On the Design of a Blockchain-based Student Quality Assessment System

Xiubo Liang[1*], Qian Zhao[1]

[1]*College of Software Technology, Zhejiang University*
Hangzhou, China
xiubo@zju.edu.cn, skzhaoqian@zju.edu.cn

***Abstract*—Blockchain technology has been applied in different fields with the advantages of decentralization, anonymity, immutability and reliability. There are quite a lot of problems, such as data decentralization, low utilization rate, high cost and unguaranteed security when managing students' study records. Therefore, we design a blockchain-based system for students' comprehensive quality assessment. This system adopts a solution of combining "onchain and offchain" data, where we use the smart contract, the interplanetary file system (IPFS) and Web Service to ensure that data flow is efficient, safe and reliable. In this paper, a network architecture based on education consortium blockchain is proposed, where we design a blockchain data structure and storage model to conveniently access to students' quality assessment data. And a data flow mechanism is designed for student data's trusted sharing and authentication protection, in which we combine the advantages of RBFT-based Hyperchain consortium blockchain and traditional data persistence. Then we use the microservices architecture to build the whole system and propose a performance optimization scheme to ensure high availability of the system. Sharing student data for research purposes will boost research innovation in education.**

Keywords—blockchain, IPFS, smart contract, security sharing, cooperation system, microservice

I. INTRODUCTION

In the era of network and datalization, traditional educational institutions lack the sense of reform, and their technical capabilities and practical strategies are relatively backward in recording learners' learning behaviors. At the same time, the contradiction between learning on network and universities' centralized management mechanism is increasingly prominent. Blockchain technology, which is characterized by decentralization and high-trust, will effectively solve the above problems. Although blockchain has some practical applications in the educational field, the practical application of blockchain in education and technology development has not received enough attention.

The core idea of blockchain technology proposed in 2008 comes from the paper "Bitcoin: A peer-to-peer electronic cash system", which is published by Satoshi Nakamoto [1]. Blockchain technology is regarded as another disruptive technology after cloud computing, the Internet of Things and big data. Blockchain technology is highly concerned by governments, financial institutions and technology companies [2]. Blockchain technology has advantages of decentralization, anonymity, immutability and high-trust, which has produced subversive innovations in the financial field. The application of "Blockchain + Education" has also attracted much attention from the society and academia. It is hoped that this technology can promote the reform of the education system and build an education information system that is compatible with the national economic, social and educational development level.

The emergence of the Internet has given chance to a new model of "Internet + Education" in the education field. The purpose of this model is to use the Internet thinking and technology to transform the traditional education ecology then realize the structural reform of the education system. There are still two problems in the development of education reforms promoted by new technologies:

On the one hand, the record data of current educational institutions including students' learning behaviors and results is scattered in various departments, and some educational institutions have not yet realized digital management. Although the certificate issued by the educational institutions largely shows the achievements of the learners during the study period, the demand for talents in the society is more multi-dimensional and high standards with the development of information technology. It is impossible to accurately assess students' abilities by evaluating students' certificates, degrees and academic achievements, which makes it impossible to accurately determine the ranking during the job search and study stages.

On the other hand, whether it is face-to-face teaching, teaching quality assurance, teaching activity monitoring, learning certification, or student learning records. The record data is subject to school-centered educational institutions, only the campus circulation causes information alone and the authenticity and originality of data are too high relying on the system center or a third-party organization. If a problem occurs in the system center, it will cause irreversible losses.

With the education becoming more and more international, it is convenient and safe for students and schools to share learning center data, which brings greater convenience for learners, educational institutions and employers. At the same time, data is becoming the most critical means of production for the development of the digital economy. With the vigorous development of the digital economy, production and lifestyle are being profoundly changed, and the effective application of data will become a strong driving force for economic and social development [3]. As the basic data in the field of education, students' learning record data will play an important role in the future. This paper studies the implementation plan of student comprehensive quality assessment, and combines the many advantages of the blockchain to build a credible comprehensive student quality assessment platform, which aims to optimize the educational business process, build an education trust system, achieve the needs of students' skills and social employment. Promoting the reform of the education system is an exploration attempt in the application of blockchain in the field of education.

The advantages of our system include the following six parts: (1) Universities can flexibly customize students' comprehensive assessment standards as their own demand. (2) We design an efficient blockchain data structure and a

978-1-7281-6512-7/20/$31.00 ©2020 IEEE

learning process record storage model for China's current educational situation. (3) We build an "education blockchain" network architecture in terms of the current education problems on wide distribution institutions and complex organizational management. (4) We realize a high-availability performance optimization scheme to ensure the system stable in complex scenarios, which optimizes from three aspects: single thread, network problem and connection form. (5) We construct a student assessment data transfer mechanism for credible sharing and verification protection to meet the privacy protection requirement of college student data. (6) We propose a data collaboration scheme based on "onchain and offchain", where using the microservices to combine the web application and the blockchain system. We combine business scenarios with the storage advantages of the four data-tier storage components of MySQL, Redis, IPFS and consortium blockchain to construct high performance students' comprehensive quality assessment system prototype.

II. Related work

At present, all walks of life have begun to pay attention to blockchain technology, and actively explored the use of this technology to solve industry problems for promoting industry innovation and development. Some researchers use the characteristics of blockchain technology in privacy protection and transparent sharing to try to combine blockchain with IOT, edge computing and energy sharing fields to promote new breakthroughs in the development of the industry [4] [5]. With the gradual improvement of the blockchain technology and the continuous expansion of the application field, some international educational institutions and scholars had begun to pay attention to and discuss the application of the blockchain technology in the education field. In the research of blockchain and education, part of the research focused on the technical flaws of blockchain, and pointed out the irrationality of applying blockchain technology. More researchers believed that blockchain technology will play a master role [6] [7]. Research by business thinkers Don Tapscott and Alex Tapscott pointed out that blockchain technology will be used to build a rich, security, and transparent global higher education network platform to promote the most efficient development of higher education in the future education field. Driven by the blockchain technology, the identity of the learner would be redefined, and the learning record data of the learner would be recorded and stored in real time. the goal of future lifelong learning were including rebuilding the classical pedagogy model, and promoting the reform of the higher education training model [8].

In October 2016, the Ministry of Industry and Information Technology issued the "China Blockchain Technology and Application Development White Paper", where it stated that "transparency of blockchain systems and immutable data characteristics are fully applicable to credit management, further employment, academic area, qualification certification, cooperation between production and education and other aspects are of great importance to the healthy development of education and employment". By analogizing the application scenarios of the blockchain in the financial field, Xianmin Yang and others summarized the application model of blockchain in education as: constructing big data for education, a platform for education Taobao, a degree certificate system, an open education ecosystem, online learning, and decentralized education system, etc. [9]. Based on the current difficulties of education resources in terms of liquidity and sharing, Lixin Quan proposed the construction of a dual-blockchain combined with smart contract resource circulation model, and created a digital resource registration chain and circulation information chain to promote education resource mobility and sharing [10]. To overcome the shortcomings of blockchain technology in storage capacity and data management, the industry has tried to combine blockchain and cloud storage technology to introduce authority nodes and then expand the controllability of system data [11].

Woolf University, the world's first blockchain university, was a challenge to traditional education models using blockchain technology. The management of the school would all rely on the blockchain platform. Blockchain technology would be used to supervise contracts, pay tuition and record students' academic achievements and credits. This new Oxford-style education was called "Uber among students, Airbnb among teachers" [12]. According to the concept of Edublocks, the Institute for the Future (IFTF) and the American College Entrance Examination (ACT) Foundation had proposed a "Learning as Earning" program [13], which was similar to the current study in colleges and universities that was used to evaluate student learning effects "credit". In addition to recording academic learning activities, the program could measure and record informal learning, such as off-campus training activities, school competitions, research presentations, internships, community services and so on. A series of Edublocks would form a distributed file ledger to record the learning credits that students had obtained at any time and any place.

Blockchain technology was now in its infancy, with most research focused on the financial sector. Compared with the financial field, the education field had stronger uniqueness and complexity. The successful application of blockchain technology in the education field would face difficulties in promotion and operation, blurred educational data property rights, limited data storage space, and the security of blockchain technology itself. Hidden dangers and other challenges caused by the privacy protection risks of teachers and students.

III. Sestem Design

A. System architecture

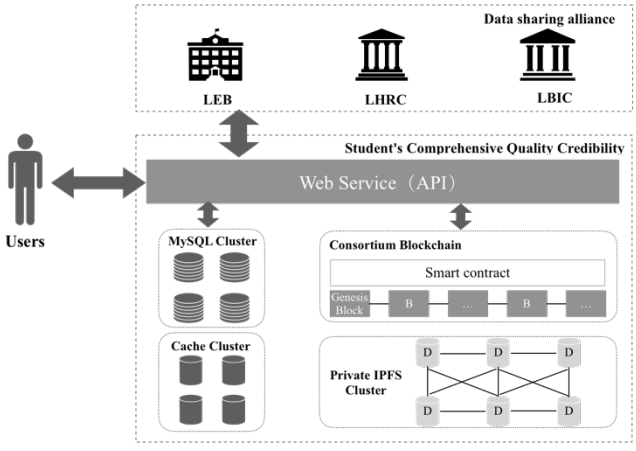

Fig. 1 System architecture

As shown in Fig. 1, a comprehensive quality assessment mechanism proposed by this paper consists of six parts: data

sharing alliance, consortium blockchain, private IPFS cluster, Web application service, relational database cluster, and cache database cluster. The three types of organizational structure, which includes the Local Education Bureau (LEB), the Local Human Resource Center (LHRC), the Local Bureau of Industry and Commerce (LBIC), participate in the consortium blockchain as authoritative nodes. They are responsible for managing and maintaining the normal operation of the consortium blockchain system, which have cores such as data maintenance, identity review, and data sharing. Learning centers such as universities and training institutions do not store data as the data nodes of the consortium blockchain, but using the services provided by the system as users. Fig. 2 shows the network architecture of the consortium blockchain. The system provides services through the B/S architecture built by Web technology. It integrates the capabilities of smart contract and IPFS into the platform's basic capabilities of the Web system, and provides services to the outside world through APIs. The system uses MySQL to build a database cluster and stores part of the data in a relational database cluster, which expands the limitations of the blockchain system in terms of computing and storage [14]. The read-write separation technology is used in the Redis cluster to make full use of the resources of the slave nodes, improve concurrency, and ensure high availability of the system. The private IPFS cluster stores the original information of the encrypted data files. It ensures data security through distributed DHT [15], Bitswap [16] and other technologies. The consortium blockchain uses the Hyperchain [17] based on the RBFT to manage and maintain the identity permissions of different roles in the system through web applications. The smart contract is used to synchronize the digital identity and the learning profile data summary to the blockchain platform. The data cooperation solution "onchain and offchain" is used to implement the business logic of user identity registration and restoration, and learning file protection and sharing.

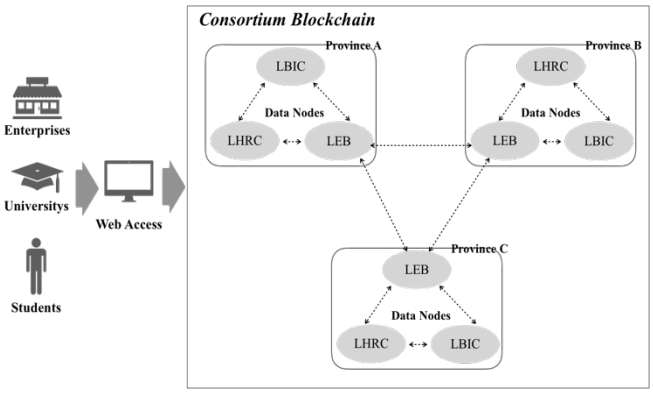

Fig. 2 Network architecture of the consortium blockchain

The system account adopts hierarchical authority management structure, as shown in the Fig. 3. There are three super administrator accounts when the system is initialized, which are taken over by the Central Education Bureau (CEB), the Central Human Resource Center (CHRC) and the Central Bureau of Industry and Commerce (CBIC). Local-level administrator accounts can be created separately with three super administrator accounts, where university accounts in the system are created by their respective competent educational departments (LEB) and the company accounts are maintained by the Local Bureau of Industry and Commerce (LBIC).

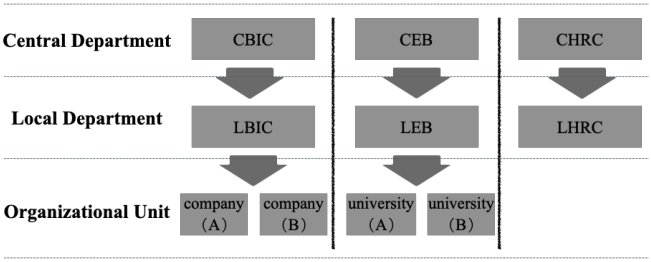

Fig. 3 System account hierarchical management structure

The system authority architecture is shown in Fig. 4. The system is divided into three subsystems, including four role identities and seven types of authority.

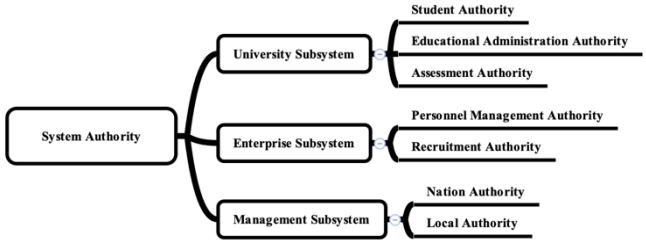

Fig. 4 System authority architecture

B. *Contract architecture*

This system adopts the data cooperation solution "onchain and offchain", and gets through the cooperation between the blockchain platform and the web application with the SDK. The smart contract is taken as the underlying capability of the web platform to conduct unified scheduling according to the requirements of different business scenarios. As shown in Fig. 5, the core smart contracts in the consortium blockchain include digital identity controller contract (DICC) and assessment data manage contract (ADMC). Following the design principle of "high cohesion and low coupling" [18], the main contract (MC) is used to encapsulate and manage the core smart contract functions in the consortium blockchain, so as to improve the expansibility of the system and ensure the benign evolution of the system.

1) Digital identity controller contract (DICC)

DICC is mainly responsible for maintaining the unique digital identity information of each participant in the system, which records the identity (UID), public key (PK), file key (cbc key pair), authority information and private key (SK) of the system user as the global contract in the consortium blockchain system. When the user registers by the web application, the corresponding DICC contract is created in the consortium blockchain system and the user's digital identity is created together.

2) Assessment data manage contract (ADMC)

ADMC is mainly composed of three parts, which includes assessment data storage contract (ADSC), assessment data authority control contract (ADACC) and assessment data sharing storage contract (ADSSC). ADMC is mainly used to realize the verification, protection, sharing and other business logic of student assessment data. The ADSC contract is mainly used for storing assessment data information, which is about data number, IPFS address, file hash value, timestamp and other information. The ADACC contract is

mainly used to audit the operation rights of visitors, including the audit logic of new data and data sharing rights whose logical judgment is based on the consistency of data permissions with relational databases. The ADSSC contract is used to store the shared record of the assessment data, including the assessment data number, the shared target identification and timestamp.

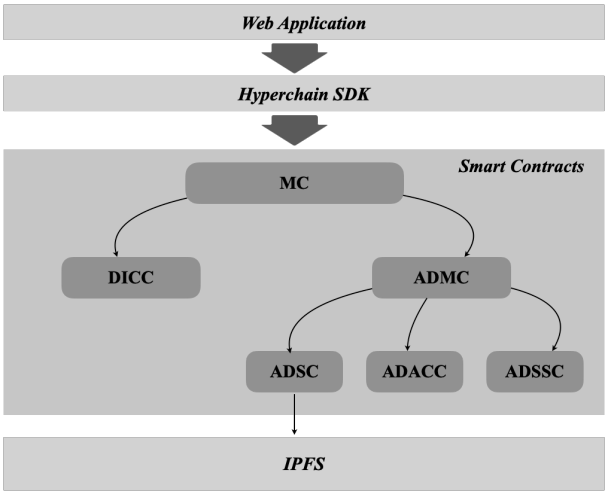

Fig. 5 Structure chart of smart contracts

IV. System Implementation

This platform can assess students' comprehensive quality, records students' learning process and achievement information, then it resolves the contradiction between the universities' plan of talent cultivation and the social demand of talents. Besides, it makes student data circles efficient, safe and reliable between the education and business. Users include college teachers and students, government managements, and enterprise recruiters. The size of the user group and the use scenarios together give raise to challenges in terms of high concurrency, high stability, high security, and high availability. The technical architecture diagram of the system is shown in Fig. 6. The whole system is built with the architecture of microservice, and dubbox [19] is adopted as the service governance framework to improve the scalability and fault tolerance of the system.

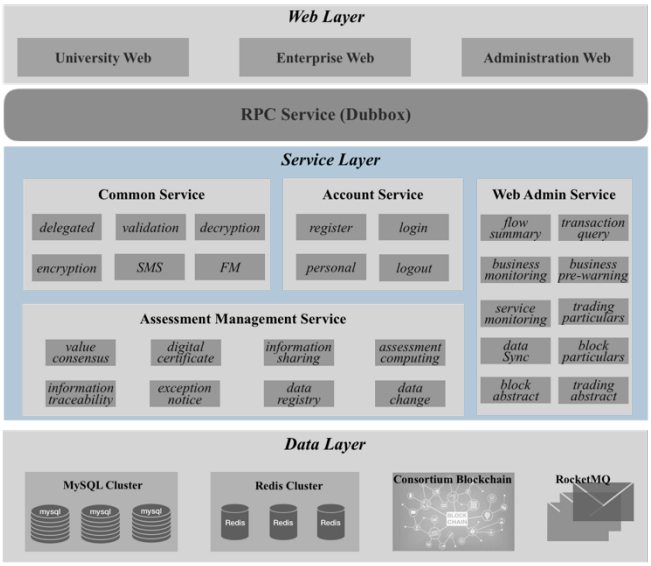

Fig. 6 System technical architecture

A. High availability caching scheme

Data storage has high performance, high concurrency and low-cost characteristics in the Internet era. When traditional database already can't satisfy the needs of Internet applications at the present stage, NoSql datasets emerge including typical of the open source database Redis [20]. Data is the valuable wealth of users, therefore the high-availability design of database in production environment is particularly important. This system adopts Redis to build cache database cluster, and proposes a high availability cache optimization scheme with high resource utilization and low fluctuation of failover service.

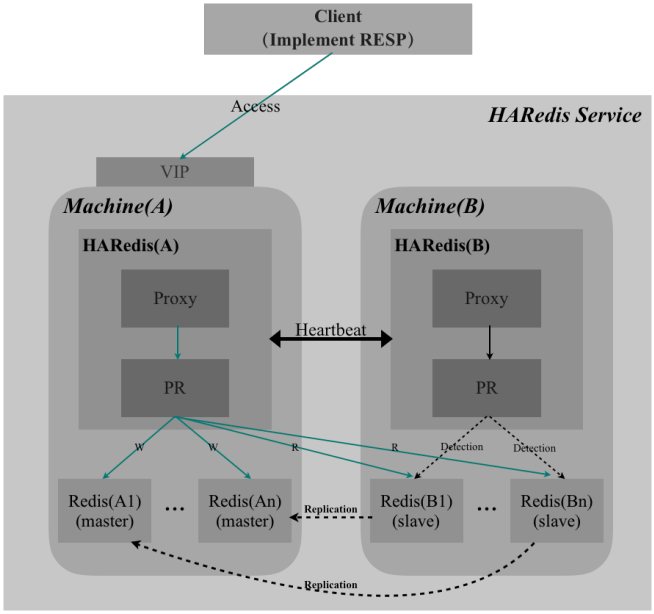

Fig. 7 HARedis system workflow

As shown in Fig. 7, machine A holds virtual IP(VIP), and $HARedis_A$ and $HARedis_B$ establish two-way heartbeat service to detect the service status. $RedisA_1$-$RedisA_n$ is n master nodes, and $RedisB_1$-$RedisB_n$ is n slave nodes. The client connects to the proxy via a VIP, and the Proxy parses the request and sends it to partitioning routing (PR). PR sends write requests to Redis of the master node based on the request Key, Similarly, it sends read requests to Redis of the slave node based on the request Key. Redis responds to the request to the Proxy, and then the Proxy responds to the request to the client. When machine A outages, $HARedis_B$ gets state of machine A through two-way heartbeat detection and updates the local route table. Then, it sets $RedisB_1$-$RedisB_n$ as the master node and "floats" the VIP to machine B. Finally, it tries to connect to $HARedis_A$. When machine A is recharged, $HARedis_A$ and $HARedis_B$ establish bidirectional heartbeat detection service again and update their respective route table, and $HARedis_B$ sets $RedisA_1$-$RedisA_n$ as slave node.

This system optimizes Redis cluster from two aspects:

1) Redis performance optimization

- Redis single-thread optimization: For Redis single-thread bottleneck problem, the solution adopted in this paper is to run multiple Redis instances on one machine. It uses segmented routing to make full use of CPU resources.

- Network optimization: We replace the original Redis with Tencent' open source f-stack-redis, and we overload network card drivers to reduce the resource overhead of kernel interrupt, memory copy and context switching.
- Connection form optimization: The short connection used by Redis will cause the overhead and delay of TCP/IP to be large. At this point, TCP/IP transmission control protocol is the bottleneck limiting the performance. Redis proxy can be selected to connect Redis with long connection form.

2) Proxy performance optimization

- Using network programming NIO technology to improve reading and writing efficiency.
- Zero-copy technology: Using zero-copy technology can reduce the times of copy of memory and then improve operation efficiency, Where buffer is allocated in direct memory instead of JVM heap memory and there is no need to copy buffer from one memory area to another memory area.
- The main performance loss of proxy is network overhead. Only one interactions of TCP is needed with Redis Pipeline, which saves the network overhead of Proxy greatly.

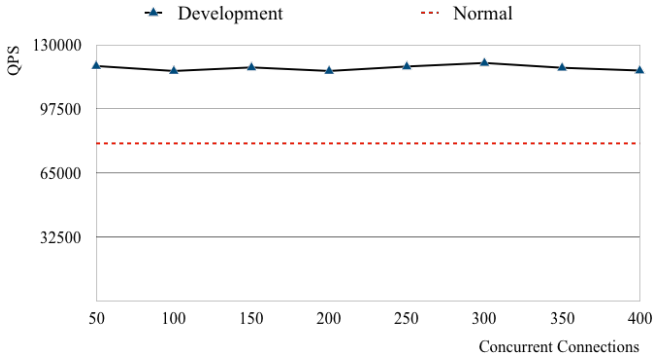

Fig.8 Result of Redis-benchmark test

The highly available optimization scheme of Redis cluster is proposed in this paper, where the data obtained by QPS of redis-benchmark test proxy under different concurrent connection numbers (TABLE 1 for the test environment configuration) is used. The results are shown in the Fig. 8, and the Proxy's QPS is stable around 120,000 QPS.

TABLE 1. Test environment configuration

Index	Data
CPU	Intel(R) Core(TM) i7-4790 3.60GHz
RAM	4G
CPU cores	4
Thread	8
Network bandwidth	GigE
OS	CentOS 7.5
Redis instance	4
Redis vesion	4.0.12

B. "Onchain and offchain" data collaboration solution

In order to solve the credible sharing problem of student' comprehensive quality assessment data in the field of "blockchain + education", in this paper, we adopt the technical solution of "onchain and offchain". We combine Web applications, consortium blockchains with IPFS to implement a highly available and highly credible students' comprehensive quality credibility assessment system. The data storage model combines the schema of "MySQL cluster + Redis cluster + IPFS cluster + consortium blockchain" with the technical solution of "onchain and offchain", which ensures the data is highly trusted, safe and immutable. According to requirements, the data collaboration scheme adopted in this paper is as follows:

1) Data consistency

This paper uses two storage methods including consortium blockchain and local database to ensure the system's core data privacy and security. The specific performance is as follows: The local relational database stores system's overall data, such as users, roles, authorities, organizations, announcements, operations, shared records, and student assessment files. Among them, the details of the students' assessment information in the student assessment files is stored in the IPFS cluster, and the data fingerprints in the IPFS are persisted in the local relational database. And the user information, authority information and student assessment information of the relational database keep in sync with the consortium blockchain, which constitutes the "consortium blockchain – local database – IPFS" mutual authentication storage model. The consortium blockchain stores the historical version data of student information and this is main datasource of the system is consortium blockchain data. We used the web application to check the data consistency, verify and restore the information in the relational database and IPFS.

2) System high availability

In the multi-user concurrent scenarios, the blockchain system is at week, which also makes the blockchain technology unable to be applied in other fields on a large scale. According to the non-functional requirements of high availability of the system, this paper adopts the "onchain and offchain" collaborative scheme to design the technical system architecture. MySQL in this system is mainly used to store business data of organization management, authority maintenance, user information management, and etc. Managing the data on users and organizations involves lots of transactional operations with a large number of users. The system uses the Redis cluster to ensure the rapidly reading and writing of data. It can solve high concurrent requests of users and reduce the storage pressure of relational databases, while it maintains the stability of Web applications. According to business scenarios, the system stores plenty of files, videos and other materials. The system builds a private IPFS cluster to scatter the pressure of the system in reading and writing large files, and this cluster has efficient and reliable data storage capacity. We use the blockchain to build a credit system to ensure that the core data of the entire system is transferred by credibly. Therefore, the entire system uses the "onchain and offchain" solution, which integrates the advantages of the convenience of MySQL, the efficient

reading and writing ability of Redis, the encrypted storage capacity of IPFS, and the credit advantages of blockchain technology to achieve a credible assessment system for students' comprehensive quality.

C. Core business process design

This part mainly introduces the flow design of the three core functions of alliance chain system in detail: (1) the registration of system users; (2) the protection and verification of student assessment data; (3) the sharing and acquisition of student assessment data.

1) The registration process for system users

After the organization is approved by the relevant agencies, the system will generate a unique identity for the organization and initialize the temporary administrator account for the organization. The administrator is responsible for creating users under the organization in the system and setting permissions for users. The system will create a unique identity for the organizations and users participating in the system, and this identity (UID) is the basis for data protection and sharing activities. The specific process for users to create identity in the system is as follows:

a) The Web system will assign a unique UID to the new user and generate public-private key pair <PK, SK> for the user according to the ECDSA [21] elliptic curve algorithm.

b) The identity of the new user and related permission information are stored in the local relational database.

c) The system will call DICC contract to save the use's identity information, including UID and key information, and call ADMC related contract to initialize the user's permission information. Among them, the user identity and authority information in the local relational database should be consistent with the information in the contract on the chain.

2) Student assessment data protection

Student assessment data is store the data on the blockchain for protecting, where we use the web application system smart contracts and the IPFS private cluster. Therefore, it prevents the student assessment data from being tampered and destroyed illegally, and it ensures verification, traceability and recovery of assessment data through consortium blockchain. As shown in Fig. 9, we construct a student assessment data storage object AssessJSON, whose attribute information includes data number (AssessID), creation time (CreateDate), detailed description (Description), operator UID, and assessment attachment (Attachments). When the student assessment data is added, the constructed object AssessJSON is encrypted and stored in the IPFS cluster, and then its IPFS storage fingerprint is stored in the ADSC contract on the blockchain. When the assessment data is updated, each newly constructed AssessJSON and related accessories file protection process. The steps for adding data are as follows:

a) When initializing user information, the Web system randomly generates a pair of keys cbc (key, iv) for user and stores them in the DICC contract for data sharing and updating.

b) Encrypted file EncryptAttachments are generated by using cbc (key, iv), and hash value ($Hash_{attachments}$)is got by hashing the attachment.

c) EncryptAttachments are stored the in the IPFS cluster with calling the IPFS storage interface to get its file fingerprint $IPFS_{encrypteattachments}$.

d) Combined with other attributes of the assessment data, the AssessJSON object is constructed.

e) We use cbc (key, iv) to encrypt the newly constructed AssessJSON object and store it in the IPFS cluster to obtain $IPFS_{encrypteJSON}$.

f) The ECDSA algorithm is used to sign AssessID, UID, $Hash_{attachments}$ and $IPFS_{encrypteJSON}$,and then we obtain a signature.

g) The ADSC contract will be called to store the assessment data after we call the ADACC contract to verify the signature through the SDK.


```
{
    "AssessID": "D67fff524e2da4c9b9e0fb4c589493351",
    "CreateDate": 1582861910954,
    "Admin": "Ue52996baf9c94708a601f977c10b3c59",
    "Title": "2018阿里云全球区块链大赛",
    "Description":
    "XX同学(21851888)，在2018年09月参加2018阿里云全球区块链大赛获得总决赛二等奖。项目名称：XXX交易",
    "category": 3,
    "status": 1,
    "Attachments": [{
        "ID": "F2fec4cf19b2a44169f1171d552d28064",
        "Title": "2018阿里云全球区块链大赛证书",
        "Hash": "a5c1815080f22e3b3437c32fd6c50758",
        "IPFS": "QmSoLV4Bbm51jM9C4gDYZQ9Cy3U6aXMJDAbzgu2fzaDs64"
    }]
}
```


Fig.9 Structure of JSON of assessment data

3) Student assessment data sharing and acquisition

The sharing and acquisition of student assessment data refers to the secure, efficient, and reliable data transfer through Web systems, smart contracts, IPFS storage clusters, and encrypted scheduling mechanisms, which involves all organizations and users of the system Through technological innovation, the traditional education data is promoted to produce value safely and reliably. The specific process is shown in the following Fig. 10.

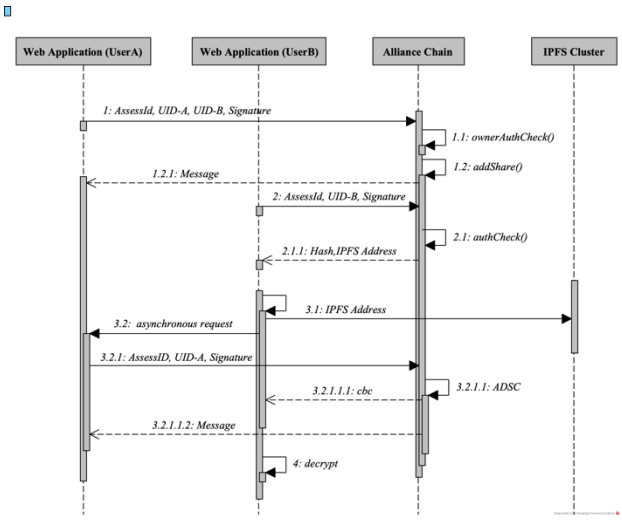

Fig.10 Flow chart of data sharing and acquisition

a) Student A (UID-A) uses the private key SK_A to sign the AssessID and the target user (UID-B), and UID-A submits the signature to the smart contract through the SDK. The ASACC contract, one of the smart contract, will first verify the UID-A identity,and the ADSSC contract will add sharing information <UID-B, AssessID> to the sharing list after the identity verification is passed.

b) Enterprise user B (UID-B) uses the private key SK_B to sign the AssessID and its own identity (UID-B), and it calls the smart contract to check the assessment data of student A. The ADACC contract will verify the identity of UID-B and check its access right. The IPFS Address of the assessment data object and its corresponding $Hash_{attachments}$ will be returned after passing the check.

c) UID-B uses the IPFS Address to obtain the encrypted assessment data object ($IPFS_{encrypteJSON}$) from the IPFS cluster. And UID-B obtains the decryption key of $IPFS_{encrypteJSON}$ in UID-A with an asynchronous https request.

d) UID-B uses cbc <key, iv> to decrypt $IPFS_{encrypteJSON}$ to get the original file object AssessJSON. It also can get the attachment ciphertext from IPFS according to the fingerprint of the file attachment in the JSON structure and decrypt it through edk.

V. Conclusion and Future Work

In view of the present education institutions on students learning record data management exists problems, such as decentralization, low utilization rate and unguaranteed security, etc., we design a students' comprehensive quality assessment system. The design idea of "onchain and offchain" is adopted to get rid of blockchain system's shortage in computing power and storage capacity and meet the demand of traditional application in information island and data tamper-proof. Government agencies, such as LEB, LBIC and LHRC, manage and maintain the system operation as data storage nodes of the consortium blockchain. universities, enterprises and other organizations participate in the system as users of the system, which greatly solves the problem of the system performance degradation caused by the increase of participating organizations. In this system, we proposed the high availability scheme of Web application, the data cooperation solution "onchain and offchain" and the data security sharing scheme. This system will greatly improve the circulation value of college students' data information and promote the seamless connection between higher education and social production talent demand.

With the advent of the DT (Data Technology) era, data is becoming the most critical production means for the digital economy development. In the future, our system will accumulate a large amount of basic education data and talents data from social development. The massive amount of basic data will support us in a more rational and scientific analysis of talent training issues, optimize training programs, build an education trust system, and promote educational reform. The huge amount of basic data will support us to analyze the problem of talent training more rationally and scientifically. It optimizes the training plan, builds the education trust system and promotes the education reform.

Acknowledgment

This work was supported by Zhejiang cultural relic protection science and technology project 2019009.

References

[1] Nakamoto S. "Bitcoin: A peer-to-peer electronic cash system". [Online], available: https://bitcoin.org/bitcoin.pdf, 2009.

[2] Wright A , De Filippi P . "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". Social Science Electronic Publishing.

[3] 2019 white paper on data infrastructure. [Online], available: https://www.useit.com.cn/forum.php?mod=misc&action=attachpay&aid=650564&tid=25414.

[4] K. Gai, Y. Wu, L. Zhu, M. Qiu and M. Shen, "Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid". IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3548-3558, June 2019.

[5] K. Gai, Y. Wu, L. Zhu, Z. Zhang and M. Qiu, "Differential Privacy-Based Blockchain for Industrial Internet-of-Things". IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4156-4165, June 2020.

[6] Mougayar,W. "The Business Blockchain: Promise,Practice,and Application of theNext Internet". Wiley,2016.

[7] Wattenhofer,R. "The Science of the Blockchain". Inverted Forest Publishing, 2016.

[8] Tapscott Don and Alex Tapscott. "THE BLOCKCHAIN REVOLUTION & Higher Education". Education Review, 2017(2):24-25.

[9] YANG Xianmin, LI Xin, WU Huanqing, ZHAO Keyun. "The Application Model and Challenges of Blockchain Technology in Education". Modern Distance Education Research,2017(02):34-35.

[10] QUAN Lixin, XIONG Qian, XU Jianbo. "Application of Block Chain Technology in Circulation of Digital Educational Resources". E-education Research,2018(8):30-35.

[11] L. Zhu, et al., "Controllable and trustworthy blockchain-based cloud data management". Future Generation Computer Systems, February 2019, vol. 91, pp. 527-535.

[12] Wolfe university: the first blockchain university. [Online], available: https://woolf.university.

[13] Sharples, M., & Domingue, J. (2016). "The blockchain and kudos: A distributed system for educational record, reputation and reward". Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 9891 LNCS, pp. 490–496).

[14] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

[15] Baumgart I, Mies S. S/Kademlia. "A practicable approach towards secure key-based routing". In: Proc. of the 2007 Int'l Conf. on Parallel and Distributed Systems, Vol.2. IEEE, 2007.1−8.

[16] Bitswap. [Online], available: https://github.com/ipfs/go-bitswap.

[17] Hyperchain. [Online], available: https://www.hyperchain.cn/products/hyperchain.

[18] Chunrui Chen, Wanjun Liu. "Construction of High Coheres and Low Coupling Software Archiitecture". Computer Systems & Applications, 2009(07):21-24.

[19] Dubbo. [Online], available: http://dubbo.apache.org/en-us/docs/user/preface/background.html.

[20] Redis. [Online], available: https://redis.io/documentation.

[21] Johnson D, Menezes A, Vanstone S. "The elliptic curve digital signature algorithm (ECDSA)". Int'l Journal of Information Security,2001,1(1):36−63.