基于区块链的校园数据安全审计研究①

万振环　洪希多　郑传钦
（厦门医学院信息中心　福建厦门　361000）

摘　要　［目的］提升校园数据安全，研究区块链技术在校园数据安全中的应用。［方法］分析了区块链的原理和核心技术，主要涉及哈希算法、共识机制和智能合约，结合校园数据安全审计需求，设计基于区块链技术的校园数据安全审计系统。［结果］设计部署安全审计系统，区块链技术与大数据中心应用系统深度结合，能形成严格的、实时的安全审计。［局限］就校园数据产生、存储、传输、使用来看，区块链技术在数据的安全应用方面还有很大的提升空间。［结论］通过探索实践，推动区块链技术在高校信息化建设中应用，提供一定参考借鉴作用。

关键词　区块链；校园数据；安全审计

Research on Campus Data Security Audit Based on Blockchain

Wan Zhenhuan　Hong xiduo　Zheng Chuanqin
（Information Center of Xiamen Medical College，Xiamen Fujian，361000，China）

Abstract　［**Objective**］In order to improve the campus data security，the application of blockchain technology in campus data security is studied.［**Methods**］This paper analyzes the principle and core technology of blockchain，mainly involving hash algorithm，consensus mechanism and smart contract. Combined with the requirements of campus data security audit，a campus data security audit system based on blockchain technology is designed.［**Results**］The security audit system is designed and deployed，which deeply combines the blockchain technology with the big data center application system to form a strict and real-time security audit.［**Limitations**］In terms of campus data generation，storage，transmission and use，blockchain technology still has a lot of room for improvement in data security application.［**Conclusions**］

①本文系福建省中青年教师教育科研项目“基于区块链的校园数据安全提升研究”（项目编号：JAT191922），福建省教育科学“十三五”规划课题“新医科卓越医生‘人工智能 & 大数据’核心素养培养研究”（项目编号：FJJKCG19–283）的研究成果之一。

Through exploration and practice，we can promote the application of blockchain technology in the information construction of colleges and universities，and provide some reference.

Keywords Blockchain；Campus Data；Security Audit

1 引言

随着信息技术的发展，传统教育环境正转向开放、智能、个性化和精细化，信息化已打破教育的时间和空间的限制。高校日常活动中积累下来的各种数字化的资源，在高校寻求跨校交流、校企合作、跨界合作的过程中，这些数字化的资源贯穿于交流合作的整个过程，数字资源已具有数字资产的特性。如火如荼的数字校园建设促进了高校的教学、科研、管理、服务水平不断提高，大量的数据资源得到了创造、采集、传输和应用。

区块链（Blockchain）是一个分布式数据库，从设计之初就具有不可篡改、可验证、可信任、可追溯的特性。区块链本质上是一个状态机副本协议，旨在建立一个去中心或弱中心化的数据库系统，实现分布式环境下安全高效的共识机制，除了在电子货币中取得的成果外，基于区块链可实现更广泛意义上的安全多方计算。因此，区块链技术可应用的领域相对电子货币更加广泛[1]。

2016年10月，我国发布了《中国区块链技术和应用发展白皮书》，指出区块链“透明化、数据不可篡改等特征，对教育就业的健康发展具有重要的价值”[2]。其后，在2018年4月发布的《教育信息化2.0行动计划》中，明确提出要积极探索基于区块链技术的“智能学习效果、记录、转移、交换、认证等有效方式”，将技术深度融入教育教学[3]。2019年10月中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，要积极推动区块链技术在教育等领域的应用。

2017年6月1日起正式实施了《网络安全法》，要求信息系统运营者落实网络安全责任，履行网络安全保护义务。信息系统审计作为督促网络安全责任落实的有效手段，能够及时发现信息系统存在的问题，揭示、抵御、预防安全风险，督促信息系统运营者及时修复安全问题，强化信息系统应对网络安全威胁和风险的能力[4]。传统审计系统是中心化系统，存在数据被篡改、无法确权、追查取证效率低、各方抵赖等问题。在应用系统的数据安全审计方面融合区块链技术，充分发挥区块链技术特长，利用分布式存储提高审计数据安全性和抗毁性，通过共识机制将审计记录存储到区块链中，采用密码学技术保证数据的安全性和可追溯性。

2 区块链技术

2.1 区块链原理

区块链概念随着比特币的火热交易被世人广泛关注。区块链技术通过分布式存储，基于点对点网络，使数据达到一致性，并在此基础上提供应用服务的一项计算机技术[5]。全网多个分布式存储的节点组成一个总库，每个完全的节点都拥有完整的区块链，最长的区块链总是被各个节点信任。区块链是由多个区块构成的有序链表，区块中的主要数据是交易记录（操作记录），每一个区块都指向前一个区块，从而形成区块链（如图1所示）。当节点构造了新的交易记录后，交易记录向全网广

图 1　区块链结构

播，具有验证和打包能力的节点收到交易记录后通过共识算法，将生成的新区块打包后全网广播，其他节点通过校验新区块后将新区块追加到节点的区块链中。

区块有唯一的区块哈希标识，每个区块通过记录上一区块的区块哈希标识来指向上一区块，通过Merkle哈希来确保该区块的所有交易记录无法被篡改。区块链系统具有去中心化的特点，去中心化主要描述的是节点有效参与共识过程的数量，参与共识的节点数量越多，去中心化程度就越高。

通常来讲，区块链可以分为两大类：公有链和许可链，其中许可链可以分为私有链和联盟链[6]。除了在电子货币中取得的成果外，基于区块链可实现更广泛意义上的安全多方计算，区块链技术可应用的领域相对电子货币更加广泛[7]。

2.2　哈希算法

哈希算法是一个单向函数，该函数可以把任意长度的输入转换为固定长度的输出，描述为：$h=H(x)$。单向函数的特点让哈希算法很容易得到固定长度的输出，但要从输出推导出输入非常困难，只能用穷举法暴力破解。一个典型的使用哈希值检验从网络下载的文件是否有被篡改的方法，可以使用MD5哈希算法计算哈希值，再与官方提供的MD5哈希值比较，如果哈希值相同则可以肯定文件没有被篡改。

一个安全的哈希函数，通常还应该满足碰撞率低和输出无规律两个要求。如果输入的是两个不同数据，而输出结果最后却是相同的，这就称为碰撞[8]。哈希碰撞的本质是把无限的集合映射到了有限的集合中，显然输出的位数越多，碰撞的概率就越低。区块链中常用SHA-256和RipeMDL160哈希算法[9]，比特币协议中对数据进行两次SHA-256通常被称为Hash256或Dhash，如果先计算SHA-256再计算RipeMDL160，通常被称为Hash160（表1为常用的哈希算法）。

表 1　常用的哈希算法

哈希算法	输出长度
MD5	16 bytes
SHA-1	20 bytes
SHA-256	32 bytes
Hash256	32 bytes
SHA-512	64 bytes
RipeMD160	20 bytes
Hash160	20 bytes

在区块链中使用Merkle哈希来防止交易记录被篡改[10]。区块中的多个交易记录分别做Hash256，将得到的哈希值两两拼接起来继续做Hash256，如果出现单数就将剩下的哈希值复制一份，继续将得到的哈希值两两拼接做Hash256直到最终的哈希值即为Merkle哈希

（图2为Merkle Hash生成方法）。修改交易记录中的任一内容，都会导致Merkle哈希改变，也导致计算出的区块哈希标识改变，下一区块指向当前区块的链接也就断了，区块链的

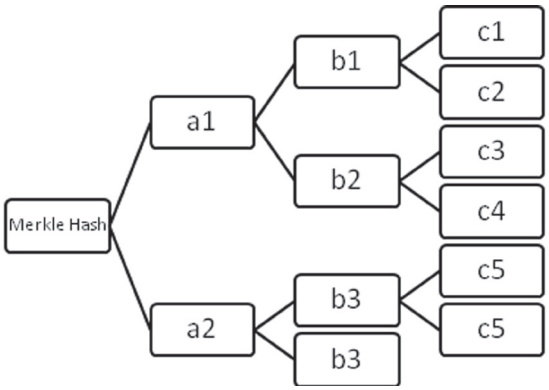

图 2　Merkle Hash 生成方法

这种设计保证了交易记录无法被篡改。

2.3　共识机制与智能合约

共识机制主要解决分布式网络中节点之间的信息不对称问题，保证数据完整性，兼容单点故障。通过共识算法保证同一个区块只能有一个节点产生和广播，其他节点只能进行验证和同步副本操作。常用的共识算法有Clique PoA（授权证明）、PoW（工作量证明）、PoS（权益证明）、DPoS（股份授权证明）、PBFT（实用拜占庭容错）等，其中Clique PoA、PoW、PoS等算法基于证明，是目前公链区块链最为常用的一种共识机制算法。区块链是一个去中心化的分布式架构，节点的注册和退出频繁，节点数量和在线比例一直在变化，基于证明的共识机制的评判标准可以引申为区块链的安全性定义。

智能合约是区块链和外部对接的接口。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议，能够使设备在不受干扰的环境下主动执行各种交易并解决其身份认证问题[11]。智能合约具有主动执行和技术信任的特性[12]。通过智能合约的调用、区块的生成和区块的共识可以确保数字资产的安全，由于区块链的存储限制，数据保全的对象是经哈希算法处理后的HASH值。智能合约在节点间共识算法的基础上完成，智能合约为区块链的应用构建了一个信任的合作环境。

3　校园数据安全审计

3.1　校园数据

随着网络技术的不断发展和应用，数字校园、智慧校园的建设如火如荼，高校的科研、教学、管理技术水平也不断提高，各种应用系统应运而生，海量的数据在校园里产生、存储、传输、使用，校园数据安全也越来越重要。2018年《智慧校园总体框架》颁布，部署了智慧校园的总体架构。2020年由于疫情的影响，跨校和跨平台直播、慕课兴起，在线教育得到了极大的发展，教与学的关系从来没有像现在这样依赖信息技术，教学管理的信息化也得到了发展。

从区块链与教育的研究热点来看，区块链在教育中的应用主要关注学习者与教育者，大致以“学分认证”“区块链成绩单”为代表的学习成果管理，作为区块链与教育融合的切入点，力图构建基于区块链技术的学习社区，增强学习体验[13]。就校园数据产生、存储、传输、使用来看，校园数据作为数据资产在数据安全方面与区块链技术还有很大的结合提升空间。

3.2　校园数据安全审计背景

信息系统审计是社会和时代不断发展、计算机技术飞速发展背景下的审计核心环节，因为利用计算机进行审计工作是建立在完善的计算机信息系统基础之上的，而信息系统审计便是专门针对计算机信息系统开展的一项现代化审计工作[14]。在业务系统、视频、大数据、移动互联网技术平台的应用发展过程中，站在

全局的角度建立完整的安全体系并符合国家《信息系统安全等级保护管理办法》的要求，将数据生命周期的不同阶段从不同角度面临的风险放到一起进行综合考虑，建立强调整体而不是某个环节的安全能力，要以信息系统数据安全的核心技术思想为指导，需加强数据平台的安全防护能力，提高数据安全审计要求，数据安全审计比信息系统审计更具有现实意义。

国家安全等级保护要求加强对安全审计功能的建设，并要求建设统一的安全审计系统，区块链技术与大数据中心应用系统深度结合，能形成严格的、实时的安全审计，并利用区块链不可篡改、不可否认及可追溯等特性加强数据安全的安全审计，防止业务系统的敏感信息泄露[15]。传统的审计系统是中心化架构存在数据被篡改的风险和无法确权的问题[16]，传统的审计系统还存在追查取证效率低，出现问题后追溯难的问题。随着高校信息化建设的推进，统一身份认证，大数据中心等平台的建设，为解决数字校园各业务应用系统的审计功能分散、审计数据孤岛等问题提供了条件。区块链技术已经在多个行业落地应用，市场已有较为成熟的应用案例，在现有的服务器和网络环境中部署数据安全的区块链审计系统不会有任何影响，构建联盟链，节点的部署可采用虚拟机方式，也可采用Docker方式进行逻辑分离部署，利用区块链技术提高大数据中心数据安全的审计管理，防止敏感数据泄露是可行的。

3.3 数据安全审计系统设计

（1）系统概述。

在区块链记账上链的过程中，其核心技术便是共识机制，通过共识机制能够确保上链的所有节点依照统一的管理协议进行自我管理，从而实现区块链中的相关数据被分布式记账与存储[17]。各业务系统通过大数据中心平台对数据进行读写、抽取操作，结合身份认证形成的操作记录和数据抽取记录，是数据安全审计的主要内容。安全审计系统通过共识算法和智能合约主动运转，将数据记录按时间顺序存储区块并加入到区块链中，可以实现数据不可篡改，同时采用密码学技术保证了数据的安全性和不可否认性，利用时间戳服务实现审计记录的可追溯。利用区块链技术特点，实现数据安全的区块链审计系统，可以采用聚龙链方案[18]。

①各应用系统的数据集中在大数中心管理。利用区块链技术构建大数据中心应用系统的审计联盟链，大数据中心应用系统的操作记录上链；

②联盟链网络中接入4A系统，采用与全网单点登录访问体系一致的数据证书，操作访问记录登记到区块链中；

③使用联盟链平台自带的CA管理系统颁布数字证书，用于大数据中心应用系统、数据共享平台访问区块链平台，确保审计记录上链的合法性；

④数据安全的审计监管，以审计节点接入审计联盟链，实现统一审计追溯功能，大数据中心平台节点、统一数据共享平台节点、身份认证平台节点为区块链的主要节点，实现并负责区块链的共识算法和智能合约的执行，并实现对安全审计的数据进行分布式记账存储功能。

（2）系统架构。

数据安全的区块链审计系统包括区块链技术平台及基于区块链技术平台实现的审计智能合约、审计区块链受理登记、安全审计应用及区块链可视化管理等功能，功能架构如图3所示。

（3）系统功能。

在区块链技术平台中，提供联盟链网络中具体的区块链服务功能，采用实体挂载服务

图 3　区块链审计系统架构

的方式，一个节点可以装配若干网络实体服务实现节点的实际功能。主要提供来自业务应用系统的账本服务、背书服务、广播服务、投递服务、智能合约服务、事件服务、节点管理服务，并提供命令行前端管理系统，实现平台的交易服务、共识服务、区块服务、状态服务、事件服务、提案服务、PKI服务及验证服务等功能。智能合约运行环境亦由区块链技术平台提供，包括编译工具、部署工具、合约框架、合约规范、合约SDK、系统合约及应用合约，为上层的定制化智能合约提供服务。

智能合约利用时间戳、智能合约服务及账本实现数据安全的安全审计相关数据在区块链中的自动处理和运转，实现对安全审计的数据进行分布式记账存储功能，具体功能如下。

①操作记录智能合约，实现大数据中心应用系统的系统操作记录、登录记录等数据登记至区块链中，同时实现操作记录的链上查询功能；

②数据共享智能合约，实现大数据中心的数据共享访问记录的登记至区块链中，同时实现数据共享访问记录的查询功能。

审计区块链受理登记，实现大数据中心平台的数据操作过程数据作为审计记录统一登记到区块链，并实现大数据中心对外数据共享访问的审计记录登记到区块链。功能模块包括消息队列模块、数据安全模块、智能合约登记模块、区块链信息查询模块及登记配置模块。

安全审计应用作为联盟区块链的节点接入，对区块链中的记录的数据操作过程数据进行安全审计，实现各信息化系统的数据操作统一安全审计，审计内容包括操作行为审计、重要安全事件审计及审计分析。

①操作行为审计，实现应用系统对数据的读写操作记录、数据共享记录的追溯，提供操作行为异常告警提醒，实现根据用户名、IP地址、操作关键字的审计查询。

②审计分析，实现数据安全相关的审计分析，提供图表化的统计功能，通过区块链可视化管理模块展示运行状态、智能合约、区块信息、账本信息等直观可视的界面（图4为区块情况，图5为审计记录），从而实现区块链技术平台的常规监控、审计异常情况警示提醒功能。

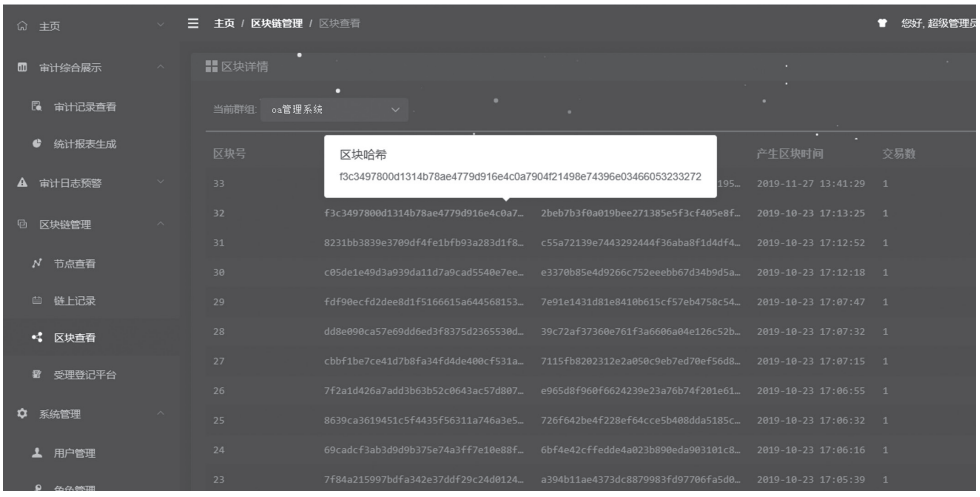

图 4　区块情况

图 5　审计记录

4　结语

本文对区块链技术在校园数据安全审计的应用机制和系统设计进行了初步的研究和应用实践。文章首先从哈希算法、共识机制与智能合约三个方面概述了区块链的基本原理和核心技术，再通过分析校园数据安全审计的需求背景，结合区块链技术的去中心化、可验证性、无法篡改等特性，从校园数据安全审计角度设计了安全审计系统。通过构建基于区块链的校园数据安全审计系统，提升了校园数据安全，探索并实践了区块链技术在高校信息化建设中的应用途径，对推动区块链技术在高校信息化建设中的应用，起到了一定的参考借鉴作用。

参考文献

[1] 刘明达，拾以娟，陈左宁. 基于区块链的分布式可信网络连接架构 [J]. 软件学报，

2019，30（08）：2314—2336.
[2] 周平. 中国区块链技术和应用发展白皮书[R]. 北京：中国区块链技术和产业发展论坛，2016：36—37.
[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[EB/OL]. [2019-11-17]. http：//www.moe.gov.cn/srcsite/A16/s3342/201804/t20180425_334188.html.
[4] 孙彦，刘贤刚，蔡磊. 美国信息系统审计机制研究[J]. 信息安全研究，2017，3（12）：1108—1114.
[5] 张亮，刘百祥，张如意，等. 区块链技术综述[J]. 计算机工程，2019，45（05）：1—12.
[6] 宋焘谊，赵运磊. 区块链共识算法的比较研究[J]. 计算机应用与软件，2018，35（08）：1—8.
[7] 刘明达，拾以娟，陈左宁. 基于区块链的分布式可信网络连接架构[J]. 软件学报，2019，30（08）：2314—2336.
[8] 贺元香，夏甜，史宝明. 区块链核心技术探究[J]. 兰州文理学院学报（自然科学版），2020，34（06）：92—98.
[9] MARTINO R，CILARDO A. Designing a SHA-256 processor for blockchain-based IoT applications[J]. Internet of Things，2020，11：100254.
[10] 袁多宝，王晓明. 基于MH树的外包数据库查询验证方法[J]. 计算机工程，2010，36（04）：115—117.
[11] 陈伟利，郑子彬. 区块链数据分析：现状、趋势与挑战[J]. 计算机研究与发展，2018，55（09）：1853—1870.
[12] 吉宇宽. 区块链下智能合约对图书馆著作权利益的限制与改进策略[J]. 国家图书馆学刊，2020，29（06）：3—10.
[13] 吴永和，程歌星，陈雅云，等. 国内外“区块链+教育”之研究现状、热点分析与发展思考[J]. 远程教育杂志，2020，38（01）：38—49.
[14] 申亚君. 信息系统审计中计算机审计的应用[J].数字技术与应用，2019，37（12）：59—60.
[15] 朱岩，张艺，王迪，等. 网络安全等级保护下的区块链评估方法[J]. 工程科学学报，2020，42（10）：1267—1285.
[16] 蒋乐平. 区块链视角下环境会计信息系统的优化与融合[J]. 财会月刊，2018（19）：52—56.
[17] 李兆东，王嘉成. 金融机构区块链审计框架研究[J]. 会计之友，2020（21）：156—161.
[18] 端震，朱嘉慧. 我国区块链技术标准发展现状综述[J]. 软件，2020，41（10）：242—245+259.