The application framework of blockchain technology in higher education based on the smart contract

Tao Wu [1*], Maiga Chang[2]
[1]*Zhujiang college of South China Agriculture University Guangzhou, China*
[2]*School of Computing and Information Athabasca University Canda*
735454848@qq.com , maiga.chang@gmail.com

***Abstract*—With the rapid development of blockchain, the two important concepts of digital innovation and regional sharing have begun to trigger changes in the field of higher education finance. This article aims to establish a new framework for the application of blockchain in higher education, and suggests the establishment of a suitable consensus mechanism and the use of smart contracts.**

Keywords—blockchain in higher education, Smart contract, Consensus mechanism, Proof of Stake component

I. INTRODUCTION (*HEADING 1*)

Since the concept of Cryptocurrency was proposed by Satoshi Nakamoto in 2008[1], blockchain technology has received various attention and attention in the past 13 years. The immutability, transparency, traceability and the instantaneous transaction of the blockchain have become a major feature of the use of Internet technology in different industries. For this reason, it has been the foundation for the establishment of a prosperous cryptocurrency market since 2009.

In 2015, Melanie Swan, the founder of the Institute for Blockchain Studies, proposed that according to the impact of technological innovation brought by the blockchain, the application of blockchain technology is divided into three stages, namely blockchain 1.0, 2.0 and 3.0 stages [2]. Based on this division method, in blockchain 1.0, the technical application of the peer-to-peer cash payment system represented by encrypted currency is the most primitive blockchain application prototype. Blockchain 2.0 represents the innovation of a new generation of consensus mechanism represented by smart contracts. Blockchain 3.0 represents the application of blockchain in various fields beyond currency and finance, health, education, government management, etc. Although some researchers have proposed the concept of blockchain 4.0 and 5.0, it can be considered as a detailed classification of 3.0.

Although the application of blockchain technology in cryptocurrency has been widely known, and the cryptocurrencies of Bitcoin, Dogecoin, and Ethereum also contributed investors extremely successful return in the market [3]. However, this encrypted currency can only be regarded as an application of one of the encryption technologies of the blockchain, the application of blockchain technology in human life-long areas such as health, commercial transaction and various aspects of life is an inspiring vision.

The application of blockchain in education has been developed for a long time, but it is mostly focused on the verification of certificates, the integrity of personal resumes, and certification and storage of college credits. It is undeniable that these are the use of the decentralized storage and the record-immutable features of the blockchain [4,5,6,7].

Few studies have put forward the concrete application of blockchain in the curriculum learning on campus, and these are precisely the basic modules for the application of blockchain technology in teaching in the future. This paper proposes classroom teaching innovations and assignment assessment mechanisms on campus based on blockchain technology based on specific consensus mechanisms. The two components of this framework are derived from smart contracts and two consensus mechanisms represented by POS (Proof of Stake) and DPOS (Delegated Proof of Stake) [8].

II. LITERATURE REVIEW

This section elaborates some core concepts of blockchain. Meanwhile, it also summarized several applications of block-chain in the education industry.

A. Blockchain

Blockchain is a distributed ledger that allows individual record transactions and tap time stamped through distributed digital records that exist in the public to be shared among nodes [1]. Current blockchain frameworks are categorized into three types: public or permission less blockchain, private or permission blockchain and consortium blockchain [9]. The current blockchain framework can be divided into three types: public or permissionless blockchains, private or permissioned blockchains, and consortium blockchains. The following is a specific explanation:

- Public blockchain: also refers to permissionless blockchain that anyone can read and send transactions for validity confirmation, and anyone can participate in the consensus process, and jointly maintain the security, transparency, and non-tampering of public blockchain data.
- Consortium chain: also known as community chain, it means that the nodes participating in the blockchain are selected in advance, and there is usually a good network connection and other cooperative relations between nodes.
- Private blockchain: The participating nodes have only a limited range, and the access and use of data have strict authority management. The write authority is only in the hands of the participants, and the read authority can be opened to the outside world.

The form of blockchain mentioned in this present paper is a Consortium chain.

*Corresponding author

B. The potential advantage of blockchain in education

Although there are many classification standards for the features of the blockchain, four features are specially extracted according to the characteristics of higher education [10]. It is elaborated more in the following content:

- Immutability: Immutability is formed based on the unique ledger of "Block+Chain": the blocks containing transactions are continuously added to the end of the chain in chronological order. To modify the data in a block, it is necessary to modify all points on the network at the same time, which is impossible. This immutability feature is very important in higher education. It ensures that all the assignments and materials submitted by students cannot be tampered with, and it ensures fair and objective standards.

- Decentralization: Decentralization is a very difficult concept to define, but in simple terms, it can be regarded as a form of equal participation of each individual and removal of regulatory pressure. Decentralization, but all logical sequences are centralized. This can be understood in this way. When the participants in the zone jointly adopt a mechanism, all participants need to comply with it and the status of the participants cannot be changed in the process. In higher education, collaborative learning is a very important section, especially in STEM subjects. Instructors or Tutor will instruct students to practice after imparting some know-how. However, Instructor's supervision and participation are not always positive for the students. Actually, the interaction between students has a great influence on the mastery and application of knowledge [11].

- Traceability: Although in the blockchain, almost all participants participate anonymously. However, because part of the chain needs to add a unique time stamp before it is stored in a part of the data structure, so that there are historical data of this imprint in other time blocks of the chain, and a piece of data on the part of the chain can be traced to its origin through the chain structure. In higher education, faculty assign tasks that are often difficult and needs group work. When a complex team task is assigned and completed, but the results are faulty, it is important to find out exactly where and who went wrong. This is not simply accountability, but an educational approach that assists and helps students to remedy the flawed part.

- Currency properties: The currency characteristic of the blockchain refers to a certain token that is generally accepted in the block, and although this token itself is worthless, it contains a certain amount of work and contribution behind it, which is measured by a certain standard. And is generally accepted in overall blocks. Several studies have confirmed that extrinsic motivation plays an important role in motivating students to learn, and that rewarding them with some kind of tokens is a way to reward their academic ability or team contribution.

The above features of blockchain are well suited for grade recording and credit allocation in higher education for group collaborative tasks in complex processes. Peer to peer evaluation in higher education based on complex engineering and teamwork has been a very troubling problem. These features of blockchain technology eliminate human interference (e.g., teachers, other peers), because the process is anonymous and automated within the zone, and the content submitted during the process cannot be changed. More details are described in Section III.

C. Smart contract

The term smart contract was first coined in 1994 by Nick Szabo, a prolific cross-disciplinary legal scholar, computer scientist, and cryptographer. A smart contract is a set of digitally defined promises, including an agreement that participants in the contract can agree to the above conditions to automatically enforce those promises. Of course time takes precedence, and whoever satisfies the conditions fastest is the performer. The two points of automated execution and temporal order are very important for the use of the teaching model mentioned later. In 2014, V. Buterin proposed a new generation of blockchain applications in his work "The Next Generation of Smart Contracts and Decentralized Application Platforms", which uses blockchain technology and smart contracts to create a new blockchain platform represented by "Ether". [12]. A new Ethereum network with an embedded programming language is proposed, which makes it possible for everyone to write smart contracts [13,14] and decentralized applications. In the smart contract mode, after an anonymous node in a certain area issued tasks, group assignments, and various questions via smart contract, each student can choose to participate. After addressed the requirements of the smart contract, the student will be rewarded and increase his or her stake value in the network. Different smart contracts and various responses will be recorded in the decentralized ledger indiscriminately. This is a summary of various teaching documents other than papers. This is a subversive classroom teaching revolution that does not require teachers and Students face-to-face, and there is no need to consider the identity and characteristics of the object. All returns are based on accuracy and time.

Generally, a smart contract implementation consists of three parts. The first step is to formulate a contract by multiple parties or one party and make provisions for the triggering conditions of the contract. This refers to the pre-defined contract. The second step is when there is an event or message that satisfies or triggers the conditions of the smart contract, which becomes an EVENT. The last step refers to the fulfillment of the contract and the transfer of certain resources to the participants who address the conditions in accordance with the pre-determined provisions. In fact, a smart contract is an automatic agent that simply and faithfully executes the conditions of the contract. A smart contract is simply regarded as "automatic agent" that a program statement consists of "If...., then....., else….". In higher education, Instructors can formulate learning tasks and learning assignments as the basis of smart contracts. In the smart contract, only the conditions and requirements need to be regulated, and then the value transfer regulations can be made to become an effective smart contract.

D. Consensus mechanism

The consensus mechanism is the core component of the blockchain. It is the basis of the operation of the blockchain and is regarded as the equational function of the basic law of human society. Actually, it is an algorithm design. Consensus mechanisms are very diverse in today's blockchain world, but the three most dominant verification

mechanisms are generally considered to be tuples. Below are some specific explanations of the classification and pros and cons of some common consensus mechanisms for blockchain.

- Proof of Work (POW), usually can only be proved from the results. The representative of this mechanism is the mining of Bitcoin. The advantage is that it does not require cumbersome supervision and is simple. But the disadvantage is that the use of this computing power is often meaningless in practice and cannot make other contributions to society at the same time[15].
- Proof of Stake (PoS) was first proposed by Quantum Mechanic at the Bitcoin Forum lecture in 2011[15]. The main idea of PoS is that the difficulty of obtaining a node's accounting rights is inversely proportional to the stake held by the node. As long as the token holder has more equity tokens, the greater the chance of him obtaining accounting rights and returns.
- Delegated Proof of Stake (DPoS) is a blockchain consensus algorithm. It was proposed and applied by Dan Larimer (now EOS CTO), the chief developer of Bit-shares in April 2014. In fact, it is also regarded as a derivative version of the PoS [16].
- Proof of Capacity (POC) is a consensus algorithm that allows mining equipment to use the idle space of the local computer's hard drive to participate in mining. It was launched by Burst in 2014. PoC puts a large number of hash calculations in the initialization stage, that is, the results of the hash calculations are written to the hard disk in advance through "surveying and mapping" (commonly known as P disk). The larger the hard disk of the miner, the more chances it is to "retrieve the positive solution" (commonly known as scan disk) before the deadline and get block rewards. This is an algorithm that has great requirements for storage space [17].

For applications in higher education, the most suitable consensus algorithm is POS. This can save computing power and give instructors and students more chance to allocate resources based on performance.

III. APPLICATION FRAMEWORK OF BLOCKCHAIN TECHNOLOGY IN HIGHER EDUCATION

A. The current application of blockchain technology in higher education today

At present, seven scenarios where blockchain is recommended for the most applications in higher education:

1) Issuance, preservation and inspection of certificates;
2) Verification of the integrity of academic qualifications;
3) Automatic credit identification;
4) Records of online teaching;
5) Tracking intellectual property rights and their rational use;
6) The Campus financial tool as an alternative to cash
7) Identify students.

However, the application of blockchain technology in higher education should be much more than that. Our research team presents a framework and proposed practical process for the application of online and offline blockchain in higher education, looking to pioneer the use of this technology in the classroom in higher education.

B. Framwork of application of blockchain in higher education

While many scholars recognize the promising applications of blockchain in higher education, few studies have proposed specific applications of blockchain in curriculum systems and course design to inform course instructors about how to use blockchain technology to achieve pedagogical goals.

This paper proposes a framework for unified mining, smart contract issuance, anonymous trading, and alternative credit usage for on-campus use.

1) Unified mining

In order to ensure that merits are not arbitrarily changed by individuals or generated by other channels, university or college must have computers with sufficient computing power for mining operations. This is an important premise.

2) Smart contract issuance

Courses on campus using blockchain technology can be obtained by the instructor of the course from the school's open course bids through a task-based smart contract. And the teacher's final assessment can be released through a smart contract. All processes are automated, anonymous and implement via Smart-contract quickly.

3) Anonymous trading

Before a student can use blockchain technology on campus they register, get a code, and don't let peer or instructor know their identity during other activities on campus. This better protects the privacy of students and the fairness of their grades.

4) Alternative credit usage

Although the tokens are obtained through the school's uniform mining, they are used on campus for academic as well as instructional purposes as it is. It is because it lies only in a channel transaction and its use is only in classroom academics that the University/College can convert such tokens into credits per unit according to its own criteria.

The framework we propose is for University/College to set its own rules, credits and subjects that are issued via smart contracts to go to specific faculty or colleges for instructor to apply for, with priority given to instructor who have more weits. To better illustrate this framework, the entire process from the issuance of the contract by the school to the receipt of the tokens by the student is explained in detail below.

As shown in Figure 1, the school issues a teaching task through a smart contract (with the acquisition condition of Weit attached), which faculty members A, B, C, and D are all interested in obtaining. Instructor A has more Weit(100) due to his excellent performance in the past, then he has the privilege to choose first. If he gives up, B, C and D (who have different weits) will wait in turn.

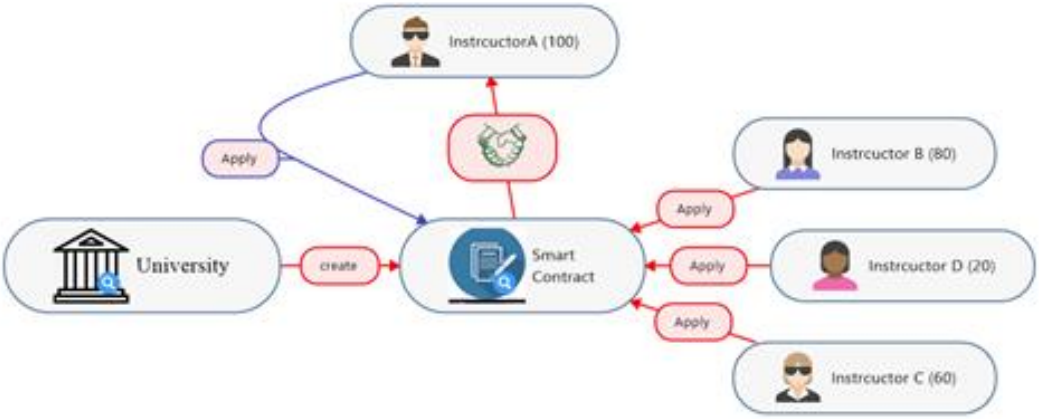

Fig. 1. University's course bidding plan

TABLE I. CONSENSUS MECHANISM

Consensus mechanism	
Types	***Rules***
PoS	The smart Contract is issued directly by the school, and invites everyone in the area, and professors who have obtained enough weit in the past have priority. Because, when a teaching activity is successfully completed, there will be weit to reward.
DPoS	When the school delegates the authority to the college, the college will issue smart contracts according to the enrollment status of the department as a node for teachers to apply. This is an extension of PoS, which is essentially five different from PoS. However, considering the resource competition between colleges, it is still necessary to follow the principle of prioritizing advantages in the past to make the past blockchain technology teaching applications better Colleges with grades are preferred.

As Shown in Table I, the adoption of an Ethernet-style consensus mechanism is advocated in this paper. This Consensus mechanism is used from schools to Instructors and even to student to ensure that experienced and competent candidates or institutions are given priority.

C. The use of blockchain technology in the teaching process

As shown in Fig.2., this is a complex team task process, issued by the teacher through a smart contract, which requires a tutor to respond to a bid and team up to complete. When we assume that tutors have gained enough weit from their successful performance in the past, they can design tasks in a new smart contract and assign these weit again as a bidding plan. Students who have earned more weit based on previous academic performance studies can successfully prioritize the right to become “Gatekeeper” and issue another new smart contracts through which invitations are sent to other students to complete tasks. When students get enough weit, they can choose to convert it into a certain number of credits, and high enough credits are replaced with access to higher level academic resources (scholarship applications or access to academic literature and tokens for programming tasks).

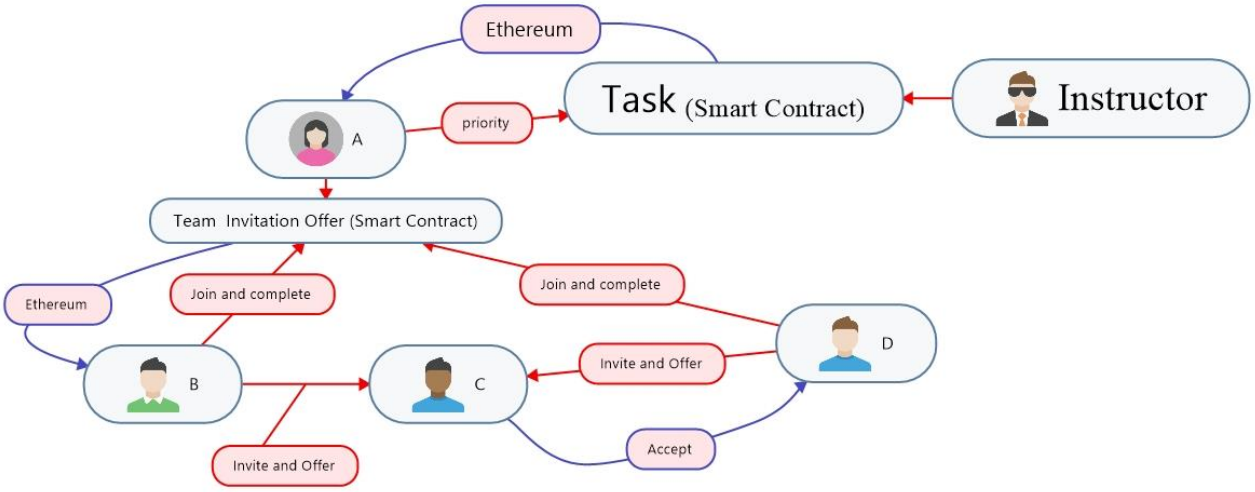

Fig.2. Distribution of learning tasks and return after completion

IV. CONCLUSION & DISCUSSION

A. Conclusion

From google trend, it is found that "blockchain + higher education" is the first popular word in 2021. It was believed that this hot spot will bring more resources and capital to the application of blockchain in higher education in future. In this paper, we propose to connect schools, tutors and students through smart contracts in an ethereal structure, and to achieve fair distribution of educational resources through reward weit and stimulate students' performance in team work through weit reward. Instead, it is suggested that blockchain technology in schools should use the consensus mechanism of PoS in order to differentiate experienced and competent instructors from novices and students with learning advantages from the average student in the group, so that students have a competitive incentive. Smart contracts are a tool for splitting tasks and transferring value, but the complexity of the contract depends on the designer. Smart contracts that can be used for teaching and learning are very demanding on the designer, and this is the current focus of attention.

B. Limitation

Two obstacles currently hinder the application and promotion of blockchain technology in higher education. One is platform construction. Because colleges and universities use blockchain technology, they need to have an initial investment, and a platform will be used for regional network. The second is the lack of enough professional talent who are suitable candidates for the creation of smart contracts.

C. Future works

Since there is not yet a university that has really gained enough experience in the use of blockchain technology in teaching and training, we suggest that as soon as possible, we should start experiments on collaborative complex tasks based on blockchain technology in STEM and computer disciplines. It is recommended to use other tokens to be issued on the platform instead of the real weit to avoid some malicious attacks due to the potentially huge value.

REFERENCES

[1] Nakamoto, S. “Bitcoin: A Peer-To-Peer Electronic Cash System,” http://nakamotoinstitute.org/bitcoin/#selection-37.419-37.724. 2008, Accessed: November 5, 2017 G. Eason, B. Noble, and I. N. Sneddon,

[2] M. Swan “Blockchain: Blueprint for a New Economy,” 1st edn. O’Reilly 2015

[3] Serena, Luca & Ferretti, Stefano & D'Angelo, Gabriele. “Cryptocurrencies activity as a complex network: Analysis of transactions graphs,” Peer-to-Peer Networking and Applications. August 2021 doi: 10.1007/s12083-021-01220-4

[4] P. Devine, “Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?” Presented at the ALT Online Winter Conference 2015, Online, (United Kingdom, 2015).

[5] DJ Skiba, “The potential of Blockchain in education and health care,” Nurs. Educ. Perspect. 2017, 38(4),pp.220–221 https://doi.org/10.1097/01.NEP.0000000000000190.

[6] Verbert, Katrien , M. Sharples , and T. Klobuar,. "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward", European Conference on Technology Enhanced Learning September 2016, pp 490-496.

[7] A.Grech and A.F.Camilleri, “Blockchain in Education,” Inamorato dos Santos, A. (ed.) EUR 28778 EN; doi:10.2760/60649 .

[8] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 469-474, doi: 10.1109/UEMCON.2017.8249088.

[9] Guegan, Dominique, "Public Blockchain versus Private blockhain," Documents De Travail Du Centre Deconomie De La Sorbonne, 2017.

[10] G.Chen, et al. "Exploring blockchain technology and its potential applications for education," Smart Learning Environments 5.1,2018:1.

[11] T. Wu, M. Chang, “Three Common Group Formations in Online Collaborative Learning,” In: Cristea A.I., Troussas C. (eds) Intelligent Tutoring Systems. ITS 2021. Lecture Notes in Computer Science, vol 12677, pp. 357-363 Springer, Cham. https://doi.org/10.1007/978-3-030-80421-3_39.

[12] S. Wang, et al. "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[13] N.Szabo, “Smart Contracts : Building Blocks for Digital Markets,” 1996, unpublished.

[14] M. Baudlet, D. Fall, Y. Takenaka and Y. Kandobayashi, "The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 17-24, doi: 10.1109/BRAINS49436.2020.9223280.

[15] C.,Li, C. , and B. Palanisamy, “Comparison of Decentralization in DPoS and PoW Blockchains,” In: Chen Z., Cui L., Palanisamy B., Zhang LJ. (eds) Blockchain – ICBC 2020, pp18-32, September 2020. https://doi.org/10.1007/978-3-030-59638-5_2 .

[16] X. Han, Y. Yuan , and F. Y. Wang, "A Fair Blockchain Based on Proof of Credit." IEEE Transactions on Computational Social Systems 6.5(2019):922-931.

[17] S. Aggarwal, , N. Kumar , and P. R. Chelliah, “Cryptographic consensus mechanisms,” Advances in Computers, Elsevier, Volume 121,2021, Pages 211-226, doi:10.1016/bs.adcom.2020.08.011.