Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 10, October 2018, pp. 2403-2413
DOI: 10.23940/ijpe.18.10.p16.24032413

Design of Outcome-based Education Blockchain

Tao Li[a,*], Bin Duan[a], Dayu Liu[b], and Zhen Fu[b]

[a]*College of Information Engineering, Xiangtan University, Xiangtan, Hunan, 411105, China*
[b]*Zhongke JiuDu (Beijing) Spatial Information Technology Co., Ltd., Beijing, 100190, China*

Abstract

In today's society, the problems of false academic qualifications and tampering of students' scores are increasingly prominent, and the social recognition of data such as students' scores is declining day by day. At the same time, the single performance of a student cannot directly reflect the level of students' ability. In this paper, the bottom technology of blockchain is studied, and the blockchain technology is applied to the outcome-based education (OBE) of engineering education. Based on the graduation requirements, students' scores can be converted into specific competency values and recorded in the blockchain. Through the decentralization of blockchain, tamper-proof, and other characteristics, a social consensus is formed. At the same time, this paper designs an association code, which is more convenient to learn how to find the records in the output blockchain than the traditional way of tracking the account balance when querying the bitcoin records.

Keywords: OBE; blockchain; association coding; DAPP; learning contract

(Submitted on July 20, 2018; Revised on August 16, 2018; Accepted on September 18, 2018)

1. Introduction

Blockchain [1-3] technology has been widely studied and applied in the fields of global finance, commercial service, and so on, but there are few mature cases and research documents in the field of education and teaching. It is well known that education has long monopolized the function of learning certification, while learners, teachers, and peers have little autonomy in learning process and results. However, with the development of technology, the traditional school-based classroom learning has a slight trend. Accordingly, lifelong learning, online learning, mobile learning, and project-based or problem-oriented distributed learning are increasingly common [4]. In recent years, with the development of digital, networked, and global learning environments, the traditional education model [5] is often inadequate.

Output orientation is the core concept of higher education quality standard (GB) and engineering education professional certification standard in China. OBE represents the basic requirements of engineering education in industry. Different from the higher education diploma, the Ministry of Education acts as a trusted intermediary. Because of the wide range of curriculum learning output, the content cannot be supervised, and the traditional education trust intermediary cannot be supervised either. How to ensure that the evaluation result of students' achievement of OBE is recognized by educational stakeholders in the absence of trust intermediary is a scientific problem that must be solved in the implementation of national standard. It is difficult for the traditional education model to record, analyze, and evaluate students' learning, states, and abilities. Moreover, society is unable to effectively appraise the teachers and students, as well as students' examination results. The distributed consensus mechanism of blockchain solves this problem well. Because of decentralization and non-tampering, blockchain is a reliable mechanism, and the development of blockchain is becoming more and more recognized by society.

According to the Washington Agreement, this paper unifies the graduation requirements of colleges and universities through professional certification. The corresponding supporting points of each course are determined. As the consensus mechanism of education blockchain (POA), the achievement of students, learning process and evidence, and quantitative

* Corresponding author.
E- mail address: 1581355882@qq.com

and qualitative evaluation are combined [6]. At the same time, the basic structure of blockchain is described. The main contributions of this paper are as follows: 1. A method of evaluating students' ability is designed. 2. The basic framework of OBE blockchain is established. 3. The correlation coding is designed, and its feasibility is analyzed. 4. The platform of OBE blockchain is constructed preliminarily.

2. Outcome-based Education

2.1. Graduation Requirement Competency Indicator

Outcome-based education is realized by the 12 requirements for graduation under the Washington Agreement (i.e., engineering knowledge, problem analysis and solution design/development, research, use of modern tools, engineering and social and environmental sustainable development, professional norms, individual and group, communication, project management, and lifelong learning.). Each graduation requirement will be supported by a number of indicators. Taking the graduation requirements of electrical engineering and its automation major, engineering knowledge and ability index 1-4 and the course of "Power Electronics Technology" as examples, the graduation ability index is shown in Figure 1.

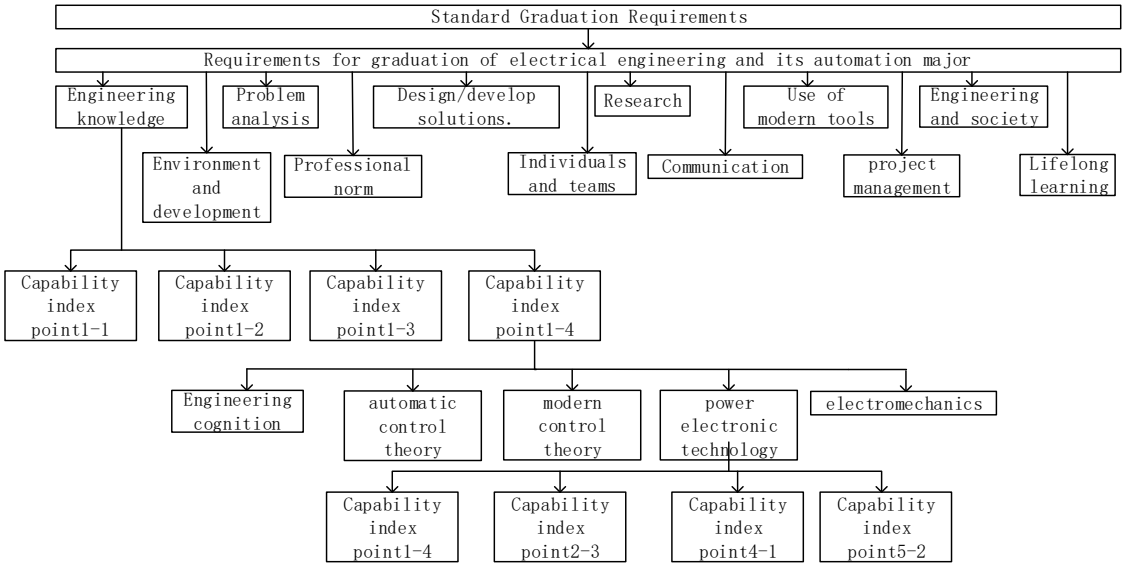

Figure 1. Graduation requirements competency indicators

Each course corresponds to a number of competency index points, and they are divided into certain weights according to the importance of the index points. At the same time, set a series of assessment methods for each index point, with each way distributing achievement according to a certain proportion. The "Power Electronics Technology" course, for example, is supported by four graduation requirements, as shown in Table 1.

2.2. Assessment of Curriculum Achievement

The evaluation methods include: (1) the quantitative analysis method, (2) the qualitative evaluation method, and (3) the questionnaire method. Each method has a corresponding implementer, and a certain weight is divided according to the general degree. Taking the course of "Electric Power Electronics" as an example, the specific evaluation method is shown in Table 2.

If the achievement value exceeds the threshold of 0.65, the student's evaluation of the degree of achievement of graduation requirements is considered an achievement. The learning contract can calculate the students' scores and evaluate the students' ability automatically, so as to generate the micro-certificate of ability.

3. Case Analysis

3.1. The Judgement of Capability Indicator Points

Taking the "Power Electronics Technology" course of Xiangtan University as an example, and taking the PMLK (Power

Management Experiment Kit) of TI Company as the experimental platform, this paper analyzes the students' degree of ability achievement. Due to the universality of the capability achievement evaluation method, this method is applied to other assessment forms as well as other courses. Here, we take the example of Experiment 1 in the Buck Suite: the influence of operating conditions on efficiency.

Table 1. Support weight value of the degree of achievement evaluation of support index points for "Power Electronics Technology" course

Graduation requirement index point	Curriculum achievement weight	Examination mode	Achievement distribution
1-4Ability to solve complex engineering problems in electrical engineering, power system, electrical equipment automation and related fields.	0.37	Paper examination	20%
		Test discussion	17%
2-3 Can analyze the complex engineering problems of electrical engineering, electric power system, electrical equipment automation and related fields through engineering principles, engineering methods and literature studies, and obtain effective conclusions.	0.37	Paper examination	20%
		Think about questions after class	10%
		Test discussion	7%
4-1 Can use scientific principles and professional knowledge to study complex engineering problems in electrical engineering, power system, electrical equipment automation and related fields.	0.2	Experimental operation and experimental report	14%
		Test discussion	6%
5-2 Can develop, select and use appropriate technologies, resources, modern engineering tools and information technology tools.	0.06	Experimental operation and experimental report	6%

Table 2. Method of degree of achievement assessment

Evaluation methodology	Evaluation content	executant	weight
Quantitative analysis of achievement	Paper test, experiment operation, and experiment report	Classroom teacher, Laboratory teachers	0.7
Qualitative evaluation method	After class homework, class performance, room for improvement	Classroom teacher	0.2
Questionnaire survey method	A questionnaire survey of employing unit and a questionnaire survey of previous/fresh graduates	Student work office	0.1

3.1.1. Decomposition of Experiments

The index points of the experiment and graduation requirements are shown in Table 3.

Table 3. Comparison between experiment I and graduation requirements

	Related knowledge points	Develop skills	Graduation requirement competency indicator
Experiment 1: effect of operating conditions on efficiency	1. Davinan theorem 2. The basic characteristic of energy storage element 3. Feedback control principle	1. The circuit can be simplified and analyzed 2. Able to use mathematical and professional knowledge to analyze and process experimental data. Can use modern tool WEBENCH to simulate and analyze the circuit	1. Engineering knowledge 1-4 2. 2. Problem analysis 2-3 3. Study on 4-14 4. Using modern tools 5-2

The proportion of ability achievement in "power electronics technology" experiment is 20%, and the proportion of each experiment is 2. In Table 3, the weight of capability index point 1-4 and 5-2 is 0.2, 0.3, 0.2, and 0.3. The evaluation of the experiment was based on a step-by-step scoring method, with a full score of 100 points.

3.1.2. Capacity Assessment

Student 1 gives the following answer to the phenomenon of "experiment one" oscillation (the corresponding capability indicator is indicated below)：

Using WEBENCH to simulate the buck circuit, the node waveform is shown in Figure 2, and the experimental waveform is shown in Figure 3. By comparing the yellow waveform in Figure 3, it is found that the yellow waveform in Figure 3 has high-frequency oscillation when the blue waveform appears jump edge. However, the red waveform in Figure 2 does not oscillate.（5-2）

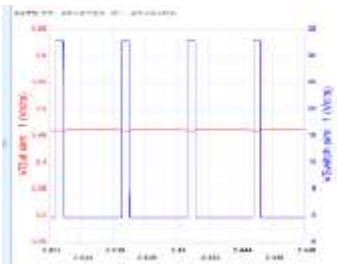

Figure 2. Node Waveform

Figure 3. Experimental waveform

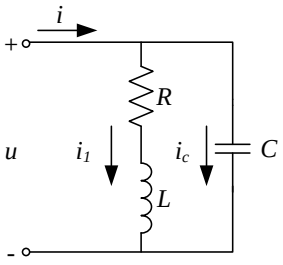

Figure 4. L-C equivalent circuit diagram

Oscillations are caused by the parasitic L-C parameters of the PCB wiring (which form a resonant loop excited by the sharp rise and fall of the switching node voltage (blue waveform).（2-3）

How to improve the simulation effect? The answer given by Student 1 is as follows: the parasitic L-C equivalent circuit of the PCB board with oscillating model is shown in Figure 4:

Circuit equivalent reactance:

$$Z=\frac{\frac{1}{\mathrm{j}\omega c}(R+\mathrm{j}\omega L)}{\frac{1}{\mathrm{j}\omega c}+R+\mathrm{j}\omega L}$$

In general, the inductance in the circuit is far greater than the circuit loss, that is $\omega L >> R$, then：

$$Z=\frac{\frac{1}{\mathrm{j}\omega c}(R+j\omega L)}{\frac{1}{\mathrm{j}\omega c}+R+j\omega L}\approx\frac{\frac{1}{\mathrm{j}\omega c}\cdot j\omega L}{R+\mathrm{j}(\omega L-\frac{1}{\omega c})}=\frac{\frac{L}{C}}{R+\mathrm{j}(\omega L-\frac{1}{\omega c})}$$

When the imaginary part coefficient is 0, Z is a real number, and the current and voltage in the circuit are in the same phase. The resonant frequency of the circuit is:

$$f_0=\frac{1}{2\pi\sqrt{LC}}$$

By adding the above mathematical models to the system model of the whole circuit, the results of WEBENCH simulation can be close to the experimental results. (1-4,4-1)

Through the above example, the teacher can judge the achievement of the student's ability index point through the students' steps (after the steps have marked out the ability index point, carry on the division score). The concrete analysis of the scoring method is as shown in Table 4.

Table 4. Specific scoring for Student 1

index point	Evaluation of the completion of the corresponding indicator points of Student 1	The value of this item	Student score
1-4	Student 1 has initially mastered the basic principles and knowledge of electronic technology. By establishing an equivalent circuit diagram, we can solve complex engineering problems by using the knowledge of Davinan theorem, equivalent reactance, resonance generation condition, and so on.	20	20
2-3	Student 1 can use the principle and knowledge of power electronics to analyze the high-frequency oscillation of WEBENCH simulation waveform and draw an effective conclusion.	30	30
4-1	Student 1 can use power electronics technology to study the high-frequency oscillation of WEBENCH simulation waveform.	20	20
5-2	Student 1 completed the experiment, used the tool correctly, and improved it to achieve the purpose of using modern tools.	30	30

Take Table 3, "graduation requirement competency indicator point 5-2 using modern tools" as an example (this experimental indicator point 5-2 accounts for 2% of the ability-achievement index point 5-2): Student 1 completed the

experiment, correctly used the tool, and improved it. The purpose of using modern tools has been fully achieved. The score is 30 points to achieve a competency value of 1 (the ability-achievement value to be calculated is based on the weight of 5-2 of the course and the proportion of the experiment to the course). When the micro-certificate of competency is finally formed, the ability of Student 1 to reach 5-2 through this item is calculated to be 0.02.

Through the above description, we can see that the core problem of OBE lies in the division of capability index points and the establishment of an evaluation mechanism for specific complex engineering problems. Whether the output capacity value is socially accepted and trusted is the question we will discuss next. Because of its decentralization, traceability, tamper-proof, and so on, blockchain technology has developed into a platform for social credibility [7]. Each school (or major) that is professionally certified in the OBE blockchain will form a node, and each data upload will be stored in each node. It is almost impossible even if a node wants to tamper with the data. On the one hand, it has to tamper with the data of all nodes. On the other hand, when it changes the hash value in the block, because of the existence of the hash pointer, each subsequent block hash will change, and it is easy to see whether block data is tampered with by creating blocks. For no more than 1/3 Byzantine nodes in the process of data upload, each node will eventually reach a distributed consensus. Therefore, the ability of students to achieve a value is recorded in the blockchain, which can form a social consensus. Next, we will analyze the underlying technology of the blockchain and the implementation of the OBE in the blockchain.

3.2. Capacity Transfer

Because of the traceability of the blockchain, in order to facilitate management, a competency index point can set up a capability achievement record for the convenience of management and the inquiry of school ability. The curriculum corresponding to the competency index point is divided into certain weights according to the importance degree, and the respective ability achievement value is summarized according to the weight. Finally, the ability-achievement of a certain student at the index point can be obtained.

The school calculates the total number of students according to the curriculum and the number of students. At the end of the semester, the school gives the ability index points according to the students' grades. Each student has a number of addresses. When the student achieves a certain ability, the school enters this achievement value into the address of the corresponding student. In a single output process, the school output capacity value can only be consumed, there is no consumption only part of the situation. When the school output capacity value is surplus, the competency value can be transferred to the address owned by the school. Of course, due to the large number of students, one input can respond to multiple outputs at the same time. With the signature of the public key and the public key owner (school) whose hash value is X [8], the student can obtain the corresponding ability value. The ability to run Student 1 via script is shown in Figure 5.

```
{
"hash": "5ab578333fbcc2246de0000kfcb6c84f1a3a24e763fcbed",
"ver": 1,
"vin_sz": 1,
"vout_sz": 2,
"in": [
{
   "prev_out": {
   "hash": "8b7999fcd364a5a5b6314af532ed893afga552646aad515c",
   "n": 0
},
   "scriptSig": "663584…"
   }
],
"out": [
{
      "ability": "0.02",
        "scriptPubkey": "OP_DUP  OP_HASH160  201752043be4ac976fcd86bd503a91d  OP_EQUALVERIFY OP_CHECKSIG"
   },
      {
      "ability": "remaining capacity",
        "scriptPubkey": "OP_DUP  OP_HASH160  8b7999fcd364a5a5b6314af532ed893afga552646aad515c  OP_EQUALVERIFY OP_CHECKSIG"
        }
   ]
}
```

Figure 5. Student 1 ability transfer program section.

Where the input is 1 (school) and the output is 2 (Student 1 ability value, the remaining ability value is returned to the school, and there are many output values in practical applications).

3.3. Data Storage and Lookup

The traditional verification of Bitcoin [3, 9-10] transaction information is done by tracking each account balance and continuing to track the trading order. For the ability value transfer, because of the students' ability, the number of ability index points is many and complicated, and the transfer of the school ability value is unidirectional. Since one-to-many and capacity transfer cannot form a complete "transaction chain" compared with traditional bitcoin transactions, the traditional verification method for traceability transactions is obviously inappropriate. For these reasons, a capability correlation matrix can be set up as shown in Table 5 to facilitate the search of capability transfer records. The ability correlation matrix is a kind of relation between ability index points and courses. The course is numbered in sequence and marked with the correlation point in the form of the ability index point + course number.

Table 5. Capability correlation matrix (local)

Subject / Index point	1. Engineering knowledge	2. Automatic control theory	3. Modern control theory	4. Power electronics technology	5. Electrical science	……
1-1						……
1-2						……
1-3						……
1-4	1401	1402	1403	1404	1405	……
……	……	……	……	……	……	……
2-3		2302	2303	2304	2305	……
……	……	……	……	……	……	……
4-1		4102	4103	4104	4105	……
……	……	……	……	……	……	……
5-2				5204	5205	……
……	……	……	……	……	……	……

The correlation code of Student 1 is 201752043be4ac976fcd86bd503a91d. Association code = record year + ability index point + course number + student address hash value. The correlation code is not just a string of simple hash values; it also includes time information, capability index point information, course information, and student information. We can quickly find the required records through the association code and related matrix.

The ability of students reached the value stored in the Merkle tree, because each point of the course ability index was completed in different periods, so each block reached a record of the ability index point of a course. In order to prove the ability to convert the records in the block, one can search inside the tree, and the tree path length is the number of transferability of the logarithm. The Meckel tree is a data structure based on hash value, so it can be constructed by association coding, which not only obtains the information of associated code data but also facilitates the search and searchability transfer record. Ability value transfer records can be found through third-party software (DAPP, detailed in 3.1.5. When a specific code is entered, different data is searched. Take Student 1 as an example; the process is shown in Table 6.

Table 6. Record lookup process

2017	52	04	3be4ac976fcd86bd503a91d
The system queries all the blocks in the blockchain in 2017	Querying capacity indicator points 5-2 blocks from 17 blocks	Search for blocks with a course of 4 from a block with a 17-year competency indicator point 5-2	Find the block of 3be4ac976fcd86bd503a91d from the block of course 4 of 17-year competency indicator point 5-2 (different schools may have blocks that meet the above conditions) and extract the information

For the sake of simple memory, the hash value of the above students can be stored in the form of a two-dimensional code or an account password.

In addition, through the setting of third-party software, Student 1 can input 2017043be4ac976fcd86bd503a91d when he wants to inquire about the ability of "power electronics technology" course. To inquire about the achievement of capability index point 5-2, one can enter 523be4ac976fcd86bd503a91d; to inquire about the achievement of all ability index points, one can input 3be4ac976fcd86bd503a91d.

4. Construction and Feasibility Analysis of OBE Blockchain Platform

4.1. Platform Design and Feasibility

4.1.1. DAPP (Distributed Applications)

Through the establishment of DAPP (distributed application) [11] and the OBE blockchain network, the trusted management of the student evaluation data is realized. The upper application is responsible for the maintenance collection of the basic data and the relevant data preparation for the OBE evaluation activities. The students' OBE performance is evaluated through the preset evaluation process, as shown in Figure 6.

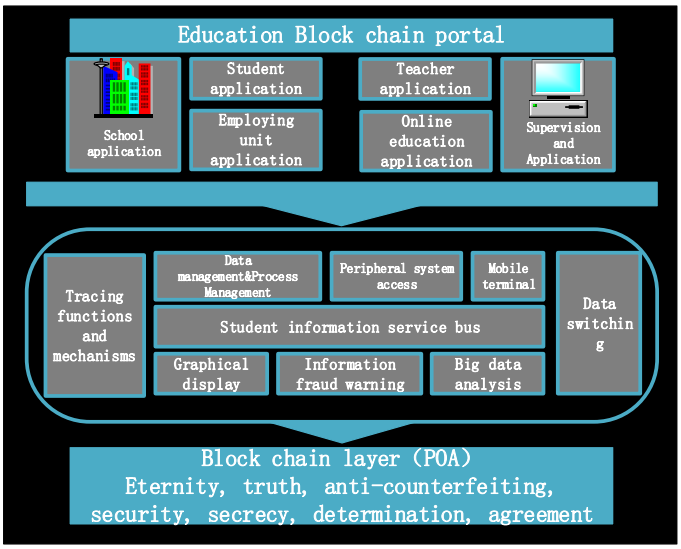

Figure 6. DAPP

4.1.2. OBE Blockchain Network

For establishing the OBE Blockchain network [12], with the school as a participating member, there are many participating nodes in the chain. The first is to consider the high availability of the system; secondly, the participating nodes can correspond to different professions. The OBE blockchain is authorized to join the blockchain network through the network authorization. As trusted nodes, they participate in the blockchain network, by running intelligent contracts, submitting transactions, querying the latest status data, and so on.

In the creation block of the OBE blockchain, there is initial configuration information of network member nodes, such as Xiangtan University node configuration. At the beginning of the OBE blockchain network, configuration information is stored in the creative block. Subsequent nodes participating in the OBE blockchain must pass a consensus mechanism, and after the existing members have reached a consensus, the resulting configuration information calculated by the system intelligence contract and system chain code will accumulate with the configuration information in the creative block. The new blocks are stored in the chain to ensure that all the join nodes are trusted nodes. The trusted node ensures that the node can communicate with other nodes in the OBE blockchain network, and the specific data rights are set according to the permission control module. The details are shown in Figure 7.

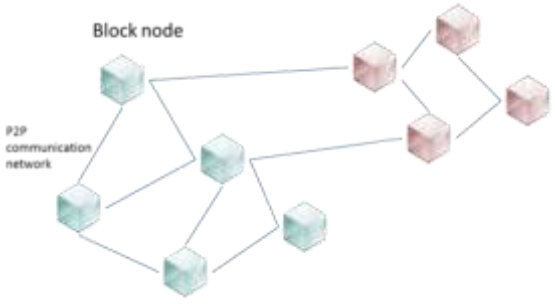

Figure 7. OBE blockchain network

4.1.3. Privacy Protection of Chain Data

Different from the data sharing and transparency of the public chain, the OBE blockchain requires the privacy of the business data [13-15], and can flexibly customize the read and write permissions according to the business requirements. Not all of the data in the account books of network members are open according to the business requirements. At the same time, some nodes in the network members can be controlled to submit transactions and query the data in the chain.

In order to protect the privacy of different members, each member of the OBE blockchain has a certificate issuing service for issuing certificates within the organization, each member has its own root certificate, and the client has a certificate issued according to different root ca-certificates. Access to the blockchain network and account books involves different permissions. The default is unable to see each other's business account data, only by other members authorized, and only other members account book data access rights. The details are shown in Figure 8.

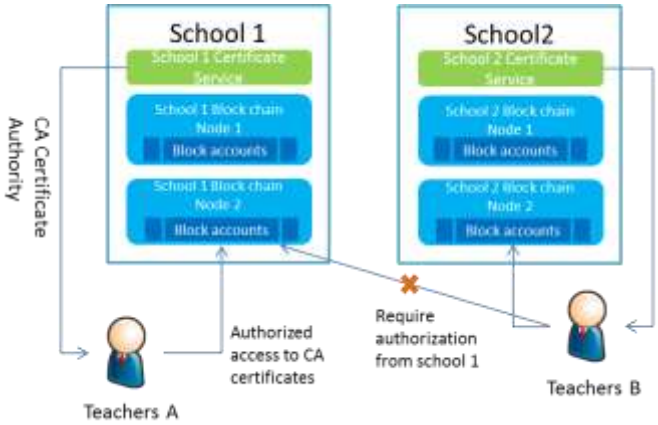

Figure 8. Privacy protection schematic for blockchain data

4.1.4. Capacity Transfer Process

The user submits a blockchain transaction request in the DAPP. The request is sent to the node, and the node generates the transaction ID while the transaction is endorsed, and the transaction version number is generated. As the premise of subsequent concurrent transaction version verification and consensus verification, the sandbox that is completely isolated (to prevent external attack) is automatically started to run the chain code (intelligent contract) on the node, input the latest account status data, and calculate the transaction results. The result of the transaction is calculated by consensus through the network, and the result of the consensus will generate new block data, which will be written into the account book of the node.

Because the consensus process is the asynchronous process of the system, it needs to be carried out in the whole network. According to the different number of nodes, the blockchain node provides an event registration mechanism. When the transaction request is provided, the client can register the callback event interface. When the consensus process is completed, the client will be notified of the final confirmation result of the transaction. The client will confirm the result, such as by updating the status of the business database, so as to achieve a distributed unified transaction. Otherwise, the DAPP end may not be able to know the exact results of the transaction and thus the business user. The capability transfer process is shown in Figure 9.

Figure 9. Capacity transfer flow chart

4.1.5. Account Inquiry

The account query does not need to submit the transaction on the blockchain, but it only requires permission verification to query the association code on the blockchain. The query request is submitted by the DAPP-client. After the authorization verification, the completely isolated sandbox is automatically started to run the chain code query smart contract, and then the association code is input and the result set is returned to the client. The process is shown in Figure 10.

Figure 10. Account query process

4.1.6. Learning Contract

The definition of learning contract [16-19] can be summed up as: "A learning contract is a set of commitments defined in digital form, including the agreement on which contract participants can implement these commitments." Digital form means that the relationship between rights and obligations embodied in the contract can be written into computer readable code. As long as the parties concerned reach an agreement on the rights and obligations established by the learning contract, the blockchain network can be executed.

The chain code on the OBE blockchain, the learning contract, is a set of computer logic codes implemented by go language, which embodies some of the most critical logic of the OBE evaluation operation, such as calculating the final score of the individual student's OBE ability by inputting the parameters of the formula. The score is submitted as a transaction to the blockchain. Chain code realizes the above function by function. Taking the POA consensus as an example, the function contains two main functions: "calculating ability value and storing" and "querying according to specified condition".

The student ability score in the account book can be identified by key word (student identification ability value), multiple transactions can update the same student ability value, and all records of the transaction are block data that cannot be tampered with. It reflects the growth course of the students' ability.

4.2. The OBE Blockchain Platform

In this paper, the OBE blockchain platform was built through the cooperation between Xiangtan University and Zhongke Jiudu Co., Ltd. Figure 11 shows the historical data of the blockchain (due to the short completion time of the platform setup, only one month of data is displayed). Figure 12 shows the data for the OBE blockchain platform, including block numbers, transactions nodes chain codes, upload time, and so on. Figure 13 shows the OBE blockchain platform.

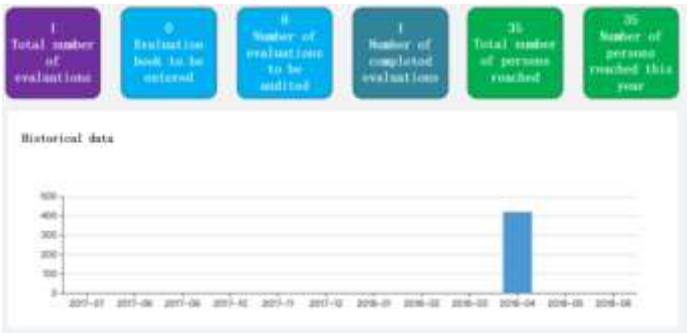

Figure 11. Historical data record

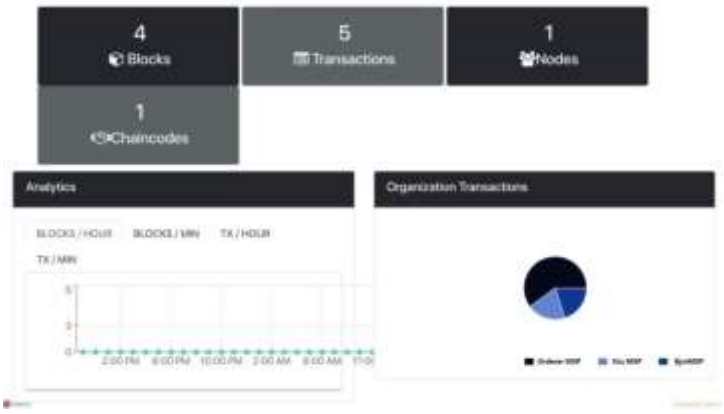

Figure 12. Basic data on the OBE blockchain

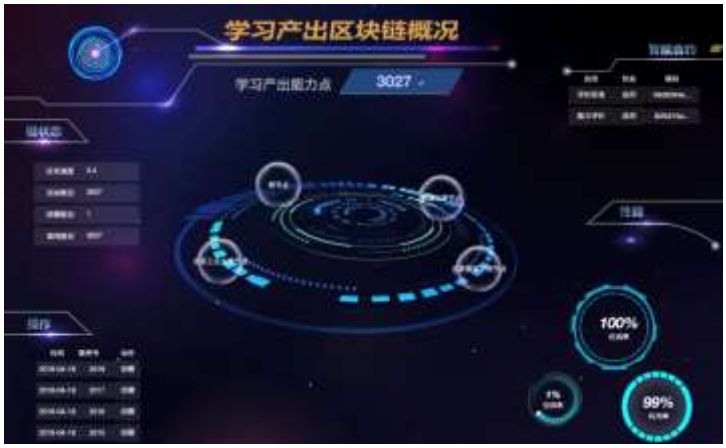

Figure 13. OBE blockchain platform

5. Conclusions

The OBE blockchain bears the values conferred by the stakeholders in engineering education and represents the belief and consensus of the group behind it on the OBE educational concept and the needs of the industry for learning output. This paper presents a blockchain design based on the OBE of engineering education. Taking the course of Electrical Science as an example, the evaluation mechanism of engineering education ability is designed. At the same time, a kind of association coding is designed, which is helpful to the search of record data. Taking Student 1 as an example, the process of transferring and querying ability value is analyzed. The feasibility of the platform is proven by the construction of the platform.

This paper is a beneficial research on blockchain technology in the field of education. Although there are still many problems in blockchain at home and abroad, it is believed that distributed accounting technology and intelligent contract, as one of the key technologies in the future digital society, will have a wide range of prospects.

References

1. W . Prinz, T . Rose, T . Osterland, et al., “Blockchain” Digitalisierung; 2018
2. M. Swan, “Blockchain: Blueprint for A New Economy,” O’Reilly Media, Inc., 2015
3. A. E. Gencer, S. Basu, I. Eyal , R. van Renesse, and E. G. Sirer, “Decentralization in Bitcoin and Ethereum Networks,” arXiv: 1801.03998, 2018
4. L. Columbus, Gartner Hype Cycle for Emerging Technologies (http://www.forbes.com/sites/louiscolumbus/2016/08/21/gartner-hype-cycle-for-emerging-technologies-2016-adds-blockchain-machine-learning-for-first-time/#6394bd121ef2)
5. P. M. Frederic, F. A. Vandome , and M. B. John, “Traditional Education,” Alphascript Publishing, 2010
6. J. J. Sikorski, J. Haughton, and M. Kraft, “Blockchain Technology in the Chemical Industry: Machine-to-Machine Electricity Market,” *Applied Energy*, Vol. 195, pp. 234-246, 2017
7. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in Proceedings of *IEEE Security and Privacy Workshops*, pp. 180-184, IEEE Computer Society, 2015
8. S. E. Skandari, J. Clark, D. Barrera, and J. Clark, “ A First Look at the Usability of Bitcoin Key Management” in Workshop on Usable Security, 2018
9. A. Brauneis and R. Mestel, “Price Discovery of Cryptocurrencies: Bitcoin and Beyond,” *Economics Letters*, Vol. 165, pp. 58-61, 2018
10. A. Sensoy, “The Inefficiency of Bitcoin Revisited: A High-Frequency Analysis with Alternative Currencies,” *Finance Research Letters*, 2018
11. G. D’Angelo and S. Rampone, “Cognitive Distributed Application Area Networks,” Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, 2018
12. N. Bozic, G. Pujolle, and S. Secci, “A Tutorial on Blockchain and Applications to Secure Network Control-Planes,” in *Proceedings of the 3rd Conference on Smart Cloud Networks & Systems*, pp. 1-8, IEEE, 2017
13. M. Ohkubo, K. Suzuki, and S. Kinoshita, “Efficient Hash-Chain based RFID Privacy Protection Scheme,” in *Proceedings of International Conference on Ubiquitous Computing*, 2004
14. L. Zhu, H. Dong, and M. Shen, “Privacy Protection Mechanism for Blockchain Transaction Data,” *Big Data Research*, 2018
15. Y. L. Zhang and H. Guo, “An Improved RFID Privacy Protection Scheme based on Hash-Chain,” in *Proceedings of International Conference on Logistics Engineering and Intelligent Transportation Systems*, pp. 1-4, 2010
16. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, Vol. 4, pp. 2292-2303, 2016

17. W. G. Peters and P. Efstathios, "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," Social Science Electronic Publishing, arXiv:1511.05740, 2016
18. A. Kosba, A. Miller, E. Shi , Z. K. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in *Proceedings of 2016 IEEE Symposium on Security and Privacy*, pp. 839-858, IEEE, 2016
19. L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," in *Proceedings of ACM Sigsac Conference on Computer and Communications Security*, pp. 254-269, ACM, 2016

Tao Li graduated from the Hunan Institute of Engineering. He is currently a Master's student at Xiangtan University, majoring in Electrical Engineering. His main research interests include blockchain and artificial intelligence.

Bin Duan is a professor and doctoral supervisor at Xiangtan University, responsible for the first class Master's degree in Electrical Engineering at Xiangtan University. He received a Master's degree in Electronics and Communication Engineering at Xiangtan University. He is a senior member of the China Electrotechnical Society and a Hunan Province 121 talent project second level candidate. His research interests include power systems and blockchain.

Dayu Liu graduated from the Software Engineering School of Peking University in 2005 with a Master's degree. He is currently working at Zhongke Jiudu Co., Ltd. His main research interests include blockchain.

Zhen Fu graduated from Beijing Forestry University in 2003, majoring in Information Management and Information Systems. He is currently working at Zhongke Jiudu Co., Ltd. His main research interests include blockchain.