基于区块链的学位学历认证管理系统

**详细方案**

**目录**

[一、项目概要介绍 1](#_Toc70014198)

[1.1 作品开发背景 1](#_Toc70014199)

[1.2 系统发展现状 1](#_Toc70014200)

[1.3 系统创新性 1](#_Toc70014201)

[二、系统详细设计 3](#_Toc70014202)

[2.1 模块设计 3](#_Toc70014203)

[2.1.1 模块划分 3](#_Toc70014204)

[2.1.2 系统类图及说明 3](#_Toc70014205)

[2.2 系统后端设计 7](#_Toc70014206)

[2.3 Fabric 联盟链系统设计 10](#_Toc70014207)

[三、可行性及效益分析 11](#_Toc70014208)

[3.1 技术可行性 11](#_Toc70014209)

[3.2 功能可行性 12](#_Toc70014210)

[3.3 社会可行性 12](#_Toc70014211)

[四、实验测试 13](#_Toc70014212)

[4.1 部署区块链系统 13](#_Toc70014213)

[4.2 数据上链测试 13](#_Toc70014214)

[4.3 性能测试与分析 14](#_Toc70014215)

[五、市场分析 16](#_Toc70014216)

[5.1 市场需求分析 16](#_Toc70014217)

[5.3 市场前景 17](#_Toc70014218)

[六、系统应用 17](#_Toc70014219)

[6.1 应用对象 17](#_Toc70014220)

[6.2 应用环境 17](#_Toc70014221)

# 项目概要介绍

## 1.1 作品开发背景

随着时代的发展和社会的进步，高等教育的浪潮逐渐向越来越多的民众靠近，平均教育水平越来越高，与此同时，各类企业单位对于求职者的学历等硬实力的要求愈发严苛。在这种境况下，学历造假、认证造假现象等在当今社会屡见不鲜。这一方面造成了用人市场一定程度的混乱以及企业信任度的降低，增加了用人成本，造成了极大的社会影响；另一方面，也反映出传统的纸质或电子学历证书在安全性和不可伪造性等方面还存在一定缺陷。

目前，只有学信网和国外寥寥几个学位认证机构能够提供国内外学位学历认证，在这种社会背景下，亟待开发一套安全性更高且具有防篡改功能、高度可靠的基于区块链的学位学历认证管理平台，将对学位学历认证与管理产生重要帮助。

## 1.2 系统发展现状

据了解，相对于去中心化、匿名性的区块链电子存证系统，现有的电子学位学历认证管理系统还存在如下的问题。

1. 安全保障：大部分学位学历认证管理系统仍然使用中心化存储，无法抵御针对中心网络节点的攻击与篡改，学位学历信息安全无法得到保障。
2. 隐私保护：传统的纸质和电子认证系统在保存、查证、授权等各个环节极易造成个人隐私的泄露，同时，大部分基于区块链的学历学位认证管理平台，其用户信息等敏感数据仍然交付第三方平台存储与管理，用户隐私安全无法保障。
3. 认证规则：传统学历学位的认证通常采用半人工审核的方式,认证规则可以被人为修改,审核人员具有较大权力,执行结果可能存在质疑。

## 1.3 系统创新性

随着社会和时代的发展，信息化成为时代的大趋势，科技含量成为评判技术平台的重要评判标准。凭借互联网的浪潮，我们能够使用较为先进的企业级技术构建基于区块链的学位学历认证管理系统。在技术层面，用较优的算法和构建设计保证系统的稳定性和学历学位的安全可信保存、查证和授权。

（1）区块链是一种用于数据可信管理的分布式账本技术，它提供了一种无需第三方可心中心协助，对数据实现可信存证的功能。运用区块链联盟链技术，通过成员机构节点共同维护区块链网络实现去中心化，因而可以有效抵御针对中心节点网络的攻击行为，保证了学位学历信息上链后不可篡改，**相比于传统的纸质和电子学历认证系统，提升了认证信息可信度，保证了认证公信力。**

（2）基于国密技术及其应用体系，运用其中的SM2椭圆曲线公钥密码、SM3杂凑算法、SM4分组密码进行证书认证、证书上链数据信息摘要的生成与用户身份信息的加密、一些关键信息的加密等。**相比于其他常见的密码算法，具有相当高的加密强度和适用性，一定程度上增加了系统的安全性，保护了用户隐私，提升了加密效率。**

|  |  |  |
| --- | --- | --- |
|  | SM2 | RSA |
| 算法结构 | ECC的一种 | 基于特殊的可逆模幂运算 |
| 计算复杂度 | 完全指数级 | 亚指数级 |
| 存储空间（长度） | 192-256bit | 2048-4096bit |
| 秘钥生成速度 | 较RSA算法快百倍以上 | 慢 |
| 解密加密速度 | 较快 | 一般 |

表2.1.1 SM2与RSA的比较

|  |  |  |
| --- | --- | --- |
|  | SM3 | Sha256 |
| 算法结构 | Merkle-Damgard结构 | 基于特殊的可逆模幂运算 |
| 消息长度 | 2^64位 | <2^64位 |
| 分组长度 | 512位 | 512位 |
| 摘要长度 | 256位 | 256位 |
| 计算步骤 | 64步 | 64步 |
| 加密速度 | 快 | 快 |

表2.1.2 SM3与Sha256的比较

|  |  |  |
| --- | --- | --- |
|  | SM4 | 3DES |
| 算法结构 | 非平衡Feistel | 使用标准的算术和逻辑运算 |
| 计算轮数 | 32 | 48 |
| 分组长度 | 128位 | 128位 |
| 秘钥长度 | 128位 | 128位 |
| 性能 | 快 | 中 |
| 安全性 | 高 | 中 |

表2.1.3 SM4与3DES比较

（3）采用 IPFS + Fabric 大规模数据上链方案。

IPFS（the Inter-Planetary File System）是一个分布式文件系统，数据块在其中存储没有顺序，每个数据块与唯一的hash地址存在映射关系。

本系统将这种hash地址与存放着学生相关信息的数据块的映射关系、数据块的数据摘要上链存储与Fabric中。由于较大的学生相关信息存在分布式文件系统IPFS中，仅需上链的是hash地址与数据块的映射关系和数据摘要，因此可以很好地解决Fabric数据存储与读取效率低下的问题。

同时，由于所有证书具体数据存储在IPFS上，将IPFS的文件存储地址和数据摘要存在Fabric区块链网络上，这样就可以实现无需全部数据上链即可产生信任。

为了保证IPFS文件系统中数据块的数据不被篡改，每条学生信息记录使用密码算法产生的数据摘要也应一并上链。这样，在查询到IPFS时再生成一次数据摘要A，与区块链上获得的数据摘要B进行比对，如果比对成功，就可以保证数据的可靠性和完整性。

# 系统详细设计

## 2.1 模块设计

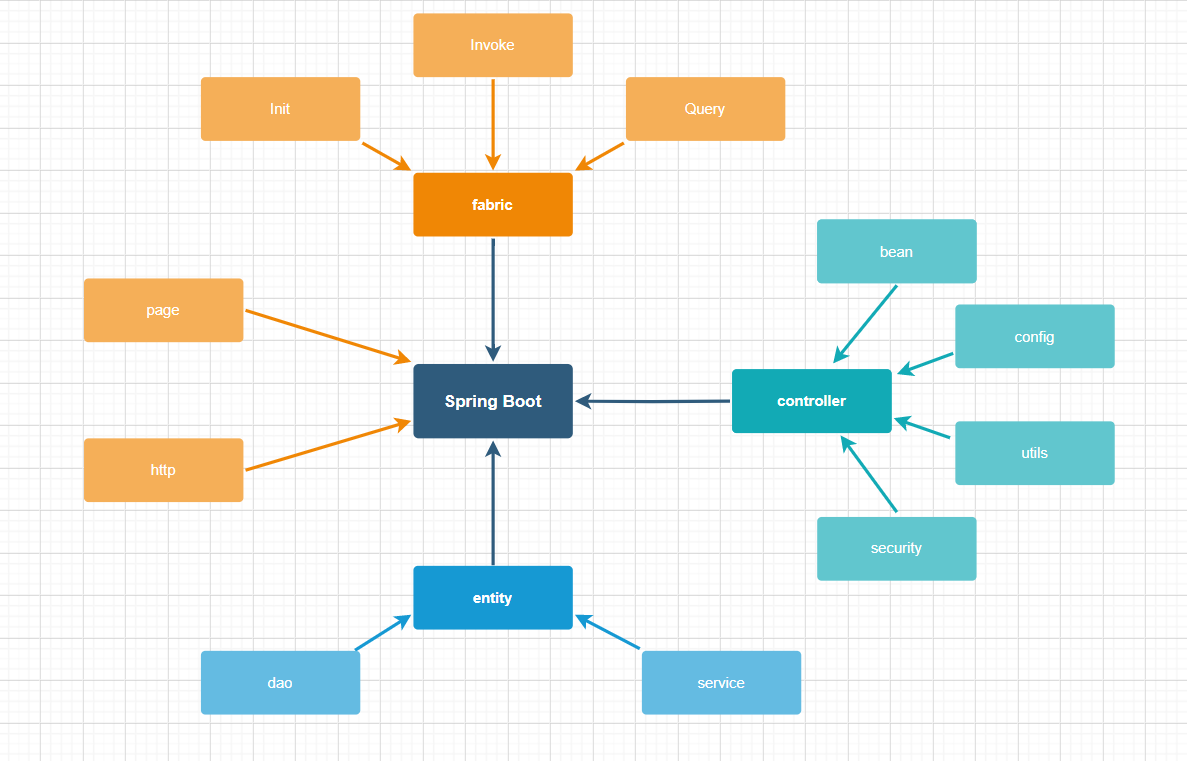
### 2.1.1 模块划分

系统大致分为证书生成、证书查询、证书核验3个模块。

1. 证书录入：用户输入证书相关信息，确认无误后点击生成，后台将根据用户输入的证书编号进行校验，如果证书编号冲突则会拒绝生成证书并且返回提示信息。否则将生成证书并将证书信息进行加密处理后上链。同时可以将学信网上已存在的学历信息导入本系统。
2. 证书查询：用户输入证书编号进行查询，后台自动检索当前登陆用户名与用户查询的证书上的姓名是否匹配。若匹配，则展示证书，否则将并返回错误状态码。
3. 证书生成：利用PDF证书模板生成动态表单，利用后台已有数据自动填充表单。在用户点击证书查询核验通过后，展示生成的证书。
4. 证书核验：用户输入证书编号，查询证书是否已经存在。

### 2.1.2 系统类图及说明

1、系统后端采用Spring Boot框架，其类图如下所示。

图2.1.2.1 Spring Boot框架图

Controller管理登录相关流程操作、学历认证相关业务操作、用户相关操作。Service层集成了所有操作（登录、学历认证、用户）所需的接口。DAO层封装了所有Service接口所需的数据库操作。Fabric层定义了连接区块链的三种基本接口（初始化、上链、查询）。Config层存放跨域、数据库持久层、RestTemplate等配置文件。Entity层存放数据库实体类。Http、Page定义了Http请求状态处理操作以及分页操作相关配置。Utils封装了国密算法、Token生成等工具类。

2、系统前端采用Vue.js框架，其类图如下所示。

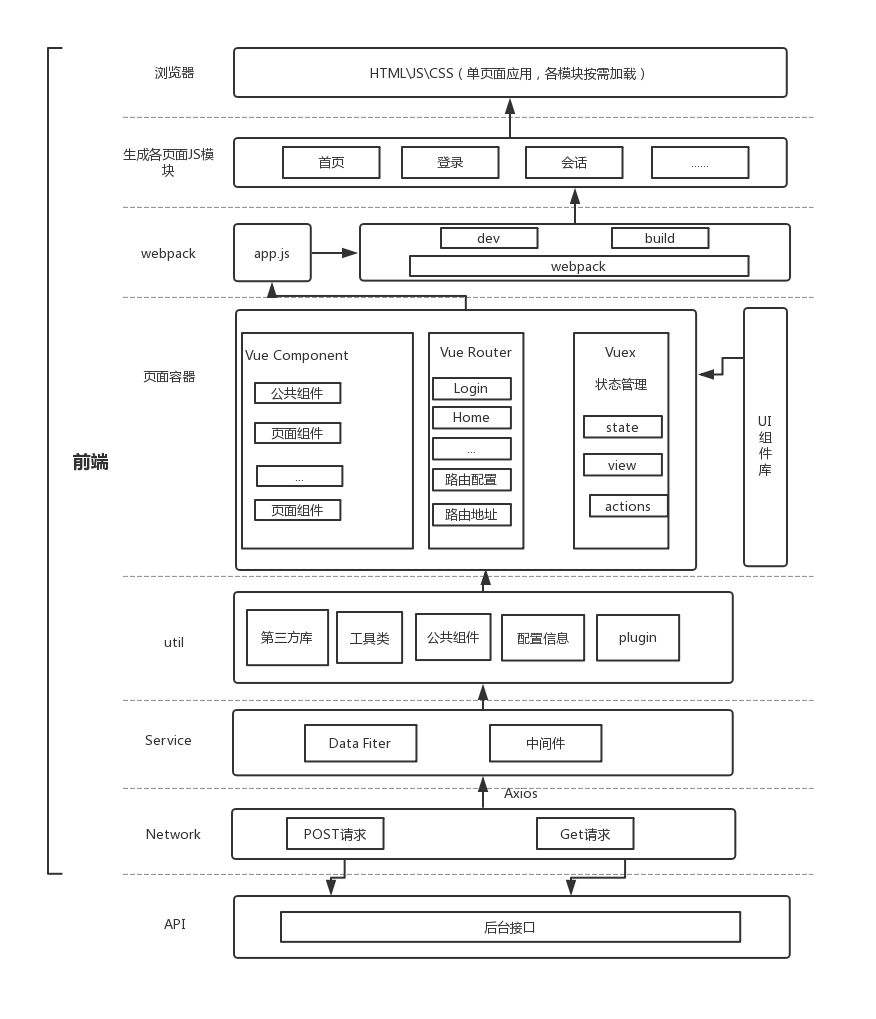


图2.1.2.2 Vue.js框架图

3、系统区块链采用Hyperledger Fabric联盟链系统，其类图如下所示。



图2.1.2.1 Fabric应用开发流程



图2.1.2.2 Fabric整体架构

本系统将Hyperledger Fabric联盟区块链技术应用于学历学位认证管理系统中，保障学生信息完整性、不可篡改性与可追溯性。极大提高了本系统的数据机密性与完整性。

（1）本系统区块链架构

开发者创建客户端应用和智能合约（chaincode），chaincode被部署到区块链网络的Peer节点上面。通过chaincode来操作账本，当调用一个交易transaction时，实际是在调用chaincode中的一个函数方法，它实现业务逻辑，并对账本进行get、put、delete操作。客户端应用提供用户交互界面，并提交交易到区块链网络上。Fabric应用开发流程如图2.1.2.1所示，Fabric整体架构图如2.1.2.2所示。

区块链采用四层架构，分为基础、核心等两大模块，核心模块包含合约层、共识激励层和网络层；基础模块包含数据层

a.数据层。按照“区块头+区块体”数据块格式进行封装，对数据记录进行加密并加入时间戳写入区块链中。基于安全性和政策性风险考虑，本方案的数据层密码算法采用国密算法SM3加密技术进行处理。

b.网络层。建立在IP通信协议和P2P网络的基础上，采用分布式组网机制、数据传播机制和数据验证机制。每一个节点都可收发信息，通过共同维护的区块链保持联络。每一个节点生成的新区块以广播方式通知其他节点，共同对这个区块进行验证。

c.共识激励层。是区块链技术的核心，规定记账者选择方式，影响整个系统的安全性和可靠性。本方案引入中药材种植企业、加工企业、第三方之间机构、政府监管部门和消费者等产业链参与方作为成员节点加入区块链。

d.合约层。在区块链中内置参与方事先拟定合约内容和触发机制等形式化规则，加载触发条件，合约自动执行，屏蔽外界干扰。本方案将有关中药材质量的政府监管条例、法律法规和质量标准等内容以智能合约形式嵌入区块链，实现药材质量的规范化和标准化管理。

（2）分布式账本

分布式账本是一个具有存在与每个参与节点、透明共享、同步更新等特点的信息库。区块链网络参与节点之间的各种信息都会被分布式账本记录，这种共享式分布账本不仅减少了访问传统中心化账本的时间，还节省了费用成本。在Fabric中一个账本表示为一个通道（Channel），而交易方是一个Channel中的不同组织（Organization）。我们设置了一个由2条通道，每条通道4个组织（其中包含1个排序节点组织（OrdererOrganization），3个节点组织（PeerOrganization））构成的联盟链网络。排序节点组织中包含一个排序节点（Orderer），3个节点组织中每个组织包含4个节点（1个提交节点（Commit Peer），1个领导节点（Leader Peer），1个背书节点（Endorse Peer），1个锚节点（Anchor Peer））。Fabric联盟链网络中的参与组织通过统一的共识机制与算法可以自动化地更新分布式账本，且不存在第三方的中心化机构来参与。这种去中心化的特征极大程度地保证了数据的安全性与不可篡改性。在我们的系统中上述两种特征经过实验也得到了很好的效果。

（3）链码设计

Fabric为所有节点部署了相同的链码。具备三种功能：初始化、上链、查询。后端Init接口通过SDK调用InitLedger类利用wallet中注册好的组织管理员权限进行（通过Fabric-CA登记注册）实例化链码服务。之后后端可以通过Invoke调用区块链Invoke服务对后端传输的数据摘要进行上链；通过query接口调用区块链Query服务查询链上数据。

## 2.2 系统后端设计

（1）SpringBoot

下图为“SpringBoot”企业级开发框架，及工作流程：



图2.2.1 SpringBoot工作流程

SpringBoot是Java企业版（JavaEnterpriseEdition，JEE，也称J2EE）的轻量级代替品。无需开发重量级的EnterpriseJavaBean（EJB），Spring为企业级Java开发提供了一种相对简单的方法，通过依赖注入和面向切面编程，用简单的Java对象（PlainOldJavaObject，POJO）实现了EJB的功能，是当今最热门的后端开发框架。

（2）MyBatis

MyBatis是一款优秀的持久层框架，它支持定制化SQL、存储过程以及高级映射。MyBatis避免了几乎所有的JDBC代码和手动设置参数以及获取结果集。MyBatis可以使用简单的XML或注解来配置和映射原生信息，将接口和Java的POJO（PlainOrdinaryJavaObject,普通的Java对象）映射成数据库中的记录。

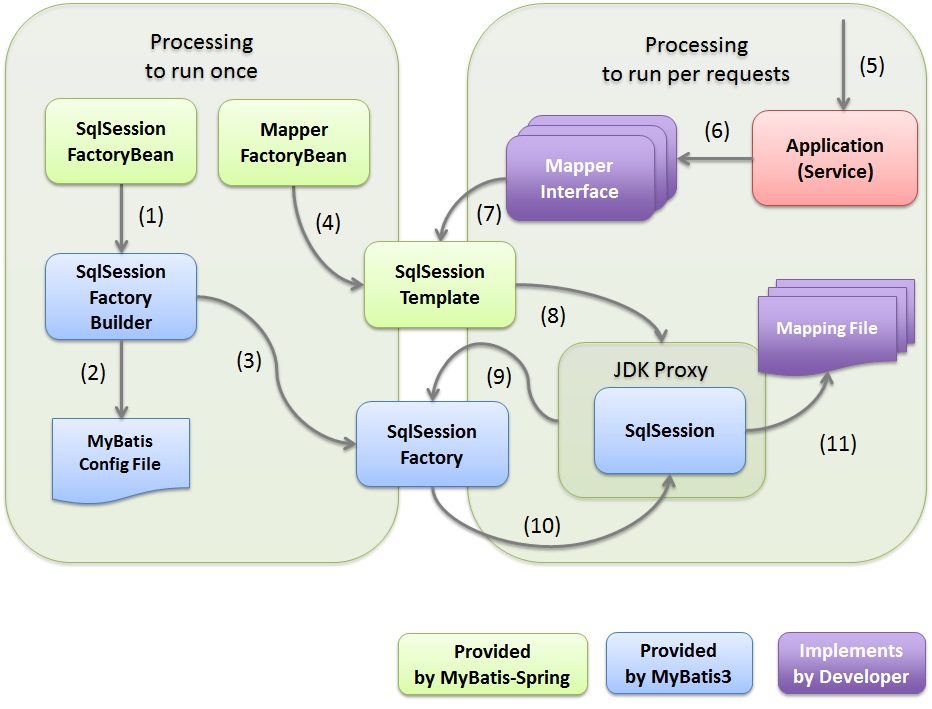
下图2.2.2为Mybatis的框架架构与工作流程：

图2.2.2 Mybatis工作流程

（3）JSON Web Tokens

JSON Web Tokens是一种用于双方之间传递安全信息的简洁的、URL安全的表述性声明规范。JWT作为一个开放的标准（[RFC 7519](https://tools.ietf.org/html/rfc7519)），定义了一种简洁的，自包含的方法用于通信双方之间以Json对象的形式安全的传递信息。因为数字签名的存在，这些信息是可信的，JWT可以使用HMAC算法或者是RSA的公私秘钥对进行签名，如今已被广泛应用于身份认证、信息交换等场景。

下图2.2.3以及图2.2.4为本系统所生成的管理员Tokens 的密文编码与明文解析：

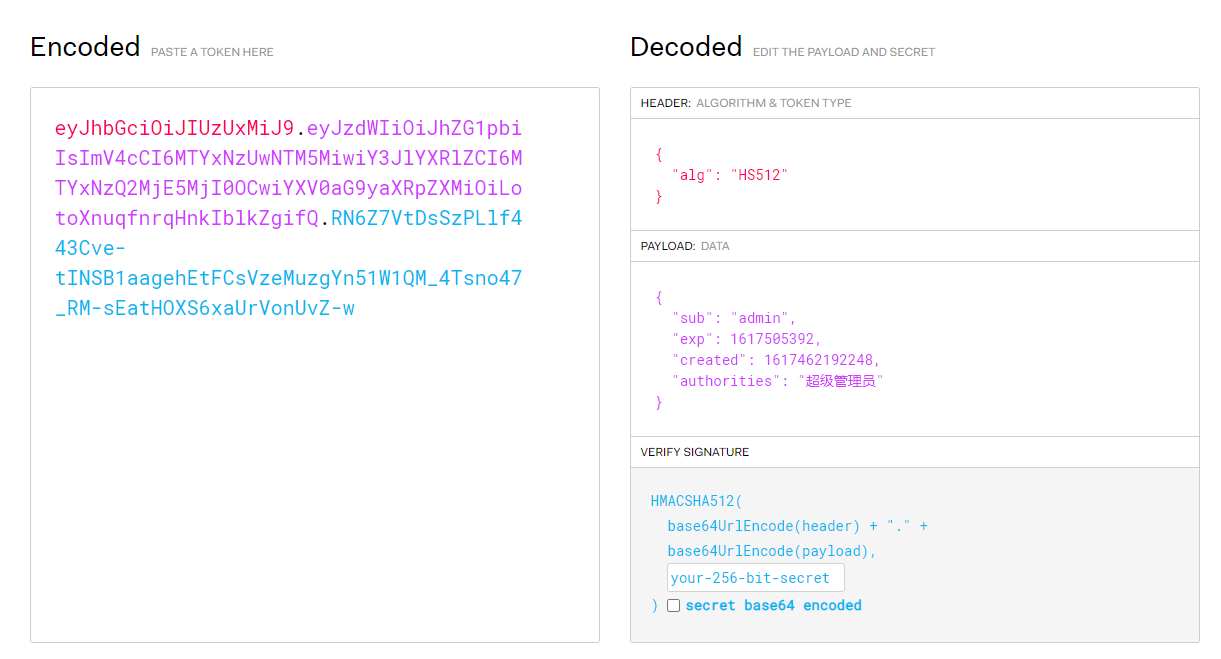
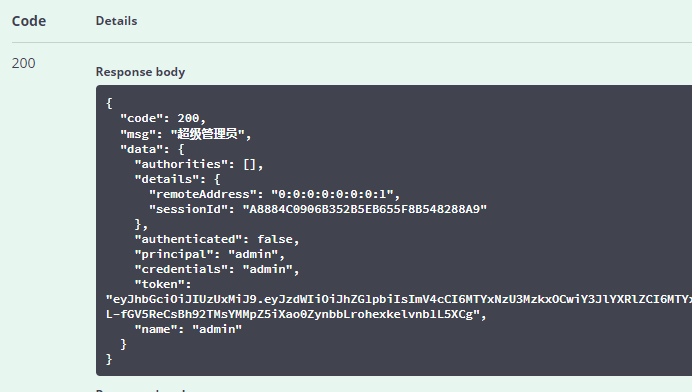
图2.2.3 本系统生成的Tokens

图2.2.4 上图Tokens的解析

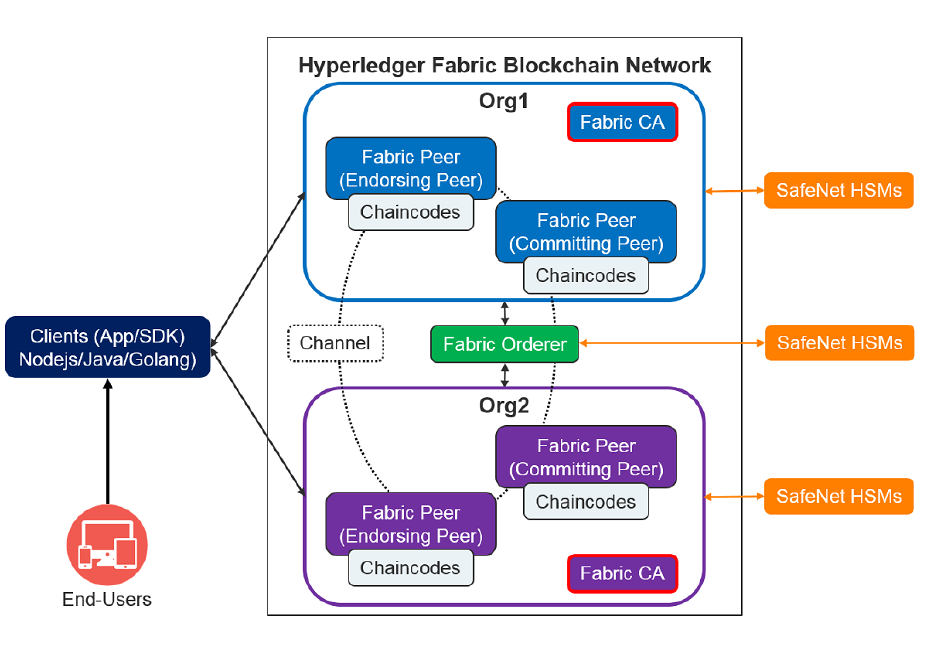
（4）国密算法

国密算法即国家密码局认定的国产自主研发的全新密码算法，主要有SM1、SM2、SM3、SM4。本系统运用SM2椭圆曲线公钥密码进行证书认证，SM4分组密码来对关键信息进行加密，还借助SM3杂凑算法来进行证书上链数据信息摘要的生成与用户账号信息的加密。

## 2.3 Fabric 联盟链系统设计

Hyperledger Fabric是一个提供分布式账本解决方案的平台。Hyperledger Fabric由模块化架构支撑，并具备极佳的保密性、可伸缩性、灵活性和可扩展性。Hyperledger Fabric被设计成支持不同的模块组件直接拔插启用，并能适应在经济生态系统中错综复杂的各种场景。

Hyperledger Fabric提供了一个独特的可伸缩、可扩展的架构，这也是Hyperledger Fabric与其他区块链解决方案的显著区别。

图2.3.1 Hyperledger Fabric的组织架构与交互流程

本系统将Hyperledger Fabric联盟区块链技术应用于学位学历信息保存中，保障证书在保存、查证、授权时的安全性和不可篡改性，保护企业和用人单位的合法权益。极大提高了本系统的数据机密性与完整性。

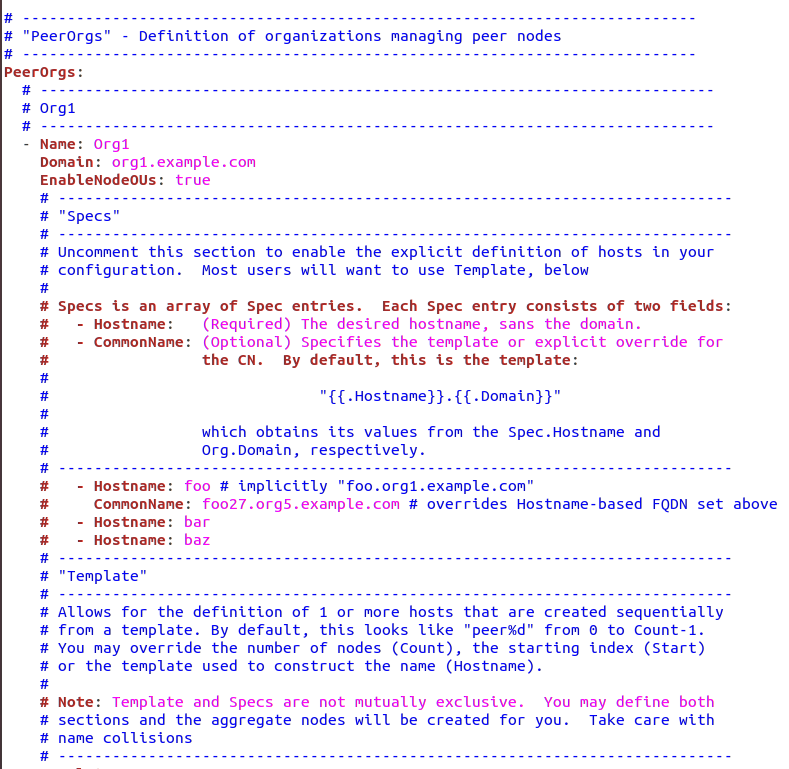


图2.3.2 本系统的Hyperledger Fabric部分配置

# 可行性及效益分析

## 3.1 技术可行性

（1）确定数据特征

我们经过调研，总结出学位学历证书主要由证书编号、个人相关信息组成。为此我们设计了一个由证书编号、防伪码、学生个人相关信息等多条要素组成的特征数据。

（2）数据真实性保证

我们采取了流式信息收集+动态时间戳绑定+第三方监管的方式有效降低了信息大规模造假的可能性。通过动态时间戳确保每个环节收集的数据不会因为某些特征十分类似而相互冲突，这也保证了已经录入的数据进行无法篡改。

（3）数据不可篡改性

我们采用了IPFS大规模数据上链方案以确保数据几乎不可能被篡改。

IPFS分布式存储系统，存储在其内部的数据块没有任何顺序，只有一个唯一的hash地址与存储数据的数据块对应。

本系统采取数据库与区块链结合的方式存储学位学历数据。将证书所有的数据条目做SM3加密处理，生成一条独一无二的数据摘要。将hash值与存储数据的对应的数据块之间的映射关系同交易数据经过加密处理的数据摘要一起上链。这样不仅可以处理数据库存储与读取效率低下的问题，也可以很好地解决数据被篡改的问题。

## 3.2 功能可行性

（1）本系统具有一套有效的用户管理功能，新用户注册后，后台数据库生成盐，用于生成令其成为有效用户的Token令牌。用户登陆时，基于token令牌的JWT访问权限控制机制校验用户身份，并在该用户之后每次的操作对后端产生的请求中都注入Token令牌。只有携带了有效Token令牌的用户才可以获得操作权限。

（2）可以提供简洁的证书查询、生成等核心服务，用户可以在相应的界面中一键生成、查询，信息更新速度快。

（3）在学生证书的信息提交时可根据服务端的接收状况进行相应的提示，保证学生证书相关信息既能成功入库上链，又防止重复入库的可能。

（4）采取前后端分离的部署模式，后台进行服务监控和性能分析，在云端为用户提供稳定、快捷的服务，系统的运行环境、监测网站配置、系统运行维护等均由服务提供方完成。

## 3.3 社会可行性

在传统的信息认证中，尤其是针对海外留学生的学历学位认证，国内各方单位认证标准不一致，而相关大学提供的认证信息往往存在这样那样的差异，不够全面，难以体系化。**但使用区块链进行存证后，借助区块链的token系统开发经济模式，可以衍生出基于token的新商业生态。**将各方所需信息联系起来，通过智能合约方式，提供去信任机制，一定程度上实现各利益主体间的自主协作和交易。实现资源的整合和各方效益的最大化，构筑新型合作共赢的生态场景。

无论对于企业用人单位、应聘者，学历学位认证管理系统都具有重要意义，随着出国留学生人数的逐年增长，市场对相关权威的学习学位认证需求不断增加，而国内下游市场也在不断扩大，需求不断增大。在未来，若通过政策等将国内学位认证信息同国外认证信息互补交融，形成更加全面的认证机制，增强公众对于平台认证学历的公信力，学历学位认证的市场规模又将激增。

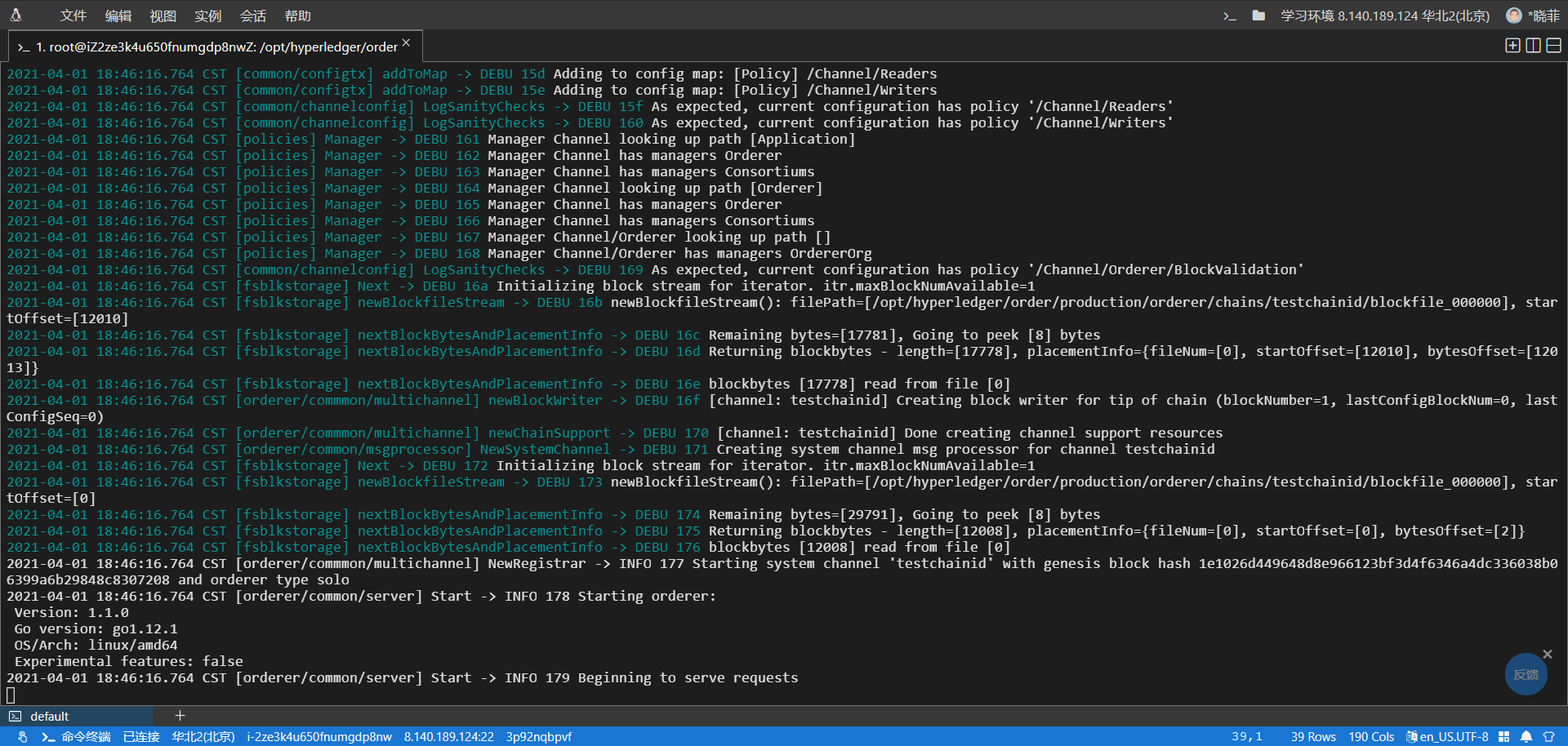
具有良好的公信力，能够增强事业单位对提供的学历证书的认可度，受认证服务受众信任的学历学位认证平台，对经济社会效益有很大的提高。

# 实验测试

## 4.1 部署区块链系统

我们通过设定core.yaml文件以及orderer.yaml文件内的参数，利用fabcar内的startFabric.sh脚本构建了一个由2条通道，每条通道4个组织（其中包含1个排序节点组织（OrdererOrganization）），3个节点组织（PeerOrganization）构成的联盟链网络。排序节点组织中包含一个排序节点（Orderer），3个节点组织中每个组织包含4个节点（1个提交节点（Commit Peer），1个领导节点（Leader Peer），1个背书节点（Endorse Peer），1个锚节点（Anchor Peer））。

配置参数如图4.1.1所示：



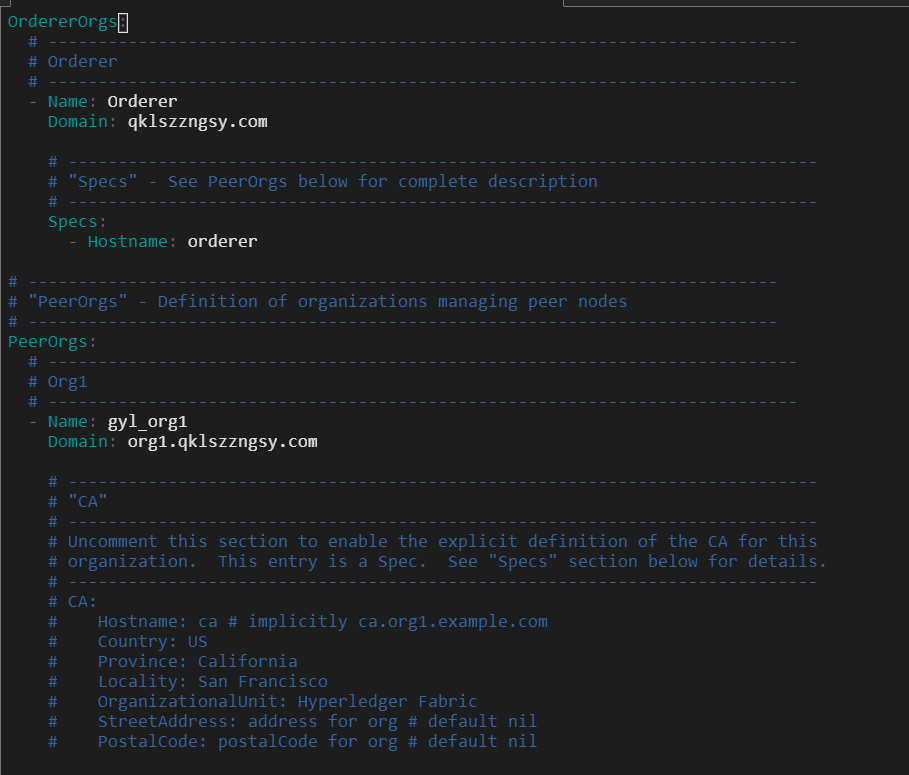
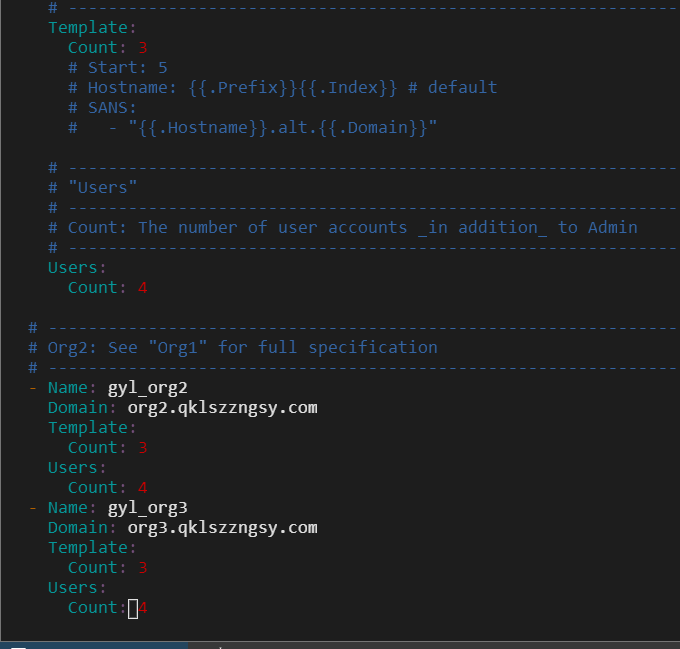
 

图4.1.1 Fabric联盟链配置参数

## 4.2 数据上链测试

利用SwaggerWeb服务框架模拟http请求，向后端发送交易测试数据（数据经过严格检查并符合规范的测试数据），进行数据上链及性能测试。测试结果见图4.2.1。

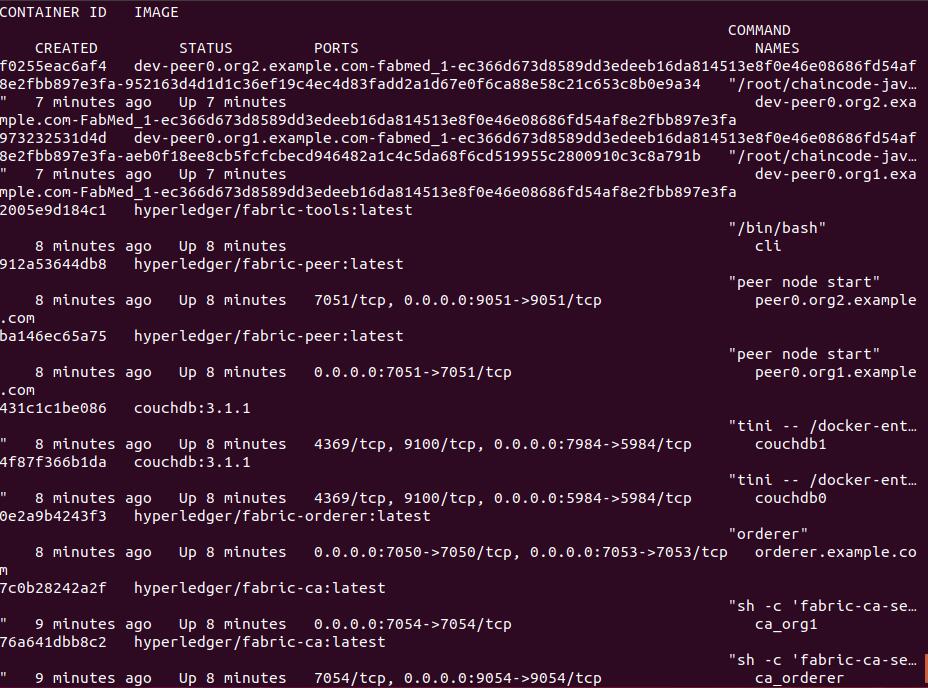
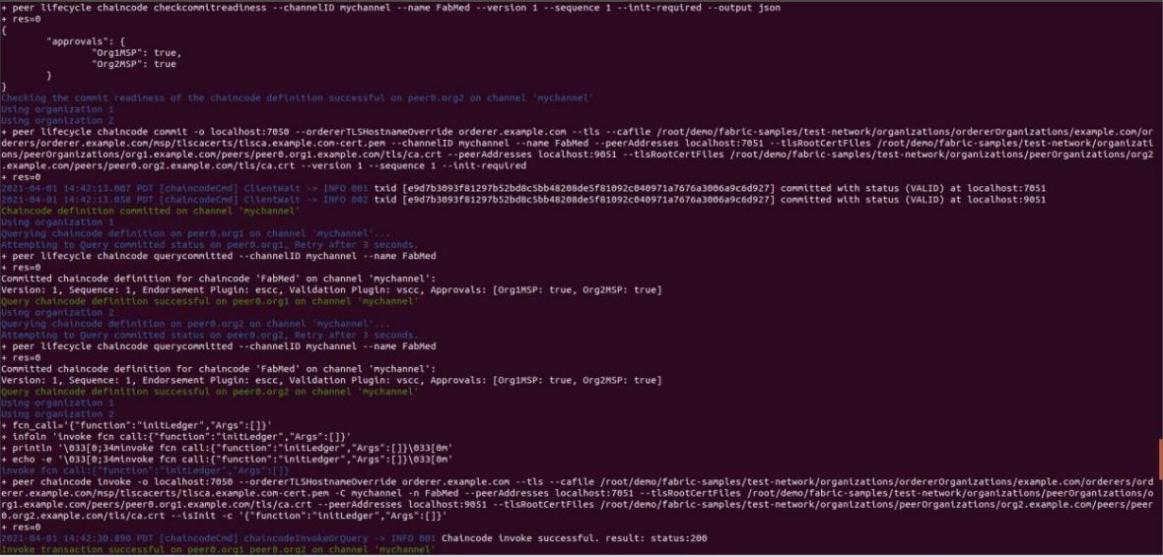


图4.2.1 Swagger模拟http请求数据上链测试结果

## 4.3 性能测试与分析

本节主要展示学位学历认证管理系统的性能测试结果并对其进行分析，采用LoadRunner对系统进行性能测试，通过创建虚拟用户，在高并发量和真实的负载环境中，实时对系统性能进行监控。通过分析测试报告及时发现系统性能问题，优化系统性能，细节如下：

1. 性能测试环境

客户端：Windows 7 x64，1核处理器2G内存，系统纯净无病毒，没有其他软件对实验结果造成干扰。

测试软件：LoadRunner 11，兼容多种浏览器，兼容windows 7系统，能够对web等多种项目进行测试，降低测试成本，提升了测试效率。

测试场景：100个用户并发，进行用户登录和药材数据入库的操作。

1. 性能测试结果

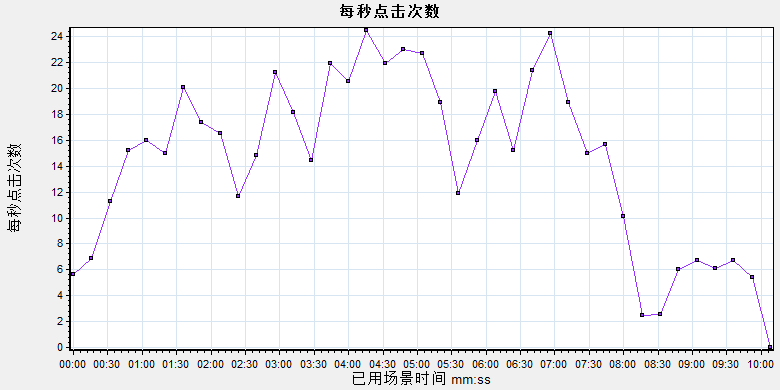


图4.3.1 虚拟用户负载测试期间每秒内在 Web 服务器上点击的次数

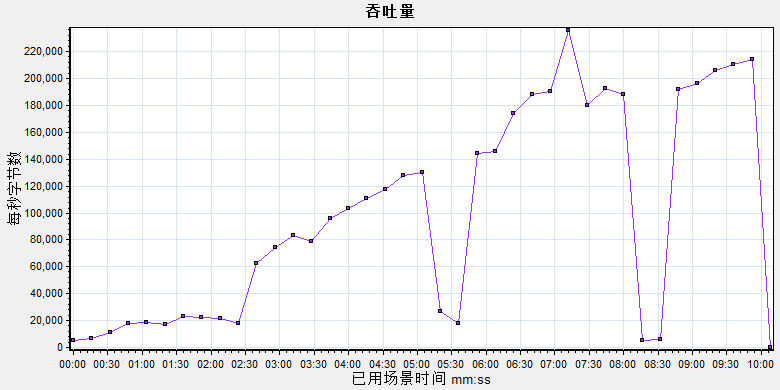


图4.3.2 负载测试期间 Web 服务器上的吞吐量（Byte）

（即从服务器接收到的数据量）

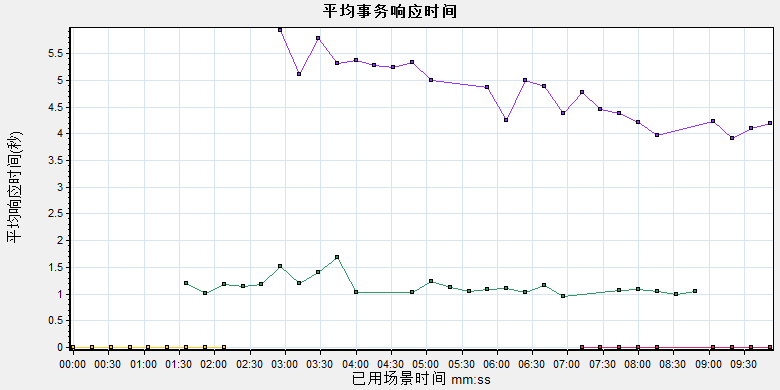


图4.3.3 负载测试期间每秒内执行事务所需的平均时间

（紫线为总执行事务，绿线为用户登录事务）

1. 性能分析

通过以上测试，创建200个虚拟用户，在10分钟内登录并完成数据入库操作的用户总数为200，成功率为100%，整个过程系统平均响应时间为4.77s，吞吐量等测试结果证明了该系统能够承载日常的并发数和并发量，将测试结果罗列成表格，如下表所示，从结果表可以看出，系统的性能可以满足预期目标。

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| 测试内容 | **实际值** | **预期值** | **测试结果** |
| 系统响应时间 | 4.77s | <5s | 通过 |
| 用户登入成功率 | 100% | 99% | 通过 |
| 数据入库成功率 | 100% | 98% | 通过 |
| 用户登入总数 | 200 | 200 | 通过 |
| CPU使用率 | 37.42% | <70% | 通过 |
| 内存使用率 | 52.55% | <70% | 通过 |

表4.3.1 测试结果表

# 市场分析

## 5.1 市场需求分析

在社会浪潮所造就的“学历热”中，学历造假早已司空见惯，甚至出现了学历造假的产业链等黑色产业。根据八方锦程在2019年对全行业调查总人数报告异常比例统计，“教育信息虚假”人数占比10.43%，其中风险点包括：学校名称有误、就读时间差异、专业名称有误、学位情况套用他人证件、伪造毕业证书、夸大学历层次等等。从根本上讲，是信息不对称造成的问题，为此，公司HR在收到求职者的简历时需要花费大量的时间和资源用于求职者的背景调查，且效率较低。需要一种手段来改善这类问题。

在近几年来，最高人民法院、最高人民检察院发布了《关于办理伪造、贩卖伪造的高等院校学历、学位证明刑事案件如何适用法律问题的解释》，对于学历造假问题有了明确的规定，与此同时，各类国企私企也呼吁学历造假问题的亟待解决，学生群体包括国内学生、国内留学生、海外留学生等，如何将其统一，且保证学历证书防伪，则是学历学位认证管理系统的市场需求所在。

## 5.3 市场前景

学历造假、认证造假等是一个全球日益普遍的现象，不仅对社会产生了巨大的负面影响，同时也极大增加了企业和单位的用人成本，造成了无谓的经济消耗。基于区块链的学位学历认证管理系统，无疑能够为解决此类问题贡献自己的力量。

在教育存证方面，区块链的应用不仅局限于学历、学位证书，而且还能完善学历、学位的认证内容，包含更多关于学生的如成绩单等的学业情况信息,提高认证内容社会认可度。

同时，在区块链技术越来越多地应用到诸如商品溯源、信息流通与可信存证等环节，进入到人们的市场生活中的大背景下，将区块链应用到学位学历可信认证管理中无疑会成为各个高校、用人企业的不二之选。

# 系统应用

## 6.1 应用对象

我们的学历认证管理系统主要面向于一些企业用人单位、各个大学内针对学生开放的学历证书查询、动态生成等需求。同时，由于海外留学生的学历认证服务在国内尚不成熟，平台可以针对该问题提供对海外留学生学历认证查询的定制化服务。

## 6.2 应用环境

1.基于区块链的学历学位认证系统可以应用于各种人才密集型企业，以便于更加精确、高效率地筛选出更好的人才。

2.基于区块链的学历学位认证系统可以应用于高等学府当中，为应届毕业生的大量学历证书的存储提供另一种途径，同时节省了资源，提高了安全性与防篡改性。

3.基于区块链的学历学位认证系统可以应用于全球教育大市场之中，人人可在证书可信的基础上进行证书的生成与上链，人人可核验证书，实现企业与人才的双赢。