doi: 10.3969/j.issn.0490-6756.2019.03.012

基于区块链技术的学籍管理系统

李中振[1], 高超越[2], 刘　敏[1], 代成琴[1], 范　轶[1]
(1. 哈尔滨工业大学网络与信息中心, 哈尔滨 150001;
2. 哈尔滨工业大学电气工程及自动化学院, 哈尔滨 150001)

摘　要: 学籍管理是高校信息化建设的一个关键模块,也是社会认证人才的重要依据.区块链技术的出现为学籍管理系统的改进提供了一种全新的思路.区块链本质上是一种分布式记账技术,其去中心化和不可篡改的特性可以保证学籍信息的安全性和真实性.本文以区块链技术、特别是智能合约在智慧校园中的应用为切入点,提出并设计了一种去中心化的学籍信息管理方案,同时基于 Fabric 框架开发了一个简单的学籍管理系统原型.

关键词: 区块链;智能合约;学籍管理
中图分类号: G623.58　　**文献标识码**: A　　**文章编号**: 0490-6756(2019)03-0450-07

Blockchain-based student status management system

LI Zhong-Zhen[1], *GAO Chao-Yue*[2], *LIU Min*[1], *DAI Cheng-Qin*[1], *FAN Yi*[1]
(1. Network & Information Center, Harbin Institute of Technology, Harbin 150001, China;
2. School of Electrical Engineering & Automation, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Student status management is a key part in university information construction and an important basis for talents certification. The emergence of blockchain technology provides a new way to improve the student status management system. Blockchain is a distributed ledger technology in nature, with its decentralized and non-tamperable features, the security and authenticity of student information can be ensured. Based on the application of blockchain technology such as smart contracts in "Smart Campuses", this paper proposes and designs a decentralized student status management systim. With Fabric framework, we developed a prototype of student status management system its demonstraiton.

Keywords: Blockchain; Smart Contract; Student status management

1　引　言

学籍系统是高校教务信息系统的重要组成部分,是完成学生学籍管理和认证的唯一途径.拥有一个良好的学籍系统,可以让行政人员的日常工作更加高效、便捷,可以让学生在校期间享有公正的受教育权利,更重要的是,可以为学生毕业后的去向单位,提供一个可信的认证依据,防止学籍学历伪造现象的产生[1].

当前绝大部分高校的学籍认证依赖于学信网下的学籍管理系统,少数高校有自己的学籍管理与认证系统,但是关于学籍的认证也会在学信网上进行.学信网极大的便利了高校的学籍管理工作,统一而不失灵活,提供权威的学籍学历认证查询等服务,为社会企业、科研院所提供了学生信息认证查询的可信依据[2].但是,也正是因为学信网的权威、统一性,其数据信息过于中心化,存在被攻击、篡改的风险隐患,一旦学信网的

收稿日期: 2018-07-31
作者简介: 李中振 (1981－), 男, 黑龙江哈尔滨人, 硕士研究生, 工程师, 研究领域为区块链相关技术及其在智慧校园中的应用.
通讯作者: 范轶. E-mail: fanyi@hit.edu.cn

学籍管理系统出现安全问题，对于高校、企业造成的影响是不可估量的. 学信网的安全问题，归根结底是因为该系统是一个“中心化”的系统，而区块链技术的出现，为中心化系统面临的数据信息过于集中，存在被篡改风险的问题，提供了一种有效可行的解决思路[3]. 区块链技术本质上是一种管理数据的新方法，具有去中心化、公开性、自治性、安全性和匿名性等特点[4,5].

本文所构建的基于区块链技术的高校学籍管理系统，把区块链技术的上述特性应用到了学生学籍信息管理中，其数据的安全性和真实性便得到了保障，而且每个节点达成共识，每个节点都作为维护网络、存储数据的一部分，减少了第三方数据管理存储的成本. 在该系统的区块链网络中，每一次数据的改动都会永久的记录在链中，链上的所有信息全部公开透明，由此保障了全部数据信息真实可溯源. 系统的每一次数字证书的查询和发放都会触发智能合约的多重签名校验，由此保证不会恶意查询[6−9].

2　开发框架的对比分析

区块链具有去中心化、去信任和不可篡改等优势特点. 特别是智能合约的出现，凭借其灵活多变、适用性强的特点，加速了区块链技术的应用进程. 然而，其基础层协议相对较为晦涩、语言欠丰富，导致其应用门槛高[6]. 因此，开发框架成为了区块链项目生态中最核心的一环. 下面将分析主流框架以太坊和 Fabric 的各自特点，说明本文基于 Fabric 进行开发的原因如下.

(1) 以太坊率先实现了智能合约的图灵完备，支持多种计算机语言的开发. 用户只要用简单的代码来实现逻辑，就能够创建一个基于区块链的应用程序，并应用于货币以外的场景. 以太坊的设计思想是不直接“支持”任何应用，但图灵完备的编程语言意味着理论上任意合约逻辑和任何类型的应用都可以被创建出来. 总之，以太坊在比特币的功能之外，旨在实现图灵完备的合约语言和内置的持久化状态存储的目标. 但是以太坊的设计原则是紧耦合，导致其扩展性较差，其共识机制采用的是 PoW(工作量证明机制)，所有的交易、发布智能合约、运行智能合约都需要消耗 GAS. 产生区块的时间也无法控制，会随着块高度的增加越来越长.

(2) 超级账本(Hyperledger)则是 Linux 基金会于 2015 年发起的推进区块链技术和标准的开源项目，目标是让成员共同合作，共建开放平台，满足来自多个不同行业各种用户案例，并简化业务流程. Fabric 是超级账本的项目之一，它的功能与以太坊类似，也是一个分布式的智能合约平台. 但不同的是，它从一开始就是一个框架，而不是一个公有链，也没有内置的代币(Token)，其共识机制允许在 No-op(无需共识)和 PBFT(拜占庭共识算法)之间选择. 作为一个区块链框架，Fabric 采用了松耦合的设计，将共识机制、身份验证等组件模块化，使之在应用过程中可以方便地根据应用场景来选择相应的模块. 除此之外，Fabric 还采用了容器技术，将智能合约代码(Chaincode)放在 Docker 中运行，从而使智能合约可以用任意的高级语言来编写. Fabric 的主要设计目标是模块化设计、组件可替换和运行于 Docker 的智能合约，其出块时间可以通过时间和交易控制，相比之下更适合灵活的应用开发[6].

因此，本文选择面向企业联盟链、灵活性和可扩展性更强的 Fabric 作为开发框架.

3　Fabric 关键技术研究及其在学籍管理中的应用

3.1　系统关键技术

Fabric 于 2017 年 07 月发布了 1.0 版本，在架构上进行了改进和重构，采用模块化架构设计，模块化的方法带来了可扩展性、灵活性等优势，会减少模块修改、升级带来的影响，能很好地利用微服务实现区块链应用系统的开发和部署.

3.1.1　*系统整体逻辑架构*　Fabric 1.0 的系统逻辑架构图如图 1 所示，其系统构建基于分布式账本技术和安全与密码学服务. 整体架构可以分为应用程序层和底层技术层，应用程序层包括身份管理、账本管理、交易管理模块和智能合约模块，底层技术层包括成员管理、共识服务和链码服务模块. 每个应用程序的实现和底层技术一一对应，身份管理对应注册登录和属性证书(Eert)，MSP 建立一套根信任证书体系，利用 PKI 对成员身份进行验证，利用 Fabric-CA 系统提供成员注册服务，并对证书进行管理. 账本管理基于分布式账本技术和 P2P 协议，完成交易需要客户端首先向背书节点提交提案获得背书，再将背书后的交易提供给排序服务节点进行交易排序，然后广播给记账节点写入本地账本，只有经过授权的用户才可以查询账本数据. 交

易管理对应排序服务和背书验证,账本数据只有通过交易执行才能更新,在交易提案提交时和排序服务之后,背书节点和记账节点会对交易进行双重交易验证. 智能合约是基于链码实现的,链码运行在安全的容器环境中,支持多种编程语言. 和以太坊相比,Fabric 链码和底层账本是分开的,升级链码时并不需要迁移账本数据到新链码当中,真正实现了逻辑与数据的分离.

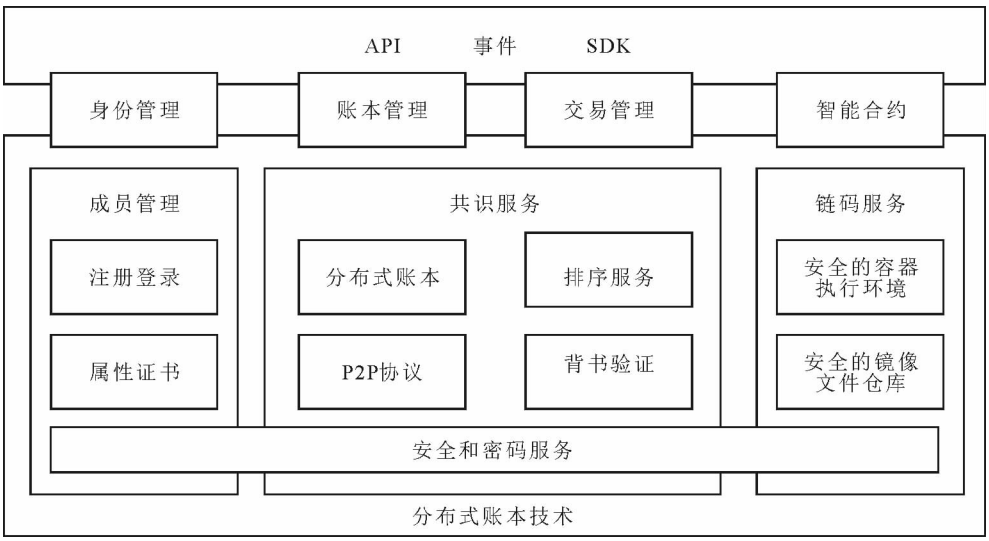

图 1 Fabric 1.0 的系统逻辑架构图
Fig. 1 Fabric 1.0 architecture diagram

通过以上架构,Fabric 框架实现了如下四大特点.

(1) 模块插件化. 功能模块可插拔,系统提供了通用的接口和默认的实现;

(2) 容器技术. 节点和链码均运行在安全的容器环境中,任何应用程序或者外部系统必须通过背书节点的转发操作链码,链码和背书节点的环境也是通过容器提供的沙箱环境隔离开,链码存在安全问题也不会影响背书节点;

(3) 可扩展性. 系统把节点分为背书节点、排序服务节点和记账节点等,多链多通道和链码可以运行在不同节点上的设置提高了并行效率和吞吐量;

(4) 安全性. 引入多链多通道的技术的基础上实现了数据的隔离,保证了使用该网络的不同组织的数据的共享的安全性.

3.1.2 网络节点结构 如图 2 所示,Fabric 1.0 的网络节点有以下几种:(1) 客户端节点. 客户端或者应用程序代表由最终用户操作的实体,它必须连接到某一个 Peer 节点或者排序服务节点上与区块链网络进行通信. 客户端向背书节点(Endorser)提交交易提案(Transaction Proposal),当收集到足够背书后,向排序服务广播交易,进行排序,生成区块;(2) Peer 节点. 每一个 Peer 节点都是记账节点,负责验证排序服务节点里的交易. 部分节点是背书节点,背书节点的角色是与具体的链码绑定的,对于某一个实例,客户端只有对实例对应的背书策略指定的特殊背书节点发起提案才是有效的,当没有触发对应链码时,该节点仅是一个普通的记账节点. 部分节点担当主节点的角色,负责在排序服务节点处获得最新的区块并且在组织内同步;(3) 排序服务节点. 负责接收包含背书签名的交易,对未打包的交易进行排序生成区块,广播给 Peer 节点. 排序服务的多通道(MultiChannel)实现了多链的数据隔离,保证只有同一个链的 Peer 节点才能访问链上的数据,保护用户数据的隐私;(4) CA 节点. CA 节点是 Fabric 1.0 的证书颁发机构(Certificate Authority),由服务器和客户端组件组成. CA 节点接收客户端的注册申请,返回注册密码用于用户登录,以便获取身份证书. 在区块链网络上所有的操作都会验证用户的身份.

每个组织都会有一条自己的专属区块链,不同链之间的数据是完全隔离的,由此保证了数据的安全性,每个组织之间的多个部门可以建立不同的通道(Channel),每个 Peer 节点可以订阅不同的通道,只有订阅后才可以查看对应通道上的数据,如此满足了不同企业的各种业务需求.

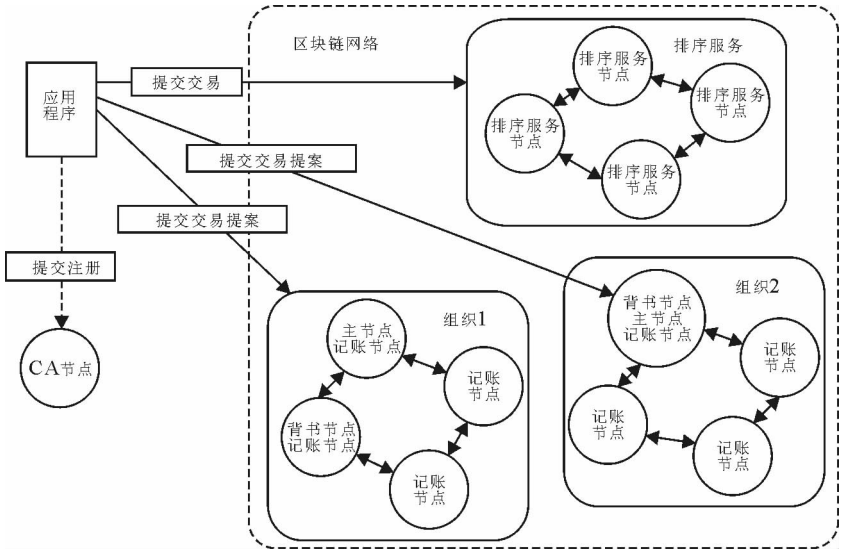

图 2　Fabric 1.0 的网络结构图

Fig. 2　Fabric 1.0 structure diagram

3.1.3　*交易流程说明*　Fabric1.0 的典型交易流程如图 3 所示. 假定各节点已经提前颁发好证书，且已正常启动，并加入已经创建好的通道. 应用程序构造好交易提案请求后，选择背书节点执行并进行背书签名. 背书节点在收到交易提案后会进行一些验证，包括：交易格式、是否双花、交易签名的有效性、交易提案的提交者在当前通道是否已授权有写权限. 验证通过后，背书节点会根据当前账本数据模拟执行链码中的业务逻辑并生成读写集(RwSet)，其中包含响应值、读写集等. 在模拟执行时账本数据不会更新. 而后背书节点对这些读写集进行签名成为提案响应(Proposal Response)，然后返回给应用程序. 应用程序收到提案响应后会对背书节点签名进行验证，网络中所有节点接收到任何消息后都是需要首先验证交易的合法性. 应用程序接收到所有的背书节点签名后，根据背书签名调用 SDK 生成交易，广播给排序服务节点. 排序服务不读取交易的内容，仅仅接收网络中所有通道发出的交易信息，按各个通道上交易的接收时间顺序对交易信息进行排序，生成区块. 排序服务节点生成区块以后会广播给通道上不同组织的主节点. 记账节点通过主节点接收到排序服务节点生成的区块，验证区块交易的有效性，提交到本地账本，至此一个交易完成.

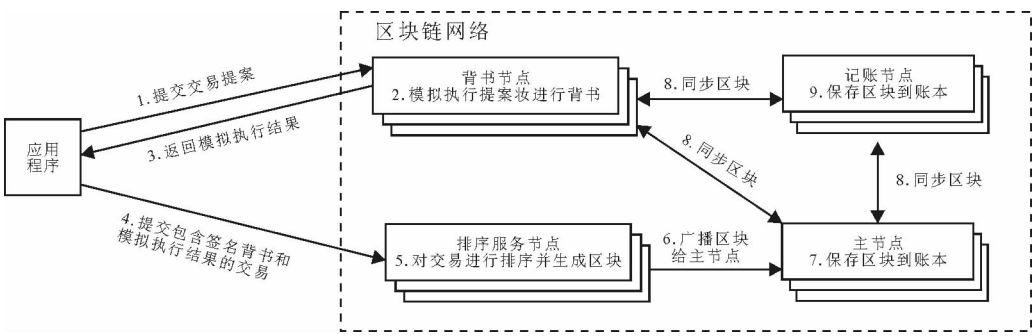

图 3　Fabric 1.0 的典型交易流程

Fig. 3　Typical transaction process of Fabric 1.0

3.2　基于 Fabric 的区块链学籍管理系统架构

如图 4 所示，学籍管理系统包括 Fabric 区块链网络、应用模块和智能合约. 其中区块链平台包含 3 种重要节点和一个数据存储服务：CA 节点用于签发本节点的自签根证书，以及管理组织成员的身份认证、授权等操作；Endors 背书节点用于智能合约代码(Chaincode)的模拟执行以及对交易请求进行背书，只有被背书后过的交易才能被提交并且最终改变账本状态；Order 排序节点对接收到的交易进行共识排序，然后按照区块生成策略，将一批

交易打包到一起,生成新的区块;CouchDB 数据存储服务用于账本数据的高效读写操作. 应用模块由 Express 框架对外提供 REST 接口,用 JWT-token 方式用于用户权限校验并由 Fabric-Node-SDK 通过 gRPC 的方式连接区块链平台进行交易的执行和查询操作. 最后,智能合约提供了外界修改和查询账本数据的能力,其内容包括合约的部署、升级、调用、执行和注销.

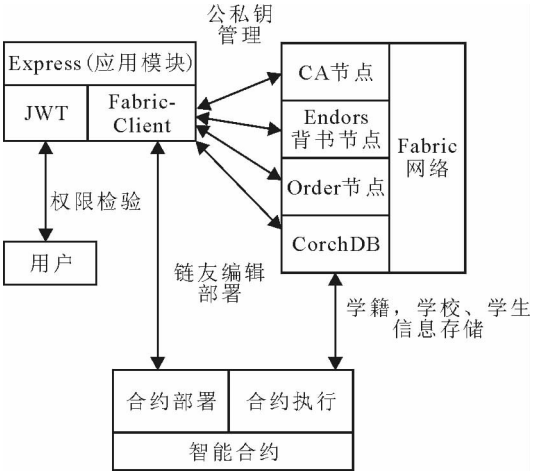

图 4 系统架构示意图

Fig. 4 System architecture diagram

4 系统最小原型的设计及实现演示

4.1 基本数据存储(CouchDB)

学校信息包括名称、地理位置;用于标识学校唯一身份的 Address;PubKey 和 PriKey 分别是学校的公钥和私钥;StudentAddress 用于存储在该学校登记入学的学生身份列表,见表 1.

表 1 学校数据表

Tab. 1 School data sheet

列名	数据类型	备注
Name	String	学校名称
Location	String	地理位置
Address	String	唯一地址
PubKey	String	公钥
PriKey	String	私钥
StudentAddress	Array	学生地址列表

学生信息见表 2,包括姓名、以及标识其唯一身份的 Address,DiplomaId 用于存储该学生学籍信息的 id 列表.

表 2 学生数据表

Tab. 2 Student data sheet

列名	数据类型	备注
Name	String	学生姓名
Address	String	唯一地址
DiplomaId	Array	学籍信息 id 列表

学籍信息表(如表 3)则由主键 id、离校时间、和离校时教育机构认定的毕业状态标志组成,其中 0 表示学生正常毕业、1 表示该学生中途退学、2 表示非正常毕业.

表 3 学籍信息表

Tab. 3 Student status information

列名	数据类型	备注
Id	Number	唯一 id
ExitTime	Number	离校时间
Status	Number	毕业状态(0、1、2)

最后,学籍操作记录表(如表 4)用于存储学籍的变更信息,操作记录只能由教育机构认证时产生. 该记录包括主键 id、教育机构身份地址、学生身份地址、学校的签名信息、记录产生时间和学籍修改状态(0—正常毕业,1—退学,2—入学,3—非正常毕业).

表 4 学籍操作记录表

Tab. 4 Student status record

列名	数据类型	备注
Id	Number	唯一 id
SchoolAddress	String	学校唯一地址
StudentAddress	String	学生唯一地址
SchoolSign	String	学校签名信息
ModifyTime	Number	修改时间
ModifyType	Number	修改状态(0、1、2、3)

4.2 最小原型的简单实现

首先,通过调用预先编写并部署好的智能合约函数,可以向账本数据中写入学校相关信息,并生成区块记录(如图 5 和图 6).

接下来,学校可以登记学生入学:即写入学生信息并写入一条标识状态为“入学”的学籍操

作记录，同时把该学生加入到本校的学生列表中. 随后，当学生正常/非正常毕业或者中途退学时，通过触发预先编写并部署好的智能合约可以自动更新该学生的学籍信息，并在账本中记录下相关的学籍操作记录、生成相关的区块，同时将学籍信息加入到学生的学籍列表中（如图 7 和图 8 所示）.

最后，当第三方需要认证学生学籍的状态时，也可以通过调用智能合约的函数进行查询.

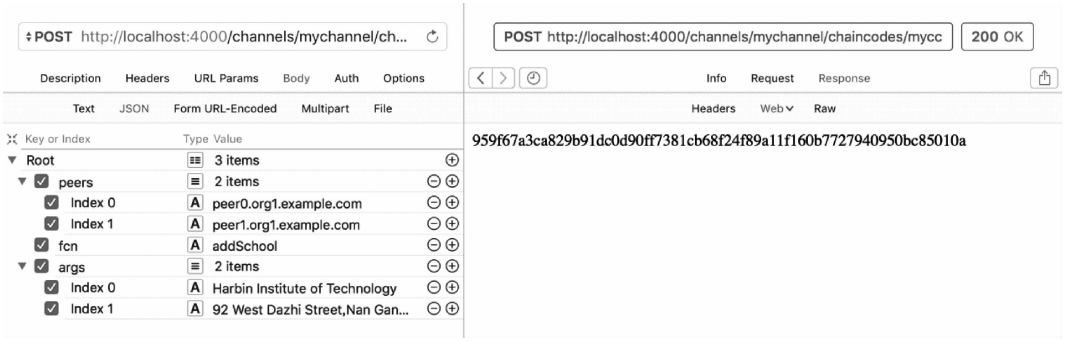

图 5　添加学校信息（POST 方式调用智能合约的 REST 接口）

Fig. 5　Add school information (POST mode calls the REST interface of the smart contract)

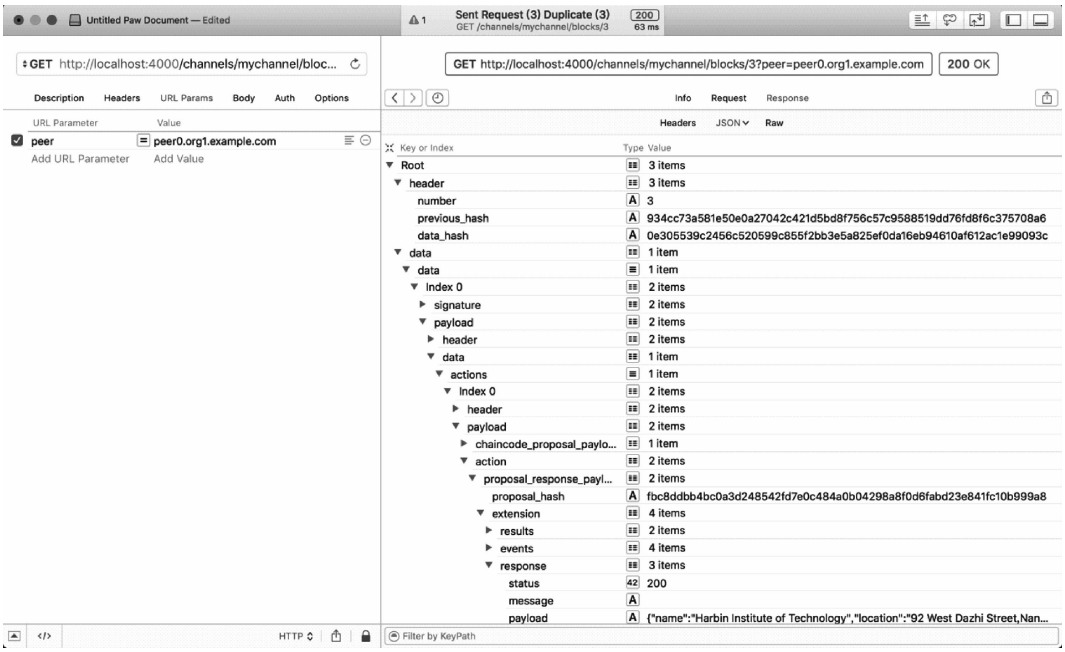

图 6　学校区块的详细信息（可通过 GET 接口获取）

Fig. 6　Detailed information on the school block (available via the GET interface)

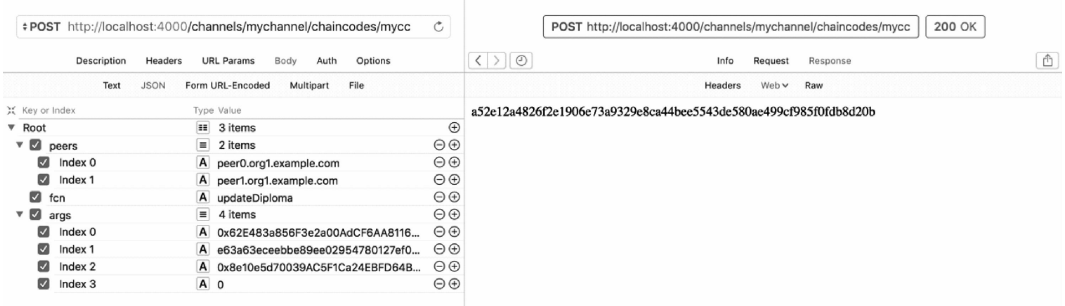

图 7　更新学籍状态（正常毕业）

Fig. 7　Update status (normal graduation)

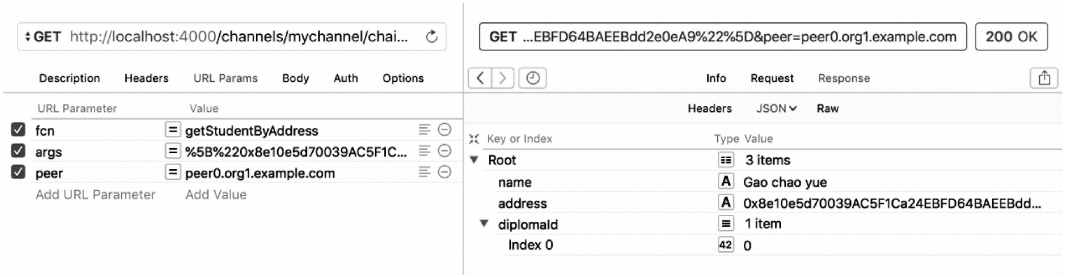

图 8 学籍更新成功并被自动加入到学生的学籍列表中

Fig. 8 The student status is updated successfully and is automatically added to the student list.

5 结 论

本文基于 Fabric 框架实现了一个由不同类型的多个节点组成的区块链学籍管理系统. 区块链技术、特别是智能合约的应用保证了学籍信息的真实性和可溯源性,保证了系统的去中心化,同时提高了系统的扩展性和安全性. 但是本文中最小系统原型实现的效果仅是基于单个高校和少数节点,随着节点数量的不断增多,实现学籍认证过程中全部操作流程时,预计还会产生新的问题,将在后续的研究工作中进一步探索.

参考文献:

[1] 陈铁军. 基于智慧校园体系下的高职院校学籍管理模式研究 [J]. 湖北函授大学学报, 2018, 31: 12.

[2] 谭少娟. 学籍管理信息化的现状探析 [J]. 教育现代化, 2018, 5: 310.

[3] 隋春霞, 葛日波. 分布式高校学籍管理系统的功能设计与部署 [J]. 教育现代化, 2018, 5: 277.

[4] Pass R, Seeman L, Shelat A. Analysis of theblockchain protocol in asynchronous networks [EB/OL]. (2017-04-01)[2018-05-23]. https://link.springer.com/chapter/10.1007/978-3-319-56614-6_22? noaccess=true

[5] 袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报, 2016, 42: 481.

[6] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究 [J]. 软件学报, 2017, 28: 1474.

[7] Kosba A, Miller A, Shi E, *et al*. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts [C]// Security and Privacy. [s. l.]: IEEE, 2016.

[8] 乔光华, 祝孔青, 赵德忠, 等. 基于区块链的学历认证和学位认证模式研究 [J]. 经营与管理, 2018, 35: 142.

[9] 朱涛, 姚翔, 许玉壮, 等. 基于 Fabric 的跨境汇款追踪平台实现 [J]. 信息安全学报, 2018, 3: 50.

引用本文格式:

中 文: 李中振, 高超越, 刘敏, 等. 基于区块链技术的学籍管理系统 [J]. 四川大学学报: 自然科学版, 2019, 56: 450.

英 文: Li Z Z, Gao C Y, Liu M, *et al* . Student status management system based on blockchain technology [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 450.