Received: 16 September 2020 | Revised: 15 March 2021 | Accepted: 30 March 2021

DOI: 10.1002/cpe.6330

SPECIAL ISSUE PAPER

WILEY

EduChain: A highly available education consortium blockchain platform based on Hyperledger Fabric

Xiubo Liang | Qian Zhao | Yanyu Zhang | Hongyu Liu | Qifei Zhang

School of Software Technology, Zhejiang University, Ningbo, China

Correspondence
Qifei Zhang, School of Software Technology, Zhejiang University, Ningbo, China.
Email: cstzhangqf@zju.edu.cn

Summary

With the problems of data sharing and information diddling in the field of education, we construct a highly available education consortium blockchain platform to ensure trusted sharing and privacy protection of education data. We employ erasure codes to process blockchain ledger files and optimize the data storage model according to the characteristics of education data, which can reduce the storage volume effectively. A HotStuff consensus algorithm is designed to access the ordering service of Hyperledger Fabric. A suitable educational blockchain network architecture based on the node complexity of education scenarios is proposed to achieve the high availability of the platform. To manage the education blockchain network, we implement the Fabric deployment based on Kubernetes and achieve the goal of including chaincode into Kubernetes environmental management. To improve the resource utilization of chaincode, we explore the new way of chaincode management by the functional computing service. Finally, on the premise of ensuring a 1/2 fault tolerance rate, the total ledger has decreased by 53.56%. Our platform enhanced the Byzantine fault tolerance while ensuring higher efficiency. Experimental results show that our platform is quite suitable for education scenario with many nodes.

KEYWORDS

blockchain, consensus algorithm, erasure codes, Hyperledger Fabric, serverless function computing

1 | INTRODUCTION

With the emergence of the Internet, a new model of "Internet + Education" in the education field occurs. This model employs the Internet technology to realize the structural reform of the education system. However, there are still two problems in the development of education reforms. On the one hand, the record data of current educational institutions which include students' learning behaviors and results are scattered in various departments, and some educational institutions have not yet realized digital management. Although the certificate issued by the educational institutions largely shows that the achievements of the learners during the study period, the demand of 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, the school-centered educational institutions ensure face-to-face teaching, teaching quality assuring, teaching activity monitoring and learning certificating. Only the campus circulation causes information alone. 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 are becoming the most critical means

Zhejiang cultural relic protection science and technology project 2019009.

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.[1] As the basic data in the field of education, students' learning record data will play an important role in the future. In the era of network and digitalization, traditional educational institutions lack the sense of reform. 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 will effectively solve the problems which are characterized by decentralization and high-trust. Although there have been some blockchain applications in the field of education, 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.[2] Blockchain technology is regarded as another disruptive technology after cloud computing, the Internet of Things and big data, which is highly concerned by governments, financial institutions and technology companies.[3] 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. We hoped that this technology can promote the reform of the education system to build an education information system, and this system is compatible with the national economic, social and educational development level.

Promoting the reform of the education system is an exploration attempt of blockchain technology in the field of education.[4] Compared with the financial field, the education field has more diverse scenarios where it has more complex data types and more caution in data privacy protection.[5] At the same time, the deficiencies of blockchain in storage and computing are particularly prominent in education scenarios. In terms of storage, Hyperledger Fabric[6] lacks an effective ledger capacity optimization mechanism, where the blockchain ledger is an append-only file. When used in education scenarios, the ledger will grow very quickly, which will cause much storage pressure to the severe nodes that save the ledger. In terms of consensus, it still lacks the ability to deal with the Byzantine fault although Hyperledger Fabric has introduced Raft consensus to enhance the decentralized feature of the platform, which cannot avoid the malicious node through its own operating mechanism. This cannot meet the high security requirements of data in the education field. Next, high availability is one of the core issues that the blockchain needs to solve urgently.[7] Next, how to efficiently coordinate the resource scheduling issues among the many nodes of the education blockchain is a problem that must be solved.

In this paper, we propose a highly available education consortium blockchain platform based on Hyperledger Fabric. Different from previous works, we proposed a series of optimization schemes, and the contributions of this paper are as follows.

1. This paper designs a data transfer mechanism to ensure the credible sharing and verification protection of education data. Meanwhile, we propose a data collaboration scheme based on "onchain and offchain", where the web application and the blockchain system are built with microservices. Considering the storage advantages of the four data-tier storage components of MySQL, Redis, IPFS, and Hyperledger Fabric, we build a high available education consortium blockchain platform.
2. This paper uses erasure codes to process blockchain ledger files. The scheme can reduce the storage pressure effectively by dividing the raw file into multiple slices and distributing them to other nodes, which can reduce total ledger storage within the network. On the premise of ensuring a 1/2 fault tolerance rate, the total ledger has decreased by about 53.56%. Considering the particularity of the education, this paper proposes to design a HotStuff consensus to access the ordering service of Hyperledger Fabric, which can introduce the Byzantine fault tolerant ability to the platform.
3. This paper completes Fabric deployment based on Kubernetes in order to solve the education blockchain run time environment problem. In the chaincode part, we designed a brand new container control plug-in for Fabric to support Kubernetes at the code-grade, which achieves the goal of including chaincode into Kubernetes environmental management. And we explore the new way of chaincode management by the functional computing service to maximize the utilization of computing resources.

2 | RELATED WORK

In recent years, the unique performance of blockchain in the "trust mechanism" has won the attention. However, the current blockchain is not enough to be flexibly applied to any scenario, especially in the education field with many limiting factors. Therefore, "Blockchain + Education" still faces many challenges.

2.1 | Blockchain + Education

At present, all walks of life have begun to pay attention to blockchain technology, and they 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 for combining blockchain with IOT, edge computing, and energy sharing fields, which will promote new breakthroughs in the development of the industry[8,9] 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 they pointed out the irrationality of applying blockchain technology. More researchers believed that blockchain technology will play a master role[10,11] 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 was including rebuilding the classical pedagogy model and promoting the reform of the higher education training model.[12]

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: a big data for education, a platform for education Taobao, a degree certificate system, an open education ecosystem, online learning and decentralized education system.[13] Considering the current difficulties of education resources on liquidity and sharing, Lixin Quan proposed the construction of a dual-blockchain combined with smart contract resource circulation model. Meanwhile, they created a digital resource registration chain and circulation information chain to promote education resource mobility and sharing.[14] To overcome the shortcomings of blockchain technology in storage capacity and data management, the industry had tried to combine blockchain and cloud storage technology to introduce authority nodes and then expand the controllability of system data.[15]

Woolf University, the world's first blockchain university, was a challenger to traditional education models, whose management 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".[16] 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,[17] 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.

2.2 | Consistency and storage

In terms of ledger storage, each block will retain the hash value of the previous block in the block header since the blockchain adopts a hash chain structure to organize data. Based on the characteristics of the hash, any point that occurs in the precursor block will lead to changes in the content of subsequent blocks, so the block ledger continues to grow in an append-only manner. Under such circumstances, the volume of the ledger will become larger and larger. For example, in Bitcoin, the current ledger has exceeded 600 G. With the increasing number of transactions, nodes will be fewer and fewer capable of maintaining the full ledger in the future. Therefore, the system tends to be more centralized than the original intention of the Bitcoin network. Such problems will be more obvious in the new generation of blockchain platforms. Because the new generation of blockchains is committed to being applied in more scenarios and the data will be more complex, so it is necessary to design effective solutions to solve the problem of ledger storage. For this problem, the current solution mainly has two directions:[18] (1) Reducing the traceability of the blockchain to release the storage burden of the ledger maintenance node, such as archiving or deleting part of the cold data to reduce the ledger volume; (2) Using technologies to realize the scalability of the blockchain system and improve the utilization of ledger data, and reduce redundant data, such as the integration of multiple chains and cross-chain interoperability.

Early blockchain consensus algorithms had the disadvantages of high-energy consumption and low efficiency, which greatly hindered the implementation of blockchain systems in other fields. At present, many new consensus strategies have been proposed in the industry to effectively avoid the problems of early blockchain consensus. According to different applicable scenarios, blockchains are divided into public blockchain and consortium blockchain, and these two different blockchains also have different requirements for consensus algorithms. In the public blockchain, nodes can freely join the network. Therefore, while pursuing high efficiency, it is also necessary to ensure that the consensus has high scalability. At present, there are three ways to improve consensus in the public blockchain:[19] (1) Combining more Different mechanisms to achieve the highest efficiency,

such as Ontology; (2) Using a shard strategy to achieve parallel consensus, which will block the blockchain network into shards. The consensus mechanisms in multiple network shards will be parallel execution, and the representative platform is Ethereum 2.0; (3) Dividing the network structure into layers to share the pressure of the underlying network consensus, such as Lightning Network, Nervos, etc. The identity of each node is known in the network in the consortium blockchain consensus algorithm, so it can be combined with more effective identification methods to ensure the authenticity of the message, such as various signature algorithms. Consortium blockchain consensus adopted the PBFT algorithm in the early days, but the algorithm has a higher communication complexity. As the number of nodes increases, it will bring higher costs when switching between communication and view. At present, the blockchain platform for the consortium blockchain has introduced more efficient consensus, such as Tendermint, HotStuff,[20] libraBFT[21] and other algorithms.

2.3 | Fabric runtime environment

Kubernetes(K8s) and Fabric are two typical technology platforms in the field of cloud computing and blockchain. The basis for deploying Fabric on K8s is that Fabric components are encapsulated in containers, and K8s is a powerful container management platform. Container technology provides standardized deployment, operation and maintenance capabilities for applications in different environments, which reduces the complexity of fabric deployment to the cloud platform.[22]

Hyperledger Fabric was born in the cloud-native era. It provides an isolated and portable cross-platform deployment based on Docker. In the cloud era, K8s has become the standard for container management in the container cloud field.[23] Fabric does not provide support for K8s, and its cloudification needs to do some K8s support transformation work. In recent years, serverless function computing technology has entered our field of vision. It handles stateless and simple services through function instances to achieve efficient scaling. Its biggest advantage is that developers only need to develop functions, and they do not care about server deployment management. Similarly, Fabric's chaincode mechanism allows ordinary developers to also not care about the blockchain network but focus on the development of the chaincode. Fabric chaincode and function computing service have overlapping similarities, but Fabric chaincode lacks the efficient scalability of function computing service.[24]

3 | SOLUTION

As shown in Figure 1, the EduChain platform proposed by this paper consists of seven parts: data sharing consortium, Hyperledger Fabric, private IPFS cluster, Web application service, relational database cluster, cache database cluster, and consortium blockchain runtime platform. The three types of organizational structure participate in the consortium blockchain as authoritative nodes, which includes the Local Education Bureau (LEB), the Local Human Resource Center (LHRC) and the Local Bureau of Industry and Commerce (LBIC). For ease of description, we construct a prototype of the comprehensive quality assessment system for students based on the EduChain, which 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 it provides

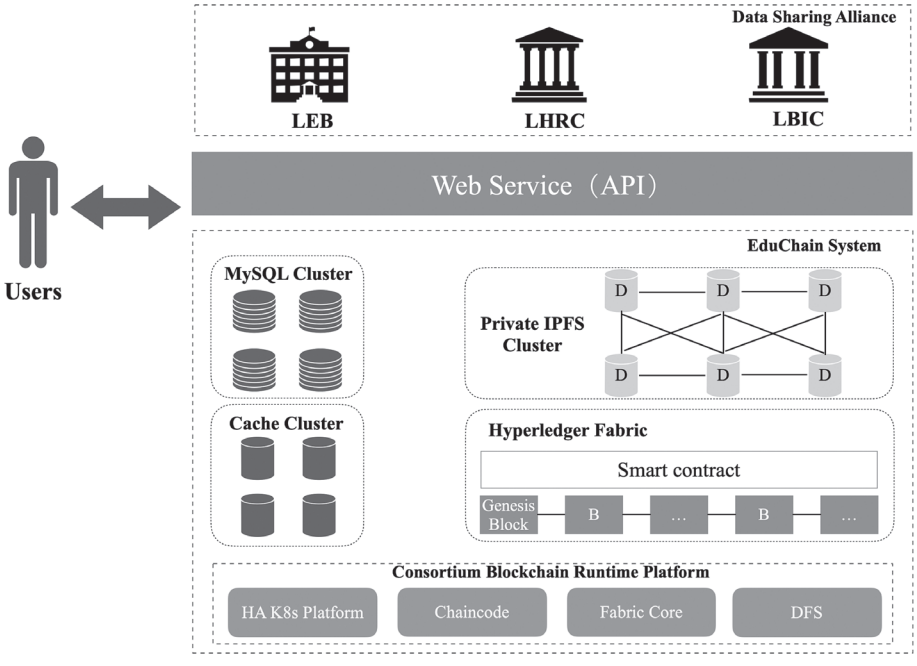


FIGURE 1 System architecture

services to the outside 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.[25] The private IPFS cluster stores the original information of the encrypted data files. It ensures data security through distributed DHT,[26] Bitswap[27] and other technologies. We use Hyperledger Fabric as the basis platform of the education consortium blockchain. For the characteristics of the data volume and security of the education scene, we have optimized the storage and consensus algorithm of Hyperledger Fabric. On the premise of ensuring a 1/2 fault tolerance rate, the total ledger has decreased by about 53.56%. And Byzantine fault tolerance was introduced into the platform. In order to ensure the stable operation of the education blockchain system, we design and implementation of Fabric deployment based on K8s. Especially the chaincode part, we design a new brand container control plug-in for Fabric to support K8s at the code-grade, and we achieve the goal of including chaincode into K8s environmental management. Each component of the EduChain platform will be discussed in detail below.

3.1 | Network architecture of EduChain

In the consortium blockchain, every entity that newly joins the consortium blockchain network participates in the consensus process and maintains the full amount of data in the blockchain, which acts as a node in the network. The entity organizations involved in this system include universities, government management departments and enterprises. According to incomplete statistics, as of June 2019, the number of universities in China is about 2956, and the number of corporate organizations is countless. In the system, every university and enterprise that participates will need to provide resources and equipment to deploy and maintain the consortium blockchain system, which will lead to huge resource costs and the current consortium blockchain cannot support it. With such a large network of nodes, large-scale nodes will also lead to a sharp decline in the performance of the blockchain system. Based on the analysis of the above actual demands, this paper proposes a consortium blockchain network architecture suitable for the "Blockchain + Education".

As shown in Figure 2, the blockchain network nodes are planned according to provinces. The three entity organizations (LEB, LHRC, and 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 use the services provided by the system as users.

The system account adopts hierarchical authority management structure, as shown in Figure 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), 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).

3.2 | Storage

3.2.1 | Erasure code processing ledger

In order to reduce the storage pressure of each node, we divide the ledger into multiple pieces, and each node in the network only retains a part of file slices. But this will bring risks, other nodes cannot restore the file if one of the nodes leave the network.

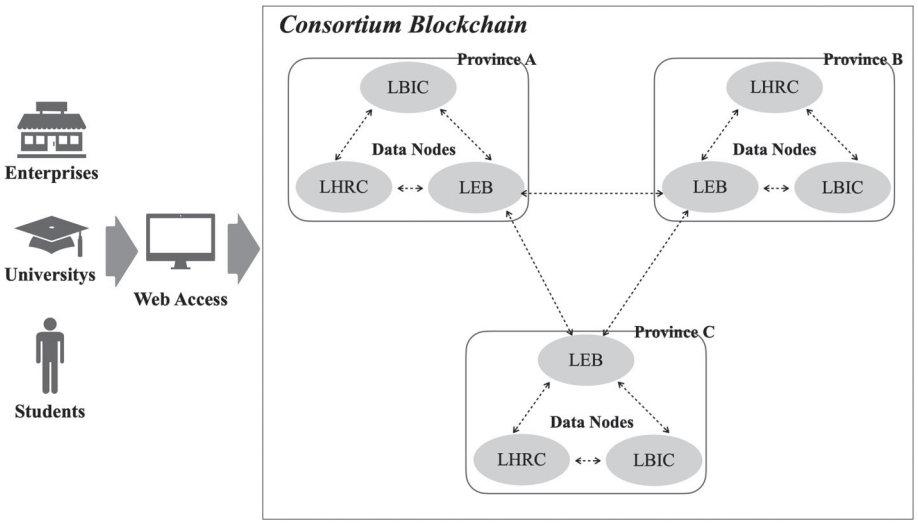


FIGURE 2 Network architecture of the consortium blockchain

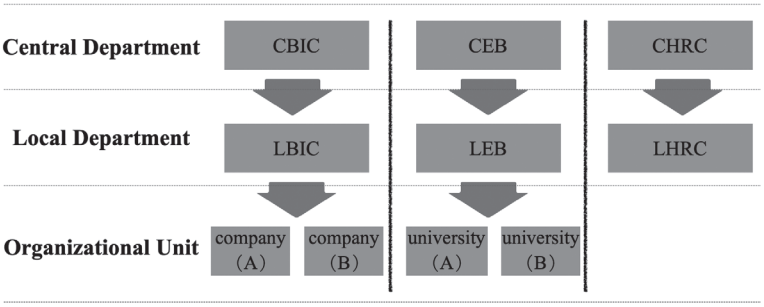


FIGURE 3 System account hierarchical management structure

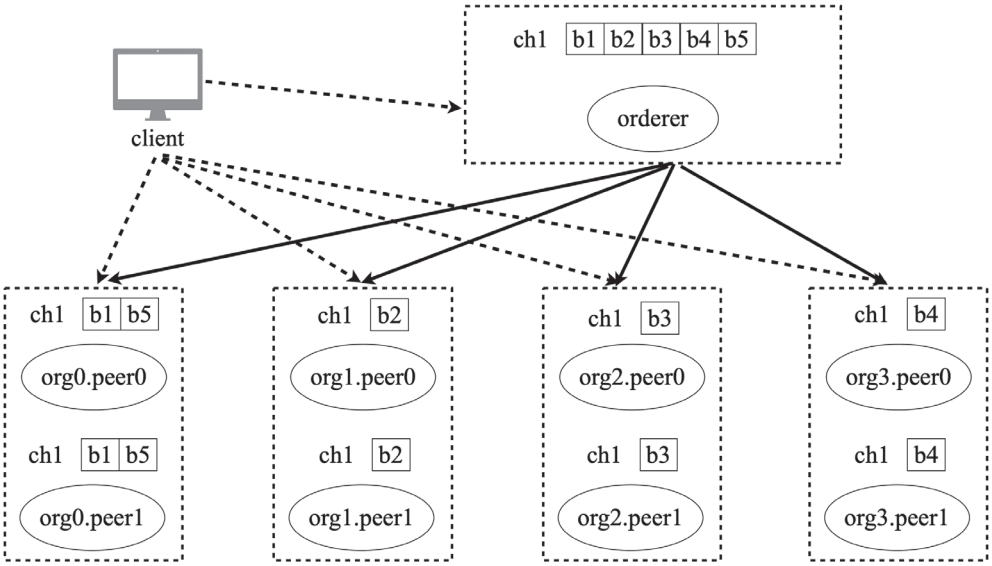


FIGURE 4 Erasure Code Processing Ledger File Model. Channel(ch), Block(b), Organization(org)

As Erasure Coding (EC) is widely used in data protection, it can divide the data into multiple pieces and add redundant data blocks at the same time. By using EC, the entire system can tolerate a certain amount of file block loss, and the degree of tolerance depends on the number of redundant data blocks. Similarly, Hyperledger fabric also use file to store the block data, and a new file will be created to append new block whenever the file size reaches the threshold.

Figure 4 shows the specific design plan. The Orderer node will monitor the increasing of the ledger file. When the ledger file reaches the threshold, a mapping table will be created, which records the order of file slices and the keeping node of each file slice. The mapping table will issue to peer node in pub-sub mode, and peer node will perform the following two operations after getting the mapping table:

1. Using EC to encode the ledger file;
2. Deleting the file slice which does not belong to itself.

3.2.2 | High availability caching scheme

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

As shown in Figure 5, machine A holds virtual IP(VIP) while $HARedis_A$ and $HARedis_B$ establish two-way heartbeat service to detect the service status. $RedisA_1$-$RedisA_n$ is nth master nodes, and $RedisB_1$-$RedisB_n$ is nth 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

FIGURE 5 HARedis system workflow

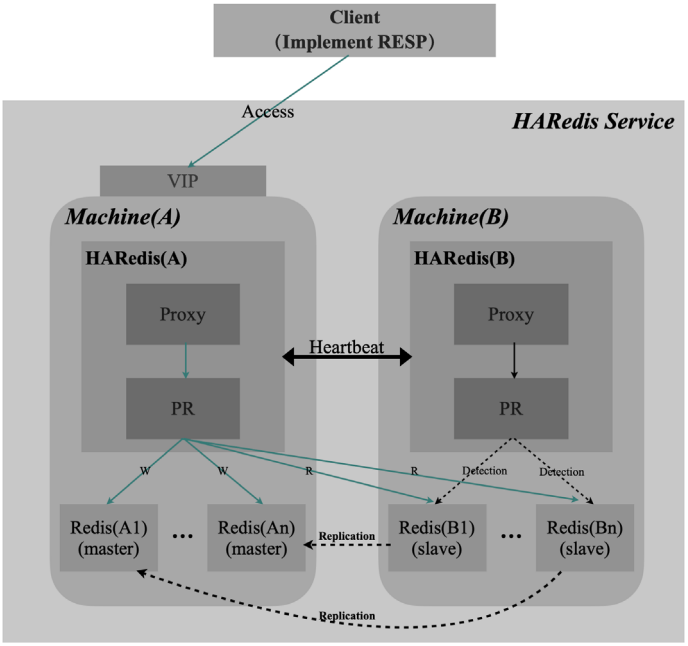


table. Then, it sets $RedisB_1$-$RedisB_n$ as the master node and set the VIP to machine B. Finally, it tries to connect to $HARedis_A$. When machine A is recharged, $HARedis_A$ and $HARedis_B$ establish bidirectional heartbeat detection service again and update their respective route table, and $HARedis_B$ 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

- Reading and writing 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 interaction of TCP is needed with Redis Pipeline, which saves the network overhead of Proxy greatly.

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) are used. The results are shown in Figure 6, and the Proxy's QPS is stable around 120,000 QPS.

3.3 | Sharing strategy

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,

TABLE 1 Test environment configuration

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

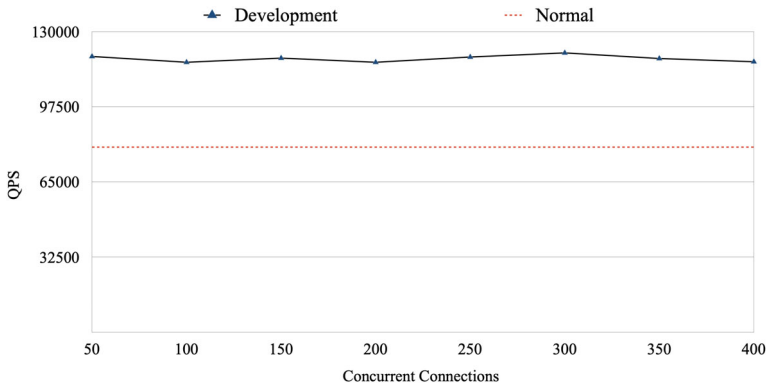


FIGURE 6 Result of Redis-benchmark test

announcements, operations, shared records and student assessment files. Among them, the details of the students' assessment information in the student assessment files are 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 are kept 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 the main data source 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.

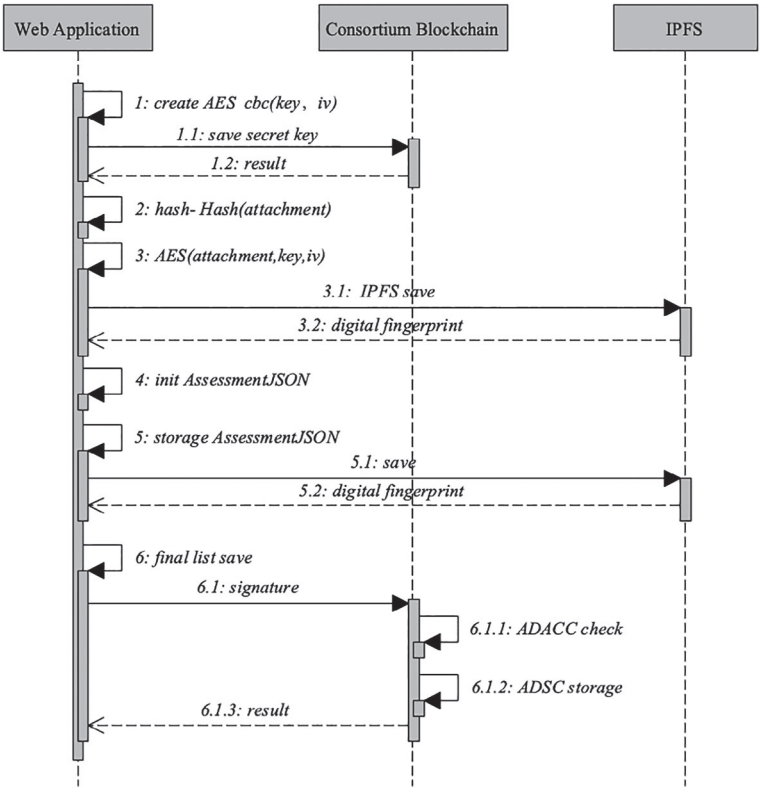
Student assessment data are stored on the blockchain for protecting, where we use the web application system smart contracts and the IPFS private cluster. Therefore, it prevents the student assessment data from being tampered and destroyed illegally, and it ensures verification, traceability and recovery of assessment data through consortium blockchain. As shown in Figure 7, 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 are 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 Figure 8:

1. 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.
2. Encrypted file EncryptAttachments are generated by using cbc (key, iv), and hash value (Hash)is got by hashing the attachment.


```
{
    "AssessID": "D67fff524e2da4c9b9e0fb4c589493351",
    "CreateDate": 1582861910954,
    "Admin": "Ue52996baf9c94708a601f977c10b3c59",
    "Title": "2018 Alibaba Cloud Global Blockchain Competition",
    "Description":
    "XXX(21851888), participated in the 2018 Alibaba Cloud Global Blockchain Competition
    and won the second prize in the finals in September 2018. Project: XXX trading",
    "category": 3,
    "status": 1,
    "Attachments": [{
        "ID": "F2fec4cf19b2a44169f1171d552d28064",
        "Title": "2018 Alibaba Cloud Global Blockchain Competition Certificate of Honors",
        "Hash": "a5c1815080f22e3b3437c32fd6c50758",
        "IPFS": "QmSoLV4Bbm51jM9C4gDYZQ9Cy3U6aXMJDAbzgu2fzaDs64"
    }]
}
```


FIGURE 7 Structure of JSON of assessment data

FIGURE 8 Flow chart of data storage



3. EncryptAttachments are stored the in the IPFS cluster with calling the IPFS storage interface to get its file fingerprint IPFS.
4. Combined with other attributes of the assessment data, the AssessJSON object is constructed.
5. We use cbc (key, iv) to encrypt the newly constructed AssessJSON object and store it in the IPFS cluster to obtain IPFS.
6. The ECDSA algorithm is used to sign AssessID, UID and Hashand IPFS, and then we obtain a signature.
7. The ADSC contract will be called to store the assessment data after we call the ADACC contract to verify the signature through the SDK.

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 by technological innovation. The traditional education data is promoted to produce value safely and reliably. The specific process is shown in the following Figure 9.

1. Student A (UID-A) uses the private key SK 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.
2. Enterprise user B (UID-B) uses the private key SK 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 will be returned after passing the check.
3. UID-B uses the IPFS Address to obtain the encrypted assessment data object (IPFS) from the IPFS cluster. And UID-B obtains the decryption key of IPFS in UID-A with an asynchronous https request.
4. UID-B uses cbc <key, iv> to decrypt IPFS for getting 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.

This platform combines the advantages of Web and blockchain to ensure the safe sharing of student assessment data. The original information of student quality assessment details is stored in the IPFS file system, and their data fingerprints are stored on the chain by Hyperchain through encryption. In the data query process, the original data in the Hyperchain and IPFS systems are uniformly requested through the Web system and exposed to the application side through an interface.

The storage operation is mainly undertaken by the IPFS cluster, fully combining the respective advantages of the IPFS cluster and the blockchain system, and storing the encapsulated data in the blockchain network. The data update operation is the process of storing and protecting each newly constructed AssessmentJSON. In the process of assessment data verification, when data abnormalities are found in the IPFS cluster, the information

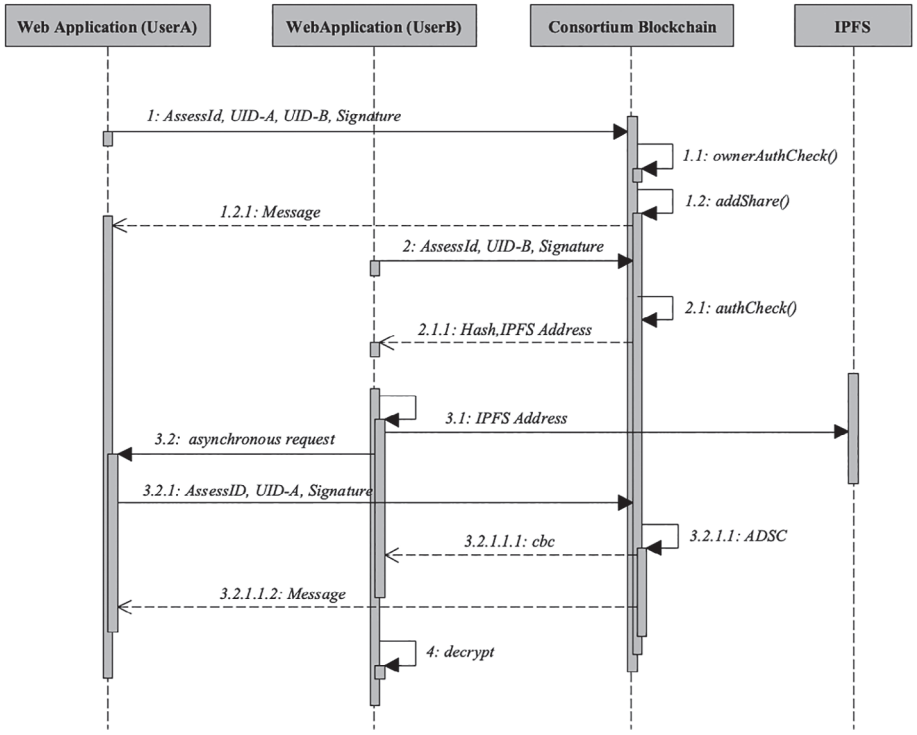


FIGURE 9 Flow chart of data sharing and acquisition

in the ADSC contract of the consortium blockchain can be restored to any correct version of the student assessment data. At the same time, when the local database information fails the verification, the consortium blockchain and the IPFS system can jointly restore and verify the student's assessment information to ensure the credibility of the data.

3.4 | Consensus algorithm

So far, Hyperledger Fabric only support CFT-level consensus algorithms, which means malicious node may degrade the reliability of the system. HotStuff is an efficient BFT consensus algorithm, and it can be used in the consortium blockchain system.

Hyperledger Fabric uses a channel design, and each channel maintains a separate consensus mechanism instance. All consensus mechanisms need to be coupled with the upper-layer message mechanism of Hyperledger Fabric by the two interfaces of Consenter and Chain. Consenter represents a sort of sorting mechanism, which only contains the HandleChain method, which creates a Chain type reference based on the resources provided by the upper layer. The chain represents a concrete consensus algorithm instance. The interface needs to implement some message injection methods, which will be used for ordering services. For example, the Order and Configure in this interface send the received messages of normal or configuration type to sorting service for processing. Figure 10 is the structure diagram of the Hyperledger Fabric consensus module.

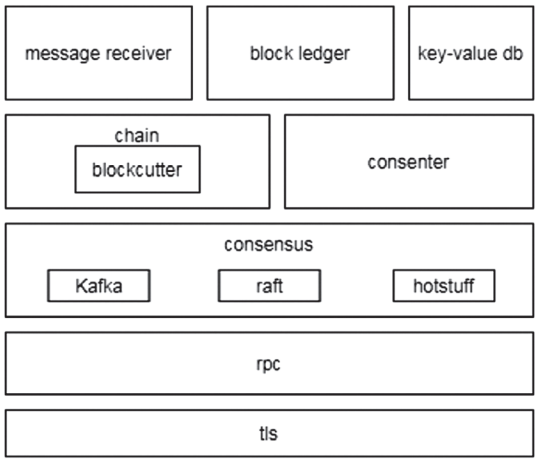


FIGURE 10 Hyperledger Fabric consensus module

In the implementation of HotStuff, the basic HotStuff model is mainly divided into four processes, but the chained HotStuff method is usually used in the actual application process. After the four stages of the basic HotStuff are analyzed, the pipeline mode can be adopted. Each stage is attempted to switch, so that each message proposal has a separate view number. The types of messages are reduced, and the transaction processing is improved. The schematic diagram is shown in Figure 11.

Each view number corresponds to a leader. The leader of the current view number will put the voting information received in this view into the QC (Quorum Certificate) and send it to all replicas together with the proposal. After the copy voting is completed, the result is not returned to the original leader but sent to the leader of the next view. According to the basic HotStuff process, the leader of the new view should enter the Pre-commit phase to verify the proposal of the previous view, but the chained HotStuff does not adopt this method. The leader of the new view will receive the voting message as a new in the Prepare stage, and the proposal is sent to other replica nodes for verification. In this mode, the result of the new view can pass the threshold signature verification, which means that the result submitted by the previous view is credible. Figure 12 shows the interaction mode between the leader node and the slave node in a view.

This paper implements the HotStuff algorithm and replaces the original consensus algorithm of Hyperledger Fabric. The access of the consensus algorithm fully refers to the design plan of the Raft consensus, effectively utilizes the original communication mechanism of Hyperledger Fabric, realizes the decoupling of the consensus algorithm and the upper-layer mechanism, and completes the consensus replacement work

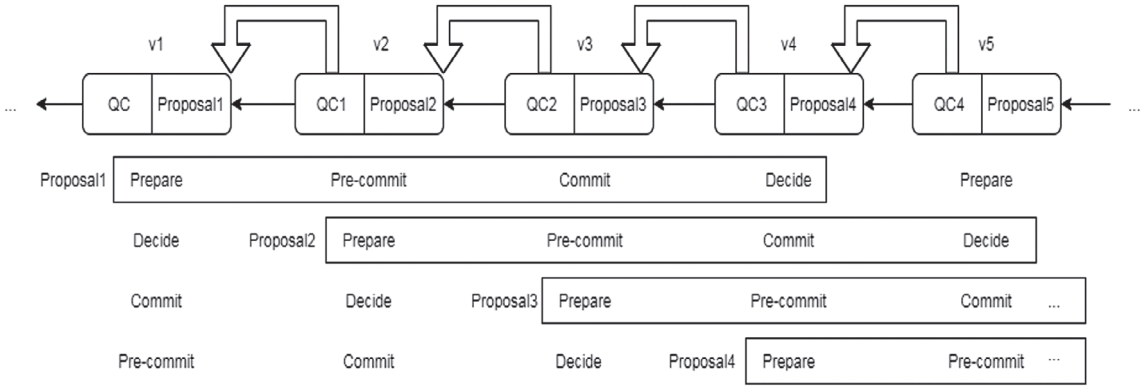


FIGURE 11 Schematic diagram of chained HotStuff

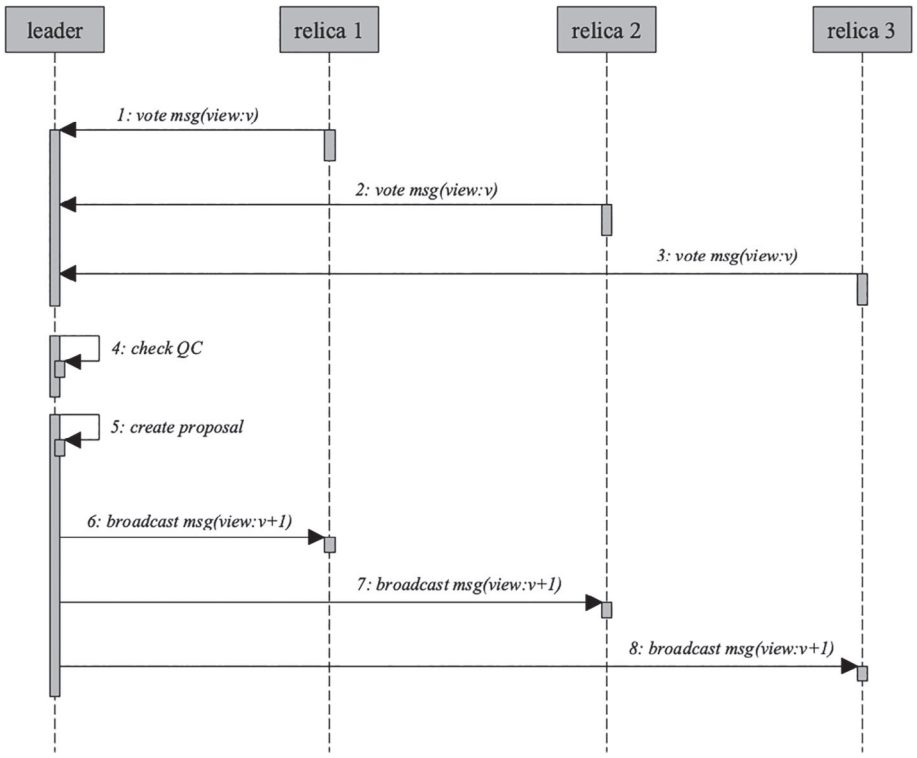


FIGURE 12 Single view timing diagram of chained HotStuff

without intruding the upper layer functions. In addition, the implementation of the algorithm itself provides Hyperledger Fabric with a consensus mechanism that supports Byzantine fault tolerance, which is closer to the design concept of the blockchain, and enables the platform to cope with diverse application scenarios.

HotStuff introduces a threshold signature technology. Each round of consensus voting messages is sent directly from each replica node to the leader node. The leader uses the corresponding algorithm to generate an aggregate signature, and then broadcasts the new message to other nodes. That is, there are a total of n nodes in the system, all nodes share a public key, but each node has its own private key. Each node signs a message m with its own private key, which is called a partially signed message. The leader uses multiple nodes m to generate a joint signed message. When at least $k = 2f + 1$ nodes provide a partially signed message, any other one The node can verify the joint signed message with the public key. Where f is the total number of Byzantine nodes that the system can tolerate, then $n = 3f + 1$. HotStuff is $O(n)$ linear complexity. Even when f leaders fail, the linear authentication complexity of $O(fn)$ can still be maintained.

3.5 | Runtime environment

The core system proposed in this question can also be divided into two layers. The bottom layer is the high-availability Kubernetes platform and the distributed file system, and the upper layer is the Fabric blockchain platform. The system architecture is shown in Figure 13. The highly available Kubernetes system is the hosting platform for the upper-level business, which carries all the service pressure of the upper-level. As a container management platform, Kubernetes must provide the upper-layer Fabric with efficient container orchestration management capabilities, and reasonably distribute application components to healthy nodes in the computing cluster.

The blockchain network layer is located on the high-availability Kubernetes platform. This layer does all the business logic of the blockchain. Fabric has two parts: static components and dynamic chaincodes. Static here means that related components are started when the network is deployed, and dynamic mainly means that the chaincode is started when the blockchain business is instantiated during the operation phase. The division of dynamic and static is related to the deployment design of the Fabric network on Kubernetes. In terms of chaincode management, the architecture adds a functional computing management module. The transformed chaincode container shares the computing node. The container will exit immediately after the calling task ends, and computing resources will be released.

Fabric is a highly plug-in system, and the runtime part is also pluggable. Its complete operating cycle includes initialization environment, chaincode installation, chaincode instantiation, chaincode upgrade, and chaincode invocation. We can build a runtime plugin that supports K8s management at code level. Docker is an underlying runtime environment of K8s, so the construction and compilation of chaincode images can be reused. In the K8s cloud environment, it is also necessary to provide a system for uploading, downloading and distributing images in the cluster. The principle of the K8s runtime plugin is to implement chaincode installation and instantiation functions according to the runtime interface of Fabric.

The chaincode installation will push the chaincode image through the docker client, and the chaincode instantiation complete the chaincode scheduling, image pull, container creation and startup through K8s client. In Docker environment, the health monitoring of the chaincode container is implemented through Docker's PingWithContext; In the K8s environment, a healthy service can be opened in the shim package of the chaincode for the port-level health monitoring. Summarize the implementation principle of the Fabric K8s runtime plugin:

1. Deploy a mirror repository service in the K8s cluster.
2. Build a plug-in to implement the runtime interface of Fabric. The chaincode installation and deployment and operation functions are respectively completed by encapsulating Docker and K8s client.

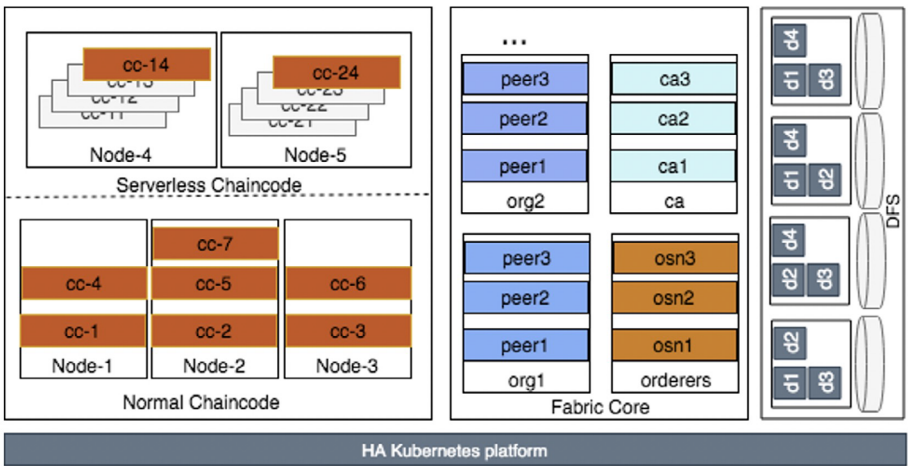


FIGURE 13 Runtime environment architecture. Chaincode(cc), Ordering Service Nodes(osn), Data(d)

3. Health monitoring, add a Heathz service to the shim package of the chaincode for Fabric to realize the health status judgment of the chaincode container through the K8s client.

4 | EXPERIMENTAL RESULTS AND DISCUSSION

Large amount of data, high data security, and strong system stability have always been prominent features of the education scene. This paper design an EduChain platform based on the education field. In order to verify the platform's capabilities in storage capacity, system fault tolerance and system resource management, we conducted a series of experiments.

4.1 | Storage model

This paper tests the processing of Hyperledger Fabric ledger files with erasure codes. The system topology diagram of the storage module test is shown in Figure 14.

In storage optimization trails, we set up four organizations, each organization contains two peer nodes. All nodes are running in Docker, each node has 1G of memory capacity and 10G of disk capacity.

In the first experiment, we mainly focus on the impact of different EC tolerance rate on whole network storage, the fault tolerance rate can be affected by adjusting the ratio of the raw data and the redundant data, Figure 15 shows the difference. The storage size of the whole network decreases when we use EC to encode the ledger file, and the degree of decline is related to the preset tolerance rate. On average, the size of each organizations' ledger will decrease as the number of organizations increases, because the total ledger capacity is certain when EC is used.

Suppose that we have n organizations in the network, each organization has m peer nodes, and the size of ledgers on every peer node suppose to be s. The total size of the network ledger is $m * n * s$. When we introduce EC to optimize the storage, we need to preset a fault tolerance, suppose to be y. Through the EC algorithm, the capacity of a single ledger will be expanded to $s/(1 - y)$. Because the file blocks are allocated according to the organization, peer nodes in the same organization will keep same data. The size of the overall network ledger is $m * s/(1 - y)$. Ideally, the ledger capacity will be reduced by $n * (1 - y)$ times after using the EC algorithm.

It can be seen from experiments that the use of erasure codes effectively reduces the total amount of data storage in the blockchain network. In the scenario where erasure codes are used, the storage optimization effect is more obvious when the fault tolerance rate is low, but the reduction of the fault tolerance rate will not bring better benefits in storage space. In addition, when the amount of data in the ledger is relatively small, there

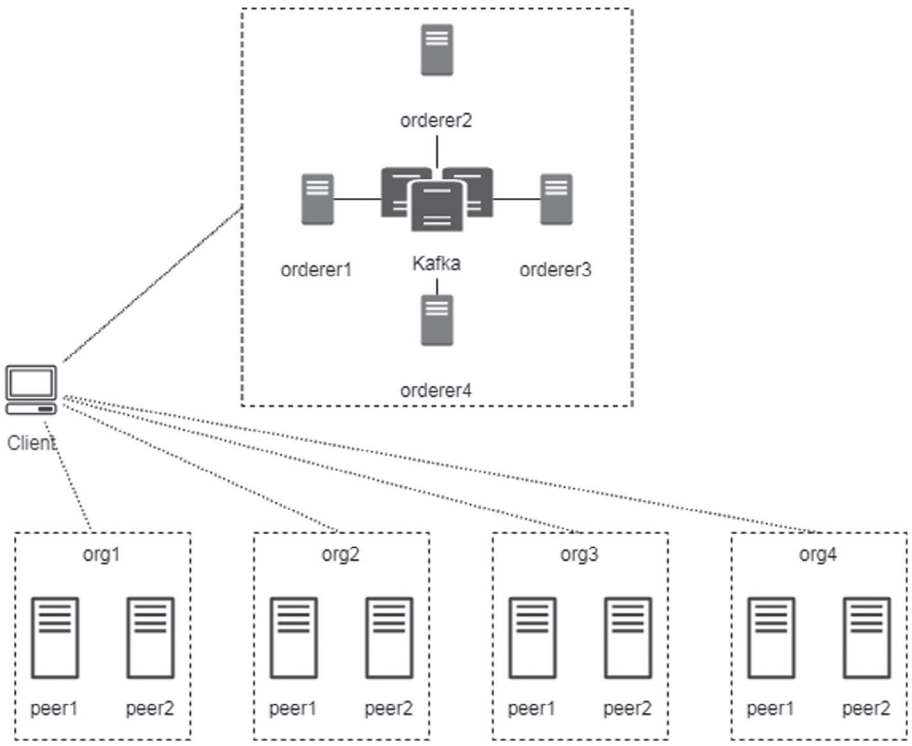


FIGURE 14 Erasure code processing ledger test network topology diagram

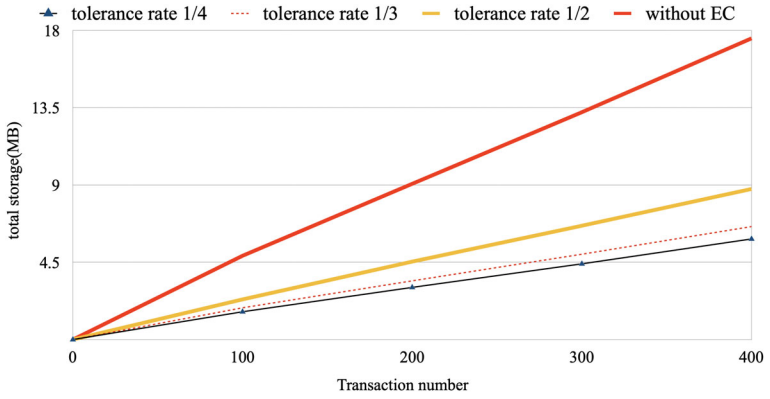


FIGURE 15 Network storage capacity under different fault tolerance rates

is no big difference between using erasure code to process the ledger and not using it. This is because when the amount of data is small, the erasure code algorithm will introduce redundant blocks. The size of the redundant data block is consistent with the size of the original data block. When the number of segments of the original data block is relatively small, the scene using erasure codes will not be particularly obvious compared with the scene not using erasure codes.

Under the original mechanism of Hyperledger Fabric, all peer nodes have a full amount of data, which is extremely reliable. After the erasure code algorithm is used, a certain degree of unreliability is introduced. When the failed nodes exceed a certain threshold, the processed ledger will be unrecoverable. However, the purpose of this design is to optimize space storage, it is necessary to combine actual scenarios to balance the reliability of the ledger and storage capacity.

In this paper, the file blocks obtained after erasure coding are allocated according to the organization. With the same fault tolerance rate, the increase in the number of organizations will not cause a change in the overall storage capacity, but due to the increase in the number of nodes, the storage pressure of each node will be proportionally reduced. Therefore, in the erasure code processing scheme designed for ledger files, the more the number of organizations, the more prominent the benefits of a single node in terms of storage.

4.2 | Consensus module

It can be seen from Figure 16 that the Raft consensus algorithm is better in terms of performance, while the overall difference between HotStuff and BFT-SMaRt is not much. As a high-performance CFT algorithm, Raft does not consider the situation of nodes doing evil. Compared with the other two consensus algorithms, it will be much simpler in message processing, so it will have an advantage in efficiency. Compared with BFT-SMaRt, there will be no significant gap between HotStuff and BFT-SMaRt when the number of nodes is small, and the advantages of HotStuff are mainly reflected in view switching. Since BFT-SMaRt is implemented based on the PBFT algorithm, its view switching communication The complexity has reached $O(n^3)$, and the complexity of HotStuff consensus switching has been reduced to O(n), so the advantages in this regard will be more obvious.

Scalability is an important indicator for the investigation of the blockchain consensus algorithm. Although there are restrictions on the participation of nodes in the consortium blockchain, the better scalability of the consensus algorithm means that it can component a larger-scale consortium. Scalability in the blockchain also has important reference value. In view of scalability, this round of testing will use 4, 8, 16 ordering nodes to test the three consensus algorithms. The specific method is to inject 100 transactions into the system through scripts, and examine the number of three consensus algorithms in different ordering nodes. The time required for execution.

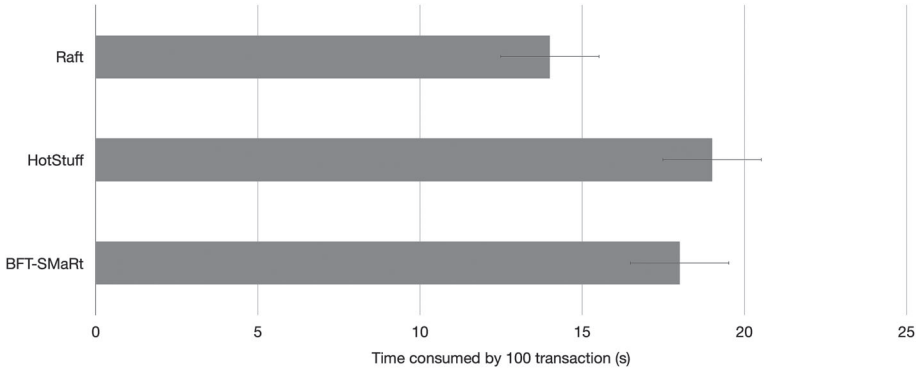


FIGURE 16 Efficiency comparison test

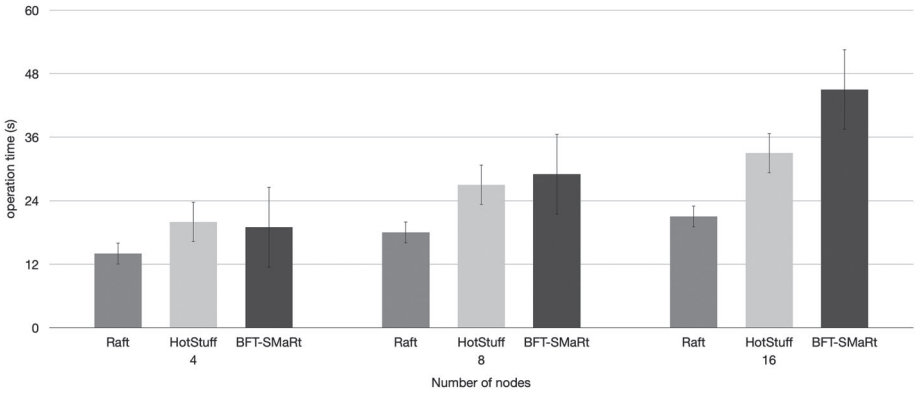


FIGURE 17 Scalability comparison test

It can be seen from Figure 17 that the three consensus algorithms often increase in processing messages after the increase of nodes, and the increase in BFT-SMaRt is the most obvious. In addition, experiments[28] show that the lowest-latency HotStuff point provides latency and throughput that are better than the latency and throughput simultaneously achievable by BFT-SMaRT at its highest throughput, while incurring a small increase in latency. HotStuff batches multiple operations in each node, which means that multiple operations can be signed at once. While the batches increase, the batching costs more than crypto, so the latency increases obviously.

4.3 | Chaincode performance

Fabric cloud deployment can be divided into static component deployment and dynamic chaincode management with K8s. In the chaincode deployment management part, we carried out secondary development on Fabric Peer, and realized the support of K8s at the code level by adding a K8sDockerVM controller plug-in.

The Fabric deployment test process is shown in Figure 18: First, create an isolated network and blockchain ledger, including three operations: create, join, and update. Then test the chaincode deployment, install, instantiate, and call chaincode in sequence, including install, instantiate, query, and invoke operations. Finally, the management chaincode is calculated by updating the chaincode test function, including install, upgrade, query, and invoke operations.

The chaincode in K8s and Docker differs in image management and operating environment. In this experiment, the performance of chaincode invocation after technological innovation is evaluated by the speed of task completion time under the same task amount. The test benchmark is the completion time of the chaincode in the Docker environment. Figure 19 shows the comparison of the chaincode call time in Docker and K8s environments. We find that the chaincode call performance of the K8s runtime plugin is similar to that of the Docker runtime. Experiments have proved that Fabric's cloud innovation in K8s will not reduce the efficiency of chaincode operation.

The management of Fabric chaincode is one of the core researches of this paper, and it is also the most complicated part of the Fabric cloud deployment. Public cloud vendors and the Fabric community generally build BaaS services based on Fabric and Kubernetes, but there are some problems in the chaincode deployment of those solutions. Alibaba Cloud manages the chaincode through some comprehensive auxiliary technologies. The Fabric Cello of the open source community manages the chaincode through DIND (Docker in Docker) technology, but none of these solutions incorporate the chaincode into the Kubernetes environment. In this experiment, a new chaincode management controller plug-in was added to support Kubernetes at the code level.

We also explored the application of functional computing service in the deployment and management of Fabric chaincodes. The current function computing service requires users to upload function code and its dependencies, and the remote service completes the compilation and storage of

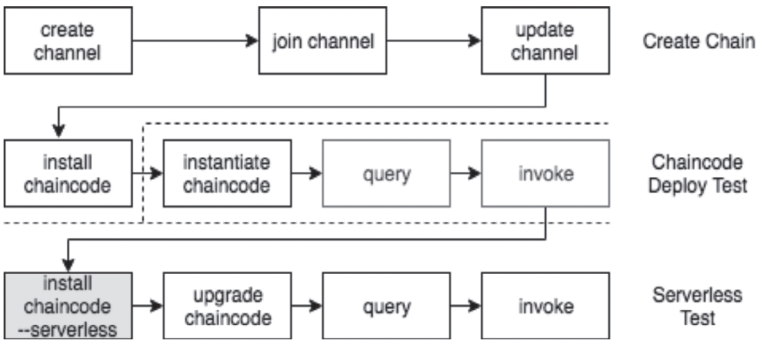


FIGURE 18 The Fabric deployment test process

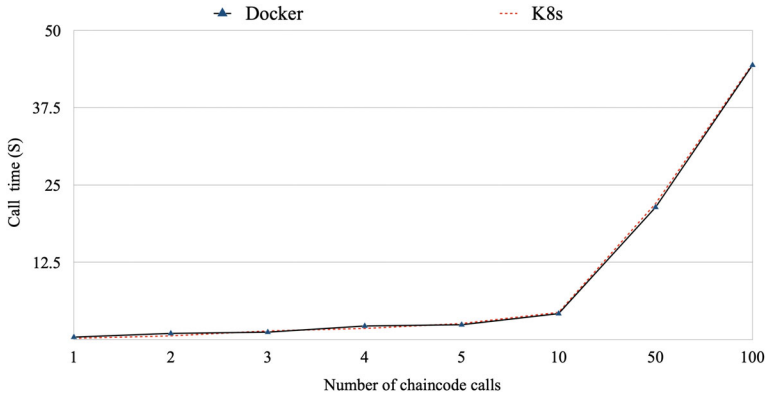


FIGURE 19 Comparison of chaincode call time in Docker and Kubernetes

the image. Due to the complexity of the dependency of Fabric chaincodes, it is temporarily impossible to directly use existing function computing services to complete remote compilation tasks. The experiments show that the execution mode of the chaincode instance is changed from "Resident waiting for call" to "Start when there is a call".

5 | CONCLUSION AND FUTURE WORK

In view of the present education institutions on education data management exists problems, such as decentralization, low utilization rate and unguaranteed security, and so forth, we design a highly available education consortium blockchain platform based on Hyperledger Fabric. 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 applications 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. According to the storage and fault tolerance problems of Hyperledger Fabric, this paper proposes to use erasure codes and HotStuff consensus to optimizes blockchain system for education data characteristics. In this system, we design and implement the Fabric deployment based on Kubernetes and achieve the goal of including chaincode into Kubernetes environmental management.

The structure of the Fabric consortium blockchain is similar to the serverless function computing. Ordinary developers only need to write chaincodes or functions without paying attention to blockchain networks or servers. The function instance is called on demand, and the instance is closed immediately after the end of the call. This mode can accommodate more low-frequency function calls without increasing computing resources. Drawing lessons from the idea of serverless function computing, we have made functional improvements to the runtime of Fabric so that it can be called when needed, and resources are closed as soon as the chaincode is called. The realization principle is to call the stop interface after the chaincode is successfully called to complete the destruction and release related resources through the K8s client. After innovation, the chaincode container will be restarted whenever the chaincode is called, so the chaincode container will take a long time to start. The significance of functional transformation is that it is very suitable for long-tail chaincodes that are not sensitive to calling time, thereby greatly reducing the resource consumption of low-frequency calls. The functional computing transformation of Fabric has given us a direction to improve the utilization of Fabric resources, but the dynamic marking of long-tail chaincodes is a difficult point, which needs to be solved with the help of big data and algorithm capabilities. This is our next step.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

ORCID

Xiubo Liang https://orcid.org/0000-0002-4749-5552

REFERENCES

1. White paper on data infrastructure; 2019. https://www.useit.com.cn/forum.php.
2. Nakamoto S. Bitcoin: a peer-to peer electronic cash system; 2008.
3. Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*. 2015.
4. Liang X, Zhao Q. On the design of a blockchain-based student quality assessment system. Paper presented at: Proceedings of the 2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS); 2020:1-7; Shenzhen, China. https://doi.org/10.1109/HPBDIS49115.2020.9130584.

5. Gai K, Wu Y, Zhu L, Qiu M, Shen M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans Ind Inform*. June 2019;15(6):3548-3558.
6. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. Paper presented at: Proceedings of the 13th EuroSys Conference; 2018:1-15.
7. Onik MMH, Miraz MH. Performance analytical comparison of Blockchain-as- a-service (BaaS) platforms. lecture notes of the institute for computer sciences. *Soc Inform Telecommun Eng*. 2019;285:3-18.
8. Gai K, Wu Y, Zhu L, Qiu M, Shen M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans Ind Inform*. 2019;15(6):3548-3558.
9. Gai K, Wu Y, Zhu L, Zhang Z, Qiu M. Differential privacy-based blockchain for industrial internet-of-things. *IEEE Trans Ind Inform*. 2020;16(6):4156-4165.
10. Mougayar W. *The Business Blockchain: Promise,Practice,and Application of theNext Internet*. New York, NY: Wiley; 2016.
11. Wattenhofer R. *The Science of the Blockchain*. Zurich: Inverted Forest Publishing; 2016.
12. Tapscott D, Alex T. The blockchain revolution & higher education. *Educ Rev*. 2017;2:24-25.
13. Yang X, Li X, Wu H, Zhao K. The application model and challenges of blockchain technology in education. *Modern Distance Educ Res*. 2017;02:34-35.
14. Quan L, Xiong Q, Xu J. Application of block chain technology in circulation of digital educational resources. *E-Educ Res*. 2018;8:30-35.
15. Zhu L, Wu Y, Gai K, Choo KKR. Controllable and trustworthy blockchain-based cloud data management. *Future Generat Comput Syst*. 2019;91:527-535.
16. Wolfe University: The first blockchain university, 2020. https://woolf.university.
17. Sharples M, Domingue J. The blockchain and kudos: a distributed system for educational record, reputation and reward. Paper presented at: Proceedings of the European Conference on Technology Enhanced Learning; Vol. 9891; 2016:490-496.
18. China Academy of Information and Communications Technology (CAICT) Blockchain White Paper 2019.10; 2018.
19. Wang H, Guo K, Pan Q. Byzantine fault tolerance consensus algorithm based on voting mechanism. *J Comput Appl*. 2019;39(6):1766-1771.
20. Yin M, Malkhi D, Reiter MK, et al. Hotstuff: Bft consensus with linearity and responsiveness. Paper presented at: Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing; 2019:347-356.
21. Baudet M, Ching A, Chursin A, et al. *State Machine Replication in the Libra Blockchain*. USA: Libra Community; 2019.
22. Oliveira C, Lung LC, Netto H, et al. Evaluating raft in docker on kubernetes. *Adv Intell Syst Comput*. 2017;539:123-130.
23. Cai L. *The Baas Platform Orientated Research and Implementation Foe Scheduling Algorithm*. Hangzhou: Zhejiang University; 2018.
24. Chen H, Zhang LJ. FBaaS:functional Blockchain as a service. *Lect Notes Comput Sci*. 2018;10974:243-250.
25. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. Paper presented at: Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress); 2017:557-564; Honolulu, HI.
26. Baumgart I, Mies S. S/Kademlia. a practicable approach towards secure key-based routing on parallel and distributed systems. Paper presented at: Proceedings of the 2007 International Conference on Parallel and Distributed Systems 2007:1-8.
27. Bitswap, 2020. https://github.com/ipfs/go-bitswap.
28. Yin M, Malkhi D, Reiter M K, et al. Hotstuff: Bft consensus in the lens of blockchain; 2018. arXiv preprint arXiv:1803.05069.

How to cite this article: Liang X, Zhao Q, Zhang Y, Liu H, Zhang Q. EduChain: A highly available education consortium blockchain platform based on Hyperledger Fabric. *Concurrency Computat Pract Exper*. 2021;e6330. https://doi.org/10.1002/cpe.6330