

本科毕业论文（设计）

英文文献翻译

|  |  |
| --- | --- |
| **文献英文题目** | **BOCA: A novel semantic blockchain-based**  **authentication system of educational certificates** |
| **学 生 姓 名** | **唐建国** |
| **学号** | **2020131040** |
| **专业** | **区块链工程** |
| **年级班级** | **2020级201班** |
| **指导教师** | **高琳** |
| **所在学院** | **区块链产业** |
| **提交日期** | **2024年1月5日** |

2023 年 7 月

成都信息工程大学 区块链产业学院

BOCA：一种基于区块链的新型语义区块链

学历证书认证制度

Minh Duc Nguyen,Cuong H. Nguyen-Dinh,Le Anh Phuong

a越南顺化大学经济大学经济信息系统系;

b顺化大学工程技术学院，顺化，越南;

c顺化大学教育大学计算机科学系，顺化，越南;

摘要：在工业和学术工作环境中，有一些人在没有完成规范的培训和教育课程的情况下，就为自己准备了非法的学历证书。在工业和学术工作环境中，一些人在没有完成规定的培训和教育课程的情况下，为了就业而制作了不合法的学历证书。这种违规行为造成了真假证书的不公正混淆。因此，在招聘过程中雇主需要一种可靠的机制来验证学历证书，以确保数据的完整性。

为此，一些大学引入并部署了区块链技术支持防止欺诈或安全访问证书。然而，这些教育系统中的知识处理方法并未得到深入研究。本文介绍了一种采用区块链和本体技术的教育证书认证框架，命名为 BOCA。学习本体（LeOn）被用来代表系统的中心知识模型，用于对领域知识进行语义管理，并将教育数据链接到区块链网络。本文详细介绍了该系统的特点，包括工作流程、LeON 本体开发和规则库构建。在 Hyperledger Fabric 上部署该系统取得了可喜的实验结果。目前的工作重点是提高系统性能，并允许在数据块上进行语义搜索。

关键词：证书认证；区块链；本体；超级账本

# 介绍

证书通过描述教育过程的教育记录来认可学习者的成就[1]。证书和历史记录对学习者本人、教育机构和雇主都至关重要 [2]。面对竞争日益激烈的劳动力市场，人们倾向于寻找一种简单的方法，比如购买或伪造证书来获得工作资格 [3,4]。伪造证书问题已成为价值数十亿美元的产业、导致 30% 以上的学位都是伪造的[5,6]。因此，证书验证一直是需要妥善解决的重要难题 [7,8]。此外，任何对证书数据的篡改都应受到严格限制并易于检测 [7]。根据这一目标，区块链概念被引入到学习和教育领域的信息通信技术中，具有去中心化系统的特点，包括透明性、真实性、完整性等。

一般来说，区块链是一种将数据存储在分布式、不可更改的账本中的尖端技术，在这种账本中，无论是单一实体或第三方都无法控制数据库。因此，基于区块链的系统的可靠性和权威性都能得到保证，从而有助于保护欺诈行为，并根据学习者、公司和教育机构的需求安全地获取证书[1,9-11]。虽然区块链已在各种证书管理系统研究中被采用，但在这些系统中处理知识以实现教育目标的方法却没有得到深入研究。本体作为语义网的核心，在表示知识模型和语义推理方面以显示出其能力[12]。各种本体论已成功应用于教育学科，如智能学习或基于游戏的学习[13,14]。

本研究介绍了一个利用区块链和本体技术的教育证书认证系统原型，名为 BOCA。学习本体（LeOn）作为知识管理中心被引入 BOCA 系统，用于获取教育知识并与区块链网络协作。基于 FOCA 的本体验证方法证实了 LeOn 本体的准确开发。在 Hyperledger Fabric 环境中部署了测试系统性能的实验，测量了写入和读取的效率。实验结果表明BOCA 系统的可靠性和建议方法的充分性。

本文其余部分的组织结构如下。第 2 节介绍了这项工作的的背景以及基于区块链的证书认证和教育本体方面的相关研究。第 3 节详细介绍了 BOCA 系统，第 4 节介绍了 LeOn 本体的验证和系统性能的测试结果。最后，第 5节给出了结束语并概述了未来的研究目标。

# 背景和相关工作

## 区块链和相关技术

发明了比特币的中本聪提出了区块链的概念[15]。基于区块链的数据库按顺序存储加密的数据块，其中包含分布式数字分类账、去中心化和独立的点对点交易以及共识机制等尖端计算技术[16]。

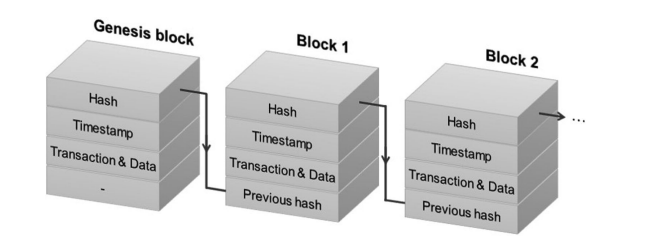


图1.区块链

图 1 展示了区块链的示意图，其中每个区块由一个唯一的加密哈希值标识，并参考前一个区块的哈希值，从而形成一个区块链。更改链中某个区块的数据是不可能的，因为这需要对该区块之后的所有区块进行持续更改。换句话说 区块链是一个不可变的网络[3]。

2014 年，Vitalik Buterin 推出了以太坊，作为基于区块链技术的开源

平台[17]。以太坊的代币(以太币）和以太坊虚拟机（EVM）允许开发人员

实现去中心化应用。以太币可用于支付交易费用、服务或气体等各种用途，而 EVM是以太坊网络中的软件，使用气体来部署和运行智能合约功能。

智能合约由尼克-萨博（Nick Szabo）提出，是一种执行合约条款的计算机化交易协议[18]。为了确保交易双方之间的信任，以及恶意或意外例外情况的发生，有人建议将合同条款（如抵押、担保）编纂并嵌入系统[19]，在区块链背景下，合同条款和条件是存储在区块链网络中的脚本，可以简化合同条款、自动执行合同并验证履行状态[9,20]。

区块链及相关技术已广泛应用于金融市场[21]、营销服务[22]和物联网[23]等领域。教育领域已在正式学习环境（如学习内容、学习者成绩或学历证书）和非正式学习环境（如研究兴趣、个人技能或学习经历）中利用了区块链的优势[9-11]。本研究旨在概述基于区块链的证书认证方法，并阐明这些方法与我们提出的方法之间的差异。有关区块链在教育领域应用的更多详情，请参阅最近的调查报告[9,24]。

# 2.2. 基于区块链的证书认证

证书的物理形式（如纸质记录）在呈现学习者的全部信息、存档、认证等方面存在许多局限性。在展示整个学习者的信息、存档、认证等方面有许多局限性。

数字形式的证书(如开放徽章1 ）旨在克服这些限制。尽管全球范围内已经推出并部署了多种证书数字化解决方案，但使用中央数据库 在确保信任、透明度和依赖性方面仍然存在制约因素。区块链利用去中心化的优势，有望压倒此类解决方案 利用去中心化方法的优势。然而 然而，区块链在大学或机构中的部署还处于原始阶段[10,24]。

一些大学已经开发了基于区块链的证书 认证系统，如麻省理工学院（MIT）、尼科西亚大学、伯明翰大学和开放大学知识媒体学院。Blockcert 是麻省理工学院媒体实验室开发的基于比特币的区块链系统，可以创建、查看和验证证书[25]。在更高的发展阶段，麻省理工学院颁发的文凭既有实体形式，也有数字形式。物理和数字形式的文凭。由于 Blockcert是在比特币平台上运行的，因此有一些局限性，如交易费用高、比特币平台的可扩展性问题 交易、比特币网络的可扩展性问题，以及所颁发证书的检索能力。最近的研究文章[26-28] 提出几种解决io ns增强Blockcert的方法。在另一项努力中、 希腊国家研究和教育网络开发了 GRNET 系统，该系统将整个验证过程与哈希值[29]的详细验证过程存储在 Cardano 平台上。

此外，Prinz 等人[1]提出了一个区块链平台，支持伪造保护、安全访问，并根据利益相关者的需求管理证书。Ocheja 等人[30]提出了一种管理学习证据的区块链，名为 BOLL（学习日志区块链），日志的权限和所有权被映射并存储到智能合约中。Guo等人[31] 利用公共和私有区块链在在线教育管理系统中展示数字权利。Bore 等人[32]介绍了如何将生物识别数据、文件和图像散列并存储在区块链中。在 Khandelwal 等人[3]提出的系统中，创建的证书在星际文件系统中通过 SHA-2S6 算法进行唯一散列。

虽然现有研究介绍了在区块链网络上创建和存储证书的解决方案，但对本体知识模型的使用还没有进行深入研究。本研究 本研究提出了一种基于区块链的证书认证系统，该系统结合本体论来捕捉学习活动的知识，并与区块链网络交互。

# 2.3. 教育本体论

Berners-Lee等人[12]发明了语义网，强调了本体在通过知识规范过程建立知识模型中的重要作用。此后，文献中提出了多种本体工程方法(OEM)[ 33-35]。大多数本体设计方法都是人工操作的，因此这些方法中的某些步骤通过应用语言学、统计学或机器学习方法实现了自动化[ 36-38]。为了服务于本体的实施，人们提出了一系列描述不同语义层次的语义网语言。例如，资源描述格式(RDF)是数据交换的标准，其派生版本是RDF-schema(RDFS)，在RDF词汇表的基础上提供类和相关属性。本体网络语言 (OWL)及其第二版--OWL-2用于代表丰富而复杂的事物知识。语义网规则语言(SWRL)旨在丰富OWL的表达能力，并创建业务逻辑。本体论已被广泛应用于教育领域的不同方向，如基于游戏的学习[14]、学习风格模型的整合[39]或智能学习[13]。关于教育领域基于语义网的应用的更多详情，在以下调查中找到有用的信息[40-42]。

据我们所知，本研究是首次在教育证书认证领域引入区块链和本体技术的混合系统。所提出的方法与以往的研究不同，主要体现在以下两点。首先，学习操作的语义信息由本体论模型提供。其次，SWRL规则集推断学习数据并将其传输到区块链网络。下文将详细介绍这种拟议方法。

# BOCA的系统结构

本节主要介绍BOCA系统的工作流程，本体模型和规则集

# 3.1. BOCA的工作程序

图2展示了BOCA系统的工作流程。参与者包括教育机构（如学校、学院、大学)、讲师(如教授、助教)、学习者（如学生）和证书申请者（如公司、组织、企业)四大方面。最初，新学员在教育机构注册时会分配到自己的ID。在ID的识别管理方面，教育机构可以利用学员的国家ID和本地ID，以确保学员ID的唯一性。此外，建议该机构使用W3CDecentralised lDen- tifier (DID)，这是一种新型标识符，可实现可验证和分散的数字身份。

接下来，讲师根据LeOn本体论中定义的知识对学习者的表现进行评估，并将结果提交给机构。各机构的教育管理系统可能各不相同，因此这些数据的格式应与知识模型中的要求相同，此后，教育数据将被允许插入 BOCA 系统，在此阶段称为链外数据。一旦认证要求得到满足，嵌入知识模型的脚本就会根据实施的规则对其进行验证。然后，教育数据 (如学习者 ID、证书ID、数字签名) 会通过创建证书交易自动传输到区块链上。

最后，机构为学习者颁发学位/证书文件，证书代码存储在区块链网络中。证书代码建议采用二维码形式，以便于追踪[43]。公司或组织可以通过为学习者颁发的证书代码查询区块链交易中存储的数据，从而检查证书的有效性。这种方法有助于教育机构保持证书的安全和透明，也有助于企业招聘合格的候选人。

# 3.2. 本体论模型的开发

本体开发的NeOn方法是最著名的方法之一，它易于理解 le,面向场景，并可用于支持文档[44]。BOCA 系统的 LeOn 本体是通过本体工程师和领域专家之间基于 NeOn 的协作过程构建的。构建LeOn 的本体工程三步流程概述如下。首先，邀请学习领域和区块链领域的本体工程师和专家协同工作。建议他们使用知名的本体建模工具，如 Protege7 或TopBraid Composer ，并在 Github 等协作项目环境中工作。9其次，通过本体需求规范文档确定 LeON本体的需求规格，本体应满足这些要求，以涵盖预定义领域的知识。最后，对现有本体资源(如 FOAF,10OWL Tme11)的重用进行了详细的规划。专家只需花费时间和精力开发本体的主要元素，其他人则可以

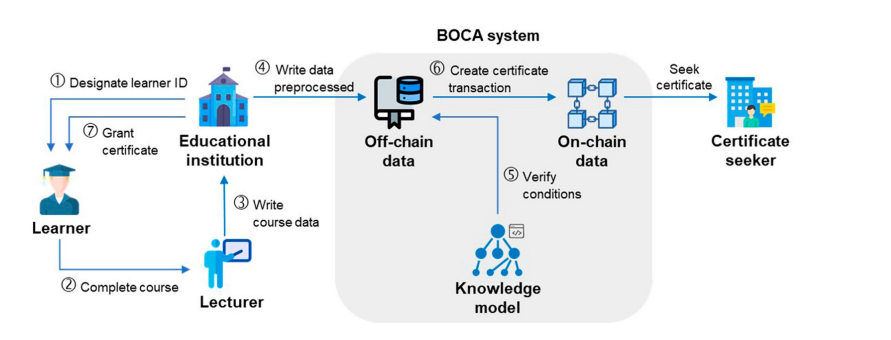


图2.BOCA系统的工作流程

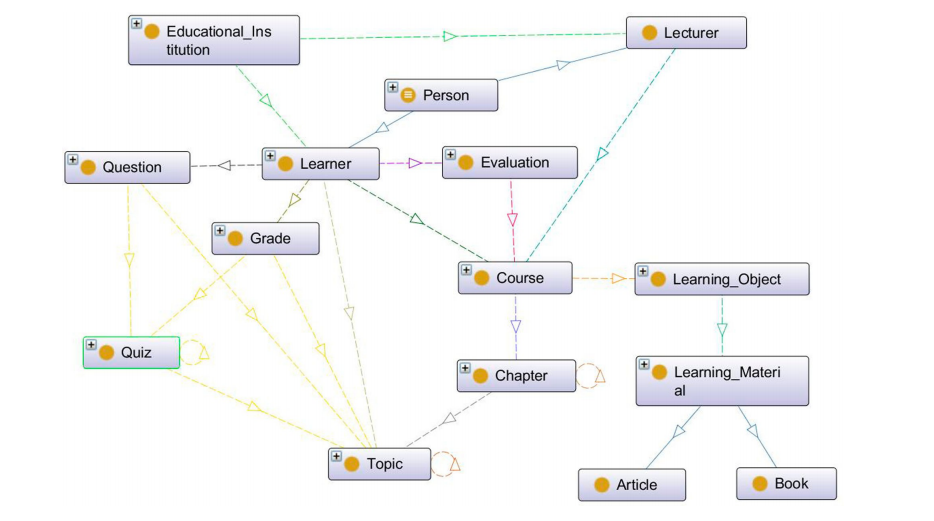


图3.LeOn本体论节选

重复使用。这三个步骤要反复进行多次，直到所有项目成员达成共识。

图3 显示了 Protee 的 OntoGraf 插件生成的 LeOn 本体的摘录。在 Protege中，对象属性用于创建类之间的关系。对于每种关系，应分别指定与源类和目的类相对应的域类和范围类。在 OntoGraf视图中，层次关系通常由浅蓝色实心弧线表示(如图 3 中从“人类到“讲师”类的弧线) 。由领域和范围类定义的其他类型的关系用不同颜色的虚线弧表示 (例如图 3 中课程类和学习对象类之间的 leOn:has 关系)。

**3.3，规则集的构建**

本研究的想法是利用OWL/SWRL的灵活性来表达学习活动尤其是认证。为了 构建 LeOn 本体，领域专家首先解释了使本体满足实际要求的公理语句。然后，本体论工程师将这些规则用自然语言编码为 SWRL规则。这套 SWRL 规则和 LeOn本体由 e与 Protege[45] 集成的本体推理器 Pelet 进行推理。简而言之，SWRL规则具有如下形式:

前件一后件

其中，前件和后件都由原子组成*a*1 ∧ *a*2 ∧ *...* ∧ *an*原子的形式可以是 C(x)、P(x, y)，其中 C是 OWL 描述P是 OWL 属性，x、y是变量。表 1列出了根据领域专家建议的自然语言规则开发的 SWRL 规则示例。例如，"校长需要注册数字签名以进行认证“的规则被转移到了SWRL 规则中，如第1条。

表1.SWRL规则示例

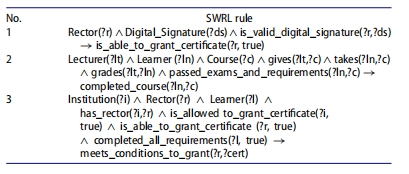


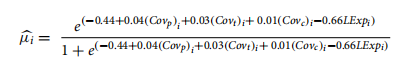
表 1.第二条规则表达了讲师、学员和课程之间的关系，即学员必须通过讲师给出的所有考试和课程要求，才能完成课程对于第三条规则，它描述了认证的条件，如机构有权颁发证书或学习者完成所有要求。

我们实施了一套简单的基于 java 的脚本，在语义 SWRL规则和区块链之间发挥桥梁作用。它可以捕捉学习者满足毕业条件的时间，然后将证书中的数据传输到区块链上。由于区块链是一个不可变的网络，因此根据各机构的认证设置，将数据存储到区块链上还需要经过人工批准

**4.LeOn 本体论的验证和 BOCA系统的实验**

**4.1.验证LeOn 本体论**

本体应经过验证，以确保其可行性。本研究采用了一种基于FOCA 技术的特定指标[46]。来验证由此产生的本体。我们收集了一系列问题，以询问专家对 LeOn 本体论的判断，这些问题遵循三个目标: (i) 目的和范围;(ii) 概念和关系的完整性;(ii) 跨领域本体论的覆盖能力:() 目的和范围;(i) 概念和关系的完整性;(iii) 跨领域本体的覆盖能力。共有 12 个问题与这些目标相关。这些问题的答案以 0-100 分的范围收集，并根据公式(1) 计算。



其中

*Covp*是目标 1类别问题的平均得分; *Covt*是目标 2 类别问题的平均得分;*Covc*是目标 3 类别问题的平均得分;*LExp*是评估者经验的权重。

本次评估过程邀请了七位学习领域的专家，由七位本体论工程师提供支持。所有专家都拥有博士学位，并在与本研究主题相关的领域工作。图4 显示了由专家评估的收集数据的分布情况，而表 2则显示了 FOCA 指标和对专家评分的 KruskalWallis 分析。

在图 4 中，最高分 88.5 分和最低分 42.9 分分别由专家 1 和专家 4 获得。如表2所示，Kruskal Wallis 检验结果的p值为 0.0686 (> 0.05) ，这意味着专家之间没有显著的评分差异。FOCA 得分为 0.9846，表明 LeOn 本体结构可靠，质量较高。不过，它仍需进一步改进，以获得更好的专家平均分。

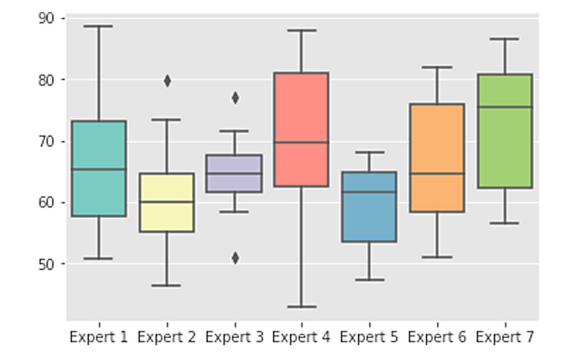


图4.收集到的数据分布

**4.2，实验设置**

为了证实 BOCA 系统的可行性，本实验旨在实际应用该系统。BOCA 区块链在 Hyperledger Fabric 中实现，HyperledgerFabric 是由 Linux 基金会 Hyperledger 项目托管的许可区块链平台。12 该平台支持模块化共识协议，允许构建、部署和定制具有保密性和隐私性的区块链应用[47]。图 5 显示了 Fabric 网络中的标准交易流程，其中有三个

节点的角色:客户、认可/承诺对等方和订购服务。图5中的交易流程可概括为以下几点。首先，客户准备一份交易建议书并发送



表2.指标得分

将其发送给背书同行。背书同行验证签名并执行交易，然后将验证值作为建议回复或背书发回客户端。接下来，客户端收集背书并将其广播给订购服务。在这里，订购服务会创建一个嵌入认可事务的区块，然后将其发送给所有对等方。最后，每个对等方提交交易，并将新区块插入其分类账中。订购服务在创建建议部署在多台设备上的区块中发挥作用该服务可以单机模式或 Kafka 模式运行。单机模式使用单个订购服务节点来执行所有交易订单，而 Kafka 模式则通过Kafka 集群中的分布式节点来执行此类订单。

在本研究中建立在由两个组织组成的 HyperledeelFabric 集群上，每个组织贡献两个对等节点。订购服务在另一个节点上以单机模式和默认参数运行。在区块链上提交交易需要每个组织至少有一个对等节点的签名。同行使用五台机器客户使用四台机器。使用 Java 版 Hyperledger Fabric GatewaySDK 开发多线程客户端，同时与区块链对等机进行交互。客户机和对等机配置相同 (i5 或 i7 CPU 、16 GB 内存和 1TB 硬盘)，运行 Ubuntu 14.04.6 LTS (Trusty Tahr ) 操作系统。所有机器都连接到实验室的局域网。网络带宽的设置足以不限制交易和数据传输的数量。

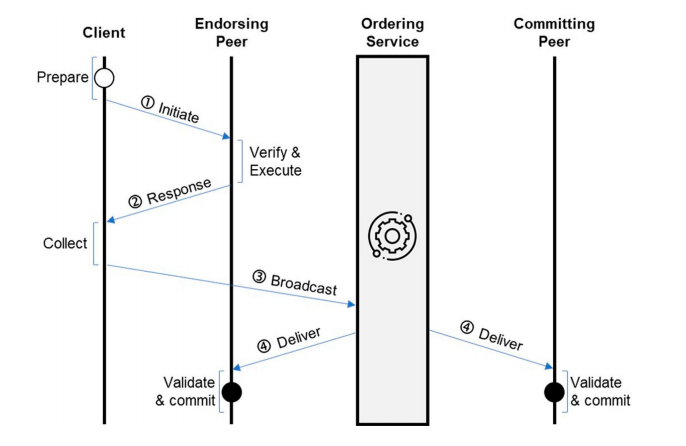
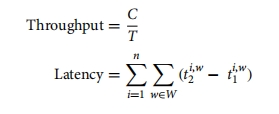


图5.Hyperledger Fabric中的交易流程

**4.3.实验结果**

为了评估系统的实施情况，本实验采用了吞吐量和延迟指标，分别由公式(2) 和(3) 计算得出。



其中

C 是成功提交到分类账的交易数量;

T是 C 单位所用的时间;

n 是交易次数;

W 是广播、认可和提交等工作负载的集合;

t2i,w 和t1i,w 分别是第i个时间段的结束时间和开始时间。

具体来说，吞吐量是指每秒成功提交到分类账的交易数量而延迟则是通过将每个工作负载中的延迟相加来计算的，延迟以交易发送和处理的时间段来衡量。在 LeOn 本体上进行语义推断所消耗的时间也被计算在内。包

利用吞吐量和延迟这两个指标来评估系统性能，同时考虑以下因素的影响: () 交易速率; (i) 交易数量;(ii) 交易次数

在每个实验中，通过不同的输入来测量学生的写作和阅读能力在每次实验中，都会通过不同的输入来测量书写和阅读性能书写性能考虑的是进行书写操作的事务，而阅读性能考虑的是进行阅读操作的事务。

阅读性能涉及的是向区块链请求教育数据的交易。以下每个实验中显示的结果均为 100 次重复试验的平均值。

**4.3.1交易费率的影响**

在本实验中，交易率被定义为在一秒内发送的达到事务数（tx/s).图6显示一旦交易速率发生变化，就通过吞吐量和延迟值对写入和读取能力进行测量。

其中，写入性能在每秒 800 次到达事务处理时达到最高吞吐量 769 tx/s，然后随着传输速率的增加而大幅下降，接近 0x/s。同样，读取性能在每秒 1000 次到达事务处理时达到 923tx/s 的最高吞吐量，然后在峰值之后开始下降。写入和读取性能的延迟线形状相似，在 200 到 2000 tx/s 的事务速率范围内持续增加。

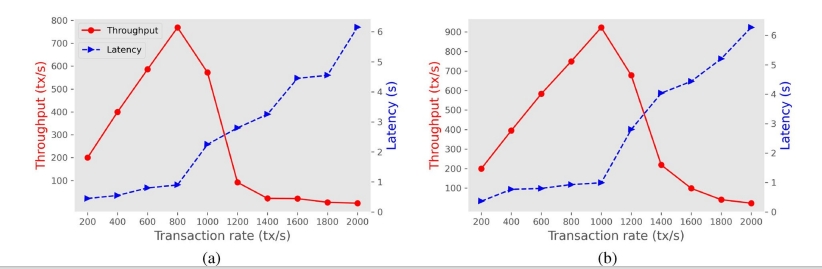


图6.事务处理率对写入和读取性能的影响 (a) 写入性能。(b) 读取性能

从图 6 中可以看出，BOCA 系统可以有效处理高达1000 x/s 的事务，延迟时间不到一秒。虽然知识模型的教育逻辑运行很费力，但整个系统还是取得了可喜的成绩。

**4.3.2.交易数量的影响**

第二个实验涉及交易数量对区块链的影响。为了分析这种影响，我们生成了 1000 到 -128,000 个单位的交易，并分别以 800tx/s 和 1000 x/s 的速率发送到区块链，以测量写入和读取性能图 7 显示了这些性能在不同交易数量下的吞吐量和延迟值。如图 7所示，事务数量对写入和读取性能没有显著影响。当事务数少于 32,000 个时，吞吐量和延迟指标保持在稳定值 (小于一秒)。

超过这一点后，这两个指标的平均值都趋于降低。显然，在本次实验中，受限的机器支持了大量的交易。

**4.3.3.组织数量的影响**

区块链网络的可扩展性是评估区块链性能的一个非常重要的问题。可扩展性可以通过许多因素来衡量，如对等体数量、通道数量、组织数量和共识机制。本研究选择组织数量作为衡量BOCA系统可扩展性的典型标准。研究人员实施了与现有两个组织配置相同的其他组织。图 8 显示了组织数量增加时的写入和读取性能。就写入性能而言，在 400 tx/s 的传输速率以下，4个和6个组织的配置具有相似的吞吐量和延迟。超过这一点后，这两种配置在吞吐量和延迟方面都出现了差距。不出所料，10 个组织的最大设置产生了最低的吞吐量和最高的延迟。关于读取性能，如果交易速率不超过 600 /s，这些设置的吞吐量差别不大。当交易速率超过 600 tx/s 时，虽然4、6和8个组织的配置基本保持了吞吐量的线性增长，但 10 个组织的最高配置性能较低。显然，写入性能在很大程度上取决于组织的数量而不是阅读表现。

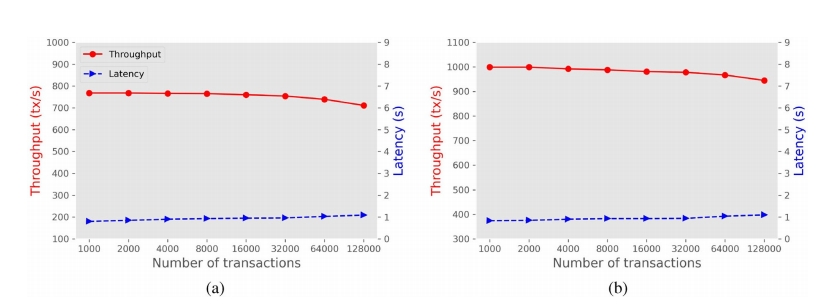


图7.事务数量对写入和读取性能的影响。(a) 写入性能。(b) 读取性能

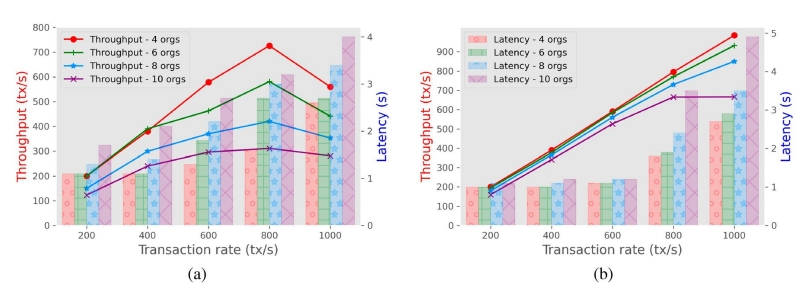


图8.机构数量对写入性能和读取性能的影响。(a) 写入性能。(b) 读取性能

**5.结论**

本研究针对开发教育证书管理系统这一关键问题，提出了一种基于区块链的教育证书认证系统。BOCA系统利用LeOn本体作为原子知识模型，捕捉学习活动的知识，并与区块链网络交互。详细介绍了 BOCA 系统的新型混合方法，包括工作流程LeOn 本体的开发和规则集的构建。LeOn 本体论通过基于FOCA 的方法论进行了验证，以确保其构造良好。区块链网络部署在 Hyperledger Fabric 中，以证明其可行性。通过改变交易速率、交易数量和组织数量，利用吞吐量和延迟这两个指标来确保写入和读取性能。本文没有将所提出的方法与其他解决方案进行比较。据我们所知，比较通常需要一个黄金数据集或相关研究的通用评估指标，如 F1 指标、精度/召回指标，而本研究范围内不支持这些指标。这就是本研究的原因、Hyperledger Fabric 被选为评估 BOCA 实施性能的平台。由于 BOCA 系统采用了知识模型和区块链网络相结合的混合方法，因此可以获得以下好处。首先，教育数据由可靠的知识模型管理。其次，可以从语义上支持教育信息检索。最后但并非最不重要的一点是，可以将知识模型扩展到法律或安全等其他领域。在进一步的工作中，BOCA 系统可以通过在不同的环境中部署不同的设置或支持授予证书的集成来进行扩展。此外，LeON本体论将得到改进和扩展，以涵盖跨领域并支持证书块的语义搜索。

参考文献

[1] Gräther W, Kolvenbach S, Ruland R., et al. Blockchain for education: life

long learning passport. ERCIM News. Proceedings of 1st ERCIM Blockchain

workshop 2018, European Society for Socially Embedded Technologies

(EUSSET) (2018).

[2] Li H, Han D. EduRSS: a blockchain-based educational records secure stor

age and sharing scheme. IEEE Access. 2019;7:179273–179289. doi:10.1109/

ACCESS.2019.2956157.

[3] Khandelwal H, Mittal K, Agrawal S, et al. Certificate verification sys

tem using blockchain. In: VK Gunjan, S Senatore, A Kumar, X-Z Gao, S

Merugu, editors. Advances in cybernetics, cognition, and machine learn

ing for communication technologies. Springer Singapore; 2020. p. 251–257.

doi:10.1007/978-981-15-3125-5\_27

[4] Rampell, C. The college degree has become the new high school degree.

The Washington Post. 2014. https://www.washingtonpost.com/opinions/

catherine-rampell-the-college-degree-has-become-the-new-high-school

-degree/2014/09/08/e935b68c-378a-11e4-8601-97ba88884ffd\_story.html

[5] Attewell P, Domina T. Educational imposters and fake degrees. Res Soc

Stratif Mobil. 2011;29(1):57–69. doi:10.1016/j.rssm.2010.12.004.

[6] Bear J, Ezell A. Degree mills: the billion-dollar industry that has sold over a

million fake diplomas. New York, USA: Prometheus Books; 2012.

[7] Bahrami M, Movahedian A, Deldari A. A comprehensive blockchain-based

solution for academic certificates management using smart contracts. 2020

10th International Conference on Computer and Knowledge Engineering

(ICCKE); 2020. p. 573–578. doi:10.1109/ICCKE50421.2020.9303656

[8] Malsa N, Vyas V, Gautam J, et al. Framework and smart contract

for blockchain enabled certificate verification system using robotics. In:

M Bianchini, M Simic, A Ghosh, RN Shaw, editors. Machine learn

ing for robotics applications. Springer Singapore; 2021. p. 125–138.

doi:10.1007/978-981-16-0598-7\_10

[9] Chen G, Xu B, Lu M, et al. Exploring blockchain technology and its

potential applications for education. Smart Learn Environ. 2018;5(1):1.

doi:10.1186/s40561-017-0050-x.

[10] Sharples M, Domingue J. The Blockchain and Kudos: a distributed system

for educational record, reputation and reward. In: K Verbert, M Sharples, T

Klobučar, editors. Adaptive and adaptable learning. Lyon, France: Springer

International Publishing; 2016. p. 490–496.

[11] Skiba DJ. The potential of blockchain in education and health care. Nurs

Educ Perspect. 2017;38(4):220–221. https://journals.lww.com/neponline/

Fulltext/2017/07000/The\_Potential\_of\_Blockchain\_in\_Education\_and.17.

aspx

[12] Berners-Lee T, Hendler J, Lassila O. The semantic web. Sci Am.

2001;284(5):34–43.

[13] Lalingkar A, Ramnathan C, Ramani S. Ontology-based smart learning envi

ronment for teaching word problems in mathematics. J Comput Educ.

2014;1(4):313–334. doi:10.1007/s40692-014-0020-z.

[14] Tsatsou D, Vretos N, Daras P. Adaptive game-based learning in multi-agent

educational settings. J Comput Educ. 2019;6(2):215–239. doi:10.1007/s40692

-018-0118-9.

[15] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized

Bus Rev. 2008;21260.

[16] Crosby M, Pattanayak P, Verma S, et al. Blockchain technology: beyond

bitcoin. Appl Innov. 2016;2(6–10):71.

[17] Wood DD. Ethereum: a secure decentralised generalised transaction ledger.

Ethereum Proj Yellow Pap. 2014;151(2014):1–32.

[18] Szabo N. Smart contracts. http://szabo.best.vwh.net/smart.contracts.html;

1994.

[19] Szabo N. The idea of smart contracts. Nick Szabo’s Pap Concise Tutor.

1997;6(1).

**附英文原文：**

