馆学会 辽宁省图书馆学会

2021年7月