Software Engineering and Applications 软件工程与应用, 2021, 10(4), 433-440
Published Online August 2021 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2021.104048

Hans汉斯

基于区块链的学位认证管理系统设计

陆佳艳

浙江理工大学，信息学院，浙江 杭州
Email: 490951632@qq.com

收稿日期：2021年3月31日；录用日期：2021年7月6日；发布日期：2021年7月14日

摘　要

知识经济高速发展的今天，一个高质量的学位证书能大大提高个人的社会竞争力。但是现有的学位管理系统大都以中心化的方式管理数据，存在易篡改、成本高、数据可信度低等问题，学历造假、认证造假现象日益严重，对社会产生了巨大的负面影响。近几年来，区块链技术蓬勃发展，其本质是一种去中心化的分布式网络，允许用户在P2P网络中进行数据通信和交换资源。文章提出基于区块链的学位认证管理系统，包含用户管理、学位管理、学位认证三大功能模块，涵盖了证书认证管理的主要环节，与传统学历学位认证相比真正实现了去中心化的数据管理。将区块链作为底层存储，保证了学位信息的安全性、防篡改性以及可追溯性。系统结合智能合约技术，无需第三方可信中心参与认证管理，在免去大量人工成本的同时，提高了系统内部可信度。

关键词

区块链，智能合约，学位认证，去中心化

Design of Degree Confirmation Management System Based on Blockchain

Jiayan Lu

School of Information, Zhejiang Sci-Tech University, Hangzhou Zhejiang
Email: 490951632@qq.com

Received: Mar. 31st, 2021; accepted: Jul. 6th, 2021; published: Jul. 14th, 2021

Abstract

With the rapid development of knowledge economy, a high-quality degree certificate can greatly improve the social competitiveness of individuals. However, most of the existing degree management systems manage data in a centralized way, which is easy to be tampered with, high cost and

文章引用: 陆佳艳. 基于区块链的学位认证管理系统设计[J]. 软件工程与应用, 2021, 10(4): 433-440.
DOI: 10.12677/sea.2021.104048

low data credibility. The phenomenon of diploma fraud and authentication fraud is becoming more and more serious, which has a huge negative impact on society. In recent years, blockchain technology has boomed. Essentially, it is a decentralized distributed network that allows users to communicate data and exchange resources in a P2P network. This paper proposes a degree certification management system based on blockchain, which includes three functional modules: user management, degree management and degree certification, covering the main links of certificate certification management. Compared with the traditional degree certification, it truly realizes the decentralized data management and takes the blockchain as the underlying storage to ensure the security, tamper-proof and traceability of the degree information. Combined with smart contract technology, the system does not need a third-party trusted center to participate in authentication management, which eliminates a lot of labor costs and improves the internal credibility of the system.

Keywords

Blockchain, Smart Contract, Degree Certification, Decentration

1. 引言

近年来，随着我国对教育行业的高度重视，高校毕业生逐年递增，社会竞争也逐渐增大，学历造假、认证造假频繁出现，成为一个全球日益普遍的现象，对社会产生了巨大的负面影响。而现有的学位管理系统大都基于中心化的数据管理方式，主要存在以下四个弊端：一，数据由中央控制，权限过于集中，可能存在私自篡改数据的现象，从而导致数据不可信；二，数据存储于中心服务器中，存在单点故障或易被不法分子恶意攻击的风险，造成数据完整性的问题；三，随着高等院校学生人数的增加，数据库建设成本和数据安全风险将会进一步加大；四，数据存储缺乏公开透明的高效约束机制以及可追溯性，难以保证数据的客观真实性。

区块链作为去中心化的网络，为上述问题提供了新的技术支持。本文通过区块链技术实现数据的分布式存储，保障学位信息的安全性、防篡改性以及可追溯性，同时通过智能合约技术，无需第三方可信中心参与即可实现业务交易的安全交互，最终实现公开透明、高效可靠、去中心化的学位认证管理系统。

2. 传统学历学位认证发展现状

目前，国内主要采用学籍电子注册制度实现学位学历认证。学生在入学时需进行新生学籍注册，且此后每年都需进行学年注册从而确保学籍的有效性，当学生在校期间完成学业后即可获取电子毕业证书的注册资格，之后高校将证书信息上传，即可在提供学位学历认证服务的专门机构查询到该学历学位证书的信息。

国内官方授权的学位学历认证机构主要有学信网、学位与研究生教育发展中心以及国(境)外学位认证系统[1]。前者提供国内学位学历认证服务，学生可将“学信二维码”置于求职简历中[2]，便于快速证明学历学位证书的有效性。后者能够通过国外学位认证系统核验国外证书的真伪。

传统学位认证虽然通过权威机构的背书，在一定程度上增加了学位证书的造假难度，但其本质依然是中心化的数据管理方式，如图 1 所示，存在权限过于集中、数据易被篡改、不可追溯、成本损耗较高

等问题，中心化数据管理方式正面临着发展瓶颈。

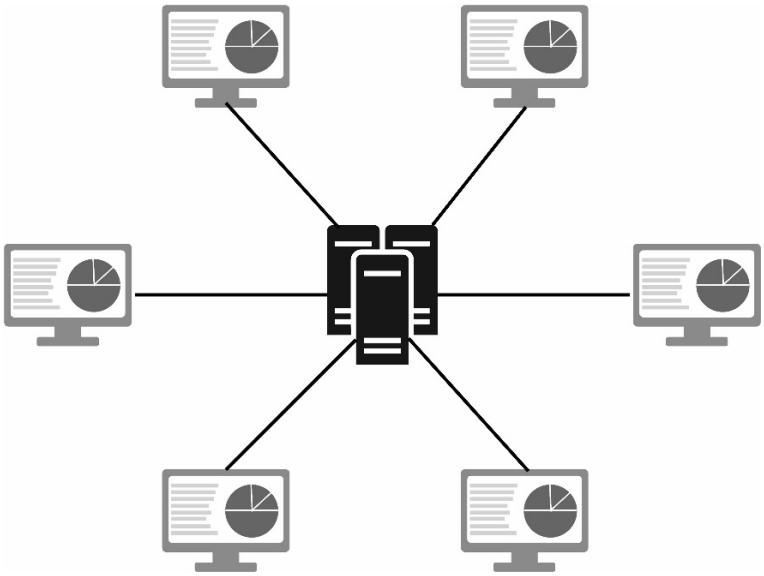

Figure 1. Centralized data management mode diagram
图 1. 中心化的数据管理方式图

3. 区块链技术简介

区块链是一种用于数据可信管理的分布式账本技术，具有去中心化、防篡改、可追溯的特性[3]，无需第三方可信机构即可实现无信任关系阶段之间的价值通信，达到去中心化可信数据共享的目的[4]。其本质是一种去中心化的分布式网络[5]，如图 2 所示。区块链决策是由区块链中的所有节点通过一定策略共同商定的，并不是由单个权威中心决定，因此可以有效抵御针对中心节点的网络攻击行为，同时能避免单点故障等问题。

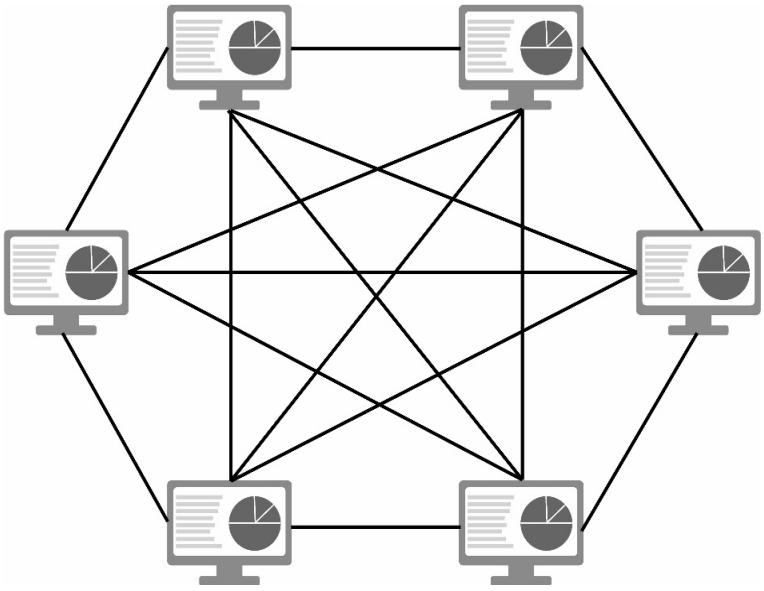

Figure 2. Decentralized distributed network diagram
图 2. 去中心化的分布式网络图

区块链中的数据结构在不同的应用场景下会有所不同，但基本上一个区块都是由区块头和区块体两部分组成的，如图 3 所示。区块头保存了上一个区块的 Merkle 根、Hash 值、时间戳、版本号和其他信息。其中，Merkle 根的值是由存储在区块体中的所有交易信息计算出的唯一哈希值决定的。区块体保存了若干条由 Merkle 树存储的交易信息。区块中任何一个数据信息的更改都会改变 Merkle 树的结构，从而改变 Merkle 根的值。因此，Merkle 根能够判断交易的数据是否被篡改过[6]。

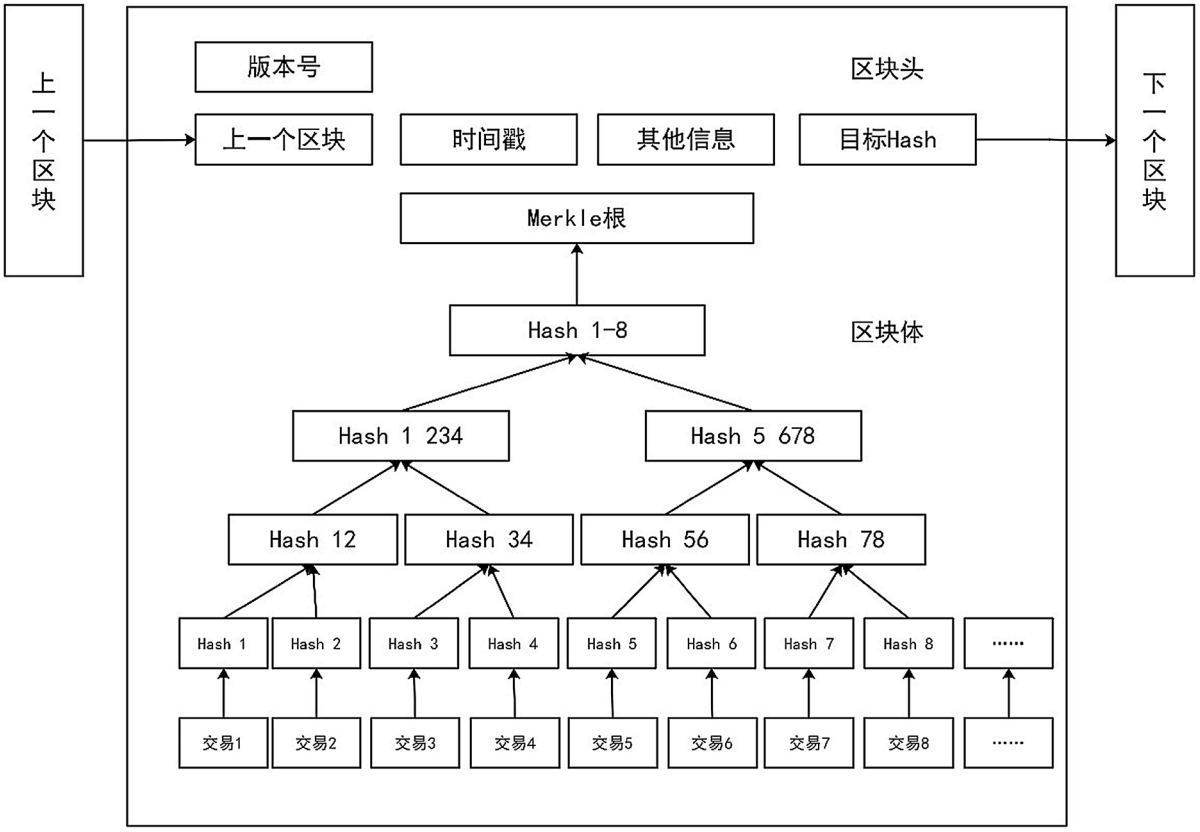

Figure 3. Blockchain data structure diagram
图 3. 区块链数据结构图

4. 系统需求

基于区块链的学位认证管理系统利用区块链技术为学位证书提供存证性证明。智能合约和链上数据在数据不可篡改和防伪可追溯特性等方面的优势能够保障学位信息的安全存储以及学位认证的高度可靠。

本系统的服务对象主要为管理员、审核机构用户和普通用户。管理员负责审核机构用户账号和权限的管理分配。审核机构用户以各大高校为主，负责证书授予、证书召回和证书查询。普通用户以学生用户和企业用户等有证书认证需求的用户为主，提供证书核验、证书查看、证书保存等功能。按照需求分析本系统可分为证书管理、证书认证、用户管理三大模块，功能模块图如图 4 所示。

用户管理功能模块面向管理员用户，用于实现对审核机构用户相关信息的统一管理。审核机构用户的账号无需注册，由管理员直接指定。同时管理员也可以查看、更改相关信息。

证书管理功能模块面向审核机构用户，主要为各大高校。审核机构用户可通过录入学生的学位信息进行证书授予，即实现学位证书信息上链。对于不符合学位授予但已经授予学位的学生，审核机构用户可选择对该学生的证书进行召回，并填写召回理由，召回记录同样会被存储在区块链上。同时，审核机

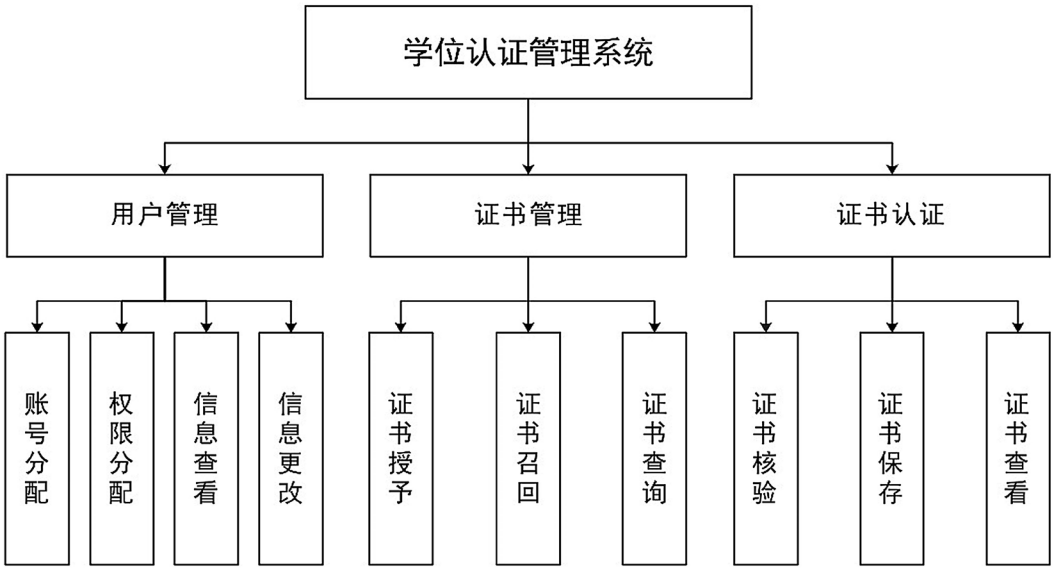

Figure 4. System function module diagram
图 4. 系统功能模块图

构用户也可以进行证书查询，快速找到相应的学位证书。

证书认证功能模块面向普通用户，即学生、企业等有证书认证需求的用户。普通用户输入学位证书信息即可对证书进行核验。若证书已被授予且无召回记录，则核验结果为真；反之，为假。对于核验为真的证书，用户可选择查看、保存证书。

5. 关键技术

5.1. VNT Chain 区块链平台

VNT Chain采用“联盟链 + 跨链 + 公有链”架构，其公有链采用了一种全新的Vortex共识算法[7]。Vortex 共识算法融入了 DPoS 算法和改进后的 BFT 算法，TPS 可高达 10,000+，高 TPS 让系统产生的交易更快的打包并验证上链。同时，还能够应对各种攻击，有效防止分叉和数据篡改。各个主流公链的 TPS 对比如图 5 所示：

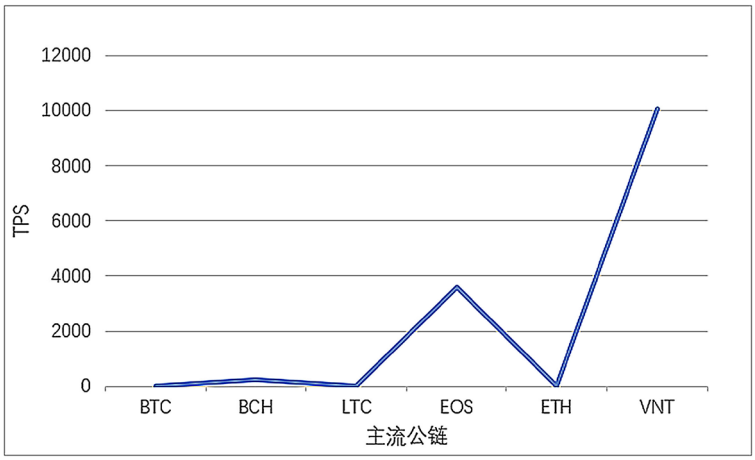

Figure 5. TPS comparison diagram of mainstream public chains
图 5. 主流公链的 TPS 对比图

系统将学位证书的关键信息存储于 VNT Chain 区块链平台，保证了学位学历信息存储的公开透明与安全。同时，低延迟、高安全及较强的并发处理能力，为学位学历认证管理操作带来全新的体验。

5.2. 智能合约

智能合约是一种以信息化方式为媒介进行传播、验证或执行合同的计算机协议[8]。在没有第三方参与的情况下，能够实现交易的安全交互。VNT Chain 的智能合约采用 C 语言进行编写，利用 Bottle 工具实现智能合约的编译以及 JavaScript 语言的 API 实现智能合约的部署与调用执行。

系统通过智能合约设计了角色管理合约用于实现合作学校权限管理的业务逻辑；设计了证书管理合约用于实现证书上链、召回、查询、核验等证书管理的业务逻辑。本系统中的智能合约部分代码如图 6 所示：

```
#include "vntlib.h"

// 每个用户的信息
typedef struct
{
    uint64 id; //用户编号
    string org;//所属机构
    string roleaddress;//用户账号地址
    string identity;//系统管理员，审核机构，普通用户

} roleinfo;
// 所有 拥有管理权限 的用户
KEY array(roleinfo) roles;
KEY mapping(string, roleinfo) role;
// 某用户是否在我们的记录当中
KEY mapping(string, bool) RoleState;


// 所有 拥有管理权限 的用户数量
KEY uint64 rolesnumber;
```

```
#include "vntlib.h"
//学位证书信息 结构体
typedef struct
{
    uint64 number;
    string name;                    // 学生姓名
    string idcard;                  // 学生身份证号
    string marjor;                  // 专业名
    string college;                 // 学院名
    string education_background;    // 学历:专科 本科 硕士 博士
    string school;                  // 学校名称
    string timestamp;               // 时间戳
    string study_id;                // 学号
    string gender;                  // 性别
    string enter_time;              // 入学时间
    string graduate_time;           // 毕业时间
    bool is_callback;               // 是否召回状态
    string callback_reason;         // 召回原因

    string diplomanumber;           //证书编号
    string filehash;                // 文件哈希

} diplomainfo;
```

Figure 6. Smart contract code diagram
图 6 智能合约代码图

5.3. XFA 动态生成电子证书

XFA 是嵌入动态 XML 的 XML Forms Architecture 表单。XFA 提供了基于模板的语法和处理规则集，它们允许用户构建交互式表单。

系统使用 Adobe Acrobat DC 中交互式表单组件实现了对 PDF 模板文件动态修改计算域内值的操作，根据每个学位证书的信息自动化生成 PDF 格式的电子证书。在直观展示学位证书的同时，大大降低了证书上链的成本。

6. 系统架构

系统以 VNT Chain 作为区块链平台，通过 WEB 端和移动端前端系统实现用户交互。本系统架构如图 7 所示，可分为应用层、服务处和存储层三层。

1) 应用层

应用层提供 Web 端和移动端两大端口，通过人性化的交互界面面向各类用户。Web 端面向所有用户群体，主要通过 VUE 框架和 Elenment UI 框架进行搭建。移动端仅面向普通用户，基于 Android 平台和 Glide 框架进行开发。

2) 服务层

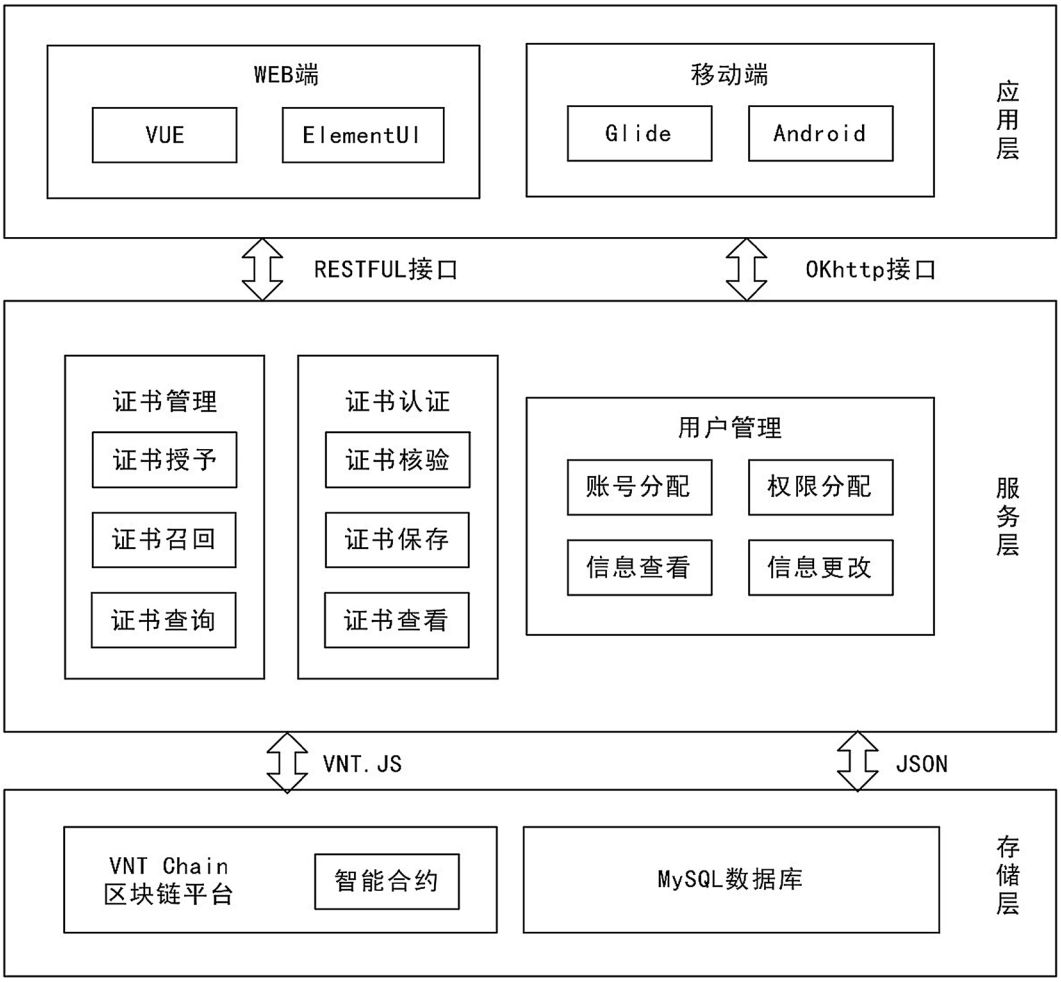

Figure 7. System hierarchy diagram
图 7. 系统层级架构图

服务层实现了本系统的业务逻辑，包含了智能合约和非智能合约两个部分，实现了应用层和服务层的连接与交互。

系统业务逻辑的智能合约实现包括证书管理合约和证书认证合约。智能合约编译部署完成后，即可利用 VNT.JS 进行调用，系统业务逻辑的非智能合约实现包括用户管理功能的实现。通过 JAVA 语言进行业务逻辑编码，以 JSON 形式与存储层中的 MySQL 数据库进行数据交换。

3) 存储层

本系统采用区块链平台和数据库两种存储引擎，两者各有优缺点。区块链上的数据具有不可篡改且防伪可溯源的特性，能够作为学位认证的依据。但通过发送交易的方式在公有链上存储数据是需要消耗数字货币的，出于系统成本考虑，仅把最重要的数据上链存储。本系统将学位信息存储在 VNT Chain 区块链平台上。MySQL 作为传统的数据库，具有操作简单和访问高效的特点，但其中心化的数据库容易出现单点故障的问题，存在较高的安全隐患。本系统将学位证书上的证件照存储于 MySQL 数据库中，在提高安全性的同时，大大提高了证件照的读取速率。

7. 结语

本文根据区块链技术的核心优势，提出了一种基于区块链的学位认证管理系统设计，创新性地以 VNT

Chain 作为底层区块链框架，其高 TPS 大大提高了系统效率，且存储于区块链上的学位信息具有更高的安全性、防篡改性以及可追溯性；系统结合智能合约技术，无需第三方可信中心参与即可实现学位认证一系列流程管理，在免去大量人工成本的同时，提高了系统内部可信度。与传统学历学位认证方式相比，本系统可以实现去中心化的数据管理，保证学位信息的客观真实性，同时具有更高的认证效率。

参考文献

[1] 涂爱爱. 浅谈学历学位认证和高校学籍档案管理[J]. 人力资源, 2019(8): 34.

[2] 学信网. 学信网推出学信二维码轻松实现学籍移动验证[J].中国大学生就业, 2017(3): 2.

[3] 胡旭东, 段兆辉, 周春天, 贾志娟. 区块链: 基于可信学位认证的研究[J].电脑编程技巧与维护, 2021(2): 26-28+36.

[4] 汪菲. 基于区块链的去中心化可信数据共享技术研究[D]: [硕士学位论文]. 南京: 南京邮电大学, 2020.

[5] 吴颖. 我国区块链技术专利特点及发展趋势分析[J]. 河南科技, 2020, 39(24): 39-43.

[6] 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(4): 481-494.

[7] VNT Chain (2019) VNT Chain Distributed Smart Value Network Whitepaper. http://vntchain.io/whitepaper-en.pdf

[8] 张蕾, 吴敏. 基于区块链技术的终身教育体系模型[J]. 西北民族大学学报(哲学社会科学版), 2020(6): 123-131.