DOI:10.13878/j.cnki.jnuist.2019.05.005

黄达明[1]

区块链技术在教育领域的应用现状与展望

摘要

区块链本质上的去中心化和安全特性,使得其很适合于解决目前教育领域面临的困难.本文首先介绍了区块链的基本技术原理,包括区块的结构和区块链的构成、区块链技术平台的体系结构、区块链的分类、共识算法、智能合约.接着分析了目前教育领域发展的终身教育和跨地区教育的新形势,以及传统数字化教育系统面临的主要问题.然后从教育相关信息的多方共享和验证、学习过程跟踪、激励和学习路径塑造、学习评估、教育管理与决策辅助等几个方面对区块链技术在教育领域的应用现状进行了介绍和分析.最后总结了目前区块链技术应用到教育领域的主要问题,并展望了未来的发展方向.

关键词

区块链技术;教育领域;共识算法;智能合约

中图分类号 TP13

文献标志码 A

收稿日期 2019-09-20

作者简介

黄达明,男,讲师,主要研究方向为信息安全、数据科学、基础教学.huangdm@ nju.edu.cn

1 南京大学 计算机科学与技术系,南京,210023

0 引言

区块链技术的基本思想最早由中本聪在其有关比特币的论文中提出[1].在没有可靠的第三方干预的情况下,因特网应用中的各个网络节点之间很难建立起信任.区块链技术通过区块链网络节点之间基于共识机制的互相合作,在不需要互相信任的条件下,通过使用分布式的 P2P 网络协议进行通信,能够提供一种去中心化、透明的数据存储模式,存储在区块链中的数据被打包进区块构成链式结构,并复制到各个节点上,被称为分布式公共账簿,通过密码学、哈希技术、共识算法和智能合约等技术的共同配合,区块链中的数据容易被验证,但是却很难被恶意修改和完全摧毁[2-3].目前区块链技术已经被广泛研究并应用于商业、财务、医疗、政府等很多领域,但是在教育领域还很少有成熟的例子,近几年已经有越来越多的工作开始投向区块链技术在教育教学领域的应用.例如阿联酋大学(UAE University)的研究者对区块链技术进行比较,并测试了区块链技术在阿联酋大学部署的性能参数,证实大规模部署区块链网络是可行的[4].

文献[5]从宏观技术层面对区块链技术应用到教育领域的需求和过程进行了分析,认为需要主要关注几个问题:1)定义运行数据的服务和参与方;2)定义加密密钥和方法;3)关注共识算法及其执行过程;4)构建定义和部署智能合约的过程.

本文对区块链技术在教育领域的应用现状进行介绍和分析,第一节介绍区块链的技术原理;第二节阐述教育领域的发展趋势和传统数字化教育信息系统面临的问题;第三节从多方面介绍和分析区块链技术在教育领域的应用及其技术细节;第四节对区块链技术在教育领域应用面临的问题和未来研究方向进行了总结.

1 区块链技术

1.1 区块链技术的基本原理

1.1.1 区块的结构

区块链中所有应用信息以交易数据的形式保存在区块中.如果区块链是一个分布式账簿,则每个区块相当于账簿中的一页.区块的结构由区块头和区块主体构成,区块头部包含前一区块的哈希值、区块时间戳、随机神奇数、交易数据 Merkle 树根等重要数据结构,如图 1 所示.区块基于哈希、时间戳、Merkle 树、数字签名、共识协议等技术生

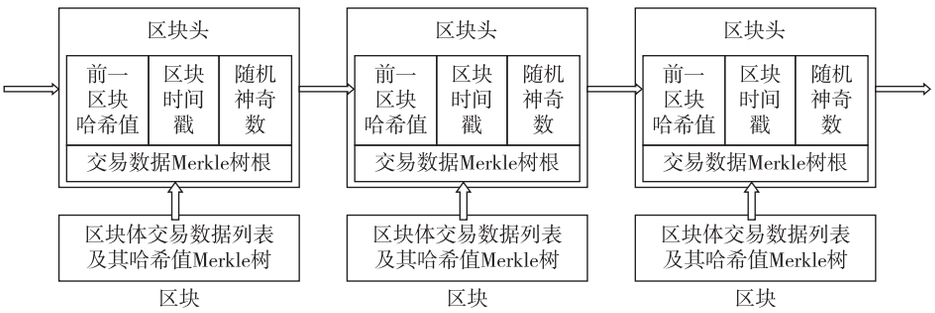

图 1　区块的结构和区块链

Fig. 1　Structure of block and blockchain

成和存储[1-3].

区块的生成节点通过在区块头部加入时间戳来标识区块生成时间,从而实现按照时间维度的交易数据可追溯性.

区块体中存储着自上一区块生成以来所完成的所有交易的数据.

在每个区块的头部包含前一区块的哈希值,通过前一区块的哈希值,可以使得所有区块构成链式结构,而新的区块按照时间顺序被加入链中,构成区块链,最初的区块被称为创世区块.而在区块体中,每笔交易数据都会被计算哈希值,然后将所有交易数据的哈希值作为叶子节点构造 Merkle 树,Merkle 树的树根作为整棵 Merkle 树的哈希值被记录到区块头部.通过这两种哈希技术的应用,对区块的篡改,包括对区块内任何一笔交易的篡改,都容易被检测到,从而保证了区块中记录的账簿数据以及区块数据本身的不可篡改性.

1.1.2　区块链技术平台体系结构

区块链技术平台体系结构综合看可以由数据层、网络层、共识层、智能合约层、应用层 5 层构成,如图 2 所示.

应用层	编程接口、用户界面、各类应用
智能合约层	脚本、虚拟机、编程语言
共识层	共识算法、激励机制
网络层	P2P网络、传播机制、验证机制
数据层	数据区块、链式结构、数据模型、文件存储

图 2　区块链技术平台体系结构

Fig. 2　Architecture of blockchain platform

1)数据层采用哈希、Merkle 树等合适的数据结构对交易、区块进行表示、组织和管理,并落实相关数据在具体节点上的存储.

2)网络层基于 P2P 对等网络技术,实现区块链节点之间的通信,完成交易和区块数据的传输以及节点间其他信息的传输任务.

3)共识层基于共识算法和激励措施,解决分布式环境下数据的一致性问题.

4)智能合约层提供构建智能合约的语言和编译服务,以及运行智能合约脚本的虚拟机和沙箱环境.

5)应用层通过提供各种可编程接口搭建基于区块链技术的各种应用,包括电子货币、商业应用、政府应用、物联网应用等,用户不必了解区块链技术的底层细节.

1.2　区块链的分类

按照区块链网络的构建和管理、节点准入条件、去中心化程度以及区块链技术的应用模式,可以将区块链分为公有链(Public Blockchain)、私有链(Private Blockchain)和联盟链(Consortium Blockchain)3 类[2-3,6].

以比特币[1]和以太坊[7]为代表的公有链,无官方管理组织机构和中心服务器,节点可以按照区块链的系统规则自由加入或退出网络,各节点具有平等的存取数据和竞争记账的权限,节点之间不需要互相信任,基于共识机制维持区块链网络展开工作,去中心化的程度最高.

以 Quorum 为代表的私有链,通常由某个组织或机构(例如企业、政府等)构建和管理,节点需要管理方授权才能加入区块链网络,且每个节点的数据读写和记账权限不完全平等,还有少数高性能的节点负责全局管理,系统的运行规则可以由构建组织自己决定并更改.在具有区块链技术不可篡改和安全性等优点的同时,只能做到部分去中心化.

以 Hyperledger/Hyperledger Fabric 为代表的联盟链,通常由多个机构和组织协商共同构建和管理,节点分属于不同的管理方,通过准入机制加入和退

出区块链网络,兼具公有链和私有链的特点,具有多中心的特征,去中心化程度高于私有链而低于公有链.在联盟链中,由预先选出的授权节点负责共识过程和区块验证.

联盟链和私有链又可以归为许可链.

公有链支持匿名化,而联盟链/私有链由于节点受管理,因此使用过程可以不匿名化,从而更容易被监管.

1.3 共识算法

区块链是存在于P2P网络上的分布式账簿式的数据库,网络中的每个节点都具有确认后的账簿状态和一系列等待打包进区块并添加到账簿的未确认的数据.为了区块链网络能够保持功能,节点需要在账簿的某个状态和将数据打包进区块的方式上取得一致意见.这是通过分布式共识算法来实现的.分布式共识算法保证足够数量的节点在分布式账簿的精确状态以及新的区块被添加到账簿的次序上达成一致,从而保证区块链网络中数据的一致性和真实性[8-10].

共识算法的主要过程由4部分构成,即选择记账节点、排序造块、验证和新区块添加到链.选择记账节点又称选主,是共识算法的核心,是根据一定的策略从所有矿工节点中选出具有记账权的节点.具有记账权的节点会将网络中当前时间段内的交易依据区块容量、交易费用、交易等待时间等因素排序后打包生成新区块,并将新区快广播给区块链网络中的其他矿工节点或代表节点.其他节点收到新区块后将独立验证其正确性.只有获得大多数参与验证的节点的确认后,记账节点才能根据规则,将新的区块添加到区块链的主链上.

以具有代表性的工作量证明算法PoW(Proof of Work)算法为例,规定每个矿工节点需要通过共同挖矿(求解SHA256数学难题),以最快者胜出的规则来确定具有记账权的节点,因此其本质是通过分布式节点的工作量或者说计算能力来竞争记账权.PoW算法是最早也是目前为止最安全可靠的公有链共识算法,但是对节点的计算能力要求较高且会造成电力等资源的浪费.因此权益证明算法PoS(Proof of Stake)中提出将节点对特定数量货币所有权定义为权益,以权益的竞争而非计算能力的竞争来确定记账权归属.

可以从容错类型、部署方式和一致性程度等不同角度出发对共识算法进行分类,综合文献[8-10],可以根据选主策略将共识算法分为证明类共识算法(例如PoW算法和PoS算法)、直接广播选举类共识算法(例如VR算法、Paxos算法和Raft算法)、轮流类共识算法(例如BFT算法)、联盟类代表共识算法(例如DPoS算法)、随机类共识算法(例如Algorand算法和PoET算法)、混合类共识算法(例如PoW+Pos混合共识算法、Pos+BFT混合共识算法)等6类.

1.4 智能合约

智能合约是可以执行合约条款的计算机化的交易协议,能够将法律协议、应用逻辑和网络中的复杂关系程序化.智能合约应该由具备专业知识的人制定和审核,具有法律效应.在区块链上下文中,智能合约的形式是具有唯一地址的存储在区块链中的程序,在区块链网络节点的沙箱环境中执行[11].

智能合约作为共享的资源被部署在区块链上,可以被外部事件触发自动执行.通过数字签名和时间戳技术,可以保证智能合约内容的不可篡改性和可追溯性,而且智能合约的所有条款和执行过程都是预先确定的,节点需要验证合约的有效性,通过共识后才能执行,合约中任何一方都不能擅自修改合约内容和干预合约的执行.

智能合约通过区块链网络的封装和共识,隐藏了区块链网络中各个节点以及节点之间复杂的行为,通过提供区块链应用层的接口,能够实现通用目的的计算,可以形成基于区块链的服务,从而能够构建各类可编程的智能资产、系统,令区块链技术具有更广阔的应用前景.

2 传统数字化教育系统面临的主要问题

很长时间以来教育机构都垄断了学习认证的功能,而学习者、教师却对于学习过程和结构无法自治.虽然技术在发展,但是传统的以学校为中心的教室学习改变很慢.另一方面,终身学习、在线学习、移动学习和基于项目以及实际问题的分布式学习变得越来越普及.近些年,随着网络的发展,学习环境逐渐数字化和全球化,传统的教育机构缺乏必要的方法、资源和能力去验证学习者的知识、技能和成果,也很难管理、认证学习者的学习活动、过程和结果[5,12-23].

传统的数字化教育系统通常采用中心化的结构,所有的教育相关数据以及处理代码通常都存储在中心化的服务器上,用户通常可以通过浏览器或移动APP与中心服务器通信,而数字化教育系统通

常由某个教育机构例如学校、某个公司、某个组织或者某个国家/地区的政府教育部门来建设和管理.

随着教育全球化和个人成长学习的终身化趋势,每个人在人生的不同阶段可能会在不同类型、不同地区乃至不同国家的教育机构接受教育.因此,不同的教育机构之间需要交换和共享学习者的相关学习数据,例如课程学分、学历证书、学习能力证书等等;利益相关第三方例如企业或政府部门需要查询和验证学习者的学习记录、成绩和结业证书等,未来雇主甚至还可能查询与应聘者所申请职位相关的课程的学习过程和课程作品等信息.而目前由某个教育机构拥有的中心化数字化教育系统在解决以上场景的问题时将会遇到很大困难.

这样的困难无法通过构建一个更大的包括相关教育机构的中心化的数字教育系统来解决.首先,从管理角度看,这些教育结构很可能来自不同的地区乃至国家的学校,也可能是不同的商业化教育机构,从管理权来说不可能归属到一个所谓更高级的教育机构中来.其次,从技术角度看,这些教育机构原先构建的数字化教育系统可能采用了不同的技术架构和产品,要实现这些系统的替换,或者连通和互操作,其代价是非常高昂甚至无法接受的.最后,从安全角度出发,建立这样一个所有教育机构都能够信任,并且能够防止未获授权的对数据篡改的中心化数字教育系统是很难的.

此外,传统的教育信息系统还面临着存储的数据维度有限、历史记录不完善等问题.

区块链本质上的安全和去中心化使得其可以成为教育领域中某些急需改进和创新的方向的完美技术解决方案.基于区块链的数字化教育系统用户包括学习者、教育机构的教师、管理者以及其他的利益相关方,例如公司、雇主等,其主要作用包括以下几点:

1)存储学习者学习资质和证书;

2)存储学习者课程成绩、学分和课程修习结果;

3)存储学习者的学习过程日志;

4)存储学习者的学习奖励;

5)提供对学习者学习结果、资质和证书的共享和验证;

6)存储课程相关信息;

7)支持对学习效果的评估以改进课程/课程体系;

8)存储教师相关信息;

9)提供对教师/课程的评估;

10)存储学校资产和设置信息;

11)完成教育部门高层次的决策分析,例如对学校、学生、教师群体特点的分析,以帮助制定教育政策;

12)为其他利益相关方提供接口,例如工业界、潜在的雇主公司、合作教育机构、后续教育机构等;

13)提供用户交互.

3 区块链技术在教育领域的应用

3.1 学习者教育相关信息的多方共享和验证

区块链技术在教育领域的最重要的应用是解决学习者教育相关信息的多方共享和验证.如第 2 节所述,在终身学习的趋势下,每个人可能会跨机构、跨城市、跨管理域甚至跨国家接受不同形式的教育,并需要在学习者个人、学校、雇主、政府部门之间共享和验证学习者所取得的教育成果、资质和证书等教育相关信息,因此需要在多个利益相关方之间架设透明和高效率的桥梁,从而无缝连接教育界内部和教育界与外部世界(例如工业界).

这里区块链网络的构建基于不同的应用需求可能会有不同的选择.早期的区块链教育网应用主要集中于对证书和学位的认证,并且大多基于比特币区块链网络.这些工作包括美国麻省理工学院的“数字证书项目”[24]、阿根廷 CESYT 学院的学位认证项目[25]等.

具有跨国家不同管理域全球化需求的教育网区块链应用,往往采用联盟链类型的区块链网络,这是因为全球化情况下,不可能建立由一个机构管理的私有链网络,而教育网应用背景下,教育机构和学习者、雇主等其他用户地位并不相同,因此联盟链比较合适.欧洲学分转换和累积系统 EDUCTX 平台[12-13]是这方面目前最为典型和成功的案例,最早是基于 ARK[26]区块链平台实现,后来的新版本基于以太坊平台.印度的研究者提出的学分转换系统[14]是 EDUCTX 之后的又一个工作,其原型也是基于 ARK 区块链平台实现的.文献[15]是基于 Hyperledger Fabric 的一个工作,实现了一个教育界-工业界信息共享的合作系统.约旦的研究者们所做的使用区块链技术构建智能教育认证的工作[27]目前主要用于约旦的 Al-Zaytoonah 大学.美国几所大学合作构建的一个教育区块链系统[16]可以连接大学和企业,并支持企业雇员的在职继续教育.

本文按照区块链网络类型和体系结构,以EDUCTX平台为主进行介绍、对比与分析,EDUCTX平台的概念体系结构如图3所示.

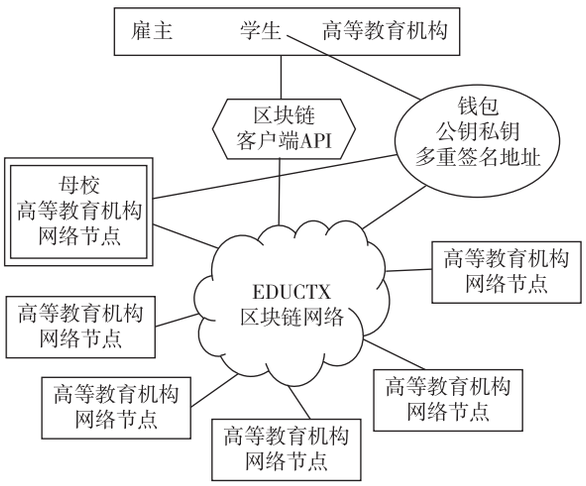

图3 EDUCTX平台体系结构

Fig. 3 Architecture of EDUCTX platform

在网络层,系统利用分布于全球的P2P网络构建,一般而言经过验证的授权高等教育机构会作为区块链网络的主要网络成员节点参与分布式共识过程,而其他用户可以匿名方式有限使用公开存储于区块链网络中的账簿信息.在数据层,在EDUCTX中,当学生在一个高等教育机构注册时,高等教育机构节点会为该学生产生一个学生ID、一个新的区块链地址以及一个公钥私钥对,同时,高等教育机构还会使用自己的公钥以及刚产生的学生公钥来生成一个新的2-2多重签名区块链地址,并将此2-2多重签名区块链地址和学生ID存储到高等教育机构自己的数据库中.学生将使用2-2多重签名区块链地址来构建自己的区块链钱包.当学生完成一门课程的学习后,事先规定好的课程相应的ECTX代币将从高等教育机构传输到学生的2-2多重签名区块链地址钱包.当雇主或其他高等教育机构要验证一个学生的学分记录时,学生将自己的区块链地址、公钥以及和高等教育机构相应的2-2多重签名区块链地址发送给验证方,验证方可以以此验证学生的学分等信息,并通过一个私有信道,验证方根据学生的区块链地址发送信息给学生,要求学生使用自己的私钥来签收,以验证学生身份的合法性.从安全考虑,学生无法独自传输所获得的学分代币,因为学分代币是存储在2-2多重签名区块链地址钱包中的,需要学生和高等教育机构的共同同意才可以传输.而在印度的学分转换系统工作中,使用的扩展的*M-B*多重签名地址,作用也是在*M*个节点中,需要*B*个节点共同确认才能保证交易的合法性,该系统相较于EDUCTX的一个改进是可以为一个学生在同一个导师下注册多门课程.

在区块结构中,交易信息中除了包含收发双方的信息以及代表学分的代币外,还可以包含外链指向更加细节的学分和证书信息,这些信息保存在相应高等教育机构自己的服务器上,每个高等教育机构可以选择是否在交易信息中包含可选的细节信息外链.

在共识层,EDUCTX使用DPoS共识协议,因此不需要耗费额外的计算资源,因为只有授权的高等教育机构构建的节点才能参与共识过程,所有节点可以使用选举投票的方式依次决定“记账员”的产生.

在智能合约层,EDUCTX扩展了以太坊的ERC20,在智能合约中增加新的结构,维护一个验证过的授权机构列表,从而可以在学分传输时检验学分传输方是否获得了相关的授权,并且通过使用定制的商业逻辑标准化“传输”函数从而能够存储所传输的特定学分代币相关的更加细节的信息.文献[16]中可以通过智能合约来自动地为企业提供其员工所接受的在职继续教育所获得的最新教育成果,包括学术成果或其他任何项目经验等.

在应用层,EDUCTX平台上所有利益相关方都是通过用户接口友好地去中心化WEB接口以及一个P2P的超媒体协议IPFS来使用EDUCTX平台,这是目前应用层接口最友好的一个实现工作.

3.2 学习过程跟踪、激励和学习路径塑造

香港几所大学构建了一个基于以太坊的“Word-Learning System”区块链数字化学习系统的概念模型,可以实现学习过程的跟踪[17].为了提升学习参与度,系统可以通过智能合约技术基于部署于区块链中的激励策略为排行前列的学习者提供额外的虚拟货币奖励,这些虚拟货币又可以被用于购买一些要求付费或者加密的文件,这可以避免抄袭并保护知识产权.作者还使用来自ISO 9126质量模型对提出的区块链数字化学习系统的功能改进、可用性以及可维护性进行了验证.

英国的研究者在数据科学教育的大背景下使用区块链技术实现了智能区块链徽章作为学习者的动态认证记录[18],不仅能够记录学习者所获得的学习成果和相关的学习技能,还能以此为依据为学习者

提供匹配的工作机会,并提供接下来的学习建议,从而实现对学习者学习过程的跟踪以及进一步学习的激励.该工作基于以太坊平台,所构建的区块链徽章系统能够与欧洲数据科学协会(EDSA)的白板系统互联,从 EDSA 的白板获取数据科学方面各种数据科学技能的需求情况.该系统的主要贡献是通过不同类型的智能合约来帮助学习者塑造适合自己的学习路径,从而达到更好的职业生涯目标,其智能合约包含以下类型:

1)徽章合约:存储在完成一门课程后所奖励的徽章的细节信息,包括头衔、描述、发放者、奖励的原则等;

2)技能感知合约:存储获得一枚徽章所需的技能列表,以及从 EDSA 白板获得的各种工作所要求的所有技能列表;

3)工作招聘合约:保存 EDSA 白板所获取的特定工作的细节信息,包括职位、描述、国家、组织、地点等;

4)工作存储合约:将工作招聘合约映射到技能,包含一个指针列表,可以将每个工作招聘合约映射到相应的工作感知合约中所持有的技能.

3.3 学习评估

在高等教育中,通过实验、测验、考试来评估学生的学习状况是很重要的任务,但是存在的问题是评估可能是不透明的、不公平的,评估结果也可能被有意更改.应用区块链技术进行学习评估可以有效解决这些问题.武汉科技大学给出一个基于双层联盟链的在线测验模式[19].

为了在保证安全性的基础上同时提高系统的效率和吞吐量,文献[9]采取 Ethereum 2.0 manve 中的双层联盟链方法,即将区块链分成一条主链和若干子链.在网络中维护唯一一条主链,主链由网络中的全功能节点共同维护;同时将整个网络分成若干个部分,每个部分维护一条子链,每个普通节点可以根据自己的任务和计算及存储能力选择加入一个或若干个子链.每个测验构成一个小组,都由其参与的普通成员节点构造一条子链.在一次测验中,所有组成员都会对测验结果进行验证,并将验证结果保存到子链中,然后由组管理员将测验结果数据发送到主链中的全功能节点,经过主链全功能节点验证后同步到主链区块中.这样各测验小组的子链可以并行操作,增加了系统的吞吐量.同时,在将测验结果发送到主链中加入区块后,子链中将不再保存测验结果的详细信息,而仅仅保存测验结果信息的哈希值以及其在主链中存储位置的索引,从而降低了子链节点的存储压力.最终,主链区块中保存的信息将包括课程名称、教师姓名、学生别名、测验时间、分数、答题细节等,而子链区块中保存的信息仅仅包括学生别名、分数、在主链中的位置索引等摘要信息.

从安全性来说,通过区块链技术可以保证匿名性,同时对每个小组使用多重签名技术,可以保证可追溯性.在双层链数据层面上,最终子链区块中的信息是由主链信息产生的,因此只要保证主链全功能节点的诚实,对主链和子链的恶意攻击将都不能得逞.

学习产出能够衡量学生通过课程学习所获得的能力,也相应地能够评价课程的教学质量.传统的教育机构由于通过人力进行评估,以及不同评估者以及所属的管理域、地区和国家不同,从而很难客观、自动、准确地去管理和认证学生的学习过程和结果.基于区块链技术的学习产出评估可以实现将对学生学习成果的评估转换为未来工作竞争力的评估结果,而学生竞争力评估的反馈则可以促进课程体系的不断改进,进而影响和提升学生的学习方法.湘潭大学的研究者在使用教育区块链技术进行学习产出评估方面进行了研究和实现工作[20].

区块中存储的数据,除了课程名、课程的权重等常规内容外,还包括了作为评估依据的各项毕业要求能力的名字,以及作为结果的课程学习产出结果值,该产学习产生结果值是结合学生的成绩、学习过程以及学习证据,通过定量和定性的方法综合评估决定的.这样,就可将传统的仅仅基于学生课程结果学分的评估提升为依据毕业要求能力索引的课程学习产生结果评估.而共识机制被用于确保课程的评估不受限于教师的主观意愿,从而保证评估结果的说服力.

此外,复旦大学也对区块链技术用于技能竞赛进行了研究工作[27],以电子商务沙箱为案例,设计了基于联盟区块链的数字化教育操作技能竞赛评估系统,可以解决不科学的竞赛和非授权的评估等问题.

3.4 教育管理与决策辅助

传统的教育管理需要依赖对学校信息管理系统搜集、录入的数据进行处理分析,但是目前现有教育信息系统中数据都是由本单位搜集、录入和维护,可能不正规或是造假的,也缺乏独立和系统化的方法

在相关信息的整个生命周期内验证其正确性,对于跨地区、跨管理机构、跨国家的教育系统中的信息的分享和使用,以及上层管理部门如教育部门基于对所辖学校信息管理系统中数据的分析来辅助政策制定,都缺乏可行与良好的支持.而基于区块链的教育管理系统可以帮助解决这方面的困难,IBM 公司的研究者在文献[22]中介绍了在非洲肯尼亚所构建的基于区块链的学校信息枢纽 SIH,该系统原型基于 Hyperledger Fabric 构建,其体系结构如图 4 所示.

在学校信息管理系统中存储着包括学生、家长、教师、学校设施和设备、学校资产等各种信息.这些信息对于教育政策的制定起着支撑作用,例如国家教育部门根据学校教师和学生人数进行教育拨款等.SIH 结构中通过学校数据接口 SDH 平台和预处理模块完成个体注册、个体相关信息收集、验证、存储和管理等工作.个体相关信息包括生物信息如指纹、脸部数据等,数字化的文档如出生证明等,教育相关信息如学生在校的画像信息、学术表现、个人学术成就等,还有很多相关的图像和视频等多媒体数据.

在区块中并不存储系统中个体的生物信息数据、文档、图像和大型的多媒体数据,而是将这些数据加密后存储在一个本地的永久性存储设施中,而区块中存储的是经过验证后的<数据哈希值,存储地址,相关事件信息>的三元组数据,由此可以通过区块链来控制这些“账本外”数据,保证其机密性、授权和完整性,并在需要的时候可以对其进行验证、分析和制作报告等.

智能合约被用于管理区块链之中的学校信息系统,用于实际控制所有的功能和服务,例如和学生有关的功能包括学生注册、学生转学、学生加入一门课程、修改个人标识信息、毕业等,和教师相关的功能包括教师注册、为课程指定教师、教师表现记录等,其他还包括资产注册、教学大纲上传和修改、创建、开始和结束课程等.

决策支持模块可以提供不同级别的和学生、教师、学校以及资源相关的分析服务.包括资源分配、预算分配、学校影响力评估、学生退学模式预警、学生择校模式分析、转学模式分析、学生相似性分析、欺诈预防、教师分布等.

在使用牵涉到教育系统中学生的数据进行评估及决策时,如何保证学生数据隐私及获得家长的授权共识也是需要解决的一个问题.印度的研究者在此方面进行了研究[23],基于 Hyperledger 系统,在智能合约层设计了授权、关联和共识等算法实现,能够确保学生数据被正确使用,并可以对抗吵闹的父母、吵闹的志愿者和黑客访问者等不同的安全威胁.

4 总结和未来研究方向

目前区块链技术已经逐步应用到教育领域的各个方向,包括学分、证书、学历等数据的共享和验证,学习情况跟踪,学习和课程评估,教育管理和决策系统等,并且有相应的实际教育区块链网络被部署,但是成熟的平台和系统并不多.

在教育区块链技术发展过程中,也暴露出一些需要解决的缺点和困难.在文献[28]中,俄罗斯研究者给出了一些观点,主要的问题可能包括:1)教育区块链建设需要必要的教育立法机关政策制定,也需要统一所有参与方的兴趣;2)区块链网络需要有足够的参与者,更少的参与者会导致更大的破坏数据的可能性,如果一些参与者不想花费资源用于计算“外部”数据而仅仅希望成为网络中的消费者,不对验证和求解算法做出贡献,会降低网络的可靠性;3)如果采用公有链,参与者完全匿名和不用授权,由

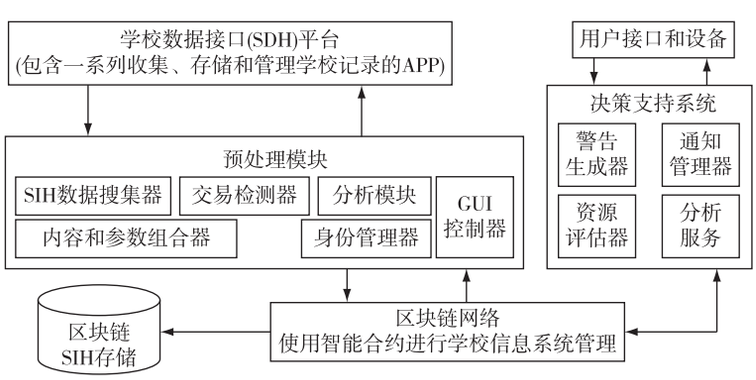

图 4 学校信息枢纽 SIH 体系结构

Fig. 4 Architecture of school information hub (SIH)

虚构的教育机构给出的专业证书数据可能会被写入区块,因此目前很多工作都是采用了联盟链作为基础.

通过现有的研究工作,也可以给出教育区块链技术未来的一些研究方向,具体如下:

1)教育并行智能区块链技术.基于并行智能理论的并行区块链技术能够提供一系列可计算、可行和可比较的建模、预测分析和制导优化方法.中国科学院的研究者以此为基础研究了并行完全教育区块链模型[29].在这个方向上,数据层、共识层和智能合约层构成的逻辑层以及应用层都有很多问题有待解决.

2)教育区块链跨链和扩展技术.区块链技术应用于教育领域的工作正越来越多的浮现,而基于不同区块链技术构建的教育区块链网络也会逐渐增多,因此实现不同教育区块链之间的通信、数据共享是一个必然要面对的问题.文献[30-31]中对区块链之间的互联互通和区块链的扩展进行了研究,可以作为有益的参考.而未来教育区块链跨链技术的研究会是区块链在教育领域应用需要解决的主要问题之一.

3)教育区块链数据分析.文献[32]对区块链上的数据分析工作进行了研究,具体到教育区块链系统,未来有两个主要问题需要研究.首先是随着区块链技术在教育领域的应用,越来越多的学习者、教师、课程、教育机构等数据会上传到链中,如果所有数据都上链的话,对于整个系统将是一个沉重的负担,并且是否所有数据都上链就合适呢? 所以研究哪些数据应该打包进教育区块链系统,哪些数据离链存储,是一个需要进一步研究的问题.其次就是如何提供合适的算法、技术、工具以及良好的人机接口来方便进行用于各种目的的教育区块链数据查询和分析,也是一个需要进一步研究的方向.

参考文献

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2019-08-08].https://bitcoin.org/bitcoin.pdf,2008

[2] 刘敖迪,杜学绘,王娜,等.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018,29(7):2092-2115
LIU Aodi, DU Xuehui, WANG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7):2092-2115

[3] 邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018,41(5):969-988
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers,2018,41(5):969-988

[4] Ismail L, Hameed H, Al Shamsi M, et al. Towards a blockchain deployment at UAE University[C]// Proceedings of the 2019 International Conference on Blockchain Technology-ICBCT 2019, March 15-18, 2019. Honolulu, HI, USA. New York, USA: ACM Press, 2019

[5] Al-Harthy K, Al Shuhaimi F, Al Ismaily K K J. The upcoming blockchain adoption in higher-education: requirements and process[C]// 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), January 15-16, 2019. Muscat, Oman. New York, USA: IEEE, 2019:1-5

[6] 朱立,俞欢,詹士潇,等.高性能联盟区块链技术研究[J].软件学报,2019,30(6):1577-1593
ZHU Li, YU Huan, ZHAN Shixiao, et al. Research on high-performance consortium blockchain technology[J]. Journal of Software,2019,30(6):1577-1593

[7] Buterin V. A next-generation smart contract and decentralized application platform[EB/OL].[2018-12-08].https://github.com/ethereum/wiki/wiki/White-Paper

[8] 郑敏,王虹,刘洪,等.区块链共识算法研究综述[J].信息网络安全,2019,19(7):8-24
ZHENG Min, WANG Hong, LIU Hong, et al. Survey on consensus algorithms of blockchain[J]. Netinfo Security, 2019,19(7):8-24

[9] 袁勇,倪晓春,曾帅,等.区块链共识算法的发展现状与展望[J].自动化学报,2018,44(11):2011-2022
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022

[10] Wang W B, Hoang D T, Xiong Z H, et al. A survey on consensus mechanisms and mining management in blockchain networks [J]. arXiv preprint, 2018, arXiv:1805.02707

[11] 欧阳丽炜,王帅,袁勇,等.智能合约:架构及进展[J].自动化学报,2019,45(3):445-457
OUYANG Liwei, WANG Shuai, YUAN Yong, et al. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica,2019,45(3):445-457

[12] Turkanovic M, Holbl M, Kosic K, et al. EduCTX: a blockchain-based higher education credit platform[J]. IEEE Access,2018,6:5112-5127

[13] Holbl M, Kamisalic A, Turkanovic M, et al. EduCTX: an ecosystem for managing digital micro-credentials[C]// 2018 28th EAEEIE Annual Conference (EAEEIE), September 26-28, 2018. Hafnarfjordur. New York, USA: IEEE,2018:1-9

[14] Srivastava A, Bhattacharya P, Singh A, et al. A distributed credit transfer educational framework based on blockchain[C]// 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), September 21-23, 2018. Allahabad, India. New York, USA: IEEE, 2018:54-59

[15] Liu Q, Guan Q C, Yang X W, et al. Education-industry cooperative system based on blockchain[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), August 15-17, 2018. Shenzhen. New York, USA: IEEE, 2018: 207-211
[16] Han M, Li Z G, He J, et al. A novel blockchain-based education records verification solution[C]//Proceedings of the 19th Annual SIG Conference on Information Technology Education-SIGITE'18, September 14-October 6, 2018. Fort Lauderdale, Florida, USA. New York, USA: ACM Press, 2018: 178-183
[17] Zhong J M, Xie H R, Zou D, et al. A blockchain model for word-learning systems[C]//2018 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC), November 12-14, 2018. Kaohsiung, Taiwan, China. New York, USA: IEEE, 2018: 130-131
[18] Mikroyannidis A, Domingue J, Bachler M, et al. Smart blockchain badges for data science education[C]//2018 IEEE Frontiers in Education Conference (FIE), October 3-6, 2018. San Jose, CA, USA. New York, USA: IEEE, 2018: 1-5
[19] Shen H J, Xiao Y A. Research on online quiz scheme based on double-layer consortium blockchain[C]//2018 9th International Conference on Information Technology in Medicine and Education (ITME), October 19-21, 2018. Hangzhou. New York, USA: IEEE, 2018: 956-960
[20] Duan B, Zhong Y, Liu D Y. Education application of blockchain technology: learning outcome and meta-diploma[C]//2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), December 15-17, 2017. Shenzhen. New York, USA: IEEE, 2017: 814-817
[21] Wu B, Li Y S. Design of evaluation system for digital education operational skill competition based on blockchain [C]//2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), October 12-14, 2018. Xi'an. New York, USA: IEEE, 2018: 102-109
[22] Bore N, Karumba S, Mutahi J, et al. Towards blockchain-enabled school information hub[C]//Proceedings of the Ninth International Conference on Information and Communication Technologies and Development-ICTD'17, November 16-19, 2017. Lahore, Pakistan. New York, USA: ACM Press, 2017, 19: 1-4
[23] Gilda S, Mehrotra M. Blockchain for student data privacy and consent [C]//2018 International Conference on Computer Communication and Informatics (ICCCI), January 4-6, 2018. Coimbatore. New York, USA: IEEE, 2018: 1-5
[24] Media Lab Learning Initiative. Digital certificates project [EB/OL]. [2019-08-08]. http://certificates.media.mit.edu/, 2016
[25] Amati F. First official career diplomas on bitcoin's blockchain [EB/OL]. [2019-08-08]. https://blog.signatura.co/rst-ofcial-careerdiplomas-on-bitcoin-s-blockchain-69-311acb544d, 2015
[26] Ark: All-in-one blockchain solutions [EB/OL]. [2019-08-08]. http://www.ark.io, 2016
[27] Kanan T, Obaidat A T, Al-Lahham M. SmartCert block chain imperative for educational certificates[C]//2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), April 9-11, 2019. Amman, Jordan. New York, USA: IEEE, 2019: 629-633
[28] Naumova O A, Svetkina I A, Naumov D V. The main limitations of applying blockchain technology in the field of education [C]// 2019 International Science and Technology Conference "EastConf", March 1-2, 2019. Vladivostok, Russia. New York, USA: IEEE, 2019: 1-4
[29] Gong X Y, Liu X W, Jing S F, et al. Parallel-education-blockchain driven smart education: challenges and issues [C]//2018 Chinese Automation Congress (CAC), November 30-December 2, 2018. Xi'an, China. New York, USA: IEEE, 2018: 2390-2395
[30] 李芳,李卓然,赵赫.区块链跨链技术进展研究[J].软件学报,2019,30(6):1649-1660
LI Fang, LI Zhuoran, ZHAO He. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649-1660
[31] 潘晨,刘志强,刘振,等.区块链可扩展性研究:问题与方法[J].计算机研究与发展,2018,55(10):2099-2110
PAN Chen, LIU Zhiqiang, LIU Zhen, et al. Research on scalability of blockchain technology: problems and methods[J]. Journal of Computer Research and Development, 2018, 55(10): 2099-2110
[32] 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(9):1853-1870
CHEN Weili, ZHENG Zibin. Blockchain data analysis: a review of status, trends and challenges [J]. Journal of Computer Research and Development, 2018, 55(9): 1853-1870

Application of blockchain technology in education: current status and future trends

HUANG Daming[1]

1 Department of Computer Science and Technology, Nanjing University, Nanjing 210023

Abstract Blockchain technology is quite suitable to solve the difficulties in the field of education due to its secure and decentralized nature. This paper introduces blockchain's basic theory and key technologies which include the

block structure and construction of blockchain, the architecture of blockchain platform, types of blockchain, consensus algorithms and smart contract.Then the new trends in modern education field such as lifelong education and cross-domain education are presented and the limitations of traditional digital education system are discussed. We give detailed description and analysis of the application of blockchain technology in the field of education such as educational data sharing and verification, learning tracing, awarding and shaping of study path, study evaluation, educational management and decision making.Finally the questions in application of blockchain technology in education field and future research directions are summarized.

Key words blockchain technology; field of education; consensus algorithms; smart contract