文章编号:1671-4229(2019)04-0083-06

基于区块链技术的学历学位证书认证设计

胡 莹[1],李志宏[2*],刘杰容[3]
(1. 广州大学 网络与现代教育技术中心,广东 广州 510006; 2. 华南理工大学 工商管理学院,广东 广州 510641;
3. 广州大学 计算机科学与网络工程学院,广东 广州 510006)

摘 要:国内目前学历学位认证存在流程复杂、耗费时间长、认证收费高等问题,难以满足毕业生和用人单位快速、公正、准确地核实信息的需求,无法实现创新应用. 区块链技术具有去中心化、防篡改、可追溯、信息更改留痕等特点,能够有效解决目前国内学历学位认证存在的问题. 在分析国外已有基于区块链技术发放教育文凭的项目后,文章提出一种基于联盟链(Hyperledger Fabric)的学历学位证书认证平台,进行了架构设计,包含业务系统层、区块层、服务层、应用层. 平台节点分为教育管理部门、可信高校、学生和用人单位四类,并描述了注册数字身份、颁发数字学历学位证书、验证学历学位证书三大功能流程. 平台技术采用基于授权的共识机制提高性能;仅存储数字文凭的哈希值,有效保护了个人隐私. 本研究尝试从学历学位认证模式和技术上进行创新.

关键词:区块链技术;联盟链;学历学位证书认证;哈希值
中图分类号:G 40-058 文献标志码:A

学历学位证书是获得者学习经历和水平能力的有效证明,是用人单位挑选人才的重要依据. 目前,教育部把学信网作为中国高等教育学历学位证书网上查询认证指定的唯一中心化网站,但是由于网络防伪技术的不完善,学历学位资料收集不齐全,社会对公章认同度高等原因,导致中心化认证流程复杂、耗费时间长、效率低下、成本增加等问题,不能满足毕业生和用人单位快捷、公正、准确的核实学历学位信息的需求[1]. 为此,2016 年工信部发布了《中国区块链技术和应用发展白皮书》[2],指出"区块链系统的透明化、数据不可篡改等特征,完全适用于学生征信管理、升学就业、学术、资质证明等方面,对教育就业的健康发展具有重要的价值."2018 年 4 月,教育部发布《教育信息化 2.0 行动计划》[3],明确"区块链技术的迅猛发展,将深刻改变人才需求和教育形态". 在高等教育阶段,由高等教育机构颁发的证书,特别是资格和业绩记录,使用区块链技术永久可靠的获得,存储和验证整个学习过程中正式和非正式成绩的完整记录,用户能够直接根据区块链自动验证证书的有效性,这将实现去中介机构,大大减少中心化机构验证证书的必要性. 本文将基于国内高校学历学位管理模式,提出基于联盟链的学历学位证书认证平台,提供一种可信、有效、开放的解决方案.

1 相关研究

1.1 基于区块链技术的学历学位证书认证研究现状

中国目前区块链技术应用于教育领域还在初期探索阶段,但在国外已有较多应用案例. 2017 年年底,欧盟出版机构率先发布了一份长达 130 余页的《区块链的教育应用》白皮书,该白皮书中提到区块链技术在正式和非正式学习认证中的应用,探索性研究了去中心化账本,特别是基于区块链的分类账本可能给教育部门利益相关者带来的价值,关注其对个人学习和高等教育数字认证的潜力[4]. 2016 年,麻省理工大学(MIT)发布了区块链证书项目 BlockCerts[5],设计了一个基于比特币区块链的数字学术证书认证系统. 系统分为发布者(Issuer)、查看者(Viewer)、模式(Schema)三个模块,数字文凭发行者签署证书并将哈希值存储在比特币分类帐中. 从项目实施效果看,BlockCerts 解决了数字证书的完整性,但由于比特币系统采用的是工作量证明机制(POW),虽然安全性较高,但是共识周期长、算力耗费巨大,并且在区块链注册时存在延迟,导致系统效率低.

其他国家政府的区块链学历学位证书认证应用包

基金项目:广东省省级科技资助项目(2017A070713036)
作者简介:胡 莹(1982—),女,高级实验师. E-mail:huying@gzhu.edu.cn
* 通信作者. E-mail:bmzhhli@scut.edu.cn

括:肯尼亚政府与IBM尝试合作建立基于区块链技术的学历证书网络发布与管理平台,力图实现学历证书的透明生产、传递和查验[6];希腊国家教育网络(GRNET)将文凭的哈希存储在区块链中,以保护学生的数据[7].通过验证Cardano区块链上的学生文凭,减少手工验证过程和假文凭的情况;伦敦大学与Gradbase合作,利用比特币区块链验证文凭真伪,打击简历造假行为[8].这些案例都是使用公有链进行设计和构建,存在加密和解密效率低的问题,而且随着数字证书在分布式总账中存储空间增大会导致效率问题更加严重.

综合国外已有的学历学位证书认证研究与应用,区块链技术已为毕业生、用人单位和学校提供了证书获取、分享和认证的一站式服务,这对我国现有集中认证模式反思、去中介化平台构建与运营提供了实践经验.基于国外应用经验存在的问题,分析现有区块链架构特征,选取适合我国的学历学位证书认证的技术架构,通过改进计算能力和存储方式来提高认证效率.

1.2 区块链架构与应用

根据组成节点的类型,区块链可分为三种类型[9],而这三种类型所覆盖的范围也是不同的.

(1)公有链(public blockchains)

公有链的优势是开放性好,节点分别属于众多不同的组织和个人,理论上任何计算机设备都可以自由加入系统,都可读取、发送交易进行有效性确认,都能参与其共识过程的区块链,共同维护公共区块链数据的安全、透明、不可篡改.比特币系统[10]、以太坊[11]等最著名的区块链系统均为公有链.

(2)私有链(private blockchains)

私有链的优势是安全、隐私性质较好,所有节点属于同一个组织,只有获得管理员批准的计算设备才可以加入系统,数据的访问及使用有严格的权限管理,写入权限仅在参与者手中,读取权限可以对外开放.目前我国各大银行内部运行的区块链系统大多属于私有链.

(3)联盟链(consortium blockchains)

节点属于有紧密联系的若干组织或个人,参与区块链节点是事先选择好的,节点间通常有良好的网络连接等合作关系.联盟链是介于公有链与私有链之间,由一组管理员来共同协调管理.联盟链是开放性与安全隐私的折中,目前我国金融界的跨企业区块链系统大多属于联盟链.

本文中,笔者将基于Hyperledger Fabric构建学历学位证书认证系统.Hyperledger Fabric[12]是由IBM带头发起的一个联盟链项目,于2015年底移交给Linux基金会,是基金会中最成熟的技术项目之一.Hyperledger的结构可分为会员服务、应用程序、节点、链代码、订购服务.Fabric支持模块化共识协议,允许系统根据特定用例和信任模型进行定制.Fabric用于许可区块链的分布式操作系统,其执行以通用的编程语言(例如go,java,node.js)编写的分布式应用程序.它在仅附加复制的分类账数据结构中安全跟踪其执行历史记录,并且没有内置的加密货币.应用程序通过Hyperledger SDK与Hyperledger网络通信.Fabric使用便携式会员概念实现许可模型,该概念可以与行业标准身份管理集成.成员服务向已识别的参与者颁发证书,包括仅允许已识别参与者参与的证书颁发机构(CA)功能,并使用证书验证其身份.目前,Fabric已用于400多个原型,概念验证、生产分布式系统,实现了跨不同行业的项目.这些项目展示了区块链技术的广泛应用,同时Fabric为区块链开发提供了透明和协作的方法.

2 基于Hyperledger Fabric的学历学位证书认证平台的构建

2.1 本文设计的教育链和BlockCerts区块链的区别

本文设计的教育链与国外现有商业化的区块链有着明显的区别,由于区块链技术在框架设计中遵守的是去中心、无监管的原则,这种构建方法不适用于中国教育管理体制.因此在设计教育链时,笔者建议从去中心化转化为去中介化,主要解决信息的持久保存、管理、共享问题.同时,保证各级管理机构可穿透式监管,不失教育链的公信力.进而,笔者从八方面对本文设计的教育链与国外现有方法进行了对比,见表1.

国内教育链的设计是希望从模式上和技术上进行创新,实现从信息互联向价值互联转换.从现有集中式管理体系向基于区块链技术的分布式、共识机制的管理,力求实现信息防伪和数据控制.区块链技术的应用,是一个全新的格局,但在设计教育链时仍应尊重现有系统的数据使用场景和数据治理规则,采取逐步改良升级的方式来实现基于中国教育管理体制的教育链.

2.2 基于Hyperleger Fabric的学历学位证书认证架构设计

基于中国学历学位证书管理模式、学历学位证书认证存在的问题,必须以改革的思路和创新的举措,实现从集中式认证向分布式、共识性机制认证建设转变,建

表 1　本文设计的教育链与 BlockCerts 区块链的对比

Table 1　Comparison between the education chain designed in this paper and the BlockCerts blockchain

项目	本文设计的教育链	BlockCerts 区块链
区块链框架	Hyperledger Fabric	Bitcoin
网络	多中心或弱中心	去中心化
发行证书	已识别的实体可以颁发证书	任何人都可以发布证书
真实性	支持	支持
共识	PBFT[13] 不需要很大的计算能力	POW 需要很大的计算能力
存储	保存证书的哈希值	保存证书的哈希值
隐私	使用 hash-and-OTP 控制提交的证书	无法控制提交的证书
应用	促进教育的公平、透明、开放	积极重构生态

设以服务驱动教育经历认证创新的新模式,推进资源整合和深度开发,构建信息防、数据可控的学历学位证书认证平台. 结合 Hyperledger Fabric 技术实现学历学位证书认证架构,系统整合的架构如图 1 所示.

基于 Hyperledger Fabric 的学历学位认证平台架构,分为四层.

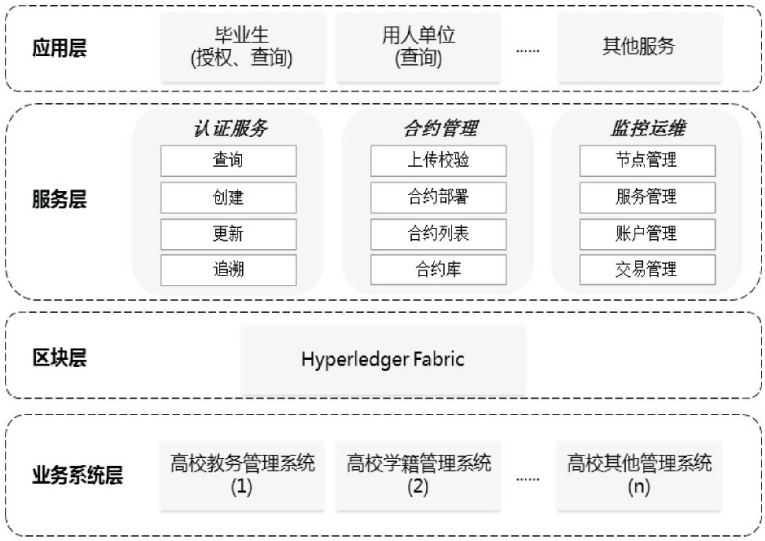

图 1　基于 Hyperledger Fabric 的学历学位认证平台架构

Fig. 1　Academic degree certificate architecture platform based on Hyperledger Fabric

(1) 业务系统层

包括国内各高等院校或地区所属部门自建的相关信息系统和教育部直管系统. 国内各高等院校基本都已建立教务管理系统,沉淀了大量的过程数据和结果数据,如学生学籍数据、学生的成绩数据等,其中部分是敏感、涉密数据,部分是可以公开、可以重复利用的数据. 依据数据治理的标准体系进行梳理,教育部只管系统,以学信网为基础,建立数据管道,实现集中数据的“上链”. 另一部分是各高等院校自主建设的系统,规范每个系统中的数据,通过密码学和算法确保多方信任,确保数据是可公开、可使用的,然后进行“上链”.

(2) 区块层

本平台架构中区块层采用 Hyperledger Fabric 架构,应用程序通过链代码将数据存储或读取到区块链中. 如果应用程序发送一个申请来调用链代码,代言人将验证申请是否正确,链代码是否正常工作. 当结果返回给应用程序时,用户将事务提交给订购服务,并发送给提交者同行. Hyperledger Fabric 不仅存储分布式分类帐,还存储名为 World State DB 的键/值 DB 中的最终状态.

(3) 服务层

平台业务应用访问区块链节点主要分为四类用户角色: ①教育管理部门,负责平台开发和运营维护,负责平台会员管理和在线服务; ②高等学校,负责相关信息登记; ③毕业生,可查询个人信息,可授权用人单位查看本人链上信息; ④用人单位,得到授权后可查看毕业生信息. 其中,教育管理部门、高等学校、毕业生作为区块

链验证节点,具有记账、读写功能,用人单位作为区块链非验证节点,不具有记账、读写功能.

Hyperledger 网络由学校组成. 每个 peer 管理 World State DB 和 Distributed Ledger,以及 Orderer 一致性,以便 Committer peer 将最终状态存储在 Distributed Ledger 和 World State DB 中. World State DB 使用 CouchDB 并存储键/值. CouchDB_Key_Value: = h(学校|部门|学生姓名|身份证号|毕业年份|学位). 其中 h 是加密安全的单向散列函数,文档二进制文件. 其值也存储在分布式分类帐中,使其不可更改.

各环节对数据进行梳理,接入区块链节点,架构中所有信息存储在分布式总帐中的个人信息文件被加密,存储在应用程序 DB 中,并且文件的哈希值存储在分布式总帐中.

(4) 应用层

基于 Hyperledger Fabric 的学历学位证书认证平台,实现了去中心化的数据汇聚,在此基础上进行教育经历认证的创新研究. 以区块链技术平台为支撑,弱化学信网的纵向中心化管理,建立横向联动的工作机制,学生正式学习和非正式学习过程中产生的信息联动和共享数据接口,建立个人教育经历模型,为每位毕业生建立信用档案,确保数据不可篡改、历史可追溯. 这种去中心化的结构,减少了人工干预、降低了成本,同时中心化系统中存在的攻击和故障问题也得到有效解决.

3 基于 Hyperledger Fabric 的学历学位证书认证平台的实现

基于 Hyperledger Fabric 的学历学位证书认证实现流程如图 2 所示,描述了数字身份的"上链"流程,基于区块链颁发数字学历学位证书,用人单位通过授权后即可查询所需的学生信息和学历学位证书信息.

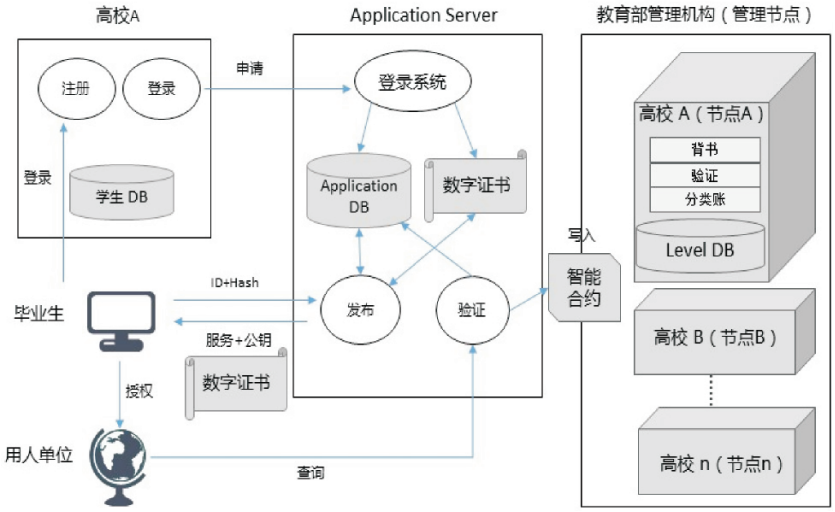

图 2 基于 Hyperledger Fabric 的学历学位证书认证流程图

Fig. 2 Academic degree certificate flow diagram based on Hyperledger Fabric

(1) 注册数字身份

①每个学校学籍管理系统都有学生信息(学校|部门|学生姓名|英文名称|出生日期|电子邮件地址|毕业年份|学位|…). 从数据库中读取学生信息,创建原始数字学历学位证书数据.

②把请求以 JSON 格式在 Application Server 的注册应用程序中注册创建数字文件和学生信息.

③Application Server 首先查找与 School ID 相对应的公共证书,并验证签名是否正确.

④验证签名后,在区块链上创建数字身份. 通过 Hyperledger SDK 调用链代码调用功能,调用的结果是向背书人同行提交交易提议. 支持者节点检查提议提交者的签名、消息格式、策略等.

⑤生成随机 AES 密钥并使用它来加密生成的文件.

⑥将加密后的文件保存到文件服务器,并记录 File_path(哈希值).

⑦应用程序在学生表中存储 primary_key |学校|学生姓名|姓名|出生日期|电子邮件地址|毕业年|度|AES-Key | File_path(哈希值).

(2) 颁发学历学位证书

①当学生要求学校签发时,学校会显示登录屏幕. 如果学生成功登录,学生将被重定向到区块链认证平台

的登录界面,其中包含学生姓名、出生日期信息和应用程序的注册应用程序.

②学生选择学历学位和毕业年份并要求发布.

③认证平台发布数字证书信息包括学校|学生姓名|身份证|毕业年份|学位信息和 File_path(哈希值).

④认证平台随机生成 OTP 并将生成的 OTP_Value 和 student_table 的 primary_key 记录在 OTP 表中.

⑤应用程序将数字学历学位证书和动态口令发布给学生.

⑥学生下载数字文件并将文件授权给用人单位.

(3) 学历学位证书验证

①用人单位访问区块链认证平台,验证应用程序并提交数字证书文件.

②调用智能合约使用获取存储的哈希值,并将需验证的数字证书哈希结果进行比较.

③如果两个哈希值相同,则通过应用程序显示验证结果正确,并在线查看数字证书.

④用人单位确认学历学位证书的真实性.

4　主要创新点

通过以上流程实现了学历学位证书的"上链",基于区块链实现的学历学位证书认证主要创新包括以下三个方面.

(1) 区块链平台实现可信的数据认证

区块链技术的最大价值在于数据的不可篡改和可验证性,基于数据信任建立起数据认证平台,进而建立起基于信任数据的个人教育经历模型,从而破局学历造假、伪造证书的现象.

平台通过教育部管理各高校节点,以及对高校学籍管理系统、教务管理系统、在校表现管理系统等业务系统进行数据共享和联动,实现高效协作的教育学习经历认证,实现互联互通、监管全覆盖,促进教育数据工作公开、标准、规范化运行,并以高效协作的方式将学历学位认证服务带入到一个全新的阶段.

(2) 去中介化,共享教育认证服务效率提升

随着传统的集中认证管理模式的成熟运行,收费认证的方式逐渐暴露出了不少弊端,高收费、乱收费现象存在于各地的认证机构之中. 去中介化的区块链平台能提供低成本的共享教育认证,简化跨机构的审批流程,提高工作效率.

将学历学位证书控制权从中介化管理移交给个人,以个人主体为对象,围绕数据、管理、安全三个维度,构建个人主体教育经历相关数据及其关系的数据集合. 在此基础上,个人授权可访问区块链中可信的个人教学经历,以此实现教育认证服务效率提升,转变认证模式,变流程审批为信任审批,变被动服务为主动服务.

(3) 构建安全的教育认证新生态

基于区块链的学历学位证书认证平台,通过使用区块链的无篡改特性来验证数字证书的完整性和真实性. 不是将原始数字证书存储在分布式分类账中,而是将数字证书的哈希值存储在分布式分类帐中,从而保护个人信息并节省分布式分类帐的存储空间. 因此,恶意节点(对等体)参与区块链网络,即使检查分布式分类帐也无法获取个人信息.

将数据记录在区块链上,使用相关的数字签名技术,从而降低信任成本,更好地规范数据管理. 通过平台的打造,以期整合现有的数据安全解决方案和区块链技术的优势,构建安全的教育认证新生态.

5　结　语

本文针对传统学历学位证书认证管理中存在的数据共享程度低、认证流程长、认证机构成本较高、认证收费高等痛点,结合区块链技术的核心优势,提出了适合于国内的基于 Hyperledger Fabric 的学历学位证书认证创新设计,从顶层角度出发,统筹建立联盟链的教育经历认证平台,各高校的相关信息系统通过抽取权限范围内的数据"上链",打破原中心化管理模式,分析了基于区块链技术建立学历学位认证的架构和实现流程,解决数据的可信问题,提高数据的使用效率,保证数据安全,实现国内学习教育经历认证模式创新和应用. 下一步,将选择部分高校开展学历学位证书认证应用的实施,充分验证学历学位证书认证效果,并根据运行的实际情况不断进行技术更新和完善,伴随着应用成熟度的提高,区块链技术将在教育领域发挥更大的作用.

参考文献:

[1] 史强. 区块链技术对未来我国高等教育的影响[J]. 高教探索,2018(10):5-13.

[2] 工业和信息化部. 中国区块链技术和应用发展白皮书[EB/OL]. (2016-10-18)[2017-12-11]. http://www.ec.whu.edu.cn/uploads/soft/171211/1_1616199501.pdf.

[3] 教育部.教育部关于印发《教育信息化2.0行动计划》的通知[Z].教技[2018]6号,2018-04-13.
[4] Grech A, Camilleri A F. Blockchain in education[J/OL]. Luxembourg: Publications Office of the European Union,2017-11-1[2018-5-26] https://www.ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-education.
[5] MIT Media Lab. Digital certificates project[EB/OL].(2016-9-1)[2018-2-1]. http://www.certificates.media.mit.edu/.
[6] Joseph Y. Kenyan government uses IBM blockchain to prevent academic certificate fraud[EB/OL].(2016-12-22)[2018-04-11]. https://www.cointelegraph.com/news/kenyan-government-uses-ibm-blockchain-to-prevent-academic-certificate-fraud.
[7] Amy C. Cardano Blockchain's first use case: Proof of university diplomas in Greece[EB/OL].(2018-01-02)[2018-06-01]. https://www.bit.ly/2DVsrYt.
[8] University College London. Academic certificates on the blockchain[EB/OL].(2018-02-01)[2018-10-02]. https://www.gradba.se/en/.
[9] 黄俊飞,刘杰. 区块链技术研究综述[J]. 北京邮电大学学报,2018,41(2):1-8.
[10] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. [2018-01-10]. https://www.bitcoin.org/bit-coin.pdf.
[11] Buterin V. A next-generation smart contract and decentralized application platform[EB/OL].(2016-01-17)[2016-11-15]. https://www.github.com/ethereum/wiki/wiki/White-Paper.
[12] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A distributed operating system for permissioned block-chains[C]//Proceedings of the 13th EuroSys Conference, Proto: Association for Computing Machinery, Inc, 2018:1-15.
[13] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems (TOCS),2002,20(4):398-461.

Academic degree certification design based on blockchain

HU Ying[1], *LI Zhi-hong*[2], *LIU Jie-rong*[3]
(1. Network and Modern Educational Technology Center, Guangzhou University, Guangzhou 510006, China;
2. School of Business Administration, South China University of Technology, Guangzhou 510641, China;
3. School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China)

Abstract: The domestic academic degree certification is inefficent in complicated process, long time and high certification fees, which makes it difficult to satisfy the needs of graduates and employers for quick, fair and accurate verification of information. It is impossible to achieve innovative application. Blockchain technology is characterized by decentralization, tamper resistance, traceability, and information change, which can effectively solve the problems existing in current domestic academic degree certification. After analyzing the foreign projects of issuing education diplomas in blockchain technology, this paper proposes an academic degree certificate platform based on the alliance chain Hyperledger Fabric, and carries out the architecture design, including the business system layer, block layer, service layer and application layer. The platform nodes are divided into four categories: education management department, trusted colleges, students and employers. It also describes the three functional processes of digital identity register, digital academic degree certificates issuing, and academic degree certificates verification. Platform technology uses an authorization-based consensus mechanism to improve performance and stores only the hash of the digital diploma, which can effectively protect personal privacy. This research attempts to innovate in the academic degree certification model and technology.

Key words: blockchain; Hyperledger Fabric; academic degree certificate; hash

【责任编辑:周 全】