

区块链技术在教育领域的应用模式与现实挑战*

□杨现民 李新 吴焕庆 赵可云

摘要：区块链技术被视为继云计算、物联网、大数据之后的又一项颠覆性技术，受到各国政府、金融机构以及科技企业的高度关注。区块链技术在本质上是一种通过去中心化、高信任的方式集体维护一个可靠数据库的技术方案，其核心技术包括分布式账本技术、非对称加密算法以及智能合约等，具有去中心化、共识机制、可追溯性以及高度信任等特征。区块链技术作为比特币的底层技术不仅在金融等领域日益应用，在教育领域同样具有较大的应用潜力，有望在互联网+教育生态的构建上发挥重要作用，推动教育体系变革。借鉴金融领域区块链应用的经验，教育领域的区块链主要体现为六大应用模式：建立个体学信大数据、打造智能化教育淘宝平台、开发学位证书系统、构建开放教育资源新生态、实现网络学习社区“自组织”运行以及开发去中心化教育系统。当然，由于教育领域自身的独特性和复杂性，区块链技术的应用也面临教育应用推广运行难、教育数据产权模糊、数据存储空间有限以及区块链技术自身安全隐患所引起的师生隐私保护风险等诸多挑战。

关键词：区块链；教育应用；应用模式；现实挑战

中图分类号：G434 文献标识码：A 文章编号：1009-5195(2017)02-0034-12 doi:10.3969/j.issn.1009-5195.2017.02.005

***基金项目：**江苏高校优势学科建设工程资助项目“江苏师范大学教育学省优势学科建设”（苏政办发〔2014〕37）；江苏省“333”工程项目。

作者简介：杨现民，博士，副教授，江苏师范大学智慧教育学院，江苏省教育信息化工程技术研究中心；李新，硕士研究生，江苏师范大学智慧教育学院（江苏徐州 221116）；吴焕庆，博士，副教授；赵可云，博士，副教授，曲阜师范大学传媒学院，中国教育大数据研究院（山东曲阜 276826）。

一、引言

区块链技术被视为继云计算、物联网、大数据之后的又一项颠覆性技术，受到各国政府、金融机构以及科技企业的高度关注（Wright et al., 2015）。2016年美国、英国、日本等发达国家相继将区块链技术上升到国家战略层面，成立了区块链发展联盟。同年，国务院印发的《“十三五”国家信息化规划》首次将区块链列入我国的国家信息化规划，并将其定为战略性前沿技术之一。当前，各行各业都开始关注区块链技术，积极探索利用该技术破解行业难题，促进行业创新发展。

在金融领域，全球银行巨头组建R3联盟，包括汇丰银行、瑞银、美国银行等40多家国际大型金融机构，共同发展区块链技术。美国纳斯达克率

先推出基于区块链技术的证券交易平台Linq，成为金融证券市场去中心化趋势的重要里程碑（袁勇等，2016）。在北京召开的数字货币研讨会上中国人民银行行长周小川指出，需要密切关注区块链等技术对金融领域带来的影响，要求探索发行数字货币（陈一稀，2016）。

在科技领域，IBM联合Linux基金会建立了一个专门区块链开源项目超级账本（Hyperledger），已经进入实质开发阶段。公司将在Watson IoT平台上提供Watson API帮助企业客户和开发者基于云计算进行物联网应用的开发与测试，以期实现利用区块链引领物联网自治。

在能源领域，国外企业已经启动能源区块链项目，比如：德国西门子与纽约新创事业合作将区块链技术应用用于微电网电力交易市场；美国的能源公

司 LO3 Energy 与比特币开发公司 Consensus System 合作，在纽约布鲁克林 Gowanus 和 Park Slope 街区为少数住户建立了一个基于区块链系统的可交互电网平台 TranActiveGrid。

在食品领域，英国萨德大学去年一份研究报告指出，如果将区块链技术应用到食物供应链中，通过让食品的各项数据变得透明，或可减少食物被浪费的现象，从而解决日益严重的食品浪费等全球性问题（金科网，2017）。此外，沃尔玛也在尝试用区块链技术记录食品来源，试图让消费者掌握更多的食品信息，从而改善目前食品行业的一些乱象。

在医疗领域，飞利浦医疗和 Tierion 进行合作，让飞利浦医疗通过区块链技术来完成关于病历资料的认证以及病人的隐私保护（张波，2016）。区块链技术有助于解决医疗行业目前遭受的大规模数据质量问题，为医疗行业提供唯一真实性数据来源，使系统不再遭受人为错误或者手工数据和解，从而解决医疗数据信任问题。

随着区块链技术的逐步完善以及应用领域的不断拓展，国际上一些教育机构和学者开始关注并探讨区块链技术在教育领域的应用。北京邮电大学李青教授指出，区块链技术在教育领域具有较大的应用潜力，有助于打造更加开放和更具公信力的教育系统（李青等，2017）。整体来看，当前区块链技术在教育领域的应用探索刚刚起步，缺少成熟的应用案例和清晰的应用思路，亟待加强产学研多方协同研究和实践推进。基于此，本文将对区块链技术的概念与核心技术进行介绍，分析来自金融领域区块链应用的经验与启示，结合现有典型教育案例探讨区块链技术的教育应用思路与价值，并对可能面临的挑战进行分析，以期推动区块链技术在教育领域的应用进程。

二、区块链概念与核心技术

2008年11月，一位自称中本聪的科学家发表了一篇名为《Bitcoin: A Peer-to-Peer Electronic Cash System》的论文，提出了一种基于P2P组网技术、数学、密码学以及时间戳技术的电子现金系统的构架理念，并于2009年1月设计了一种加密数字货币——比特币，标志着比特币正式诞生。此时人

们并没有注意到区块链的概念，直到比特币系统在没有专人维护安全运行多年后，比特币系统的底层核心技术——区块链，作为一种去中心化的数据库技术才开始进入人们的视野。

1. 区块链的概念

区块链（Blockchain）的概念源于数字货币——比特币，是一种把区块以链的方式组合在一起的数据结构（Wang et al., 2016）（见图1），它不依赖中心机构的管理，而在网络中分布式记录与存储。区块按照时间顺序生成并记录待处理的交易信息，由区块头和区块主体两部分组成，区块头负责通过主链连接到下一个区块，区块主体负责存储数据信息。当区块和链形成时系统会自动生成时间戳并为数据信息打上时间标签，这是区块链数据库的一大创新点（Pilkington, 2015）。区块链的运作机理是将传统由中心机构统一记录和管理的记账账单变为全网公开并由各个节点共同维护的账单，每笔交易信息都可以通知到全网的用户，账本中的信息可以由所有用户共同核对，这样交易在缺少第三方信用主体时一样可以得到信用担保，从而保障信息的真实性与可信度。

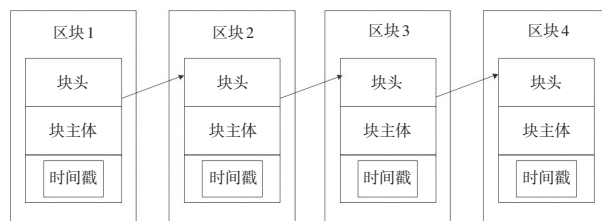


图1 区块链结构示意图

2. 区块链核心技术

区块链技术是一种通过去中心化、高信任的方式集体维护一个可靠数据库的技术方案，数据库中的每个区块包含系统的全部数据信息，使用数字签名验证信息的有效性和完整性，通过密码学原理链接到下一个区块并形成一条主链（Kosba et al., 2016）。区块链技术基于密码学原理，使得任何达成一致的双方可直接支付，从而不需要第三方平台的参与，解决了中介信用问题。通过区块链技术，比特币实现了在没有任何中介机构参与的情况下完成双方可以互信的转账行为。区块链的核心技术主要包括分布式账本技术、非对称加密算法以及智能合约。

(1) 分布式账本技术

分布式账本技术就是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的都是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。其本质是一个可在由多个机构、不同地理位置或者多个节点组成的网络里进行数据共享的资产信息库 (MBA, 2016)。不同于传统数据库技术由中央管理员进行数据记录与存储，这种账本能在点对点网络中的不同节点之间相互复制，处在同一个网络里的用户均可获得一个真实账本的副本，该账本里存储信息的安全性和准确性通过公开密钥 (Public Key)、私有密钥 (Private Key) 以及数字签名 (Digital Signature) 的使用来控制账本的访问权，从而实现基于密码学原理的信息维护。

(2) 非对称加密算法

非对称加密算法使用公开密钥 (公钥) 和私有密钥 (私钥) 来解决区块链网络中用户信息的安全问题 (Wild et al., 2015)。公钥和私钥同时生成，任何用户都可以使用公钥来加密信息，以保证信息的真实性；私钥严格保密，只有信息拥有者才能使用对应私钥解密信息，以保证信息的安全性。

(3) 智能合约

智能合约是一种类似于业务规则的数字化合约，具体体现为交易时自动执行的预先定义好的规则和程序，适合任意区块链数据结构 (Victoria, 2016)。智能合约的透明脚本代码，在各方监督下，符合条件时会自动执行，无法干预、操纵、反悔和篡改，在可信数据的基础上保证了程序运行结果的可信度。

3. 区块链技术特征

区块链特殊的数据结构与运作机理，使区块链技术具有四个主要特征：去中心化、共识机制、可追溯性以及高度信任 (Underwood, 2016)。

(1) 去中心化

区块链是由众多节点共同组成的点对点网状结构，不依赖第三方中介平台或硬件设施，没有中心管制，通过分布式记录和存储的形式，各个节点之间实现数据信息的自我验证、传递和管理。数据在每个节点互为备份，各节点地位平等共同维护系统

功能，因此系统不会因为任意节点的损坏或异常而影响正常运行，使得基于区块链的数据存储具有较高的安全可靠性的。

(2) 共识机制

共识机制主要指网络中的所有节点间如何达成共识的认证原则，去认定一份交易信息的有效性，保证信息的真实可靠。有了该机制，区块链应用中便无需依赖中心机构来鉴定和验证某一数值或交易。共识机制可以减少伪冒交易的发生，只有超过51%的节点成员达成共识，数据交易才能发生，有利于保证每份副本信息的一致性，建立适用于不同应用场景的交易验证规则，从而在效率与安全之间取得平衡。

(3) 可追溯性

区块链中的数据信息全部存储在带有时间戳的链式区块结构里，具有极强的可追溯性和可验证性。区块链中任意两个区块间都通过密码学方法相关联，可以追溯到任何一个区块的数据信息。

(4) 高度信任

区块链是建立信任关系的新技术，这种信任依赖于算法的自我约束，任何恶意欺骗系统的行为都会遭到其他节点的排斥和抑制。区块链技术具有开源、透明的特性，系统参与者能够知晓系统的运作规则和数据内容，任意节点间的数据交换通过数字签名技术进行验证，按照系统既定的规则运行，保证数据信息具有较高的可信度，降低了系统的信任风险。

三、来自金融区块链的启示与思考

从区块链技术的发展来看，金融是其最先应用和发力的领域，当前国际上的诸多区块链应用案例也都来自金融领域。区块链技术受到风险投资的高度关注和热捧，逐渐成为全球创新领域的热点话题，正在掀起新一轮资本战争。多家世界知名金融机构联合成立了R3 CEV和Hyperledger等区块链技术应用联盟，以应对金融领域这场技术标准的竞争和颠覆式创新浪潮 (王硕, 2016)。

1. 金融区块链的主要应用模式

区块链技术正在改变金融体系间的核心准则 (林晓轩, 2016)，因其安全、透明、不可篡改等特

性,使得金融体系间的信任机制不再依赖于第三方管理机构。许多银行业务都将实现“去中心化”,从基于中介服务的交易模式转变为实时点对点交易模式,能够显著降低交易成本,提升交易效率(蔡钊,2016)。当前,区块链技术在金融领域的应用主要集中在数字货币、跨境支付、供应链金融与证券交易等四个方面。

数字货币领域。当前,以比特币为代表的数字货币已受到欧美市场的逐步接受和认可,应用覆盖面越来越广,不仅能在商场用比特币购买商品,而且出现了替代现行银行借记卡的比特币借记卡和支取比特币的ATM机等应用产品。通过区块链发行数字货币既可以降低传统纸币的流通和发行成本,提高支付结算的便捷性和效率,又能增加货币交易的透明度,有效控制洗钱、偷税漏税、非法资产转移等违法犯罪行为,帮助央行构建绿色、透明、高效的金融服务和监控体系,提高央行对货币流通的掌握力。

跨境支付方面。麦肯锡利用区块链的分布式账本技术,在付款方和收款方之间创建直接的付款流程,能够降低操作成本和费用,提高交易安全性以及加快交易总体速度。随着经济全球化的速度和程度在不断加快和加深,跨境支付业务将成为下一个蓝海。据粗略估算,在B2B跨境支付与结算业务中应用区块链技术,每笔交易成本可以降低约40%。对于商业银行而言,他们更希望区块链技术的介入,一方面能够突破现有的系统间割裂的现状以及额度等监管限制,另一方面能够在解决互信问题的基础上构建扁平化、低成本、高效运转的全球一体化支付体系(张苑,2016)。

供应链金融领域。国内贸易融资市场规模巨大,增长率很快,预计到2020年将增长到20万亿元。但是,由于当前的交易模式存在流程复杂、参与方众多、自动化程度低等诸多原因,导致供应链金融发展陷入高成本、低收益的窘境。区块链技术与贸易金融融资业务的结合,既能够简化交易流程,提高交易效率,又能提高交易与结算的透明度和安全度,优化客户体验(Morgen Peck,2016)。

证券交易方面。各国证券监管部门逐步认识到,区块链可能为证券发行与交易带来新的商业模

式和机遇,并开始行动起来。2015年纳斯达克在拉斯维加斯召开的Money20/20大会上发布了首个基于区块链技术的数字化证券产品管理系统平台Linq;2016年中国由上海证券交易所牵头组建ChinaLedger联盟,探索应用区块链技术建设场外交易平台。区块链技术让金融交易流程更加公开、透明,让每个市场参与者享用平等的信息知情权,让证券交易日和交割日时间间隔从1-3天缩短至10分钟,从而提高了交易的效率、公平性和可控性,降低了交易风险。

2.对区块链在教育领域应用的启示

区块链技术的应用正在为金融领域带来颠覆性变革,创造新的商业契机。通过研究区块链技术在金融领域的应用模式,发现其对金融领域创新与发展的价值主要体现在:剔除中间交易平台,降低交易成本;实现实时交易结算,提高交易效率和资产利用率;分布式存储交易数据,不可篡改和高安全性;基于智能合约实现交易流程的自动化运行。区块链技术在金融领域的应用场景与模式,为其在教育领域的应用提供了如下启示:

(1)加强知识产权保护,搭建教育信任体系。数字货币的可追溯性可以降低银行在反洗钱、反欺诈等合规验证和审计方面的费用支出,有效控制偷税漏税、洗钱等违法行为的发生。在教育领域,可以利用区块链技术的可追溯性实现对教育资产与智力成果的版权保护,从源头上解决知识产权纠纷问题。此外,数字货币存储在区块链上具有较高的安全性与可靠性,在教育领域可以将学生成绩、个人档案以及学历证书等重要信息存放在区块链上,防止信息丢失或被恶意篡改,构建安全、可信、不可篡改的学生信用体系,助力解决当前学生信用缺失以及全球学历造假等问题。

(2)优化教育业务流程,实现高效、低廉的教育资源交易。在跨境支付方面,区块链利用去中心化特性摒弃中转银行角色,实现点到点快速且低成本的跨境支付。在教育资源共享方面,利用分布式账本技术实现用户与资源间的直接联系,能够简化操作流程,提高资源共享效率,以此来促进教育资源的开放共享,解决资源孤岛问题。在教育资源交易方面,利用去中心化特性剔除交易中介平台,实

现消费者与资源的点对点对接，从而减少费用支出，简化操作流程，打造高效、低廉的教育资源交易平台。

(3) 利用去中心化特性构建去中心化教育系统。区块链技术应用于供应链金融业务，通过剔除中间交易机构，减少人为介入，从而降低成本及操作风险。Wave已与巴克莱银行达成合作协议，将信用证与提货单号及国际贸易流程的文件放在公链上，通过公链进行认证与不可篡改验证，建立完全透明的“游戏规则”，实现验证规则的去中心化。在教育领域，区块链可以用来开发去中心化教育系统，打破传统教育服务被学校或政府机构垄断的局面，使得任何具有教育资质的机构均可以开展教育服务并颁发有效的学历证书，实现正规教育与非正规教育的有效融合，推动全民参与教育体系的变革。

(4) 分布式存储与记录可信学习数据，实现校企之间高效对接。区块链技术让证券交易市场变得更加公开、透明、绿色、公平和高效，使原本高度依赖中介机构的传统模式变为分散的平面网络交易模式，实现数据的分布式存储与记录。在教育领域，学生的个人信息、学习成绩、成长记录等内容都可采用类似的存储记录方式，分布式存储在教育系统中，在保证信息真实安全的基础上，可以向其他学校或招聘单位共享数据内容，作为学生求职面试的重要依据。利用分布式账本技术向用人单位展示自己的学业成绩与专业技能，搭建学生与企业交流的桥梁，建立校企合作新模式，以此实现学生与用人单位的高效对接。

(5) 开发教育智能合约，构建网络资源及平台运行新模式。区块链中的智能合约技术能将当前金融交易过程中大量的人工及半人工验证和管理工作实现自动化运行，提升交易系统的智能性。在开放教育资源建设方面，利用智能合约的透明、自动执行等特性，可以实现资源上传、认证、流转、共享等工作的自动化执行，降低资源共享成本，提高资源共享效率，构建网络资源流转新形态。此外，利用智能合约可以建设高效、智能的网络学习社区，实现学习社区的“自组织”运行，并实时监控社区生态环境，自动屏蔽删除不当言论，营造积极向上的社区氛围。

四、区块链技术在教育中的应用模式

2016年10月，工信部颁布《中国区块链技术和应用发展白皮书》，指出“区块链系统的透明化、数据不可篡改等特征，完全适用于学生征信管理、升学就业、学术、资质证明、产学研合作等方面，对教育就业的健康发展具有重要的价值”（周平，2016）。调研发现，当前国内外区块链技术的教育应用正处于萌芽状态，少数教育机构开展了积极的探索。互联网+教育是全球教育发展变革的大趋势，其宗旨是应用互联网思维、技术和模式改造传统教育生态，实现教育系统的结构性变革（杨现民等，2016）。区块链技术有望在互联网+教育生态的构建上发挥重要作用，其教育应用价值与思路主要体现在六大方面：建立个体学信大数据、打造智能化教育淘宝平台、开发学位证书系统、构建开放教育资源新生态、实现网络学习社区的“自组织”运行以及开发去中心化的教育系统。图2显示了基于区块链技术构建的互联网+教育新生态体系。区块链技术有助于推动教育体系变革，加速教育系统进化发展。

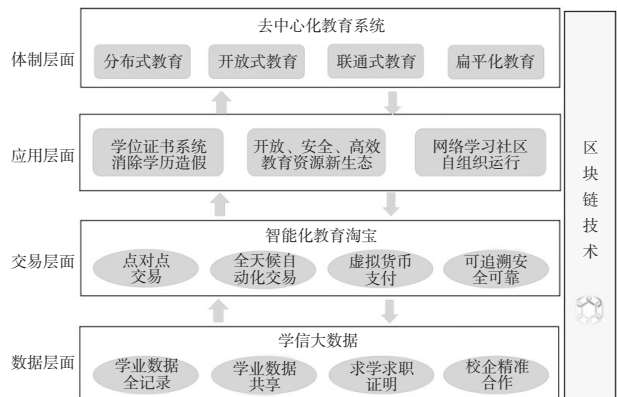


图2 基于区块链技术的互联网+教育新生态

1. 建立个体学信大数据，架起产学合作新桥梁

区块链技术在教育领域可以用做分布式学习记录与存储，允许任何教育机构和学习组织跨系统和跨平台地记录学习行为和学习结果，并永久保存在云服务器，形成个体学信大数据（李青等，2017），有助于解决当前教育领域存在的信用体系缺失和教育就业中学校与企业相脱离等实际问题。用人单位招聘时，可以通过合法渠道合理获取学生的任何学习证据数据，用于精确评估应聘者与待招岗位间的

匹配度。此外,学信大数据还是高校开展人才培养质量评估以及专业评估的重要依据,有助于实现学生技能与社会用人需求无缝衔接,有效促进学校和企业人才培养上的高效精准合作。

未来教育研究所(IFTF)和美国高考(ACT)基金会提出的“学习即赚钱”(Learning as Earning)计划(Sharples et al., 2016),其中心思想源于Edublocks概念,类似于当前用来记录和评估学生学习的“学分”。除了跟踪学术学习活动外,Edublocks还可以测量和记录非正式学习,比如培训活动、学校比赛、研究演示、实习经历、社区服务等,一连串的Edublocks形成一个分布式账本或电子公文包,让学生在任何时间、任何地点都能获得所发生的学习信用。学术顾问将专注于帮助学生在其电子信息数据库中获得最多的“收入”。毕业时形成的个人电子信息数据库,包含“赚取”的各种技能,即学生在学习期间获得的所有Edublocks,将作为学生求职面试时的简历,也将成为招聘单位选拔人才的重要参考依据。

索尼全球教育(Sony Global Education)在一份报告中指出,发达的区块链底层架构系统将促进学术进展记录,可将区块链技术作为一个去中心化且又很安全的系统来加密传输学生数据(Educational Week, 2017)。特别是与考试相关的学生学业水平的统计与测量数据,依托区块链技术设计全新、安全的基础设施系统,不仅能在网络上安全共享,还能永久安全地存储在云服务器中,随时供查询、获取,为学业水平的测评和记录方式开拓新的可能,打造未来教育新平台。该平台允许学生转移数据信息,可以将自己的成绩单发送给心仪企业的老板,为学生求职面试和企业招聘均提供了极具说服力的材料。

2. 打造智能化教育淘宝平台,实现资源与服务的全天候自动交易

通过嵌入智能合约,区块链技术可以完成教育契约和存证,构建虚拟经济教育智能交易系统。该系统中各种服务的购买、使用、支付等工作全部由系统自动完成,无需人工操作,同时购买记录无法篡改、真实有效,所有的交易和合约数据都将被永久保存(李青等,2017)。消费者在该平台发出购买

信息后,系统会根据智能合约的运行规则自动将对应的学习资料发送给消费者,该资料的物流信息也将被智能合约追踪,当消费者确认收到学习资料时系统自动完成支付,无需手动付款。此外,该平台还提供在线学业辅导和工具下载等服务,学习者可根据学习需求选择恰当的学习服务,包括一对一在线辅导、知识点精讲微课、难点习题讲授等,所有资源和服务均可依据学习者的个性需求实现自主消费。

基于区块链技术的智能化教育淘宝平台与其他交易平台相比,具有独特的优势:(1)智能合约程序记录在区块链上,具备公开、透明、不可篡改等特性,可以保证交易信息的真实有效,杜绝欺诈行为的发生。(2)智能合约程序可以控制区块链资产,能够存储并转移数字货币和学习资料,学习者购买资料和服务等交易信息可随时被追踪查询并被永久保存,从而为保障商家和消费者权益提供强大的技术支撑和过程性证据。(3)智能合约程序由区块链自动执行,人工无法干预、篡改,一方面能够提高平台交易效率,满足消费者对于知识获取实时性的需求,另一方面能够保证交易平台的可靠性与稳定性,防止交易平台出现系统性崩溃现象。(4)智能交易无需类似支付宝的第三方支付平台,可以实现学习者与培训机构、学习者与教师、机构与机构之间的点对点交易,既能节省中介平台的运营与维护费用,同时又能提供有质量保证的在线学习服务。

3. 开发学位证书系统,解决全球性学历造假难题

随着就业市场竞争的加剧以及科技的发展,学历造假成为阻碍教育全球化发展的重要因素。伊利诺伊大学物理学教授George Gollin曾对文凭造假现象做过调查,他估计每年约有20万份虚假学历证书从非法文凭提供商处售出。国际知名调查公司HireRight的一项调查结果显示,约86%的受访雇主表示他们曾发现应聘者提供虚假学历信息。为了解决学术欺诈尤其是学历造假这一国际性教育难题,麻省理工学院、霍伯顿学校、肯尼亚信息和通信技术部等机构开始尝试引入区块链技术,构建全新的学位证书系统,以实现学历信息的完整、可信记录。

麻省理工学院的媒体实验室（The MIT Media Lab）应用区块链技术研发了学习证书平台（MIT Media Lab, 2017）。证书颁发的工作原理如下：首先，使用区块链和强加密的方式，创建一个可以控制完整成就和成绩记录的认证基础设施，包含证书基本信息的数字文件，如收件人姓名、发行方名字、发行日期等内容；其次，使用私钥加密并对证书进行签名；接下来创建一个哈希值（Hash），用来验证证书内容是否被篡改；最后，再次使用私钥在比特币区块链上创建一个记录，证明该证书在某个时间颁发给了谁。在实际应用中，上述工作虽然能一键操作完成，但是由于区块链自身透明化特性所带来的一系列隐私问题，目前该软件系统仍在不断完善中。

霍伯顿学校（Holberton School）是一所软件工程师培训学校，也是世界上首个使用区块链技术记录学历信息的学校，它从2017年开始将学历证书信息在区块链上共享，这一做法受到众多招聘公司的赞赏（Market Wired, 2017）。霍伯顿学校的联合创始人 Sylvain Kalache 认为，利用区块链去中心化的、可验证的、防篡改的存储系统，将学历证书存放在区块链数据库中，能够保证学历证书和文凭的真实性，使得学历验证更加有效、安全和简单，同时能节省人工颁发证书和检阅学历资料的时间和人力成本，以及学校搭建运营数据库的费用，这将成为解决学历文凭和证书造假的完美方案。另外，一些国家也开始行动起来，例如，肯尼亚政府强烈意识到学历造假给国家教育乃至社会经济带来的严重影响，为了严厉打击造假文凭的非法行为，目前正在和 IBM 密切合作尝试建立一个基于区块链的学历证书网络发布与管理平台，让所有学校、培训机构等都可以在区块链网络上发布学历证书，实现学历证书的透明生产、传递和查验（比特币中文网，2017）。

4. 构建安全、高效、可信的开放教育资源新生态

近年来，开放教育资源（Open Educational Resources，简称 OER）蓬勃发展，为全世界的教育者和受教育者提供了大量免费、开放的数字资源，但同时也面临版权保护弱（余平等，2009）、运营成本高（李莹等，2014）、资源共享难（韩锡斌等，2012）、资源质量低（保罗·川内等，2013）等诸多现

实难题。如何构建安全、高效、可信的开放教育资源新生态，成为当前国际 OER 领域发展的新方向。区块链技术有望成为解决上述难题的“利器”，推动 OER 向更高层次发展。

（1）应用区块链技术加强资源版权保护。基于非对称加密算法保护的版权信息其安全性与可靠性更高，同时鉴于区块链公开透明的特点，任何资源创建信息都可以被使用者查询、追踪、获取，进而有助于从源头上解决版权归属问题。资源上传者可将 OER 的版权信息和交易信息记录在区块链上，包括资源创建者、创建时间、资源类型等内容。因此，任何教育资源的创建和更新可随时被追踪和查询，并被有效证明（Guo et al., 2016）。

（2）应用区块链技术降低 OER 运营成本。将区块链技术的去中心化应用到 OER 建设中可节省大量中介成本。用户与用户间可直接通过点对点的传播方式进行资源共享，从而减少在大量中介平台上研发与管理维护的投入，改变 OER 运行机制，有效降低 OER 运营成本。

（3）应用区块链技术促进资源共享。利用区块链的分布式账本技术，将教育资源分布式存放在不同的区块中，通过点对点的传播方式，所有节点将通过特定的、达成共识的软件协议直接共享学习课件和工具软件等资源，既有助于提高共享效率，又可以解决资源孤岛问题。未来，借鉴金融领域的跨境支付业务，全球用户都将实现无障碍的点对点资源共享与实时交易，形成全球无缝流动的超大规模信息资源开放共享网络。

（4）应用区块链技术提高资源质量。图3显示了基于区块链的智能合约与共识机制构建的 OER 网络认证机制。具体步骤如下：资源创建者将资源

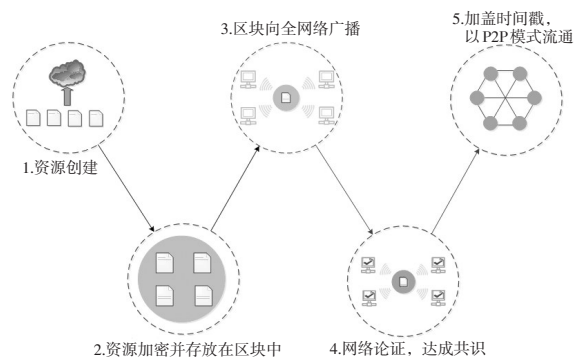


图3 基于区块链技术的OER网络认证机制

上传云端平台；利用非对称加密算法使用公钥和私钥对教育资源进行分别加密，并存放在区块中；将承载教育资源的区块广播全网并等待认证；超过51%的节点达成共识通过认证，承载资源的区块加盖时间戳并在网络中以P2P的模式流通。资源认证机制中的认证、流转、共享等环节均由区块链底层内置的智能合约自动完成，全过程公开透明、不可篡改，各个节点上的资源用户共同认证新上传资源的应用价值。基于区块链技术的OER网络认证机制可以杜绝重复、无效、低质量资源的产生，能有效提升资源质量和资源流通效率。

5. 实现网络学习社区的真正“自组织”运行

区块链与在线社区的结合，也是区块链技术在教育领域很有前景的应用方向。区块链技术可以优化和重塑网络学习社区生态，实现社区的真正“自组织”运行，其应用主要体现在以下三个方面：

(1) 使用虚拟币提高社区成员参与度，形成社区智慧流转体系。应用区块链技术建立社区虚拟币产生与流通机制，学生可通过发帖、提问、回答等行为的发生自动赚取虚拟币，并可利用虚拟币购买社区学习资料与服务，从而激发社区成员的参与度，形成以虚拟币作为核心激励机制与衡量社区贡献度重要指标的集体智慧生成与流转生态。

(2) 保护社区成员智力成果，生成观点进化网络。利用区块链的可追溯性，能对社区成员发表的帖子和观点自动追踪、查询、获取，从源头上保护社区成员的智力成果，防止知识成果被抄袭，从而有利于创新性、原创性观点的迸发。此外，依托分布式账本技术，将发表的观点分布存储在网络中，根据各个观点之间的语义联系生成可视化的知识网络图。随着观点的不断生成与进化发展，社区将聚小智为大智，形成具备无限扩展能力的群体智慧网络（杨现民，2015）。

(3) 净化社区生态环境，实现社区成员信誉度认证。智能合约保证网络社区的自动运行，发帖、提问、回答等内容将自动推送到社区平台，根据预先定义好的规则程序对社区论坛进行自动化监控，对于歪曲客观事实或具有误导性的谣言信息自动屏蔽删除，以达到净化社区生态的目的。同时，可根据社区成员发帖内容与次数对成员信誉进行认证，

信誉度认证较高的社区成员可享有社区特权，如多次下载学习资料或发言无限制次数等，以此鼓励积极向上的发言，从而营造健康向上的社区氛围。

除了促进社区的自组织运行外，区块链技术还可以在增强社区学习的适应性方面发挥作用。目前，国内的喵爪机构已经应用区块链技术，通过喵爪币众筹AltSchool的方式创建了可以为每个孩子提供定制学习服务、以项目为导向的自适应学习社区——极客豆学院（上海喵爪网络科技有限公司，2016）。在创新学习正式开始前，极客豆学院的教师通过与学生聊天勾画出详细的学习者档案。教师通过向学生提问数学、语言等方面的问题，了解学生自身的性格癖好、学习方式、强项和弱点等个性特征。基于学习者的档案信息，极客豆学院可以为每个孩子确定全年的学习目标并细化为每周都会更新的游戏清单，学生可每天在清单上挑选不同的项目学习，从而实现个性成长。

6. 开发去中心化教育系统，全民参与推动教育公平

当前教育系统的高度中心化和集权化主要体现在教育体制的中心化上。教育体制是教育机构和教育规范两个要素的结合体，其中教育机构是载体，包括实施机构和管理机构；教育规范是核心，即维护机构正常运转的制度（刘义兵等，2014）。现阶段的教育体系仍以正规教育为主导，由政府机构或学校提供教育服务并进行认证，个人对某一特定学科的精通程度，仍需由受认可的大学颁发文凭或证书来证明，导致教育的管理权被学校和政府所垄断。

利用区块链技术开发去中心化教育系统，有助于打破教育权利被学校或政府机构垄断的局面，使教育走向全面开放，形成全民参与、协同建设的一体化教育系统。未来，除了政府机构批准的学校、培训单位等教育机构具有提供教育服务的资质外，将有更多的机构、甚至个体承担专业教育服务提供商的角色，并且基于区块链的开源、透明、不可篡改等特性能保证其教育过程与结果的可信。比如，一些企业、社区或其他组织均可提供教育服务并进行认证，其颁发的证书将与传统高校颁发的证书一样可在全网流通，并可有效证明学生是否掌握了某一知识技能。校际边界也将逐步模糊，学习者

可以自主选择在任何学习中心或培训机构学习某门课程,获得具有同等效力的课程证书,有效证明自己在某一领域的专业知识和技能。多门课程证书的获得以及学分的积累,将使学生有资格申请获得国家以及国际教育组织认定的学历学位证书。

五、区块链技术应用面临的挑战

区块链技术现在正处于起步发展阶段,大多数研究聚焦在金融领域。与金融领域相比,教育领域具有更强的独特性和复杂性,区块链技术在教育领域的成功应用将面临推广运行难、教育数据产权模糊、数据存储空间有限、区块链技术自身安全隐患所引起的师生隐私保护风险等诸多挑战。

1. 教育领域实践经验少,推广运行存阻力

目前国内外在区块链技术应用领域尚未普及标准且大多数研究聚焦在金融领域,其在教育领域的推广运行将面临缺乏政策保护与实践经验两方面的挑战。首先,由于缺乏政策保护与引导,去中心化属性对传统教育管理机构将造成强烈冲击,在利益分配上使得传统教育平台遭受重大损失,导致相关机构和部门对区块链技术在教育领域中的应用持谨慎态度,不利于区块链技术的大规模推广与应用。其次由于区块链技术在教育领域的应用案例较少,专家学者对其在教育领域的推广应用更多持观望态度,缺乏推动其进一步应用的动力。

为解决区块链技术在教育领域的推广运行问题,可从以下三个方面入手:第一,我国应尽快出台区块链技术在教育领域应用的法律法规,从运营机制、技术应用、体制管理等多个层面制定保护细则,切实保障国家、机构、个体在区块链技术与教育应用上的合法权益。第二,制定切实可行的利益分配方案,妥善处理好传统教育管理机构 and 运营平台之间的利益分配,使区块链技术在教育领域的推广应用得到各部门认可,减少推广运行阻力。第三,依托中国区块链技术和应用发展联盟等组织,联合教育领域专家,从区块链国际化制定中借鉴先进经验,深入研究区块链技术在教育领域推广应用的热点和难点问题,制定区块链技术在教育领域的应用标准与规则。因此,教育工作者应积极与区块链专家联合,尽早制定区块链技术在教育领域

的应用标准,打通应用通道,提升应用效果。

2. 区块链数据存储虚拟化,教育数据产权有争议

区块链的去中心化特征淡化了教育管理机构的职责,学生数据管理等工作相对弱化。由于去中心化特性,使得区块链上的数据分布式存储与记录,造成学生数据的产权变得模糊。当前教育中的数据管理一般由学校教务处负责,而区块链技术的应用淡化了实体管理部门的职责,使得数据都存储在虚拟区块链上。因此这些虚拟数据的归属权属于谁?使用权属于谁?基于数据分析产生的成果的所有权又属于谁?这一系列的数据产权问题都将成为区块链技术在教育领域进一步推广应用过程中亟待解决的问题。

基于区块链技术存储数据的产权问题,相关教育部门需要制定详细的数据归属标准体系与利益价值分配方案。首先,区块链存储的教育数据,其归属权应该属于数据产生者,即教师、学生和教育管理部门,而不是第三方平台,这是区块链数据存储的基本原则。其次,任何数据的使用都需要经过数据产生者的书面授权同意,可以授权给公司企业以开发更大的商业价值,但保证数据产生者的个体利益与隐私,却是数据使用的前提。最后,在进行校校合作或校企合作过程中,教育数据产生的商业价值需要制定明确的利益分配方案,除了书面授权涉及的约定收益外,还可以参考著作权使用费的模式,由平台按固定比例将利益分配给数据产生者、数据提供者以及数据价值开发者,或者可以征得用户免费授权,将成果利益完全归属于数据价值开发者。只有制定明确的数据产权归属与使用规范,才能打消教师和学生对于教育教学活动产生的数据所有权的顾虑,从而更好地促进区块链技术在教育领域的应用。

3. 系统网络容量小,数据存储空间遇瓶颈

区块链技术是互联网金融技术的创新,但众多技术特性特别是网络容量仍处于发展的初级阶段。区块链数据库记录了每一笔交易从开始至今的所有数据信息,任何想要进行数据存储的用户都需要下载并存储承载所有资源信息的创世块(Creation Block)。随着大数据技术在教育领域的应用,教师、学生以及教育管理部门产生的数据量将会呈现

井喷式增长,导致区块链中的区块承载的数据信息越来越多,这对区块链数据库的存储空间提出更高的要求。各类数据量越来越大,一方面导致数据存储空间受限,影响教师、学生以及管理部门上传与更新数据信息,另一方面将会降低数据传播效率,影响师生对数据获取实时性的需求。

与其他存储技术优势互补形成协同效应是解决区块链数据存储空间受限的有效途径。可将区块链技术与云存储技术相结合。Storj利用区块链搭建去中心化云系统,将教师、学生以及管理机构产生的数据“切片”处理,对各个分片数据进行加密,通过分级存储的方式被分散存储到互联网上其他学校或教育部门贡献出来的硬盘空间上,从而解决数据存储空间问题。同时,为保证数据信息的不可篡改性,Storj采用一种叫做Merkle树的数据结构,通过对比Root节点的哈希值(Hash)就可判断数据是否被修改,如果某些数据信息被修改或不可用,Storj通过纠删码的方式,从其他可用的数据块重构该数据信息,并保存到其他节点上。因此,将Storj云存储技术应用到教育数据存储中,既可解决数据存储空间问题,又能保证数据的不可篡改性。此外,McConaghy等学者提出巨链数据库(Bigchain-DB)的概念,即去中心化数据库,数据信息可以达到每秒百万次写入,数据存储量以PB计算(Gmbh, 2016)。其特点主要体现在:去中心化控制,免疫攻击;节点数量可线性扩展,实现基于NoSQL语言的高效查询和权限管理;容量可扩展,任何具备法律约束力的合同及证书都可安全存储在区块链的数据库上。因此,基于区块链技术的各类教育数据存储均可采用巨链数据库的核心理念,不仅能够免受攻击,保证师生数据的安全可靠,还可扩大数据存储空间,实现教师、学生以及教育部门数据的高效查询与管理,从而解决区块链技术在教育领域应用中面临的数据存储空间受限问题。

4. 匿名技术尚未成熟,师生隐私保护有风险

区块链技术通过隔断交易地址和地址持有人真实身份的关联,达到匿名效果,防止因交易信息公开透明而导致用户隐私泄露,但这样的保护通过观察和追踪区块信息以及用户ID依旧可以追查到用户的个人信息(Zyskind et al., 2015)。因此,区块链技术

在教育领域的应用面临师生隐私被泄露的风险,主要来自以下两个方面:一是所有交易信息公开透明,任何信息都可以被追踪查询,进而推断出某些结论,或对教师和学生的状态和行为进行预测,不利于教师和学生个人隐私的保护;二是区块链的安全性通过算法保障,理论上只有超过51%的节点用户同时被黑客攻破后数据信息才会被泄露或篡改,但是随着数学、密码学和计算技术的发展,很难保障今后该算法不被破解,造成教师和学生信息的泄露。

区块链自身存在的安全问题在各个领域都引起了广泛的关注与讨论,结合区块链技术在教育领域面临的安全挑战提出如下应对策略:第一,对教师、学生以及教育管理部门产生的数据信息进行权限管理,利用非对称加密算法对各类数据进行加密处理,只有拥有对应私钥的用户才可以访问用户的数据信息,保证师生的个人信息不被泄露。第二,采用算法技术与现实约束相结合的方式,在提高系统算法水平的同时通过法律保障、部门监管或者信用抵押等方式进行联合管控,防止黑客入侵事件的发生。第三,利用大数据技术应对高级可持续攻击,通过对黑客攻击模式、时间、空间等特征进行处理分析,搭建应对黑客攻击的防御系统,与区块链自身安全体系形成协同效应,全面升级师生隐私保护系统。

参考文献:

- [1] 保罗·川内,肖俊洪,杨伟燕(2013). 开放教育资源质量保证准则——TIPS框架[J]. 中国远程教育, (10):11-21.
- [2] 比特币中文网(2017). 肯尼亚政府利用IBM区块链预防学历证书欺诈[EB/OL]. [2017-02-18]. <http://www.xwtoutiao.cn/p/9tv7cesf/>.
- [3] 蔡钊(2016). 区块链技术及其在金融行业的应用初探[J]. 中国金融电脑, (2):30-34.
- [4] 陈一稀(2016). 区块链技术的“不可能三角”及需要注意的问题研究[J]. 浙江金融, (2):17-20.
- [5] 韩锡斌,周潜,程建钢(2012). 基于知识分享理论的开放教育资源共建共享可持续发展机制的研究[J]. 清华大学教育研究, (3):28-37.
- [6] 金科网(2017). 用区块链保证食品安全[EB/OL]. [2017-02-18]. <http://www.vdai.com/article/10521.html>.

- [7]李青,张鑫(2017). 区块链:以技术推动教育的开放和公信[J]. 远程教育杂志, (1):36-44.
- [8]李莹,丁唯佳,赵莹(2014). 大学开放教育资源项目能否实现资金的自给自足——来自美国杨百翰大学自主学习项目的案例报告[J]. 现代远程教育研究, (3):32-38.
- [9]林晓轩(2016). 区块链技术在金融业的应用[J]. 中国金融, (8):17-18.
- [10]刘义兵,付光槐(2014). 教师教育一体化发展的体制机制创新[J]. 教育研究,(1):111-116.
- [11]上海喵爪网络科技有限公司(2016). 利用区块链技术建立 AltSchool 式的教育机制——结合喵爪币谈区块链技术定制化教育中的应用[J]. 中小学信息技术教育,(6):53-56.
- [12]王硕(2016). 区块链技术在金融领域的研究现状及创新趋势分析[J]. 上海金融, (2):26-29.
- [13]杨现民(2015). 泛在学习环境下的学习资源有序进化研究[J]. 电化教育研究, (1):62-68.
- [14]杨现民,赵鑫硕(2016). “互联网+”时代学习资源再认识及其发展趋势[J]. 电化教育研究, (10):88-96.
- [15]余平,祝智庭(2009). 开放教育资源的版权与访问许可研究[J]. 开放教育研究, (6):42-47.
- [16]袁勇,王飞跃(2016). 区块链技术发展现状与展望[J]. 自动化学报, (4):481-494.
- [17]张波(2016). 国外区块链技术的运用情况及相关启示[J]. 金融科技时代, (5):35-38.
- [18]张苑(2016). 区块链技术对我国金融业发展的影响研究[J]. 国际金融, (5):41-45.
- [19]周平(2016). 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:36-37.
- [20]Educational Week(2017). 'Blockchain' Tech Pushed by Sony. Does It Have a Future in K-12?[EB/OL].[2017-01-18]. http://blogs.edweek.org/edweek/DigitalEducation/2016/02/block-chain_tech_for_schools_ey.html.
- [21]Gmbh, A.(2016). Bigchain DB: A Scalable Blockchain Database[A]. Proceedings of The Block Chain Conference[C]. San Francisco.
- [22]Guo, Y, & Liang, C.(2016). Blockchain Application and Outlook in the Banking Industry[J]. Financial Innovation, 2 (1): 24-36.
- [23]Kosba, A., Miller, A., Shi, E. et al.(2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[A]. Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP) [C]. University of Maryland and Cornell University.
- [24]Market Wired(2017). Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain [EB/OL].[2017-01-28]. <http://www.marketwired.com/press-release/ts-academic-certificates-with-bitcoin-blockchain-2065768.htm>.
- [25]MBA(2016). Distributed Ledger Technology[EB/OL].[2016-12-15]. <http://wiki.mbalib.com/wiki/DLT>.
- [26]Mit Media Lab(2017). Degree Requirements[EB/OL].[2017-01-18]. <https://www.media.mit.edu/posts/degrees/>.
- [27]Morgen Peck(2016). A Blockchain Currency That Beats Bitcoin on Privacy[J]. IEEE Spectrum, 53(12):11-13.
- [28]Pilkington, M.(2015). Blockchain Technology: Principles and Applications[EB/OL]. [2016-12-20]. <https://ssrn.com/abstract=2662660>.
- [29]Sharples, M., & Domingue, J.(2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward[A]. Verbert, K., Sharples, M., & Klobučar, T. (eds) (2016). Adaptive and Adaptable Learning[M]. EC-TEL 2016. Lecture Notes in Computer Science, vol 9891. Springer, Cham.
- [30]Underwood, S.(2016). Blockchain Beyond Bitcoin[J]. Communications of the Acm, 59(11):15-17.
- [31]Victoria, L.(2016). Trusting Records: Is Blockchain Technology the Answer?[J]. Records Management Journal, 26 (2): 110-139.
- [32]Wang, H., Chen, K., & Xu, D.(2016). A Maturity Model for Blockchain Adoption[J]. Financial Innovation, 2(1): 2-12.
- [33]Wild, J., Arnold, M., & Stafford, P.(2015). Technology: Banks Seek the Key to Blockchain[EB/OL]. [2017-01-28]. <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64>.
- [34]Wright, A., & De Filippi, P.(2015). Decentralized Blockchain Technology and the Rise of Lexcryptographia[EB/OL].[2016-12-20]. <https://ssrn.com/abstract=2580664>.
- [35]Zyskind, G., Nathan, O., & Pentland, A.(2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data[A]. Proceedings of IEEE Security and Privacy Workshops[C]. Chicago.

收稿日期 2017-02-20 责任编辑 刘选

The Application Model and Challenges of Blockchain Technology in Education

YANG Xianmin, LI Xin, WU Huanqing, ZHAO Keyun

Abstract: Blockchain technology is regarded as another disruptive technology after the cloud computing, Internet of things and big data, which is received high concern by the governments, financial institutions and technology enterprises. Essentially, blockchain technology is a kind of technical scheme to maintain a reliable database by means of decentralization and high trust. Its core technologies include distributed accounting technology, asymmetric encryption algorithm and intelligent contract. Furthermore, it has the distinguished characteristics such as decentralization, consensus mechanism, traceability and high trust. Nowadays, as the underlying technology of bitcoin, blockchain technology is not only applied in the field of finance, but also has great potential in education. What's more, it is expected to play an important role in the construction of internet + education ecology to promote the reform of educational system. According to the experience and enlightenment from the application of blockchain in the financial field, the blockchain in education is mainly embodied in the six application modes: establishing individual knowledge big data, creating intelligent educational platform of Taobao, developing degree certificate system, constructing new ecology of open education resources, achieving "self-organization" operation of network learning community and developing the decentralization of education system. Obviously, due to the uniqueness and complexity in education, the blockchain technology application in education is also faced with many challenges, including the difficulty to operate in education application, the confusion of educational data property, the limited data storage space and the security risks of teachers and students' privacy protection caused by blockchain technology itself.

Keywords: Blockchain; Educational Application; Application Model; Realistic Challenges

(上接第33页)

Embodied Cognition: The Origin of Theory, the Logical Assumptions and the Future Trends

ZHAO Mengcheng, WANG Huiting

Abstract: Embodied cognition has been proposed to object to the deviation of the traditional cognitive science. In the traditional cognitive science, human mind has been simplified into the exact mirror image of nature and the world. Meanwhile, cognitive activity has been rejected to embed the body and experience. Embodied cognition truly regards human beings as "all-rounds", which proposes cognition as the interactive production of brain, body and environment and emphasizes the all-rounds development of body and mind. It stresses "embodiment" and "situatedness", which switches the understanding of cognition from the researches on individual processed frame to the analysis of social practical activity; it also proposes that cognitive structure has time attribute, which means at any moment cognitive state is just an immediate state in the continuous dynamic state change. So it proposes that the real-time and concrete analysis of cognitive process needs to combine the experimental method and the natural approach in real and nature situation. Compared with behavioral psychology and disembodied cognition, embodied cognition has its advantages and value in some extent and has made some achievements as well. However, it still has some questions needed to be paid attention to, for instance, the chaos of research ideological trend, the parochialism of research theme, the inappropriateness of research method and so on. In order to promote the efficient development of embodied cognition, prospecting and presupposing its future trends should be made from the levels of ontology and methodology.

Keywords: Cognitive Science; Embodied Cognition; Theory Origin; Logical Assumptions; Future Trends