ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

Realize the safe storage and efficient sharing of educational resources based on IPFS+ blockchain

Xiaotian Yang[a], Ran Ma[b], Fei Gao*

Tibet University School Tibet Lhasa

[a]778920383@qq.com, [b]824041393@qq.com, *337679107@qq.com

Abstract: Guided by the framework Construction of University High-quality Education Resource Platform Based on Block Chain [1], the paper introduces IPFS as the data repository of education resources, and realizes the safe storage and efficient sharing of university high-quality education resources by combining IPFS+ block chain technology, and completes the bottom construction of university high-quality education resource platform.Ensure the efficient and secure uploading and sharing of educational data.

Keywords: IPFS; Blockchain; Educational resources

1. Introduction

All Influenced by economic development, China's higher education presents the phenomenon of unbalanced development between the east and the west [2].Students are eager to have access to and use quality digital education resources.However, the existing digital education resource sharing platform has problems such as data loss, poor credibility and resource copyright disputes.According to the article "Framework Construction of High quality Education Resource Platform based on Block Chain", an efficient and high quality education resource platform based on "block chain" technology is proposed [1].In this paper, ethereum is used to write and deploy smart contracts, IPFS is used as a database, and blockchain is used to realize the underlying architecture of high quality educational resources in colleges and universities based on block chain, aiming to solve the uploading, encapsulation, audit, broadcast and other links of high quality educational resources platform data.IPFS+ blockchain can be used as a new, low-trust, low-cost computing and collaboration mode for digital construction,It can be used in the "blockchain + education" data storage and transmission mode, which has the characteristics of decentralization, traceability, efficient transmission and safe storage. At the same time, it can effectively solve the drawbacks of block chain not being able to upload large amounts of data and uploading data slowly. By storing original files in IPFS and storing file hash in block chain,To ensure that data can be uploaded in large numbers and data will not be lost, which provides a basis for the subsequent optimization of the platform.

2. Related knowledge

Blockchain：Blockchain was proposed by Satoshi Nakamoto and originated from bitcoin [3], It is a new technology that attracts attention of many countries， chain block is a peer-to-peer network, is not affected by centralized organization, between nodes can trust each other, the organizations and individuals in the peer-to-peer network can cooperate directly, can make without centralized organization form global collaboration.Blockchain technology is one of the indispensable technologies in the era of globalization and the challenges of the 21st century.This technology has potential application value in various industries and has far-reaching impact on social economy.Blockchain is both a network and a database, as shown in Figure 1:The database consists of a series of blocks, and the data is stored in the form of blocks, where the data upload and update are recorded directly.Each block is encrypted and assigned a unique identifier to form a block header, and each block header contains information such as version number, previous node information, Merkle root, timestamp, workload, and so on.Block data is stored in block body in

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321
merkel-tree mode, in which data information is encrypted and uploaded to block body through elliptic encryption algorithm, digital signature and smart contract to ensure data security.Online all nodes have a copy of the database, through consensus mechanism to ensure that the nodes in the absence of other nodes in the consensus to change of the database, but a piece of form, the block will be permanently stored in the chain of blocks of data in database, the block in the right order linear time mutual connection, each block contains a hash value, the hash value depends on before a hash value,Blocks are joined together to make the input data tamper-proof.Smart contracts are automatically executed, written directly into the program.All nodes on the network work together, keep accounts together, and jointly maintain the security of the blockchain network.Blockchain is decentralized, open and transparent, traceable and unmodifiable.

IPFS, also known as interplanetary file System [4], is based on distributed storage and is a new generation of Internet technology, integrating blockchain, big data and other technologies.It is one of the important technical supports to build Web3.0 in the future.IPFS uses Hash to address locations, implements data sharing, verifies Hash to determine whether data has been changed, and accesses computers and shared files anywhere in the world using IPFS directly from its own computer without uploading or sharing data through third-party applications.Compared with traditional networks, PFS has the following characteristics:IPFS is a distributed decentralized storage structure. Data upload and download do not need to go through the central server;IPFS adopts distributed fragmentation transmission, which can effectively improve upload and download speed.IPFS has the characteristics of low cost, because of its unique transmission mode, can save 60% of the network bandwidth, and use hash automatic deduplication, reduce the cost of storage;IPFS high security:IPFS has the characteristics of high transparency and immutable, which can effectively prevent hacker attacks.In addition, IPFS has the characteristics of traceability. All file uploads are fragmented, and the holder can determine who the data copyright belongs to by the degree of fragment matching.

Solidity Ethereum [5] :Ethereum is known as Blockchain 2.0,Ethereum is based on blockchain,It is programmable and allows smart contracts to be written and executed on ethereum virtual machines. By writing smart contracts to write data, process data, and talk to other layers, it can serve different blockchain applications, allowing developers to deploy their own applications on Ethereum virtual machines.Metamask is an Ethereum wallet,We need to use blockchain network in the development process, we must need a corresponding extension to use ethereum network [6], through Matemask we can connect to the local Ethereum network through personal account, and can use Matemask to interact with smart contract, Matemask has add delete account,Deploy the function of modifying the network and setting the gas value.Truffle: Truffle is a framework [7],It will allow us to create our applications on the Ethereum network, and it will give us a set of tools that will enable us to write smart contracts using the Solidity programming language, a framework to test smart contracts, and a toolset to deploy smart contracts to the blockchain..Truffle is an Ethereum-friendly app that aims to simplify Ethereum development and promote Ethereum.Ganache[8] can simulate Ethereum to generate a local Ethereum for deployment and testing of its own Ethereum network.

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

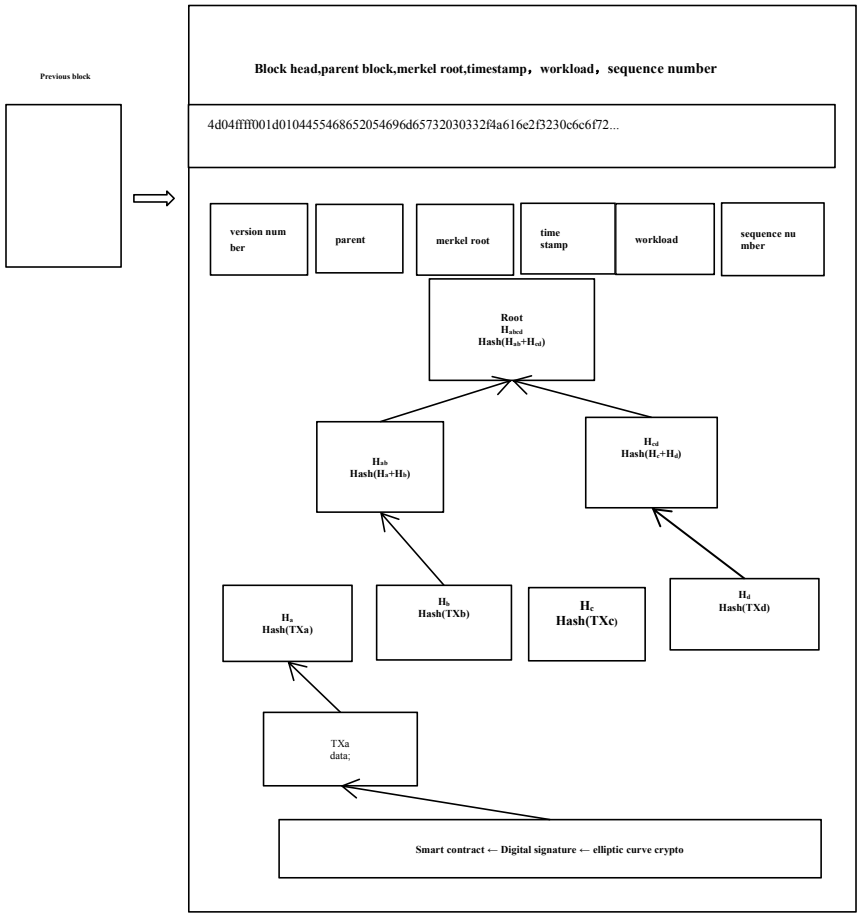

Figure 1. Blockchain structure

3. System design and experiment

3.1 System architecture and system design

This system aims to realize the underlying architecture of the article "Building the Framework of University High-quality Education Resource Platform Based on Block Chain", as shown in Figure 2:Data upload and storage are completed, text, pictures, audio, video and other resources are encapsulated into blocks, and then connected to the client, which responds to the blockchain server [1].The overall system design is divided into six steps, as shown in Figure 3. 1.The user first establishes a link with the blockchain, the blockchain and the front end (the development environment used)2. The user sends the file to the front-end and stores the file temporarily on the web page.3. The front-end interface interacts with the IPFS to receive and store files.IPFS returns the Hash value to the front-end after receiving the file. 5. The front-end adds the returned Hash value to the blockchain.

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

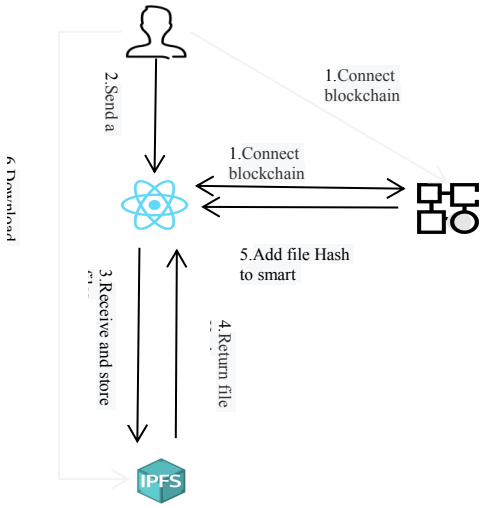

Figure 3. Frame drawing

In view of the proposal proposed in the article "Framework Construction of University Quality Education Resource Platform Based on Block Chain" [1] , we will take countermeasures in the following aspects:

- Data upload:Teachers or institutions upload their courseware and works through the platform, and the platform directly uplows them to IPFS and links them. Then The author can obtain the Hash corresponding to the file, and the Hash has been saved in his corresponding blockchain account, and then the author can use the Hash corresponding to the file to access the uploaded data such as:https://https:ipfs.io/ipfs/+Hash(The url format used for local IPFS storage is like this when we build the system.) Of course, other scholars can also access the corresponding url through the file.The data upload module will be used for: user data upload, file upload (including file backup, learning process data record, system file audit and other parts).

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

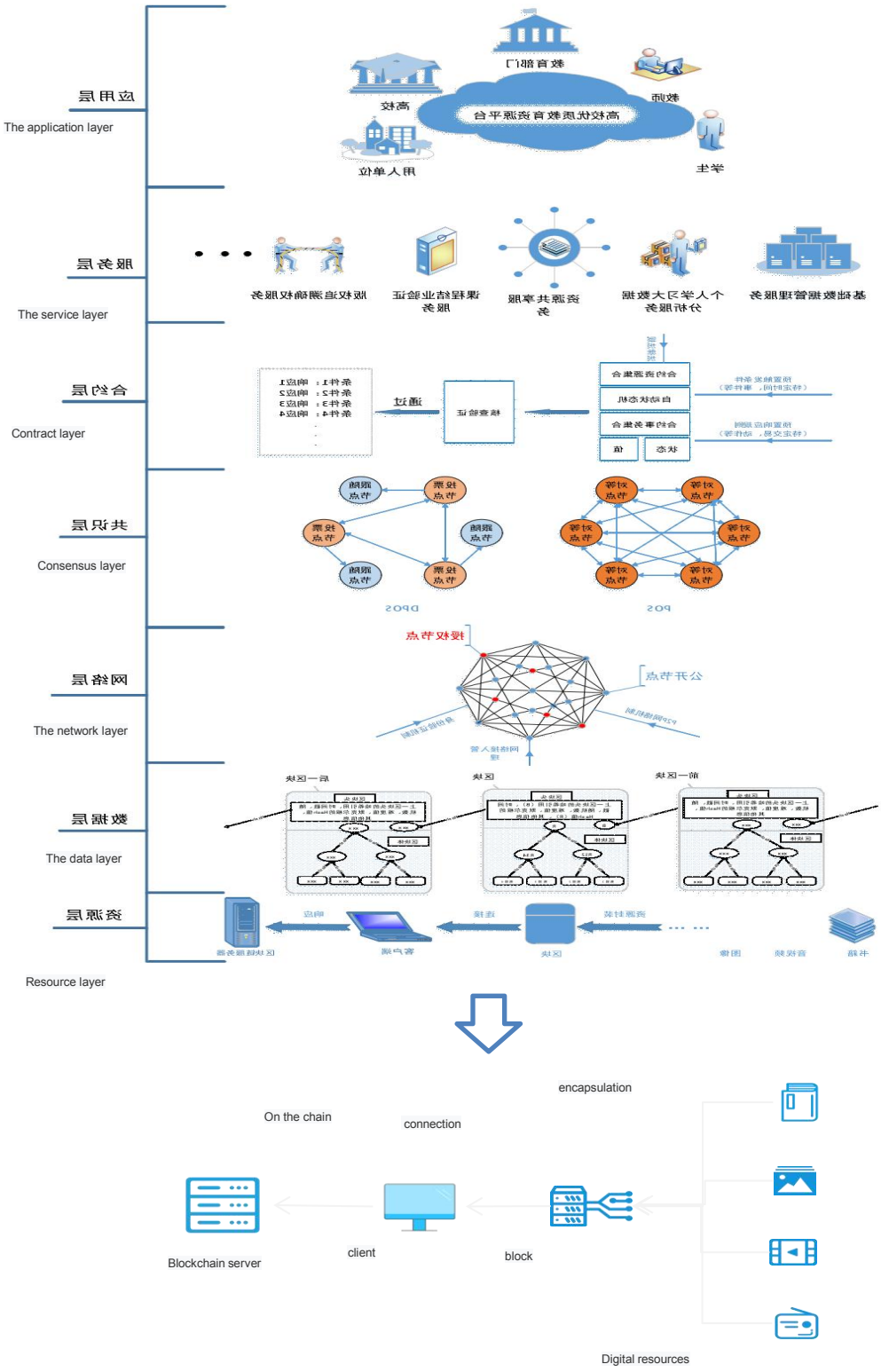

Figure 2. Underlying Architecture Diagram

- Data sharing:In order to facilitate resource sharing, we can't directly access the file through Hash, because then we can't confirm whether it is the file we want. We need a platform similar to YouTube.You need to first show the data to everyone through the platform. You can preview and select what you want to learn and browse through the data display. After selecting, you can study directly on the platform.Of course, everyone can upload the education resources they think are of

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321
high quality, and the files will be directly uploaded to the sharing community after approval, so that everyone can browse and view the shared content directly on the platform.

- Data review:each teacher students can under their accounts published his book and courseware including video, PPT, articles, etc., but upload resources need to be by appraisal institution evaluation in advance, only after audit can be uploaded to the Shared platform, and identified themselves with audit qualification of the audit staff can present audit results, finally, audit results,Determine whether the audit is approved.

3.2 System Design

The essence of the system is a Dapp, which is a decentralized application, and the data is shared with each other.We first use the HML javaScript and CSS to write client applications, and are not connect it to the back-end web server, we connect it to the installation of local block chain server, we use intelligent contract will all code written in our application, compile intelligent contracts, and deploy it to the local block chain,And allow accounts on the network to use our application.The specific implementation is shown in figure 4, which is divided into the following parts :(screenshot showing file uploading as an example).

- Users write smart contracts by connecting the front-end platform with Truffle framework: The realization of smart contracts is divided into four parts:

a. Modeling data: building file body structure: including file Id (Id and file composition form a mapping relationship), file corresponding Hash (used to store Hash value returned by IPFS), and file upload address.

b. Save data: Save data in blockchain.

c. Upload data: Check whether the data exists by checking whether the file Hash and file address exist.

d. List data: The Hash value of the returned file.

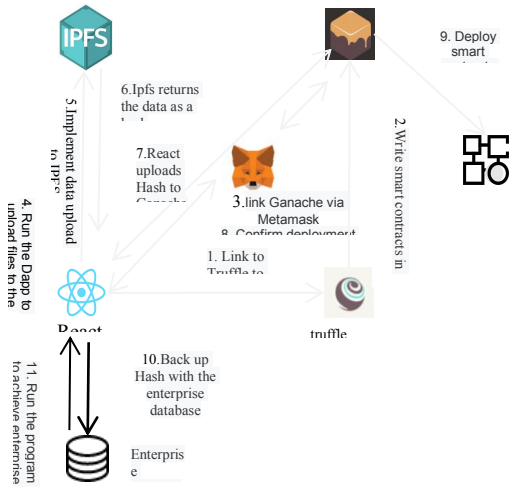

Figure. 4 Flowchart of system design and implementation

- Truffle writes the smart contract written to Ganache:It is shown in the diagram 1 and 2 on the left of Figure 5,By first running Ganache as a local blockchain, Ganache will provide 10 Ethereum accounts, each with a unique identity, and each Ethereum account body has a total of 100 Ethereum coins.We build a local network through Ganache HTTP://127.0.0.1:7545, write the same IP and port when deploying Truffle, write the smart contract into the local blockchain Ganache, and generate the corresponding ABI file.

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

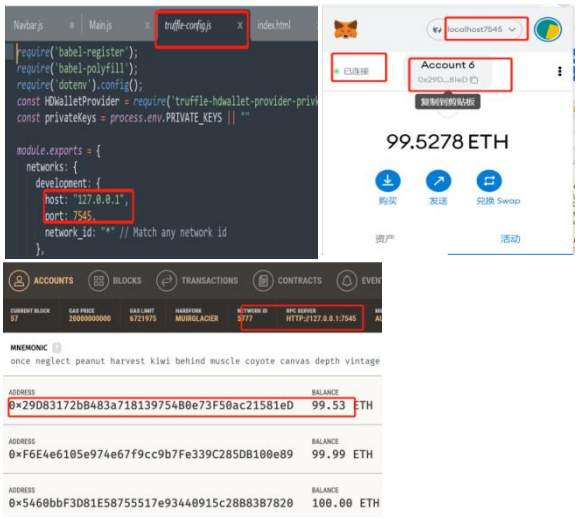

Figure. 5 Screenshot of experimental environment configuration

- Connect Metamask through the front-end, and Metamask connects to Ganache through sharing the same API: as shown in figure 5 on the right, we connect Metamask to the local network 127.0.0.1:7545, and connect to import the first account of Ganache.
- Upload files to the network by running Dapp and React: as shown in the first picture on the left of Figure 6, pictures are stored in the webpage in the form of array.
- Users can use React to store files in IPFS and upload files to IPFS.
- IPFS returns the corresponding Hash: After the file is uploaded to the local IPFS, the corresponding Hash is automatically generated.
- React upload file Hash value to Ganache (local blockchain) :As shown in figure 6 left 2 figure we upload the three sets of files, and lists the corresponding name, description, format, upload file time, size, upload, and stored in the corresponding IPFS Hash value, and we can figure in the lower right corner connection direct access to download the files stored on the IPFS
- Users confirm whether to deploy to blockchain through Metamask's connection with Ganache, and Metamask acts as a wallet to ensure account security.
- Deploy contract to blockchain after Metamask confirmation: as shown in Figure 6 on the right: When running Dapp: Confirm by deployment through Metamask request and show Gas value spent by exchange.

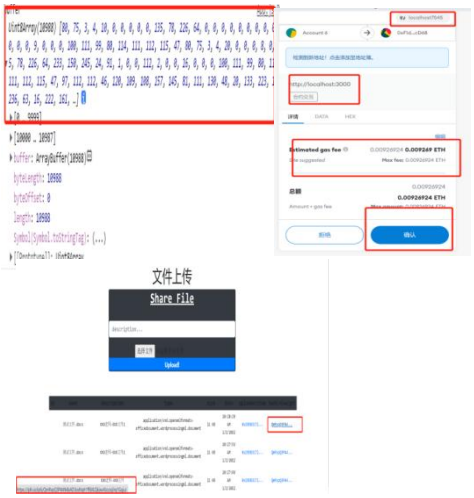

Figure 6 . Deployment process screenshot

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

3.3 Experimental results and analysis

3.3.1 Experimental results

- Result diagram of file uploading module: as shown in the figure7:The uploaded file will be deployed on the blockchain, and Gas will be consumed for each deployment. After the file is uploaded, the file displays the detailed data of the uploaded file, including name, description, format, upload time, size, upload time, and the Hash value stored in IPFS. You can click the Hash value to download the corresponding file directly.

Figure 7 .File upload module screenshot

- Result diagram of file sharing module: Similar to YouTube, uploaded videos can be displayed, which can be clicked to browse and expanded in the form of list. Corresponding labels can be added to describe uploaded files when files are shared. as shown in the figure8:

Figure 8 .File Sharing ScreenshotFigures and Tables

- Result diagram of document review module: as shown in the figure, we can review the submitted documents. After passing the review, the review result will be added by 1. Finally, we can determine whether the documents are approved by counting all the review results. as shown in the figure9.

Figure 9 .Screenshot of document review module

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321

3.3.2 Experimental analysis

Compared with traditional data transmission and sharing systems, IPFS+ blockchain mode has better performance in data transmission rate protection, ensuring safe and efficient data transmission, storage and sharing.As shown in Table 1, we compared the transmission of traditional data and the sharing system at the intersection of IPFS+ blockchain as data storage and sharing (we did a lot of experiments on data transmission, comparing different platforms and different sizes of data, IPFS can upload 5.6g video with just over 1 minute, and the transmission rate is far higher than that of traditional systems).

TABLE I. IPFS+ BLOCKCHAIN AS THE INTERSECTION OF DATA STORAGE AND SHARING OF TRADITIONAL DATA TRANSMISSION AND SHARING SYSTEM COMPARISON TABLE

To compare	IPFS+ blockchain data sharing platform	Traditional data transmission shared channel
Transmission rate (1.6 GB video upload as an example)	Upload on the local IPFS network The upload time is 11.43 seconds	The comparison time of QQ upload was 2 minutes and 1 second
Whether it is influenced by a third party	Data is stored in IPFS, Hash is stored in blockchain, completely independent of the control of third parties, is decentralized.	Data is stored in a third-party database and is affected by third-party organizations in terms of privacy and security。
Check whether data transmission is restricted	Data transmission is unlimited and can transmit data of any size.	Limited data transmission (take QQ as an example, the upload limit is less than 2G).
Reliability of data store sharing	High reliability. Once data is uploaded, it is stored in IPFS and Hash is generated. Once the Hash is uploaded, it will not be modified.	ordinary, data stores are affected by third-party databases. If a third-party database becomes faulty, data is seriously affected.
System flexibility	High, once the infringement occurs, rights can be directly completed through the matching degree of fragments.	ordinary,After infringement, third-party institutions must be contacted for audit, which takes a long time and is inefficient.
The economic situation	Low bandwidth and low data storage cost.	Data transmission is high and data storage is expensive.
other	It is a new technology with good prospects	Change is needed

4. Conclusion

IPFS is the next generation of Internet development drivers, a tool that can fundamentally reshape society and the economy, leading us into a more decentralized era.IPFS combined with blockchain can effectively realize the secure storage and sharing of data, which can promote the landing of blockchain industry more efficiently.Is the new trend of future development.This solution can effectively solve a natural disadvantage of block chain, that is, low storage capacity and speed, which cannot realize large-scale storage of data.IPFS+ blockchain mode can effectively solve the problem of large-scale data link. Original files are stored in IPFS and the corresponding file address is stored in blockchain to achieve large-scale upload and permanent storage of files.In this paper, IPFS+ blockchain is introduced as the underlying structure of the high-quality education resource platform of colleges and universities, which provides a new idea for the storage and

ISSN:2790-1688 DOI: 10.56028/aetr.2.1.321
sharing of data in the future. In the future study, we will realize the integration of modules and gradually improve the platform from easy to difficult.

References

[1] Gaofei,Yangxiaotian,Maran,Lijiang,Liuliting. Construction of high quality education resource platform framework based on block chain[J].Plateau scientific research,2021,5(02):117-124.

[2] Wu daguang,Wang yiqian1. Analysis on the development level of higher education in the east and west of China[J]. Journal of Lanzhou University (Social Sciences),2021,49(05):1-8

[3] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system[J]. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008,

[4] Benet J. Ipfs-content addressed, versioned, p2p file system[J]. arXiv preprint arXiv:1407.3561, 2014.

[5] Dannen C. Introducing Ethereum and solidity[M]. Berkeley: Apress, 2017.

[6] Lee W M. Using the metamask chrome extension[M]//Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA, 2019: 93-126.

[7] Latif R M A, Farhan M, Rizwan O, et al. Retail level Blockchain transformation for product supply chain using truffle development platform[J]. Cluster Computing, 2021, 24(1): 1-16.

[8] Lee W M. Testing smart contracts using ganache[M]//Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA, 2019: 147-16