CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 40 卷第 Suppl(1)期 2018 年 11 月
Vol. 40, No. Suppl(1), Nov. 2018

文章编号:1007-130X(2018)Suppl(1)-0103-06

工程教育学习产出区块链设计*

段 斌,李 涛,旷 怡,肖祥香
(湘潭大学信息工程学院,湖南 湘潭 411105)

摘 要:提出了一种基于学习产出的区块链技术,以专业认证高校毕业要求标准为基础,建立达成度评价智能合约,将基于成绩、过程和数据,通过学习产出智能合约定量定性相结合的课程学习产出达成值,并将数据记录在梅克尔树中。只有通过该课程达成度评价完成智能合约的学生所获得的能力能达成社会共识,从而完成了学生课程达成度评价到工作后的能力评价结果转化的显性化记录,并能将学生能力评价的反作用给课程,实现对课程的持续性改进。

关键词:工程教育学习产出;区块链;智能合约;梅克尔树
中图分类号:G642.4 **文献标志码**:A
doi:10.3969/j.issn.1007-130X.2018.Suppl(1).019

Block chain design for engineering education learning outcomes

DUAN Bin, LI Tao, KUANG Yi, XIAO Xiang-xiang
(School of Information Engineering, Xiangtan University, Xiangtan 411105, China)

Abstract: We propose a block chain technique based on learning output. Firstly, based on the graduation requirements of professional certification colleges and universities, we establish a smart contract for achievement evaluation. Based on the grades, processes and data, through learning outcomes and smart contracts, we conduct a quantitative and qualitative analysis on the learning output, which is then recorded in the Merkel tree. Only the students who can complete the smart contract through the completion of the course can achieve social consensus, and thus obtain the explicit record of the transformation from the assessment for curriculum completion to the competence evaluation after work. Moreover, the students' capability evaluation can serve as a feedback for the curriculum, thus realizing a continuous improvement.

Key words: engineering education learning outcome; block chain; smart contract; Meckel tree

1 引言

区块链技术已在全球金融业、商业、服务业等领域得到了比较广泛的研究和应用,但在教育教学领域鲜有成熟的案例和研究文献。众所周知,教育机构长期以来垄断着学习认证的职能,而学习者、教师以及学习同伴对学习过程和结果几乎毫无自主权。

然而,传统的以学校为中心的课堂学习随着技术的发展日趋式微,相应地,终生学习、在线学习、移动学习以及基于项目或现实问题导向的分布式学习日益普遍[1]。近年来,随着数字化、网络化、全球化的学习环境不断发展,传统的教育模式往往力不从心。

产出导向是我国高等教育质量标准(国标)和工程教育专业认证标准的核心理念,学习产出代表工业界对工程教育的基本要求。与高等学校学历文凭有教育部作为信任中介不同的是,课程学习产出因涉及面广、内容繁杂而无法监管,传统教育信

* 收稿日期:2018-07-15;修回日期:2018-09-21
通信作者:李涛(1581355882@qq.com)
通信地址:411105 湖南省湘潭市湘潭大学信息工程学院
Address: School of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, P. R. China

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

任中介无能为力。如何在信任中介缺失的环境下,保证学生学习产出达成度评价结果得到教育利益相关方的认可,是实施国标必须解决的科学问题。而传统教育模式往往很难全方面地记录、分析、评价学生学习、状态以及能力的达成度。并且社会也很难信服老师对学生的评价,以及学生的考试成绩等。而区块链的分布式共识机制很好地解决了这个问题。区块链有去中心化与不可篡改等特性,是一种可信任的机制,随着区块链的发展将越来越被社会认可。

本文根据《华盛顿协议》[2],统一通过专业认证高校的毕业要求指标点,并确定各课程的相应支撑点,将其作为教育区块链的共识机制 POA(Prove Of Accreditation),实现将学生的成绩、学习过程作为证据,定量和定性评价相结合对学生能力进行评价[3],同时对区块链的基本构成进行了描述,以及对智能合约、梅克尔树、哈希指针等技术进行了说明,设计了学习产出评价机制与学习产出区块链,通过第三方机构,形成学生能力微文凭。

2 工程教育学习产出

2.1 毕业要求能力指标

工程教育学习产出 OBE(Outcomes Based Education)智能合约是《华盛顿协议》所提出的十二条毕业要求(即:工程知识、问题分析、设计/开发解决方案、研究、使用现代化工具、工程与社会、环境可持续发展、职业规范、个人与团队、沟通、项目管理、终生学习)来编写的。每条毕业要求将由若干指标点支撑。以电气工程及其自动化专业毕业要求,工程知识能力指标 1-4 以及“电机学”课程为例,毕业能力指标如图 1 所示。

每门课程对应若干个能力指标点,根据该指标点的重要程度划分权重。同时,对每个指标点设定一系列考核方式,每种方式按照一定成绩比例分配。以“电机学”课程为例,该课程由 3 个毕业要求指标点支撑,具体如表 1 所示。

Table 1 Support weight of the completion evaluation of the support index points of “Electrical Engineering” course

表 1 “电机学”课程支撑指标点达成度评价的支撑权重值

毕业要求指标点	课程达成度权重	考核方式	成绩比例/%
1-4 能够综合运用所学知识解决电气工程、电力系统、电气设备自动化及相关领域复杂工程问题。	0.45	卷面考试	40
		测试讨论	5
2-3 能够通过工程原理、工程方法和文献研究综合对电气工程、电力系统、电气设备自动化及相关领域复杂工程问题进行分析,并获得有效结论。	0.45	卷面考试	30
		课后思考题	10
		测验讨论	5
4-1 能够运用科学原理及专业知识,针对电气工程、电力系统、电气设备自动化及相关领域复杂工程问题进行研究。	0.1	实验操作及实验报告	10

2.2 课程达成度评价

每次考核对学生达成度进行评价,评价方法有:(1)成绩定量分析法;(2)定性评价法;(3)问卷调查法。每种方法都有相应的实施者,并且按照重要程度划分权重。以“电机学”课程为例,具体评价方法如表 2 所示。

具体计算方法:

(1)成绩定量分析法:

$$\alpha = \sum_i \delta \times \frac{\vartheta_\alpha}{\mu_\alpha} \tag{1}$$

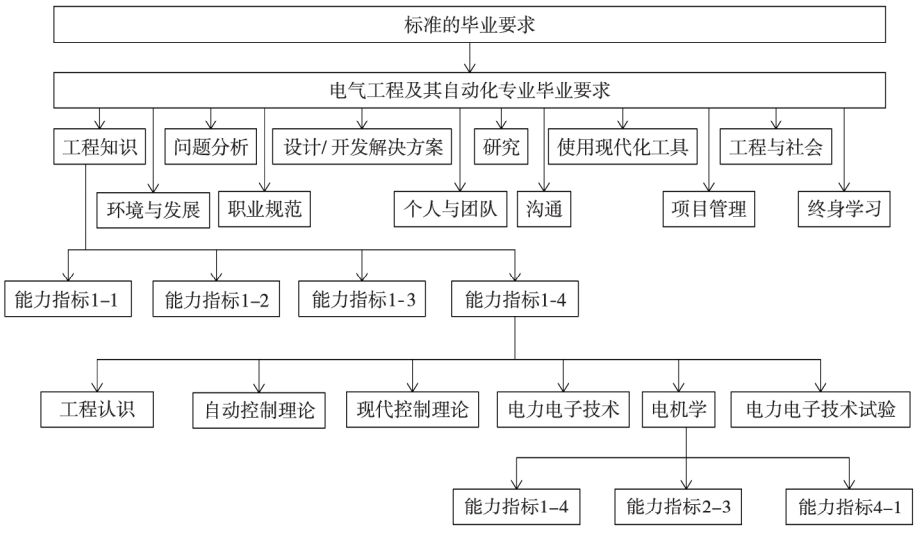

Figure 1 Graduation ability requirement index

图 1 毕业能力要求指标

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Table 2　Achievement assessment methods

表 2　达成度评价方法

评价方法	评价内容	实施者	权重
成绩定量分析法	卷面考试、实验操作及实验报告	任课教师、实验室教师	0.7
定性评价法	课后作业、上课表现、进步空间	任课教师	0.2
问卷调查法	用人单位问卷调查、往届/应届毕业生问卷调查	学生工作办公室	0.1

其中,α 为考核成绩达成值,i 为各指标点,δ 为权重值,θ_a 为学生在相应环节得分平均值,μ_a 为指标点涉及环节的总分。达成值超过阈值 0.65 即认为课程在该方法下为达成。

(2)定性评价法:

$$\beta = \sum_i \delta \times \frac{\vartheta_\beta}{\mu_\beta} \tag{2}$$

其中,表示课程定性评价值,ϑ_β 为学生在指标点定性评价得分的平均值,μ_β 为指标点涉及环节的总分。达成值超过阈值 0.65 即认为课程在该方法下达成。

(3)问卷调查法:

$$\gamma = \sum_i \delta \times \frac{\vartheta_\gamma}{\mu_\gamma} \tag{3}$$

其中,γ 为课程问卷达成值,ϑ_β 为对应指标点基本达成以上样本数,μ_γ 为调查卷宗总样本数。达成值超过阈值 0.65 即认为课程在该方法下达成。

按照相应的权重将这三种评分机制的分值汇总,可以得到毕业要求达成值,计算方法如下:

$$\varphi = \frac{\sum_i \frac{\omega}{\zeta}}{\theta} \tag{4}$$

其中,φ 为毕业要求达成值,ω 为学生在指标点得分平均值,ζ 为指标点所涉及环节的总分,θ 为指标点个数。若达成值超过阈值 0.65,则认为该学生对毕业要求达成度的评价为达成。

2.3　能力评估

当学生成绩通过达成度评估方法的阈值,智能合约能够自动对所提取到的学生成绩进行计算,对学生能力进行评估,从而生成能力微证书。具体如图 2 所示。

3　区块构建

3.1　数据获取

在一门课程结束后,教师将学生的试卷分数、课堂表现、实验成绩、平时作业、问卷评价等各方面成绩记录在分布式账本中。区块链的智能合约通过学校内部分布式账本获取学生成绩原始数据,经过合约代码的计算,最终输出达成度评价。

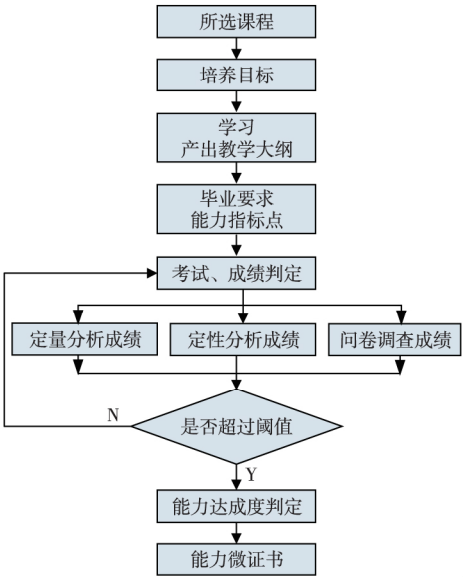

Figure 2　Project education capability assessment

图 2　工程教育能力评估

3.2　智能合约(Intelligent contract)

智能合约相当于学生和老师签订的一种契约,学生选定一门课程即签订智能合约,合约自动执行,且具有强制性。智能合约包含自然语言文档和程序代码,自然语言文档表征教学大纲,程序代码从学校内部分布式账本读取输入,并将输出写入联盟分布式分类账。一个没有自然语言作为支撑的智能合约是不合理的,因为这会让智能合约的所有者处于这样一种局面:他们似乎想要达成他们事先并不知情的事,特别是代码中非常有可能存在错误[4]。将表征教学大纲的自然语言文档和控制程序写入分布式账本的好处是,各方都可以看到这些程序,并随时监视学习成果产出流程的进展。需要验证的是,计算机程序是否正确编码了书面自然语言文档。该问题的验证需要对智能合约代码和自然语言文档的形式化表达,然后运用指称语义赋予每个语言语法元素与抽象数学实体或其语义的关系,最后,运用认知计算方法,通过对带有语义的数学实体进行推理来推断程序的属性。

3.3　分布式账本技术

分布式账本技术 DLT(Distributed ledger)消除了信任需求的原因主要得益于三个方面的属性:第一,分布式账本技术只允许在参与者们事先同意的情况下将内容写入账本,对分布式账本上的变量参与者呈“共享状态”,任何在分布式账本上添加内

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

容的人都知道其他参与者已经看到了内容,在博弈论的语境中,参与者(包括教师、学生、用人单位)具有共同的知识,这使得任何参与者都不可能在随后的某个时间里否定账本的内容;其次,分布式账本最新内容以加密的方式链接到过去的内容上,形成区块链中的"链条",这种内容的串联意味着对过去内容的任何改变都要求改变所有后来的内容,因此,过去的记录不可改变或删除;第三,共享账本不是只存储在一台机器上,而是将副本存储在每个参与者的机器上,这些副本的内容保持同步。这对任何希望破坏或改变内容的人都造成了重大挑战,因为需要攻击每台参与的机器。

3.4 区块记录与储存

通过智能合约处理过的数据进入到分布式账本联盟。由通过专业认证的分布式账本联盟成员通过共识机制 POA 对其数据进行验证,通过专业认证的学校或专业构成区块链的各个节点,节点间形成统一的验证标准,对学生的能力数据达成共识。由于拜占庭等错误节点的存在,当超过三分之二的节点反馈正确时,认为该数据正确。正确的数据将被打包存入区块链。同时,智能合约为一系列储存在区块链上的代码,合约状态存储在区块链中,通过合约节点执行合约代码,当学生完成所选定课程时,节点能够通过分布式一致性算法的合约计算结果,并将结果储存在区块链中,并更新合约的状态[5]。智能合约促使区块链的状态从一开始就不断进行改变,区块链的状态改变如式(5)所示:

$$\sigma = \gamma(\sigma_t, T) \tag{5}$$

其中,γ 为区块链状态转移函数,表示区块链在不同时刻 T 的状态变化量 ;σ_t 为区块链在 t 时刻的状态,T 为学生能力评估值。

由于区块链的可溯源性,每个区块都可由哈希值所指代,所以从整体上来说状态改变如式(6)所示:

$$\sigma_{t+1} = \gamma(\cdots\gamma(\gamma(\sigma_t, T_0), T_1), \cdots) \tag{6}$$

每个区块记录同一门课程的达成度评价,通常记录的信息有:课程名称、学生学号、达成值、学习产出能力指标点、课程权重。为了追溯查询,这些数据都将被储存在梅克尔树(Merkle trees)中,不仅可以生成最新的状态数据,还可以快速查找所需信息。最后用哈希函数、数字签名、时间戳等技术计入区块链。

3.5 哈希指针

区块链中区块与区块之间是通过哈希指针所链接的,即每个区块头部都存在之前的哈希指针,指向最近的数据区块。哈希指针具有碰撞阻力、隐秘性、谜题友好的特性,因此具有很好的安全性能。比如当攻击者试图改变区块链的其中一个数据,这将会导致下一个哈希指针不正确,数据无法修改成功。即使改变所有的哈希指针,也不能改变创世区块。因此只要掌握了创世区块,就能够掌握区块链的所有哈希指针,并判断区块链中数据是否被修改。

4 案例分析

本文以湘潭大学 2017 年自动化专业为例,就该专业必修的一门"电机学"课程展开分析,由于学习产出智能合约的普遍性,本文方法对其他课程也同样适用。

选取 5 名同学,分别对其在"电机学"课程中的考试成绩、作业成绩、实验成绩、课堂表现、问卷调查的数据进行统计,并且按照数据各自的权重计算出总成绩,具体如表 3 所示(以学生 1 为例:总成绩=83×0.5+94×0.2+95×0.1+87×0.1+8=86.5)。

上述数据从学校内部数据库(或学校内部分布

Table 3 "Motor Learning" course evaluation scores

表 3 "电机学"课程评估成绩

项目	考试成绩	实验成绩	课堂表现	作业成绩	问卷调查	总成绩
指标点	1-4 2-3	4-1	1-4 2-3	1-4 2-3	1-4 2-3 4-1	1-4 2-3 4-1
权重	0.5	0.2	0.1	0.1	0.1	1
1	83	94	95	87	8	86.5
2	72	56	85	83	7	71
3	90	86	83	92	8	88
4	74	81	83	95	8	78
5	58	72	87	78	8	67.9

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

式账本)提取,输入智能合约进行处理并判断各学生指标点达成情况,具体如表 4 所示。

Table 4　Achievement of indicator points

表 4　指标点达成情况

学号	1-4	2-3	4-1	是否达成？
1	1	1	1	1
2	1	1	0	0
3	1	1	1	1
4	1	1	1	1
5	0	1	1	0

由表 4 可知只有学生 1、3、4 通过智能合约的达成判断,能够进行能力达成度的计算,并将计算结果进行储存。

综上,可以构建学习产出构建区块链如图 3 所示。首先智能合约通过区块链脚本从学校内部分布式账本中获取学生考核的原始数据。接着智能合约将对获取的数据进行处理,先判断能力指标点的达成情况,然后将达成能力指标点的学生进行能力达成度情况计算。将计算好的能力达成值输入分布式账本联盟,通过分布式共识的数据将计算好的达成值打包进入区块链储存在梅克尔树中。最后当培养计划所有项目进行完之后,第三方机构(如图 4 所示)从梅克尔树中获取数据,统计并制作出学生的能力微文凭(表 5 所示)。同时用人单位可以通过对应哈希值在区块链中查找学生在大学四年的能力达成数据。由于区块链的不可篡改性,这种数据是真实可信的。

图 4 为湘潭大学与中国科学院研发的学习产出区块链平台。

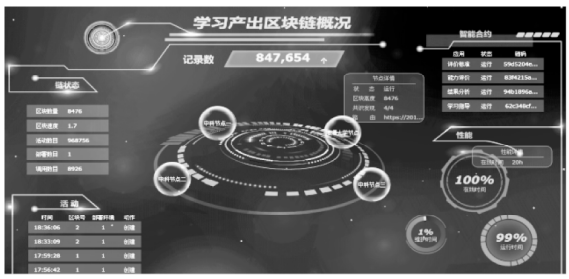

Figure 4　Learning outcome block chain platform

图 4　学习产出区块链平台

表 5 为通过工程教育认证毕业要求的学生的微文凭。相比普通的毕业文凭,记录在区块链中的能力微文凭包含了学生大学四年达成的毕业要求指标点,使得整个学习过程都能得到认证,并最终体现毕业生的差距,而不是仅有一张毕业证书。

5　结束语

学习产出区块链,承载的是工程教育利益相关者群体赋予的价值观,代表的是其背后群体对 OBE 教育理念和工业界学习产出需求的信仰和共识。本文提出了一种基于工程教育学习产出的区块链设计。以“电机学”课程为例,设计了具体工程教育能力评估机制。对区块链的底层技术进行了分析,构建了工程教育学习产出区块链,并通过第三方机构产生能力微文凭。

本文是对基于区块链技术在教育领域的一种有益研究探索,有抛砖引玉的效果。尽管国内外区

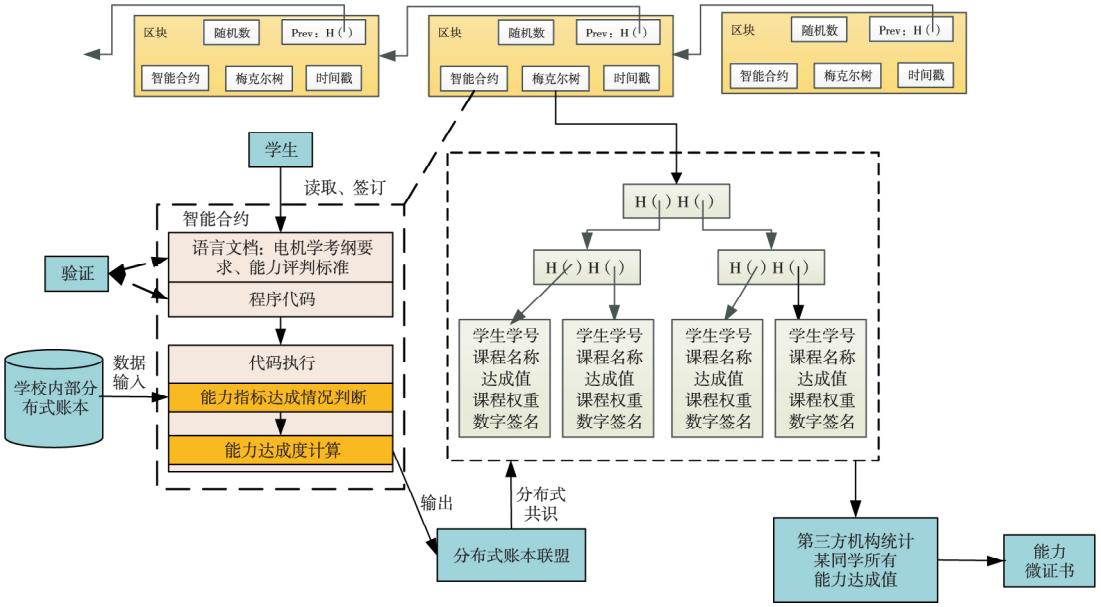

Figure 3　Learning the principle of the outcome block chain

图 3　学习产出区块链原理

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

块链还有许多需要面对的问题,但相信分布式账本技术和智能合约作为未来数字社会的关键技术之一,将具有广泛的前景。

Table 5 Microdiploma of competence

表 5 能力微文凭

毕业要求/索引点/结果(目标值:结果值)		
工程知识	1-1	达成(0.65:0.75)
	1-2	达成(0.65:0.79)
	1-3	达成(0.65:0.90)
	1-4	达成(0.65:0.69)
问题分析	2-1	达成(0.65:0.76)
	2-2	达成(0.65:0.91)
	2-3	达成(0.65:0.92)
	2-4	达成(0.65:0.83)
…	…	…
项目管理	11-1	达成(0.65:0.91)
	11-2	达成(0.65:0.87)
	11-3	达成(0.65:0.87)
终身学习	12-1	达成(0.65:0.81)
	12-2	达成(0.65:0.82)

参考文献:

[1] Gartner hype cycle for emerging technologies, 2016 Adds blockchain &machine learning for first time[EB/OL]. [2016-08-21]. http://www.forbes.com/sites/louiscolumbus/2016/08/21/gartner-hype-cycle-for-emerging-technologies-2016-adds-blockchain-machine-learning-for-first-time/#6394bd121ef2.

[2] Lin Jian. Methods of understanding and solving complex engineering problems[J]. Researches in Higher Education of Engineering, 2016(5):17-26. (in Chinese)

[3] Sikorski J J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market [J]. Applied Energy, 2017, 195: 234-246.

[4] Magazzeni D, Mcburney P, Nash W. Validation and verification of smart contracts: A research agenda[J]. Computer, 2017, 50(9): 50-57.

[5] Huang Jie-hua, Gao Ling-chao, Xu Yu-zhuang, et al. The design of smart contracts on crowd funding private blockchain [J]. Journal of Information Security Research, 2017, 3(3): 211-219. (in Chinese)

附中文参考文献:

[2] 林健. 如何理解和解决复杂工程问题 — 基于《华盛顿协议》的界定和要求[J]. 高等工程教育研究, 2016(5): 17-26.

[5] 黄洁华, 高灵超, 许玉壮, 等. 众筹区块链上的智能合约设计[J]. 信息安全研究. 2017, 3(3): 211-219.

作者简介:

段斌(1966—),男,湖南湘潭人,博士,教授,研究方向为软件集成与信息安全和区块链。E-mail:782826921@qq.com

DUAN Bin, born in 1966, PhD, professor, his research interests include software integration and information security, and block chain.

李涛(1994—),男,湖南湘乡人,硕士生,研究方向为区块链。E-mail:1581355882@qq.com

LI Tao, born in 1994, MS candidate, his research interest includes block chain.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net