Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9875210, 1 page
https://doi.org/10.1155/2023/9875210

Retraction

Retracted: Design of Data Sharing Platform Based on Blockchain and IPFS Technology

Wireless Communications and Mobile Computing

Received 25 July 2023; Accepted 25 July 2023; Published 26 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] W. Li, Z. Zhou, W. Fan, and J. Gao, "Design of Data Sharing Platform Based on Blockchain and IPFS Technology," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 3937725, 7 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3937725, 7 pages
https://doi.org/10.1155/2022/3937725

Research Article

Design of Data Sharing Platform Based on Blockchain and IPFS Technology

Weijing Li, Zicheng Zhou, Wen Fan, and Juan Gao

School of Computer and Information Technology, Cangzhou Jiaotong College, Huangpu, Guangzhou 510700, China

Correspondence should be addressed to Wen Fan; wfan@czjtu.edu.cn

Received 6 May 2022; Revised 2 June 2022; Accepted 3 June 2022; Published 13 July 2022

Academic Editor: Kalidoss Rajakani

With the continuous development of the information age, data sharing and exchange are gradually increasing. The Internet and big data technology provide a guarantee for data sharing and transmission. At present, as the amount of data increases rapidly, how to realize data sharing has become a huge challenge. To solve this problem, this paper proposes a data sharing platform based on the combination of blockchain and interplanetary file system (IPFS) technology to solve the data sharing and storage. Firstly, by constructing the alliance blockchain, the consensus mechanism of computing power competition is used to maintain the data written into the blockchain, and the IPFS data storage system is established to store data using distributed storage, file splitting, and splicing technologies. Secondly, a data sharing platform composed of blockchain module, IPFS module, encryption and decryption module, and fast retrieval module is built. Data encryption is processed by encryption and decryption module, and the processed data is uploaded to THE IPFS module; the abstract and other information are finally written into the blockchain through the blockchain module. The fast retrieval module can quickly locate the required data according to the retrieval conditions in the mass blockchain data; finally, the security and storage of data sharing platform are guaranteed through security and performance evaluation. The research results solve the problem of large amount of data sharing, realize the data decentralization, and ensure the data storage security.

1. Introduction

With the rapid development of information technology and digitalization, the data generated in people's daily life continues to increase, such as office documents, pictures, and videos. Data has become an indispensable element in people's life, and the information construction of data has also become the urgent need of the development of The Times. At present, data informatization construction is faced with the lack of convenient and efficient data sharing platform, no unified data storage system, data islands, and data security problems [1]. Therefore, it is of great value and significance to study data sharing and storage in the construction of data informatization.

There are endless researches on data sharing, but few of them are applied on a large scale. Some researchers set up data sharing system based on data processing of cloud service, adopted data collection method to deal with the problem of frequent data generation and large concurrency, and proposed adaptive method of multiformat data to solve the problem of data format [2]. With the development of blockchain technology, it has the characteristics of "traceability," "hard to tamper with," and "decentralization," providing a new idea to solve the problem of data security. Some researchers have proposed a data sharing scheme based on blockchain technology to ensure data privacy security and sharing through access permission setting and data storage [3]. Some researchers have designed a data sharing platform combining blockchain and machine learning technology to solve problems such as data loss and data tampering. Some scholars have proposed the data unchained storage mode of cloud + blockchain to realize data storage and transmission in the cloud and greatly improve the running speed of blockchain network [4].

On the basis of data sharing, data storage becomes an urgent problem to be solved. At present, data storage mainly includes public chain, attribute encryption, and cloud storage, but all of them have certain limitations. Public chain

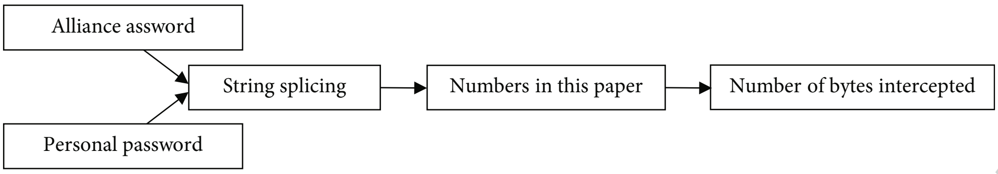

Figure 1: Key generation.

processing efficiency is low and cannot guarantee data security; the cost of attribute encryption is high, so it cannot be widely applied. Cloud storage increases trust risks and costs. Interplanetary file system (IPFS) is a distributed hypermedia transfer protocol, which can not only store and use data permanently but also address and version content. Some researchers proposed to build a data sharing platform by combining alliance chain and IPFS technology to solve the problems of data transmission efficiency, data security and privacy, and data sharing and storage [5].

In order to solve the problem of data sharing and storage, this paper proposes a data sharing scheme of alliance blockchain +IPFS, which uses the consensus mechanism of computing power competition to maintain the data in blockchain, and uses distributed storage, file splitting and splicing, redundant backup, and other technologies to build IPFS data storage system [6]. By building a data sharing platform composed of blockchain module, IPFS module, encryption and decryption module, and fast retrieval module, the security and performance evaluation of the data sharing platform is carried out, so as to solve a large number of data sharing and storage problems.

2. Materials and Methods

The rapid development of information technology produces a large amount of data. The storage and maintenance of these data is very important, and the safe storage and backup mechanism of data is very important. The data sharing model provides a direction for the safe storage and maintenance of data.

2.1. Key System Technologies

2.1.1. AES Encryption Algorithm. When data is generated, the AES encryption algorithm is used to encrypt it (Figure 1). Figure 1 shows that the key generation process is as follows: Blockchain each node has the user to set the password, after the system input user password, set the alliance with the password and user password for string concatenation, using digital technology to calculate the 20 bytes of output, output by intercepting 20 bytes of the first 16 bytes to form the encryption key of AES algorithm, greatly reduces the risk of data privacy disclosure [7].

Through AES encryption algorithm, after the data is uploaded to the IPFS system, the data is encrypted with the federation password and stored in the local database. When the user forgets the password, he/she can retrieve the data from the node where the data was generated, or he/she can reset the password and upload the data again. In this case, the original block in the blockchain is invalid, and the content in the hash table needs to be updated to the new block.

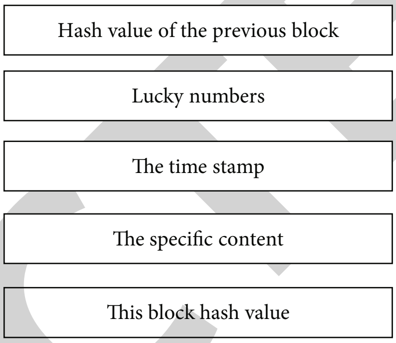

Figure 2: Block internal structure.

2.1.2. IPFS Data Storage System. IPFS is a distributed data storage technology that uses point-to-point protocol to address data content to store data such as pictures, videos, and files. If the contents of an existing folder are modified, you can upload the modified version of the file to the IPFS system. When multiple folders are modified, all folders can be compressed into a compressed package and uploaded to the IPFS system [8]. At the same time, the system will fragment and copy the file to each NODE of IPFS and return an IPFS string as the address to access the file.

To ensure data storage security, the IPFS system can be operated only on the internal network, and each node is connected through VPN. IPFS files with IPFS address as the file name cannot keep the file extension, only in the blockchain record file information contains file extension, so by renaming the IPFS file name and decrypting the file in the decryption system to achieve the file view or download.

2.1.3. Alliance Blockchain System. Blockchain is divided into public, federated, and private chains according to their scope of use. Federated chain is selected in this paper, and all users should operate and maintain the blockchain system in strict accordance with the provisions of the agreement. When the data is uploaded to the IPFS system, the user package, the IPFS address, and key information of the file into Java objects, which are transmitted to the nodes of the alliance blockchain in the form of serialized files, obtain the current time and reset the timestamp, and maintain the data written into the blockchain through the consensus mechanism of computing power competition. The block structure is shown in Figure 2.

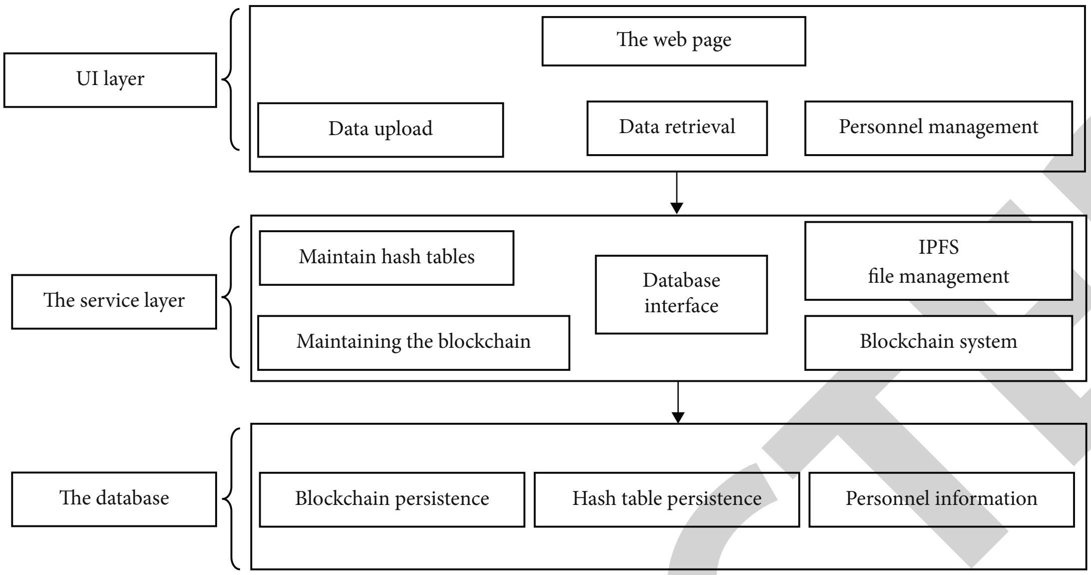

Figure 3: System architecture.

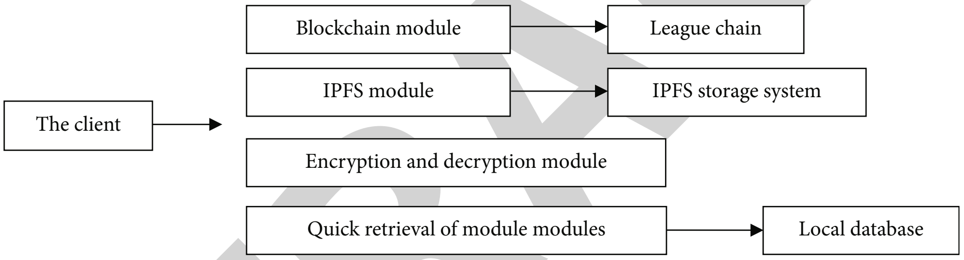

Figure 4: System design diagram of data sharing platform.

```
Public static void decodestream(byte[]b, inputstream is, outputstream os)
Throws Exception{
Int mode=Cipher. DECRYPT_MODE;
Key key=new secretkeyspec(b, "AES”);
Cp .init(mode, key);
Usecipher(cp, is, os);
Is. Close();
Os. Close();
System.out.println(“File decryption completed”);
}
```

Algorithm 1: Encryption and decryption model.

2.1.4. Data Retrieval Technology. Because of the huge amount of data in the database, data retrieval needs to consume huge cost of computing power. In this paper, the data structure of a hash table is maintained in memory and only the user ID and the data primary key block ID are stored to achieve efficient data retrieval.

2.2. System Architecture. The system architecture (Figure 3) is divided into UI layer, service layer, and database. The UI layer mainly provides data uploading and data retrieval services. The service layer stores data through IPFS technology, writes data information through the alliance blockchain system, and maintains nodes of the blockchain system through servers. The database mainly realizes the permanent preservation of blockchain and data information.

On the hardware, the server maintains the blockchain and hash tables through memory resources. As the amount of blockchain data continues to increase, memory consumption is reduced by deleting the blocks generated earlier and only retaining the new blocks, thus ensuring timely modification of the data in the event of a fork in the blockchain [9]. At the same time, the server also needs to provide large

```
Public void function block bk) {
byte [] b;
t ry{
b=hashcaculate. Hashstring(bk.tostring());
while(flag){
bk.setlucky(bk.get lucky()+1);
if(b[∅]i=∅}}b[1]i=∅) {
b=hashcaculate.hashstring(bk.tostring());
}
else{
informstop();
break;
}
}
} catch(exception e) {
e .printstacktrace();
}
}
```

Algorithm 2: Procedure of consensus mechanism.

enough persistent storage space to store images, videos, and other data, as well as complete blockchain and hash tables.

In software, each node in the background maintains an array of IP addresses and port numbers of other nodes. Therefore, when the data is generated, the information through the array is sent to other miner nodes based on TCP. The data to be processed through the browser is realized by the background business logic [10]. At the same time, the local server backs up the blockchain data and updates the hash table information in time to solve the system data recovery problem after the server downtime.

3. Results

3.1. Overall Design of Data Sharing Platform System. The data sharing platform system (Figure 4) is divided into blockchain module, IPFS module, encryption and decryption module, and fast retrieval module. As the interface for users to access the system, the browser enables users to interact with each module through web pages and send HTTP requests to the background to complete corresponding functions. At the same time, HTML, CSS, and other technologies are used to convert data into pages to achieve interaction. The front end of the background provides blockchain, IPFS, data encryption and decryption, fast data retrieval, and other functions [11].

Realization of data sharing platform: users upload data using browser, data through the background blockchain module to complete data input; for encrypted or decrypted files, by the background encryption and decryption module to complete the file encryption or decryption; the uploaded files are stored in IPFS module after traffic. Send retrieval instructions through the browser, and the fast retrieval module in the background realizes fast data retrieval [12].

3.2. Front-End Page Implementation. Users mainly access the system through the browser to achieve visual front-end page and system interaction. First of all, the background by writing asp page, after Java parsing into browser readable HTML page, the front-end browser page can realize data upload and view, data encryption and decryption, and data management [13].

Table 1: Record table structure.

The name	Type	The length
Id	Int	11
Last_hash	Varchar	255
Time	Timestamp	0
Lucky	Int	11
This_hash	Varchar	255
Date	Date	0
Ipfs_addr	Varchar	255
Des	Varchar	255
Miner	Int	255

Data upload is mainly by the user through the browser to the background, and the background controls the blockchain data write and update the database. The uploaded data information includes ipFS address, file type, data timestamp generated in the background, lucky number, and node of the block. In the data encryption part, the front-end page inputs personal key, alliance key, and file path, and the background carries out symmetric encryption and decryption for the data under the path.

3.3. Implementation of Background Functions. Background through Java language to build business logic, mainly using JDK1.8 development kit and Tomcat Web server. Background business mainly includes data encryption and decryption module, IPFS upload module, and blockchain module [14]. The codes of each module are independent from each other and cooperate with each other functionally to jointly complete data sharing tasks.

3.3.1. Data Encryption and Decryption Module. The data encryption function includes generating the final encryption key, encrypting files using the AES algorithm and encryption key, and uploading encrypted files to IPFS with the returned address reserved. The data decryption function includes generating a decryption key, using the AES algorithm and decryption key to decrypt files, and renaming decrypted files based on suffixes [15].

The encryption key is generated by USING AES algorithm and digital digest tool to realize file encryption. Upload the encrypted file to the IPFS system and keep the address and upload the file address and summary information to the blockchain system. AES is a symmetric encryption algorithm. The decryption key is the same as the encryption key, and their generation process is the same. The program is shown in Algorithm 1, where the decryption model is invoked.

3.3.2. Blockchain Module. The data is uploaded to the client and forwarded to the RecordService class to complete the blockchain writing. The RecordService class includes socket parts, blockchain data, and consensus mechanisms.

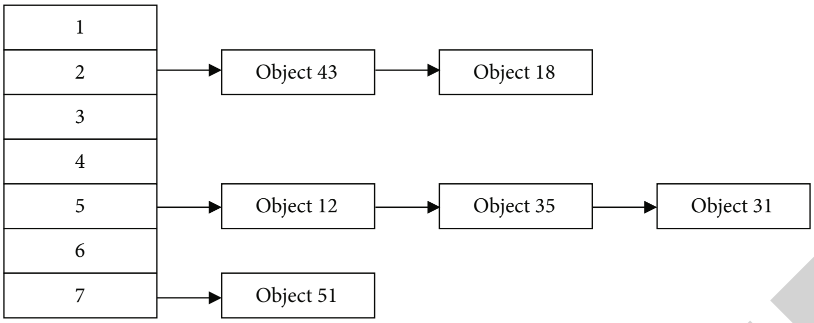

Figure 5: Structure of hash table.

The socket part works by broadcasting real-time data and notifying other nodes to start writing blockchain data in a power-competitive manner. When a node first calculates the legitimate block, it serializes the Java object and broadcasts the operation of computing power competition in time. The notified node deserializes the data into A Java object to verify the validity of the block and at the same time stops competing for computing power and adds the valid block to the end of the blockchain [16].

Consensus mechanism is to solve the competition of computing power. The hash value obtained is verified by adjusting lucky value. When the hash value meets the legal form, the calculation is stopped and other nodes are informed through broadcast. The node that receives the data completes the validation and writes the validated data to its own blockchain. The program is shown in Algorithm 2, wherein HashCaculate is the realization of the hash calculation algorithm. Flag: when other nodes compute legitimate blocks first, the Flag is set to false and the hash calculation is terminated. InformStop notifies other nodes to stop computing when a valid block is computed.

3.4. Implementation of IPFS Module. By setting up a VPN server, each node of the system resides on the same virtual Intranet to access each other. Devices with large disk space and stable running are used to access Intranet devices to store data. The IPFS software is installed on all nodes to form a stable data storage system. At the same time, data is uploaded and downloaded through the running mechanism of IPFS software. The front-end visual interface provided by the system realizes the interaction between the IPFS device and Java background [17].

IPFS software uses imperative tools. To upload data, run the ipfs add file path command on the CLI. If the access address of the file is returned after the file is successfully uploaded, the file name and suffix are lost. Access addresses and file-related information are entered into the client and passed into the Java background to write to the blockchain. To download data, you only need to open the command line window and enter the command "ipfs get file name." If the file cannot be opened, you need to find the relevant suffix information and rename it to view the file.

3.5. Implementation of Database Part. Select mysq15.5 and install database management software on Linux system environment, mainly used to store blockchain data. Record table is used to store blockchain to determine the area of data, only data write permission, cannot be modified, or delete. At the same time, the data in the record table of all nodes should be consistent. Table 1 shows the Record table structure, where ID is the index of each Record, last hash is the hash value of the previous block, time is the timestamp generated by the block, lucky is the lucky number calculated for the valid block, and this hash is the hash value of this block. Ipfs addr is the address of the data in the IPFS system, des is the suffix of the data file, and Miner is the miner node whose valid blocks are calculated [18].

3.6. Quick Retrieval Module. Tree structure and hash table structure can realize fast retrieval. In this paper, hash table structure is selected (Figure 5). The ratio of total Java objects to the length of array is load density. The position of array is called bucket, and each blockchain position is placed in the corresponding bucket. The remainder of the data number divided by the length of the array is mapped to the bucket and placed at the end of the blockchain list. When searching, you only need to enter the number to find relevant objects and database-related data. As the amount of data continues to increase, so does the loading density, and the retrieval time naturally becomes longer. In this paper, the critical value of the load density is 0.75. By doubling the length of the array and redistributing it to the corresponding bucket, the load density and retrieval time are stable.

3.7. System Performance Analysis. The data sharing system adopts the scheme of data content and abstract separation, encrypts and stores the generated data in IPFS system, and stores the data address in blockchain system. Due to the IPFS distributed storage mode, data content and data address have a lot of backup, can respond to various security attacks and timely recovery of data.

When some nodes of the system are attacked simultaneously, such as data corruption, the system can restore the data of the unattacked nodes to the local database. When a node in the system is maliciously manipulated, for example, illegal data is written into the node, the consensus mechanism discards the illegal data to ensure that the data is valid. When users upload wrong data to IPFS storage system, charging will be provided for storage resources to limit this operation.

Blockchain has the characteristics of decentralization and tamper-proof, but it also has the disadvantages of low data writing efficiency and high computing power overhead. The algorithm force competition consensus mechanism is adopted to control the probability of data generation by restricting the format of legitimate data, so as to control the time when data is written into the blockchain. Meanwhile, the consensus rules are dynamically adjusted according to the system's algorithm force to ensure that the time of data writing into the blockchain is relatively fixed.

The data sharing system creates a hash table in memory to realize data retrieval. The hash table calculates the hash value with ID as the keyword and stores the package of ID and block_ ID into the hash table. This solution can reduce the number of IO interactions by half and reduce node maintenance. Since the data retrieval efficiency mainly depends on the number of interactions between memory and hard disk, the data retrieval time can be effectively reduced by using hash table. Blockchain application is still in the initial development stage of the laboratory, and there is no intuitive and available mature product. Compared with Internet technology, people can use browsers, apps, and other specific applications to browse, transmit, exchange, and apply information. However, blockchain obviously lacks such breakthrough applications and faces high-tech barriers. Another example is the problem of block capacity. Because the blockchain needs to carry all the information generated before copying, the amount of information in the next block is greater than that in the previous block. In this way, the block write information will increase infinitely, and the problems of information storage, verification, and capacity need to be solved.

4. Conclusions

Data sharing is an urgent problem to be solved in information construction. This paper proposes a data sharing scheme based on blockchain technology and IPFS technology, carries out the design and implementation of the data sharing system, and evaluates the security and performance of the system. The results show that:

(1) Using alliance chain blockchain, with the help of the characteristics of the platform to solve the data storage and access control problems; distributed file system IPFS is used to store data, which solves the problem of database storage security and avoids the risk of data leakage by virtue of its natural decentralized characteristics. The data sharing system is constructed by combining alliance blockchain and IPFS technology, and the method of constructing hash table in memory is proposed to improve the speed of data retrieval

(2) Realized the data sharing system composed of blockchain module, IPFS module, encryption and decryption module, and fast retrieval module; upload data by browser, write data through background blockchain module, encrypt or decrypt files through encryption and decryption module, and realize data storage by back-end IPFS module; use the server to set up the web background service to run the blockchain and IPFS nodes, build the internal shared network, and provide service interfaces for the front segment; through the browser to send retrieval instructions by the background of the rapid retrieval module to achieve rapid data retrieval, and finally to the data sharing platform security and performance evaluation

(3) The data sharing platform based on blockchain and IPFS technology has the advantages of decentralization, preventing data tampering, protecting data security, and maintaining data spontaneously among nodes, which solves the main difficulties of data sharing. Most of the applications of blockchain technology in commercial banks are still being conceived and tested, and there is still a long way to go before they are used in life and production, and there are many difficulties in obtaining the recognition of regulatory authorities and the market

Data Availability

The figures and tables used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Thanks are due to those techniques who have contributed to this research. The Research of Transaction System Based on Blockchain is the key research and development program guidance project of Cangzhou city, the project number is 204102013. The Project Content: With the help of blockchain platform, research and design a decentralized application. In decentralized systems, direct peer-to-peer transactions between users and merchants are implemented. The transaction data will be published to the Ethereum blockchain through smart contracts, and the off-chain storage function will be realized through event monitoring mechanism, so as to truly realize a decentralized distributed transaction system.

References

[1] M. Wysel, D. Baker, and W. Billingsley, "Data sharing platforms: how value is created from agricultural data," *Agricultural Systems*, vol. 193, no. 5, pp. 103241–103770, 2021.

[2] N. Qin, Z. Tang, and Y. Wang, "The data sharing platform system of electrical main wiring based on the results of 3D digital GIM," *Journal of Physics: Conference Series*, vol. 1952, no. 3, pp. 303–321, 2021.

[3] Anonymous, "New member of ship data sharing platform consortium," *Sea Technology*, vol. 62, no. 5, pp. 34–73, 2021.

[4] T. Devriendt, M. Shabani, and B. Pascal, "Data sharing platforms and the academic evaluation system," *EMBO Reports*, vol. 21, no. 8, pp. 4–23, 2020.

[5] J. Sookhyun, K. Jaeeun, C. Taeyoung, and S. JaeSeung, "Requirements analysis for test and verification methodology of smart city data hub as data sharing platform," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 45, no. 5, p. 6, 2020.

[6] C. P. Jean, L. Carl, and N. E. Paul, "Re-integrating scholarly infrastructure: the ambiguous role of data sharing platforms," *Big Data & Society*, vol. 5, no. 1, pp. 36–56, 2018.

[7] Z. Zhao, J. Ma, and Chinese Centre for Disease Control and Prevention, Beijing, China, "Application of blockchain in trusted digital vaccination certificates," *China CDC weekly*, vol. 4, no. 6, pp. 106–110, 2022.

[8] S. Henningsen, "Blockchain in der Chemie," *Chemie in unserer Zeit*, vol. 56, no. 1, p. 73, 2022.

[9] Z. Sun, Q. Xu, and B. Shi, "Price and product quality decisions for a two-echelon supply chain in the blockchain era," *Asia-Pacific Journal of Operational Research*, vol. 39, no. 1, pp. 98–125, 2022.

[10] Y. Chen and B. Yang, "Cooperative decision making of supply chain members of shipping logistics services under the background of blockchain," *Asia-Pacific Journal of Operational Research*, vol. 39, no. 1, pp. 43–78, 2022.

[11] P. Leibfried and H. Petry, "Blockchain in der Finanzberichterstattung," *Controlling & Management Review*, vol. 66, no. 1, pp. 54–59, 2022.

[12] L. Huizhen, P. Benhong, L. Zhi, Y. Zg, and X. Zhenhuan, "Research on logistics information management system based on blockchain perspective," *Academic Journal of Business &amp; Management*, vol. 4, 2022.

[13] Z. K. Hou, H. L. Cheng, J. L. Hai, D. P. Zhang, and R. C. Gao, "Fracture Mechanics Model of the Initiation and Growth of HydraulicFissures During Hydraulic Fracturing of Shale," *Journal of Yangtze River Scientific Research Institute*, vol. 37, no. 5, pp. 99–107, 2020.

[14] Z. K. Hou, H. L. Cheng, S. W. Sun, J. Chen, D. Q. Qi, and Z. B. Liu, "Crack propagation and hydraulic fracturing in different lithologies," *Applied Geophysics*, vol. 16, no. 2, pp. 243–251, 2019.

[15] J. Wei, H. Cheng, B. Fan, Z. Tan, L. Tao, and L. Ma, "Research and practice of "one opening-one closing" productivity testing technology for deep water high permeability gas wells in South China Sea," *Fresenius Environmental Bulletin*, vol. 29, no. 10, pp. 9438–9445, 2020.

[16] W. Zhang, Z. Cheng, H. Cheng, Q. Qin, and M. Wang, "Research of tight gas reservoir simulation technology," *IOP Conference Series: Earth and Environmental Science*, vol. 804, no. 2, article 022046, 2021.

[17] X. Wei, Y. Guo, H. Cheng et al., "Rock mass characteristics in beishan, a preselected area for China's high-level radioactive waste disposal," *Acta Geologica Sinica*, vol. 93, no. 2, pp. 116–126, 2019.

[18] J. Han, H. Cheng, Y. Shi, L. Wang, Y. Song, and W. Zhnag, "Connectivity analysis and application of fracture cave carbonate reservoir in Tazhong," *Science Technology and Engineering*, vol. 16, no. 5, pp. 147–152, 2016.