大数据背景下基于区块链技术的高校网络信息安全模式研究

徐 军[a],姜 奎[b],张宗宇[a],陈士超[b],孙前祖[c]

(蚌埠工商学院 a.计算机与数据工程学院;b.科研与规划处;c.现代教育技术中心,
安徽 蚌埠 233000)

摘 要:区块链技术作为一项新兴的信息科学技术,已上升为国家战略层面。大数据技术的产生和发展也为信息的共享和使用奠定了基础,在大数据背景下,将区块链技术与大数据信息共享相结合,利用区块链技术中"信任"与"共识"等机制在保证信息使用的同时提高网络安全和信息安全,构建高校联盟链的信息共享模式,提出了一种能保护用户隐私的高校网络安全理论框架。

关键词:大数据;区块链技术;高校联盟链;信息安全

中图分类号:TP309.2 **文献标识码:**A **文章编号:**1674-344X(2023)02-0005-06

1 引言

现今社会,随着计算机技术、网络技术、数据库技术的不断发展,信息和数据已成为重要资源。网络成为生活中不可或缺的部分,时刻产生数以亿计的信息和数据,大数据技术为数据的共享和使用奠定了基础,人类开启了智能时代。国务院办公厅在2016年7月发布的《国家信息化发展战略纲要》[1]中提出全面推进我国大数据发展和应用,加快建设数据强国。《"十三五"国家信息化规划》[2]中强调要构建可靠安全、互联互通的数据共享开放体系。数据隐私对人们的生活和工作产生了很大的影响,在医疗健康、金融等领域,数据隐私保护已成为重中之重。传统系统的中心化他信机制由于不基于完全可靠的第三方,数据隐私容易泄露,并且数据在第三方中也不能由用户自己控制,数据的不可控性也会产生一系列的安全问题。[3]

2017年5月,国务院发布《政务信息系统整合共享实施方案》[4],提出政务类数据的开放共享有助于国家政策的推进与部署,是我国政府顶层设计的重要环节之一。国家主席习近平在向2018年5月26日于中国贵州省贵阳市举行的中国国际大数据产品展览会中致贺信,并表示我国高度重视中国大数据分析的蓬勃发展,同

收稿日期:2022-11-15

基金项目:2020年安徽省高等学校省级质量工程项目"Access数据库应用基础"(2020kfkc312);2021年安徽省高等学校省级质量工程项目"计算机公共基础课程教学团队"(2021jxtd179);"计算机科学与技术试验实训中心"(2021sysxzx018);2021年安徽省高等学校自然科学重点项目"大数据背景下基于区块链技术的高校网络信息安全模式研究"(KJ2021A1236);2022年安徽省高校学科(专业)拔尖人才学术资助项目(gxbjZD2022099)

作者简介:徐 军(1972-),男,安徽淮北人,副教授,硕士,中国计算机学会(CCF)会员,研究方向为大数据应用、区块链技术、信息安全。

姜 奎(1990-)男,安徽宿州人,讲师,硕士,研究方向为金融数学、区块链。

张宗宇(1984-)男,山东沂源人,讲师,硕士,研究方向为计算机应用技术。

陈士超(1982-)男,河南商丘人,讲师,博士,研究方向为数据可视化分析。

孙前祖(1990-)男,甘肃白银人,工程师,研究方向为信息系统管理与优化。

时将秉持开放式、资源共享、技术创新的经济发展思路，围绕着“数化万物·智在融合”的博览会主旨，积极促进中国大数据分析行业再创新高。2018年3月17日，Facebook客户信息泄露事件已经演变成为重大的政治事件、经济事件，也是金融事件、科技事件、大数据事件，反映出很多数据泄露方面的深层次问题，比如在高校管理工作中，需要各种信息系统、数据库来管理和使用学生信息，在大数据背景下，数据量大，数据共享透明，学生对于隐私信息保护和防范意识较弱，现有的数据存储和管理模式也存在着安全隐患，给一些不法分子以可乘之机。2016年9月湖南某大学因学生信息泄露，18名大学生发现“被贷款”50余万元；2018年9月江苏某大学大量学生信息泄露，信息疑被内地多家企业用于偷逃税款。这类实例不胜枚举，现今网络诈骗、电信诈骗日渐猖獗，国家增强反诈骗宣传力度并推出反诈骗APP，各高校同时开展防诈骗宣传教育等活动。因此，在大数据背景下，如何保证信息安全，保证网络安全，防止信息在共享和使用中泄露，成为高校校园网安全重点研究的问题。

2　区块链背景知识及技术特点

2.1　区块链背景知识

区块链来源于比特币，但从根本上来说，它是一个分布式的资源网络，所有储存在这里的资源或数字，都具有无法篡改、全程留痕、可溯源、公开透明化、共同维护等特点。而所有这些基本特征正契合了大数据背景下学生信息在校园网络中共享和使用中的安全需求。通过区块链技术建立起强大的“信任”基础和可信的“合作”关系，同时创造出一个去中心化的、无需信用积累的信息系统是新的高校网络信息安全模式在区块链中，每一位成员的行为均被妥善记录，再使用加密算法保证这个信息体系的高安全性。这种分布式无中心的共识机制，使得区块链技术应用于校园网络安全时可以极大提升数据在共享使用过程中的安全等级。

2.2　区块链技术特点

区块链技术特点：(1)去中心化——一笔交易在区块链中，不需要任何第三方机构的信任背书，通过代码就可以完成。(2)公开透明——区块链系统都是开放的，除交易过程双方当事人的私有信息被严格加密之外，所有链条上数据都对所有人开放。(3)独立自治——区块链采用基于协商一致的规范和协议，不依赖其他第三方，不需要任何人为的干预。(4)更加安全——区块链使用了密码学算法和共识机制，区块链数据具有不可篡改性，具有非常高的稳定性和可靠性。(5)匿名——各区块节点的身份信息都不要求发布或认证，因此消息传播都可以通过匿名方式完成。

以上技术特点如果能用于校园网络，将会构建一个开源、包容、安全、私密的校园网络环境，校园数据可以共享，隐私得到保护。区块链技术在银行和其他金融机构中已经实现了相对充分的开发和使用，其本身具有很高的安全性，因此应用于高校网络信息安全中也一样可以发挥重要作用。随着区块链应用越来越广泛，技术愈发成熟，基于区块链技术，考虑以大数据、人工智能等先进技术为核心打造综合性教育服务平台，利用区块链技术建立全新的教学资源信息库，可以为每一位学生量身打造最优质的培养方案，帮助学生跨越式成长。

3　研究现状

区块链是当下流行的加密数字货币体系的核心和底层技术，随着现代通信与互联网技术的发展，区块链技术在诸多领域与具体生产应用结合，其基于特殊的加密算法和核心机制，成为多数国内外学者共同关注的热点。2013年12月，以太坊创始人维塔利克·布特林(Vitalik Buterin)[5]发布了以太坊白皮书，定义了去中心化应用平台协议，2015年6月发布第一个正式版本，以太坊正式运行，并成功将智能合约应用于区块链，使区块链领域发生了翻天覆地的巨大变化。

2015年Melanie Swan[6]认为，区块链应用前景广阔，可以适用于社会的方方面面。

Clare Sullivan等[7]学者认为，爱沙尼亚(E.Residency)理念的提出是区块链技术所带来的令人印象深刻的重要事件之一，爱沙尼亚项目提供一个值得信赖的欧盟公民身份来帮助投资者启动和运行全球业务，这一身份是区别于目前的实体证件的一种虚拟证件。这种虚拟证件的应用必然有着基于区块链技术的个人信息认证和信任过程，可见区块链技术对于网络中个人信息的认证和保障信息安全方面有着深远的考量。

ZYSKIND等[8]认为在传统的中央节点数据系统中,数据存放在中心服务器,而中心服务器的管理缺失或设备故障都可能导致数据的损失或泄漏。

2016年AITZHAN等[9]认为利用去中心化的操作系统架构,将数据和数据的存储权限分离。运用区块链的去中心化体系架构和核心保密工作机制,能够大大减少资源管理中信息泄露的危害性。

4　高校网络信息安全区块链架构理论框架

通过区块链的智能合约能够缩短认证流程,将校内与校外的优质教育资源加以融合,从而建立了校内的区块链联盟,每一名教师和学生都能够跨越地域通过任一区块链资源节点,获得联盟的资源共享。并且,区块链的分布式架构能够使每个学校共享的信息数据不会因为某一块链节点失效而失去同时使用的可能。消除单独故障提高了整个高校的区块链信息数据的安全性和完整性,从而缓解高校高质量在线教育信息和学术研究资料面临无法跨学校、跨地域、跨联盟共享的困境。

目前的区块链一般包括公有链、私有链[10]和联盟链等3类,公有链面向公众开放,任何用户无须注册都可以匿名参加,在未经授权的情况下访问网络和区块链,为确保安全使用密码学算法确保数据不被修改。私有链通常在机构内部使用,按照私有机构的规则制定其读写权限和参与记账权限。不同于公有区块链,联盟链仅仅限于联盟成员参与,它是需要注册许可的区块链,其读写权限和参与记账权限根据联盟规则制定。其特点适合应用于高校校园网络,通过将校园网的各类用户划分角色,赋予每类用户节点以不同的权限。[11]通过上述分析,不难看出联盟链运行于多个机构之上,用户入网前须经过注册认证,其共识过程由多个成员共同参与[12],其原理应用在校园网的实名认证是完全可行的。

4.1　利用智能合约与身份认证构建网络安全防线

20世纪90年代尼克萨博(Nick Szabo)首次提出了智能合约理念,并将它形容为“一个以数字形式描述的合同,并且合同参加方遵守它们规定的合同”。[13]我们把其工作原理应用于高校学生信息收集存储、共享等场景嵌入区块链技术,构建基于区块链的高校应用创新信息化平台的理论框架。使用区块链信息技术中的智能协议来实现数据信息集成存放与收集,减少使用APP软件信息收集不及时的现象。智能契约并非是形式上的数字化契约[14],其最终目的是提供优于传统合约的安全措施,并减少与合约相关的其他交易成本,避免了在传统交易系统中要求第三方组织进行贸易监督的问题。类似一个人可以在同一部电脑上或计算机中按预置设定,自动履行规定的内容契约。在区块链上智能合约还具备了很多特点,比如可编程、不可修改、去信任等,并且通过智能合约还可灵活嵌入各种数据和数字资产,安全有效的进行信息、质量控制与管理。为构建可编程资、系统和社会提供服务支持。[13]

以迎新开学为例,假设新生已入校,但发现其在报到后有尚未完成的入校记录,一般汇总后出现遗忘再去高校补办,效率将相当低,但如果使用智能合约来完成学生信息登记,效率就会提升很多。这种做法在高校区块链中被设定为两种情况:情况一,当本科新生志愿录入时高校信息已全部进入录取高校,系统中必须设定具体时间并检查是否已被成功执行;情况二,当学生报到到达或进入校园,必须和校园的安检系统联动验证通过,来证实学生已入校。而一旦智能合约系统确定已入校,学生的所有个人信息便开始注册登记,不用学生再去主动验证。相比于传统公有区块链,注册与登记通过联合区块链中最特殊的身份机制方式实现,实现联盟准入机制[15],实现隐私数据对外不可见的要求,这对于高校信息网络的安全来说有着重要意义。

考虑到当前学校疫情防控常态化管理,身份认证注册[15]可以采用线下线上混合模式。步骤如下:第一步,学生可以在线下通过身份证向学校信息化管理部门CA机构提交用户名和密码申请,然后在客户端上使用用户名和密码在线发出登录申请;第二步,学校信息化管理部门CA机构会在学校中心数据库中标识该用户名和密码,并返还注册证书给学生;第三步,学生通过注册证书,再向CA提交TLS证书用以连接本校联盟的区块链网络;第四步,CA审查数据库中是否识别了该登录学生,如已识别将返还TLS证书到应用客户端。高校联盟链身份注册认证机制如图1所示。

4.2　校园联盟共享数据存储与管理

区块链是去中心化的记账系统,校园联盟共享数据存储要使用可信的方式来记录数据,使得用户信任区块链记录的数据,不需要假设记账节点的可信性,我们在这个框架系统设计里对数据存储和管理采用分布式

存储来实现，并利用共识机制解决分布式存储中的一致性问题。

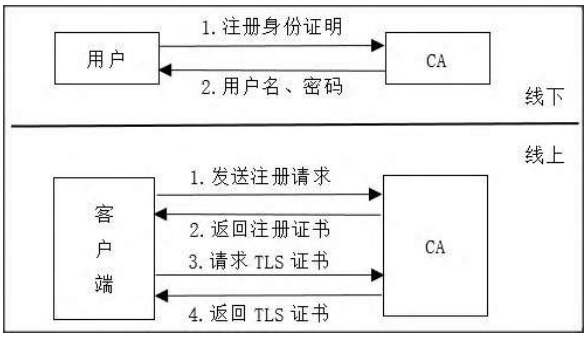

图1　身份注册认证机制

Hyperledger Fabric[16]作为当前使用较为普遍的企业级联盟链，由于其具备节点权限准入、实名身份验证、高性能共识管理机制等特性，再加上高度可程序设计的信息保障智能协议，Fabric可以有效解决大学校园信息网络中对安全保障的要求，因此，选择采用联盟链作为高校网络信息系统的区块链实现平台。通过区块链技术的分布式信息储存功能可以把过去集中式信息存放方法彻底取代，不必再构建大型的信息数据库系统，从而能够极大限度减少信息的成本。高校的各类学生证书、成绩单、获奖资料、学籍信息等大量数据资料都能够通过时间戳标记，并分别存放到区块链结点上。建立“校园联盟”能够推动学校资源整合。通过建立校园联盟链，可以实现数据共享，减少数据烟囱，促进学校资源的有效配置与利用，从而推动了院校间的信息合作开展，最终实现除私密信息之外的已发布的所有信息数据和共享，整个校园联盟的安全性与稳定性就会得到有效地防护。基于区块链的校园联盟共享架构体系如图2所示。

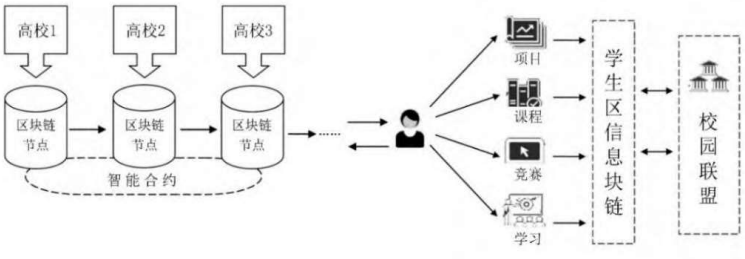

图2　基于区块链的校园联盟共享架构体系

4.3　高校联盟网络信息系统区块链分层架构

随着区块链的蓬勃发展，为了实现不同目的[17]的各种区块链平台纷纷诞生，尽管它们的体系结构并不完全一致，但依然存在相通之处。以设计高校联盟网络信息系统为例，把高校联盟网络信息系统平台分为四层，分别为数据层、网络层、共识层和应用层，如图3所示。

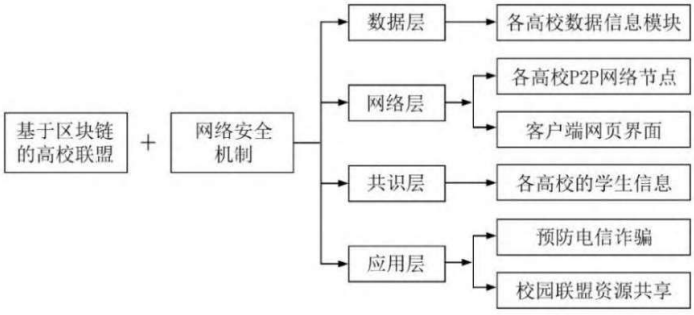

图3　基于区块链的高校联盟网络信息系统框架图

4.3.1　数据层

在数据层，采用封装的链式结构、非对称密码、共识计算等手段来实现信息的保存以及交易的安全实现，相比传统的数据库，它提供了更为高效的链式存储，并使用加密形式的数据为信息系统提供了隐私和数据完整性的基础保护功能。在Haber等[18]-[20]的研究基础上，结合使用哈希指针来实现各高校区块之间的连接，同时在节点间采用共识算法确保信息的统一性，让整个区块链在全网开放的状况下确保了信息的不能伪造与可追溯。将计划通过分布式账本系统，依托校园联盟内的高校主体，有序地将学生个人信息、校园成长轨迹信息、学籍档案信息、竞赛社团信息等纳入高校信联盟信息系统数据库，形成“区块链+学生+高校”模型，充分完善学生各类信息。

4.3.2　网络层

区块链网络层采用的协议一般有P2P协议、加密传输协议、路由协议和底层OSI协议。本文基于区块链的高校联盟网络信息系统采用对等节点的方法进行组网，校园网数据与资料的传送可以通过每一个节点进行，实现节点端口智能技术融合，授权和验证技术融合，共识机制融合，分布式账本融合等。

4.3.3　共识层

共识层主要解决两个问题：(1)谁有权利；(2)如何防止作弊。在一个区块链的分布式系统中，除了建立在P2P连接上的可靠数据传输外，分布式共识层为维护区块链网络中数据的排序，为其本身的依次性和原创性提供了核心功能。各节点之间通过某一机制在短时间内排除恶意节点的干扰达成共识。区块链和传统分布式系统提出的CAP[21]评价标准相比较，去中心化、可扩展性、安全性三者不能同时满足。共识协议依赖于半集中式共识框架和更高的数据传递开销，以提供网络的即时共识评论，并提高交易处理的吞吐量。无权限的共识机制[22]更适合于对节点的同步和行为进行松散控制的区块链网络，在有限延迟和大部分节点为诚实节点的情况下，以较低处理效率为代价的无权限共识协议明显为校园网络的可伸缩性提高了更好的支持。

4.3.4　应用层

区块链应用于高校校园网具有独特的框架和技术体系，适合作为高校信息系统的底层支撑，用于管理分布式网络节点之间的数据或交易驱动的交互行为。应用层除针对具体的高校学生信息管理应用业务情况独立开发一个专门的应用系统外，还能够运用对深度数据分析与行业的融合功能来进行联合应用，从而构建适应功能增强的区块链信息技术研究与高校公共服务网络平台，构建“区块链+高校联盟”模式，在高校档案共享、信息资源共享、学术资源共享等方面取得应用。

5　结语

本文借助联盟区块链技术提出了一种能保护用户隐私的高校网络安全理论框架模型，建立基于区块链技术的高校教育资源应用框架，分别从数据层、网络层、共识层、应用层等方面进行探究，解决高校跨部门、跨校区及跨高校中存在的信息资源不共享、不对称等问题。在大数据背景下，使得学生信息无论是在各高校之间的横向，还是在从高中到大学到研究生的纵向教育体系中都得以快速共享和使用。此项研究对于构建学生的个人档案、学习档案、诚信档案等都具有重要意义。借助区块链的不可篡改及安全性特征，建立以区块链为基础的网络安全机制，防止学生信息恶意泄露，预防电信诈骗事件的发生，加强了的隐私保护，保证了学生信息的安全性，减少了学生信息的维护成本。

参考文献：

[1]中共中央办公厅，国务院办公厅.国家信息化发展战略纲要[Z].北京：人民出版社，2016.

[2]中共中央办公厅，国务院办公厅.《“十三五”国家信息化规划》[Z].2016-12.

[3]王童，马文平，罗维.基于区块链的信息共享及安全多方计算模型[J].计算机科学，2019(46)9：162-168

[4]国务院办公厅.《政务信息系统整合共享实施方案》[Z].2017-05.

[5]BUTERIN V A.Next-generation smart contract and decentra-lized application platform[J].Etherum Whitepaper(2014)(January)1-36.

[6]Swan M.Blockchain thinking：the brain as a decentralized autonomous corporation[J].IEEE Technology and Society Magazine，2015，34(4)：41-52.

[7]Clare Sullivan,Eric Burger.E-residency and blockchain[J].computer law & security review,2017(33):470-481.
[8]ZYSKIND G,NATHAN O.Decentralizing privacy:Using blockchain to protect personal data[C]//IEEE Security and Pri-vacy Workshops,May 21-22,2015,San Jose,CA,USA.Pisca-taway:IEEE Press,2015:180-184.
[9]AITZHAN N,SVETINOVIC D.Security and privacy in decen-tralized energy trading through multi-signatures,blockchain and anonymous messaging streams [J].IEEE Transactions on De- pendable & Secure Computing,2016(99):1.
[10]Judmayer A,Stifter N,Krombholz K,et al.Blocks and chains:introduction to bitcoin,cryptocurrencies,and their consensus mechanisms[M]//Blocks and chains:introduction to bitcoin,cryptocurrencies,and their consensus mechanisms.[S.l.]:Morgan & Claypool,2017.
[11]宁卓,李牧阳,等.基于联盟区块链的物流信息平台LIP-Chain [J].计算机技术与发展,2019,29(8):190-194.
[12]刘懿中,刘建伟,张宗洋,等.区块链共识机制研究综述[J].密码学报,2019,6(4):395-432.
[13]胡甜媛,等.智能合约的合约安全和隐私安全研究综述[J].计算机学报,2021,44(12),2485-2514.
[14]刘彦松,夏琦,李柱,等.基于区块链的链上数据安全共享体系研究[J].大数据,2020,6(5):92-105.
[15]刘宇,陈哲,李孟恒,覃团发.基于联盟区块链的体域网信息安全方案[J].计算机工程与应用,2020,56(4):57-62.
[16]ANDROULAKI E,BARGER A,BORTNIKOV V,et al.Hyperledger fabric:a distributed operating system for permissioned blockchains[C]//Proceedings of the thirteenth eurosys conference.Porto,Portugal:ACM,2018:1-15.
[17]郭上铜,王瑞锦,张凤荔.区块链技术原理与应用综述[J].计算机科学,2021,48(2):271-281.
[18]BAYERD,HABERS,STORNETTAW S.Improving the effi-ciency and reliability of digital time-stamping[C]//Sequences II:Methods in Communication,Security and Computer Science.NewYork,USA:Springer G Verlag,1993:329-334.
[19]HABER S,STORNETTA W S.How to time-stampa digital document[C]//Proceedings of the Advances in Cryptology-CRYPTO'90 (CRYPTO).Santa Barbara,USA,1990:437-455.
[20]HABER S,STORNETTA W S.Secure names forbit-strings[C]//Proceedings of the 4th ACM Conference on Computer and Communications Security(CCS).Zurich,Switzerland,1997:28-35.
[21]GILBERTS,LYNCHN.Brewer's conjecture and the feasibility of consistent,available,partition-tolerant Web services [J].ACM SIGACT News,2002,33(2):51-59.
[22]王瑞锦.区块链技术与应用[M].北京:人民邮电出版社,2022.

University Network Information Security Mode Based on Blockchain Technology in the Context of Big Data

XU Jun[1], JIANG Kui[1], ZHANG Zong-yu[1], CHEN Shi-chao[2], SUN Qian-zu[3]
(1.School of Computer and Data Engineering, 2.Scientific Research and Planning Division,
3.Modern Education Technology Center, Bengbu Business College, Bengbu Anhui 233000, China)

Abstract: As an emerging information technology, blockchain technology has been risen to the national strategic level. The emergence and development of big data technology has also laid a foundation for information sharing. In the context of big data, blockchain technology is combined with big data information sharing. Mechanisms such as trust and consensus in blockchain technology are used to ensure information use, improve network security and information security, and build an information sharing mode of university alliance chain, This paper proposes a theoretical framework of university network security that can protect users' privacy.

Key words: big data; blockchain technology; university alliance chain; information security