

区块链技术在数字教育资源流通中的应用

全立新, 熊谦, 徐剑波

(湖南财政经济学院 信息管理系, 湖南 长沙 410205)

[摘要] 数字教育资源流动和共享是教育开放的重要基础,但是因其自身的特殊性和当前流通机制不健全等因素,使得数字教育资源流动和共享进展缓慢。文章通过对区块链技术的研究,设计了一种开放的、去中心化的资源流通模式,即双区块链结合智能合约的模式。在该模式下,通过数字资源注册链管理流通对象、业务控制由智能合约自动完成、流通账本由流通信息链进行管理,以构建一种开放的、资源自增长、自我管理的流通系统。该系统既能促进数字资源在供需双方之间的流转,又能保护资源提供者的合法权益,还能实现对流通资源的管理和监控。

[关键词] 区块链; 数字教育资源; 资源流通; 资源注册; 智能合约

[中图分类号] G434 **[文献标志码]** A

[作者简介] 全立新(1969—),男,湖南花垣人。教授,硕士,主要从事信息技术原理与应用、区块链原理与应用研究。E-mail:qlx5594965@163.com。

一、引言

区块链因中本聪所撰写的文章 *Bitcoin: A Peer-to-Peer Electronic Cash System* 而得名,但在其文献中并没有提出区块链的定义和概念,只在其中指出区块链是用于记录比特币流通账目历史的数据结构。在维基百科上给出的定义中,将区块链类比为一种分布式数据库技术,通过维护数据块的链式结构,可以维护持续增长的、不可篡改的数据记录。

区块链技术被认为是继互联网革命之后又一项人类社会颠覆性变革的技术,受到各国政府、金融机构及科技企业的高度关注^[1]。我国已于2016年把区块链和人工智能技术上升为国家战略,工业和信息化部于2016年9月发布了《中国区块链技术和应用发展白皮书(2016)》。2018年1月23日,在2018年全球经济年会——冬季达沃斯论坛上,有学者提出2018年将是区块链应用元年^[2]。区块链技术在全球金融业、商业服务业等领域得到广泛的研究和应用。同样,区块链技术正在影响着我们的教育教学,虽然它在教育教学中的应用大多处于萌芽阶段或仅停留在前瞻性

的概念,但对推动区块链在教育教学中应用无疑有着积极的现实意义。通过对“中国知网”的文献查询得知,目前,国内相关的研究还比较少,更凸显其研究的价值所在。

二、国内外研究现状

目前,区块链在教育领域中的实质性应用还不多,根据美国著名信息技术咨询公司 Gartner 所提出的技术成熟度曲线来说,区块链技术在教育中的应用处于技术萌芽期^[3]。国内外只有少数大学、研究机构和商业企业对区块链技术在教育中的应用开展了早期的实践。比如,中央财经大学联合世纪互联公司和微软公司共同研发“校园区块链”项目,该项目利用区块链技术帮助学生记录在校期间的所有学业成就,形成一条终身有效、不被篡改、不可造假、去中心化的信用链条^[4],方便用人单位获取和查证。

有资料表明,塞浦路斯尼科西亚大学是世界上最早把区块链技术运用在教育中的大学之一,他们把学生的学习成果记录在分布式账簿上,保证记录的不可篡改、安全和可信^[5]。2015年,麻省理工学院已利用区

基金项目:湖南省教育科学“十二五”规划一般资助课题“基于语义 Web 服务的教育资源云应用研究”(课题编号: XJK013BXX004)

区块链技术颁发人才的数字证书,用来认可其全球研究伙伴计划的行业人才^[5]。2015年,索尼公司以区块链技术基础设施,构建服务全球教育机构的平台——“索尼全球教育”^[6]。该平台使学校之间呈网状结构,学习者的学习过程和结果在学习者本人、教师、家长、学校之间实现共享,减少教育行政部门在学习过程和结果评价中的干预,促使教育更加公平,大大提高了教育管理效率。2017年,美国霍伯顿学校开始在区块链上共享学历证书信息,并发行数字徽章。澳大利亚国立大学、英属哥伦比亚大学、波士顿大学、荷兰代尔夫特理工大学和瑞士联邦理工学院已经签订协议,将应用区块链技术,以每所学校为核心节点,构建共享学校系统^[7],类似国内传统意义上C9大学联盟。

三、数字教育资源流通模式分析

当前数字教育资源流通模式主要有数字资源分享平台和内容平台二种^[8]。

分享平台模式主要以百度文库为典型代表。这类模式通过联合教育合作机构、知识工作者和资源需求方等多方力量,利用平台开放性和资源自增长性的特点,汇聚了分类较全的海量共享文档文件。但是这类平台提供的数字资源存在形式单一、内容不一定严谨、质量参差不齐、优劣难以筛选、个性化服务不强等问题。而且,平台管理难度大,内容没有得到很好监管。

内容平台模式主要以网易云课堂、101网校等为典型代表。这类平台以市场机制开发了形式多样的优质数字教育资源,通过平台优势,针对用户个性化需求提供较优质的数字教育资源收费服务,满足不同人群的数字教育资源需求。但是,这类平台存在开放性差,数字资源非常有限、自增长性不强,资源提供者的权益没有得到很好保护等问题。

本文提出的一种数字教育资源的流通模式将是一个去中心化、系统自治、资源自增长、流通高效、账本强背书的社会系统。流通模式如图1所示。

从图中可以看出,这种流通模式将以区块链技术作为底层技术,将由矿工(它获得了经济激励)来运维系统,这样可保证系统的自治性、开放性、去中心化和流通信息强背书性;系统的开放性可以使不同机构、组织、人员参与自组织模式开展数字资源开发和管理,保证资源的自增长;系统上的资源进行注册可保证资源供应方的权益,提高资源生产者的积极性;资源在系统中实现点对点流通,资源采用互联网传输,交易由智能合约^[9](不受任何一方控制的计算机代码,在满足一定条件下自动触发)充当传统的第三方机构执行,既保护了供需双方权益,又降低了流通成本。

四、数字教育资源流通方案设计

(一)方案设计原则

针对当前数字教育资源流通模式面临的各种问题和前文提出的对未来流通模式的设想,本节将给出数字教育资源流通方案设计的四个原则,具体如下:

(1)方案必须是一个开放的、自治的、去中心化的社会系统,尽可能吸引教育机构、数字资源开发企业、知识工作者参与资源开发和管理,并能够保护资源供应方的合法权益。

(2)资源流通渠道的严密性、合法化,流通信息的精准化,定价透明化和流通成本低廉化。

(3)流通过程无需第三方担保,能够做到“钱货两清”和隐私保护,流通记录可追溯、可查询、可申诉且交易信息不可被篡改。

(4)流通能够接受相关职能部门的监督和审查,保证流通内容和流通行为的健康发展。

(二)基于区块链技术的数字教育资源流通系统架构

根据 Brewer 著名的 CAP(Consistency Availability Partition Tolerance)理论,结合本文方案设计原则,从用户、管理员、应用开发者的角度对将来组成系统的各部分的搭配和安排进行假设。即本节将提出一种基

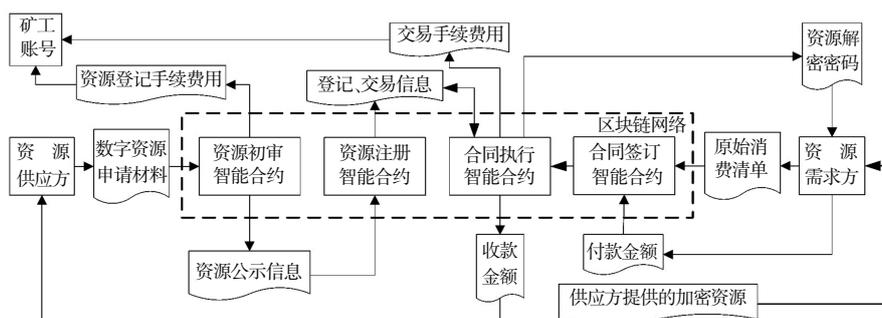


图1 教育资源流通模式示意图

于区块链技术构造出的数字教育资源流通平台的参考架构,如图2所示。

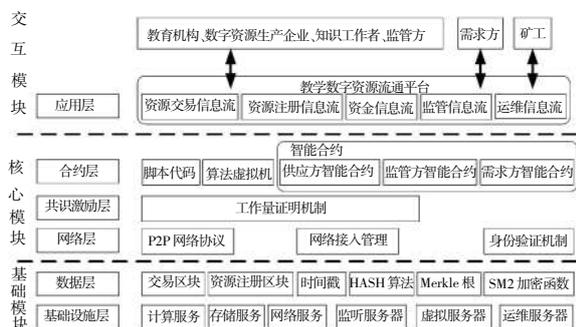


图2 区块链技术构造出的数字教育资源流通系统架构

从图中分析来看,流通系统的架构主要分为应用层、合约层、共识激励层、网络层、数据层和基础设施层六个逻辑层,其中,数据层、网络层、共识激励层属于协议层,是构成区块链技术的必要层级,是实现区块链技术的基本保障,缺一不可。系统架构把六层划分为三大模块,应用层(流通系统用户接口)为交互模块;合约层、共识激励层和网络层为核心模块;数据层和基础设施层为基础模块。

1. 应用层

应用层封装了资源注册、流通和监管等应用场景,为使用各方人员之间以及人员与系统之间提供直接的信息交互的载体。供需双方可以通过应用层实现物流、资金流的全程记录。监管机构通过相应的智能合约智能地监管系统中的资源流通,保障流通系统的健康发展。

2. 合约层

合约层由各类脚本代码、算法虚拟机以及智能合约构成。其中智能合约是合约层的核心,通过嵌入在区块链的合约代码来实现。参与方事先拟定合约内容和触发机制,以代码的形式嵌入系统,一旦满足触发条件,合约自动执行,外界无法干扰。这样可以节约人力和交易成本,提高流通效率。表1罗列了适合本文方案的智能合约名称和类型。

3. 共识激励层

共识层封装了整个系统的共识算法,是实现系统自治性、去中心化、保证网络不被恶意节点攻击的关键,是必需的经济激励措施。考虑到数字资源流通中小额流通较频繁,对区块链流通延迟比较敏感,同时,为防止矿机矿池的算力攻击,方案的共识层拟采用基于成熟的POW(Proof of Word)共识的变种算法Ethash协议作为共识和激励机制^[9]。

4. 数据层

大部分信息平台在使用现代密码学算法时会采用AES、ECDSA、SHA2等国际标准,但考虑到系统的安全性和政策性风险,本方案的数据层密码算法拟与国内金融机构选用的密码学算法保持一致,即选择国密算法,采用SM2加密技术进行加密。

通过这样一个基于区块链技术的架构设计,可以使供需双方获得一个透明、可靠、去中心化、去信用的流通系统,可以实时查看状态,降低流通成本、追溯数字资源,从而提高数字教育资源流通和使用效率。当发生纠纷时,举证和追查也变得更加清晰和容易。

(三)方案构建

1. 数字教育资源流通系统组成

表1 数字教育资源流通的智能合约

合约主体	智能合约名称与类型	合约内容
供应方	资源初审	当资源提供方发送数字产品及相关材料后,通过智能合约在系统已注册的资源中进行初审,并在全网公示
	资源注册	经过公示期无异议的资源,资源注册智能合约自动生成注册记录供矿工打包成资源注册区块
	合同执行	当交易记录被打成交易区块,合同智能合约将自动执行,即向供应方转移需求方预付资金,同时,在交易记录中公开用需求方公钥对供应方资源解密密码的数字摘要(需求方可以用自己解密数字摘要即可知资源解密密码)
需求方	合同签订	当合同智能合约收到需求者提供的资源注册号、流通信息时,核实单价、数量和付款人预付资金等,通过智能合约实现流通合同签订并生成交易记录
	折扣	当消费者购买一定数量的产品之后,可以通过折扣智能合约实现自动折扣
监管方	税收	数字资源提供方的税收缴付由智能合约自动实现
	申诉	当出现资源与描述不符、不合格或超出权限使用资源等情况时,需求方或提供方可以向系统提出申诉,申诉智能合约实现自动处罚
	处罚	当申诉方申诉成功后,智能合约实现自动处罚被诉方

整个数字教育资源流通系统主要分为用户客户端、区块链网络和参与者(包括机构)三部分。数字教育资源流通系统组成如图3所示。

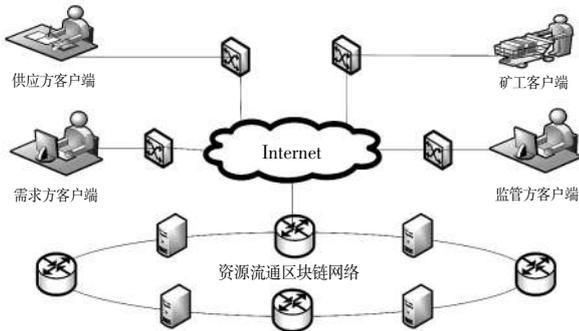


图3 数字教育资源流通系统组成示意图

(1)用户客户端

是为简化用户与区块链网络信息交流,实现用户之间、用户与区块链网络之间的连接和通信隐藏的客户端平台。它包括用户的注册、认证、接入和钱包(用来保存用户的私钥、账户余额)管理;发送资源登记注册和资源流通请求;显示资源注册信息和流通信息;协助流通双方完成数字资源流通的追溯维权等功能。用户客户端一般不保存用户钱包之外的数据。

(2)资源流通区块链网络

资源流通区块链网络是在经济激励机制下自发组成的P2P网络,它连接到互联网中。任何个人、机构和企业都可以注册并下载,安装相关软件者可以成为网络中的节点。网络节点是数据存储中心和系统运行核心,它负责生成区块(挖矿)形成区块链,区块结构如图4所示。从图4可以看出,区块是由区块头和区块体组成,区块头包括时间戳等数据,区块体包含多条交易记录。如果篡改了某一条交易记录,则可以通过相应的哈希值进行检测,也可以通过区块头的梅克尔树根快速检测。由于区块头包含时间戳、上一区块头哈希值等数据,很难伪造一个区块。

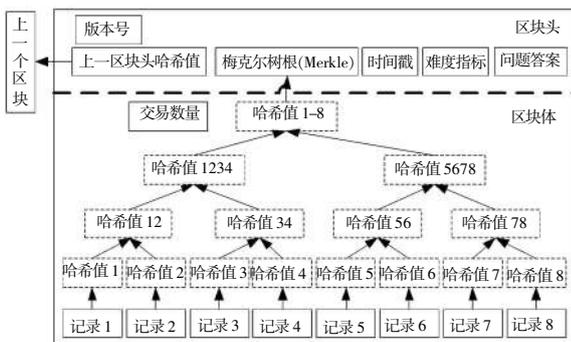


图4 流通系统区块结构示意图^[10]

节点还负责维护保存资源登记注册链和资源流

通信息链,新的区块产生以后,将链接在链的尾端,如图5所示。本方案采用教育资源注册链和资源流通信息链的双区块链结构。考虑到现实中资源版权认定的复杂性和差异性,方案只对本文中提出的教育资源注册链上的数字资源进行强背书,流通的资源也仅限于本系统注册的数字资源。

(3)参与者

参与者由资源供需双方、监管机构、系统运维的社区技术人员和矿工等组成,是业务发起人或系统监管和维护者。他们的主要作用是提供数字教育资源注册登记的外部数据、流通信息,监督区块链记录的正确性,存储和维护可共享的隐私数据,向系统提供数字资源的描述,发起相关查询等。

2. 流通系统的初始化

(1)流通系统可以由一个开源社区或一家公司发起并构建。系统构建好以后,发起方首先以成员身份注册申请加入,然后通过系统生成数字教育资源注册登记和资源流通的创世区块(创世区块里作为区块链的第一个区块,只记录建立时间等信息,并没有具体流通的记录,两种区块链区块的数据结构是完全相同的,区块的结构如图4所示)。最后,采用相应策略对流通系统进行网络宣传和推广,系统正式启动。

(2)系统参与人员通过向流通系统发送数字证书(可以是第三方发放的或自制的)申请加入系统,通过流通系统审核确认后,将此数字证书作为平台注册账号并与成员真实身份对应。参与人员注册成功后,就可以根据自己需求进行资源注册登记、流通、挖矿和监管等相关业务。

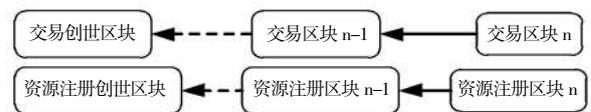


图5 数字资源流通区块链示意图

3. 数字教育资源注册流程

首先,资源供应方对需要进行流通的数字资源向系统申请注册。注册除了需向系统发送供应方ID、其他机构颁发版权号、数字资源类型、数字资源信息描述、使用权限、流通价格以及交付形式等资源证明材料外,还需向系统支付登记费用。这个费用用于支付矿工算力贡献,也是防止恶意注册的经济措施。其次,流通系统自动启动初审智能合约对申请资源进行初审,并把部分注册费用支付给出审核算力的矿工;初审通过后在全网公示,经过公示期的资源由注册智能合约生成资源注册记录并打上注册生效时间戳。该

记录的结构如图 6 所示。“挖矿”节点每经过一个固定时间段将汇集的注册审核通过的记录打包形成区块,随后将区块广播到全网所有节点进行审核和共识,共识通过的区块,“挖矿”节点将获得所有打包记录的剩余注册费用,并负责将新区块链接到资源注册链的末端,如图 5 所示。最后,系统向流通客户端发送最新资源注册链信息。



图 6 数字资源注册记录结构示意图

数字资源注册链主要特征如下:

(1)流通系统按一定时间段(比如 1 小时)汇总通过的资源申请,生成每个申请的记录号、登记时间并进行相应的初审,然后,生成一个区块并广播到全网所有的节点。

(2)矿工获得待审区块,将给出工作量证明(给出问题答案);重新计算梅克尔树根哈希值;给区块头打上时间戳,然后将区块广播到全网审核并取得共识。这样的过程使得此链可具有为注册的资源内容强背书的功效。同时,也为发生申诉时提供原始材料。

(3)链上的区块只能新增,不能更改和删除,链上区块中的记录内容无法更改和删除。

(4)所有已注册人员都可以对此区块链进行检索和下载,系统以一定方式显示所有已通过审核的注册信息,形成对流通系统的监督。

4. 资源流通流程

(1)资源流通先决条件

通过系统进行数字资源流通需要满足三个先决条件。条件一:资源供应方需要在流通发生前,对需要流通的资源在系统中进行登记注册(同一个资源只要注册登记一次),以方便系统发布所有资源的相关信息供需求方选购。条件二:供应方需要提供流通规则的智能合约给系统预付违约“头寸”并公开合约内容,目的是让流通和违约处罚是在无人值守的情况下自动完成。条件三:如前所述,需求方也需要在系统注册,然后开通个人电子钱包,完成流通前的准备工作。这里的电

子钱包可以存放流通所需要的代币,也可存放自己的私钥等其他隐私数据。代币将作为系统资源流通的价值表现,可以通过系统方便与传统的记账货币兑换。

(2)资源流通流程

通过系统进行数字资源流通,大概需要 6 个步骤。

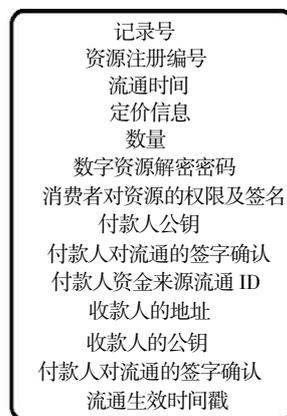


图 7 数字资源流通记录结构示意图

步骤 1:首先,需求方通过系统查询到所有注册的数字资源时,根据供应方 ID 列表,可获取资源类型、交付形式、资源使用权限、定价以及流通智能合约内容等信息。其次,拟定确定流通对象和资源注册编号。最后,根据公布的资源地址下载数字资源。

步骤 2:需求方根据注册链上信息拟定流通信息,包括登记注册编号、付款人电子钱包地址、单价、使用权限、数量等,然后用自己的私钥对流通内容进行数字签名确认,并把流通内容连同自己的公钥一起发给系统。

步骤 3:系统接收到需求方发来的流通信息后,自动启动智能合约签订,生成流通电子合同,然后预执行电子合同即冻结消费者的预付款,索取资源解密密码,用双方提供的公钥进行数字签名确认,给流通内容打上流通生效时间戳。最后,把电子合同交向全网广播。

步骤 4:系统定时广播新区块工作量证明问题。系统中各个节点把对应固定时间段内收到的电子合同生成流通记录,给出工作量证明并打上区块生成时间戳生成待审区块。然后用洪水算法广播到全网中待全网审核和共识。通过审核的区块中包含的流通记录均被视为合法流通。

步骤 5:获得全网共识的待审区块将被链接在流通区块链的末端,如图 5 所示。然后,触发生成该区块节点上的流通智能合约处理区块中的所有流通,并自动完成“钱货两清”的过程,即向资源提供方转移预付款、向资源消费者发送资源解密密码。

步骤6:如果发生流通纠纷向系统投诉(比如,资源内容与说明不符等)或监管处罚,资源登记注册链和信息流通链将为维权者提供证据支持,同时,智能处罚智能合约将从资源提供者的预付违约“头寸”中自动罚没。

从资源流通流程来看,流通信息链主要的特征有:

(1)流通信息链中的记录都有双方数字签名和时间戳,没有办法篡改和抵赖,对流通的安全性、公平性提供保证;

(2)流通链信息是存储在区块链网络的节点上的,实现了分布式记账功能,非常安全可靠且不容易被伪造;

(3)系统参与人员都可以对流通链进行下载和检索,可形成对流通系统的监管,同时,也为后续的流通追溯和申诉提供证据。

五、结束语

数字教育资源注册链的建立是流通商品的展示和流通的前提,它为资源供应方权益提供保护,也为需求方维权提供依据。流通信息链提供了点对点流通的公共账本,无法篡改和删除,并可接受监管部门监督。资源注册链、流通信息链结合相关智能合约,很好地完成了业务需求与业务规则的自动执行,使数字资源及其价值转移在系统中流动是高效、去中心化且可管、可控的,这也是数字教育资源流通模式的一种重要创新。下一阶段将继续深化对数字教育资源注册链、流通信息链和相关智能合约的深入研究,完善细化其在整个数字教育资源注册、监管、维权以及流通等过程中的作用,在数字资源注册、流通、监管、申诉、结算等环节中,真正实现可控的去中心化管理目标。

[参考文献]

- [1] 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.
- [2] 廖松强.数字文明走来-2018 区块链应用元年将启[EB/OL].(2018-01-29)[2018-02-01].http://economy.jschina.com.cn/rddt/201801/t20180129_1381008.shtml.
- [3] COLUMBUS L. Gartner hype cycle for emerging technologies: 2016 adds blockchain & machine learning for first time[EB/OL].(2016-08-21)[2018-01-15]. <https://www.forbes.com/sites/louiscolombus/2016/08/21/gartner-hype-cycle-for-emerging-technologies-2016-adds-blockchain-machine-learning-for-first-time/#6394bd121ef2>.
- [4] 网易新闻. 中国首个校园区块链项目落地 [EB/OL].(2016-09-23)[2018-01-18]. <http://news.163.com/16/0923/01/C1K2R01L00014AED.html>.
- [5] 李青,张鑫.区块链:以技术推动教育的开放和公信[J].远程教育杂志,2017,35(1):36-44.
- [6] Sony Global. Sony Global Education develops technology using blockchain for open sharing of academic proficiency and progress records[EB/OL].(2016-02-22)[2018-02-10].<https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html>.
- [7] 沈忠华. 新技术视域下的教育大数据与教育评估新探——兼论区块链技术对在线教育评估的影响 [J]. 远程教育杂志,2017,35(3):31-39.
- [8] 张作为.数字教育资源电子商务市场模型与平台发展研究[J].职教通讯,2014(11):1-4,18.
- [9] 杨保华,陈昌.区块链原理、设计与应用[M].北京:机械工业出版社,2017.
- [10] 申屠青春.区块链开发指南[M].北京:机械工业出版社,2017.

Application of Block Chain Technology in Circulation of Digital Educational Resources

QUAN Lixin, XIONG Qian, XU Jianbo

(Department of Information Management, Hunan University of Finance and Economics, Changsha Hunan 410205)

[Abstract] The flow and sharing of digital educational resources is an important foundation for education opening. However, limited by its characteristics and imperfect circulation mechanism, the flow and sharing of digital educational resources are slow. Based on the research of block chain technology, this

paper designs an open and decentralized resource circulation model, that is, a double block chain combined with smart contract. In this model, the circulation object is supervised by digital resource registration chain, business control is automatically completed by smart contract and the transaction accounts are managed by trade information chain. In this way, an open, self-growing and self-managed circulation system can be built. The system can not only promote the circulation of digital resources between the supplier and the buyer, but also protect the legitimate rights and interests of the resource providers, and realize the management and monitoring of transaction resources as well.

[Keywords] Block Chain; Digital Educational Resource; Resource Circulation; Resource Registration; Smart Contract

(上接第 63 页)

- [2] 许良. 技术哲学[M]. 上海: 复旦大学出版社, 2005: 53-54.
- [3] 夸美纽斯. 大教学论[M]. 傅任敢, 译. 北京: 教育科学出版社, 1999: 57, 63.
- [4] 中共中央马克思恩格斯列宁斯大林著作编译局. 马克思资本论(第一卷)[M]. 北京: 人民出版社, 1975: 408-483.
- [5] 刘文海. 技术异化批判: 技术负面效应的人本考察[J]. 中国社会科学, 1994(2): 101-114.
- [6] 颜士刚. 论教育领域技术异化的特异性及其弱化的现实困境[J]. 中国电化教育, 2009(11): 7-10.
- [7] 沈书生. 从教学结构到学习结构: 智慧学习设计方法取向[J]. 电化教育研究, 2017(8): 99-104.
- [8] 沈书生. 形态视角下的信息化教学设计探析[J]. 电化教育研究, 2015(12): 65-69.
- [9] 林琳, 沈书生. 设计思维的概念内涵与培养策略[J]. 现代远程教育研究, 2016(6): 18-25.

Transition of Learning Space and Transformation of Learning Paradigm

SHEN Shusheng

(College of Educational Sciences, Nanjing Normal University, Nanjing Jiangsu 210097)

[Abstract] In the development of educational informatization, the innovation of technology promotes the important changes of learning space in form and other aspects. The learning space characterized by "instruction" is convenient for students to form the knowledge of the known world. The learning space characterized by "inquiry" can help students to use the knowledge of the known world to solve the problem in unknown world, but these two kinds of space are more convenient for teachers to provide common education for learners. After the emergence of learning space characterized by "adaptation", learning will be able to embody personalization and meet different needs of structured talents in the future. However, learning space itself does not lead to changes in learning and may even lead to alienation. Only from the perspective of the learning paradigm and recognizing the roles and responsibilities of middle school students, teachers and various learning support and service systems in the new paradigm, the adaptive learning will become the new normal in education.

[Keywords] Learning Space; Learning Paradigm; Adaptive Learning; Learning Hierarchy; Learning Role Responsibility