2022 21st International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)

Application of Ship Data Based on Blockchain

Liu Zixiang, Cheng cheng, Zhao Feng
China Ship Scientific Research Center
Wuxi, China
291013422@qq.com

Wang Xiang, Wu Feng
Fengshun Technology Information Service Co. Ltd
Hangzhou, China

***Abstract*—Aiming at the need for controlled sharing and application of data during ship design and research, a method based on blockchain is proposed in this paper. Blockchain is introduced in this method for data encryption and storage, as well as property authentication and usage log. Data-driven program is used for data application, making data invisible while accessible for users. A ship resistance prediction program based on dynamic surrogate model with relevant data is used as demonstration and successfully implemented the intended functions, showing this method available for practical application.**

Keywords-blockchain; data sharing; data authentication; surrogate model

I. INTRODUCTION

With the coming of information era, data has been widely considered as a new type of means of production. It has become an essential boosting power for many industries, including military industries like ship research and designation. Institutes like China Ship Scientific Research Center (CSSRC) has accumulated large amount of data from the R&D works, and these data could produce considerable benefits if applied properly and sufficiently. However, the application of data still remains limited today, due to the management system and IT technical level [1]. To confront these questions, a new mode of cooperation, sharing and innovation should be established. We should build an application service system towards ship R&D, with data and professional intelligence collected and applied. This is a necessary step for the development of the ship industry.

The new mode of cooperation and sharing can effectively overcome the disadvantages of the classical R&D mode, but the new mode also has its own problems. The property authentication and controlled sharing are the key to application of data in the new mode, which may cause damage to the cooperation partners' benefits, or even the leaking of data. This paper introduced a method for sharing and application of ship data based on blockchain. In this method, blockchain is applied for data encryption, storage and transmission. Data is applied through data-driven (data-mining) programs, which makes data invisible while accessible for users. The usage log and digest of data is saved on the blockchain as a tamper-proof ledger to authenticate data and preserve the benefit of data owners. This method could provide technical support for the new mode of cooperation and sharing.

II. SYNOPSIS OF BLOCKCHAIN

According to the white paper on technology and application development of blockchain published by the Ministry of Industry and Information Technology[2], blockchain can be defined as a distributed ledger or database based on block-chain data structure. On a wider sense, the blockchain technology is a new distributed computing mode with block-chain data structure, consensus algorithms, encryption and smart contracts contained. The most noteworthy feature of blockchain is its data structure. A chain is established by data blocks arranged in order, each block contains the characteristic hash of its previous block. Any alteration in one single block will affect all the following blocks, and alteration without permission and consensus of the majority of partners will be invalid. Valid alteration with consensus will also be logged, and that's why blockchain is traceable and tamper-proof.

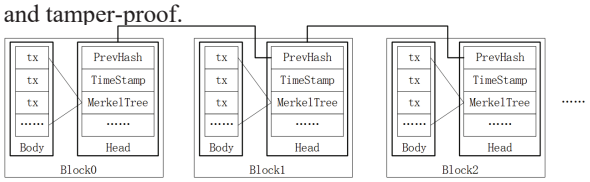

Figure 1. Block-chain structure

The technical features of blockchain include high reliability, privacy preserving, tamper-proof, action traceability and self-establishment of trust [3]. These features make blockchain applicable to the controlled and safe sharing (transmission) of data, and researches have been carried out in this area. Hyperledger Fabric set up channels in the blockchain system to enable access control, making particular data accessible only to the peers in the channel. Blackberry uses blockchain to enable the safe sharing of healthcare data between patients, hospitals and researchers. DARPA launched a project to develop encryption software to preserve the safety of military intelligence, while U. S. Navy has applied blockchain to the data transmission between 3D printing stations [4]. Wang [5] established a model of controlled data sharing and access, enabling accurate access control and safe sharing. Wu [6] introduced a data protection method for information systems based on blockchain, using multi-chain system to control the data access and operating authorities of peers. Guo [7] introduced a data sharing protocol of blockchain based on digital digest matching algorithm, enabling the controlled sharing of data with privacy preserved. Xia [8] established a data property preservation and transaction platform based on blockchain to authenticate data and enhance system safety and reliability. Liu [9] built the DSOC framework based on homomorphic encryption algorithm to share data safely on the blockchain.

In the ship industry, Blockchain is mostly applied in shipping logistics and maritime managements at present, the application in R&D is still limited. One example is that the China Classification Society (CCS) has established its

2473-3636/22/$31.00 ©2022 IEEE
DOI 10.1109/DCABES57229.2022.00023

ship data sharing platform based on blockchain[10], enabling the safe sharing of data between shipyards, designers, inspectors and shipowners.

III. APPLICATION SCENARIOS

The classical modes of data sharing can be sorted into two categories: 1) authorized remote access of data without living the local domain, 2) data collected and applied in one central domain. The classical mode may cause data producers attacked with network ports exposed. What's more, the safety and privacy of data is totally relied on the system server, the data itself and the log may be falsified, and causing data be leaked, stolen or misused.

The classical way of data application also has its shortcomings. Usually the original data is directly transmitted to the authorized recipients, which may lead to the leak of data, and the recipients may copy and keep the data without permission from owners, or even give the data to the third party. This will cause data being out of control, leading to intellectual property disputes and confidentiality problems.

These problems indicate that we need new method to enable data application with preserving data safety, and the new method needs new technology. Blockchain is introduced in this method for data encryption and storage, as well as property authentication and usage log. The authorized users can only use data through data-driven programs without accessing original data, and their actions will be logged by blockchain. The following works should be done to have the mentioned functions achieved.

1. Building of the blockchain system. Hyperledger Fabric is the most widely used alliance blockchain framework at present, and it is established with cooperation partners as peer nodes. Customized functions such as data encryption-decryption, authentication, logging, and system and account management need to be developed according to specific scenarios.

2. Development of data authentication and controlled sharing functions. The data of ship R&D needs to be classified according to its basic characteristics such as objects, discipline and confidential rank, and collected with the classification rules. The hash DNA of data based on data's characteristics, content and provider is used as certificate of authentication. Data access is controlled by the authority limits and confidential rank of users and data itself, and the users' identities, organizations and time of access will be logged on the blockchain.

3. Combination of data-driven programs and blockchain. Data is applied through data-driven programs in this method to make data accessible while invisible. Data-driven programs in this paper includes programs for ship performance prediction, evaluation and optimization, which need external data to train surrogate models. These programs need to be integrated with blockchain framework to enable them to get access to data and upload the usage log.

IV. SYSTEM FUNCTION DESIGNATION

There are two main functions to develop in this method:

- Storage and authentication of data. Data provided by cooperation partners is uploaded and storage on the blockchain with encryption. Authentication certification is auto generated, and duplication is prevented through hash checking.
- Application and logging of data. Data is applied through programs without direct access to users, and usage log is uploaded to the blockchain automatically.

In addition, there are also specific functions such as account and system administration.

The function of data storage and authentication is shown in fig.2, and the major steps are as follows:

a) Data providers organize their local data by the data collection rules, and upload data to the system.

b) Basic characteristics of data is reviewed by system administrator, and the unsatisfactory data will be returned to the provider.

c) Hash of the data is calculated as its authentication certification.

d) Duplication checking of the new uploaded data by comparison with data hash already existed on the blockchain. The new data will be authenticated if there's no duplication, or it will be returned.

e) The successfully authenticated data will be encrypted and storage on the blockchain. Specific characteristic parameters will not be encrypted in order to be retrieved by programs.

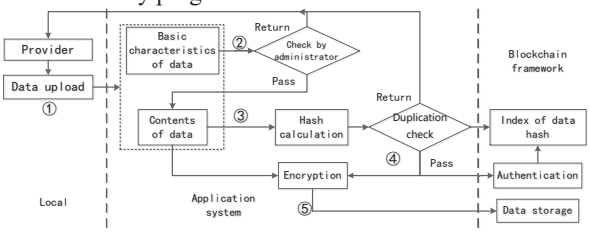

Figure 2. Storage and authentication of data

The function of data application and logging is shown in fig.3, and the major steps are as follows:

a) User runs the program, and program sends data request to the blockchain.

b) Data available for retrieve is limited by the confidential rank of users, and available data can be retrieved by specific characteristic parameters.

c) Decrypt the retrieved data and return it to the program which sent the request.

d) Program receives data and shows the execution result to the user, the result can be uploaded to the blockchain if necessary.

e) Save the usage log on the blockchain.

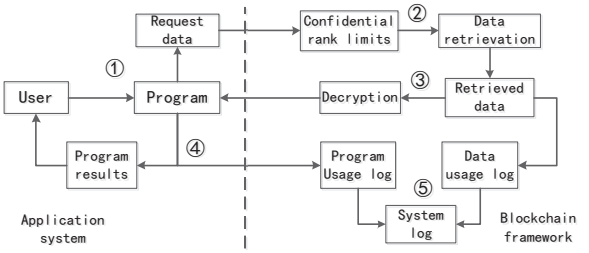

Figure 3. Application and logging of data

No users nor administrators have direct interaction to the blockchain framework, but through the application system. The main function of the application system is to

serve as the GUI and API integration platform. No data is stored in the application system server, and the providers could only see the content of their own data, while administrators could see the basic characteristics.

V. DEMONSTRATION AND TEST

To test and verify the data sharing and application method introduced in this paper, a demonstration has been established. A blockchain framework and application system is set up, and multi servers are employed to simulate multi cooperation partners. An array of ship resistance data from CSSRC is applied for the system function test, and the ship resistance prediction program based on dynamic surrogate modelling, which needs external data to execute, is used as a demo. Execution process of the program is shown in fig.4, including major steps as following:

a) User runs the program and enters information need for prediction on the GUI, including principal dimensions, hull-form parameters and speed.

b) Program retrieves data on the blockchain according to its predetermined rules and the user's input.

c) Program trains surrogate models based on the data retrieved.

d) Ship resistance calculation with the model and user's input.

The most significant feature of this program is dynamic modelling instead of fixed models. When the program runs, data of several ships which are the most similar with the target ship, whose resistance needs to be predicted, will be retrieved and applied for surrogate modelling. Specific surrogate prediction models will be built for different target ships based on different data in this program, which could enhance the performance of modelling as well as prediction. Readers can refer to the reference [12] for detailed introduction of the modelling method applied in this program.

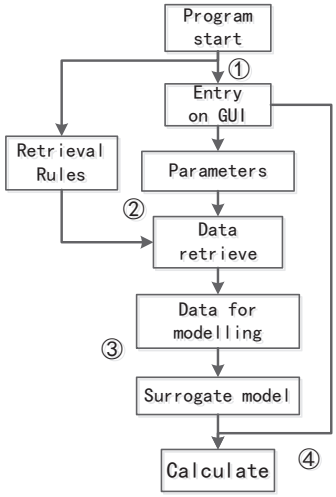

Figure 4. Execution process of the demo program

Multiple users are created on peer servers as simulation of different cooperation partners for the test. The demo data is assigned to different simulated partners and upload to the blockchain and stored with authentication certification after duplication checking. System administrators have the authority to see the basic information of all the data stored on the blockchain as shown in fig.5, but not the contents.

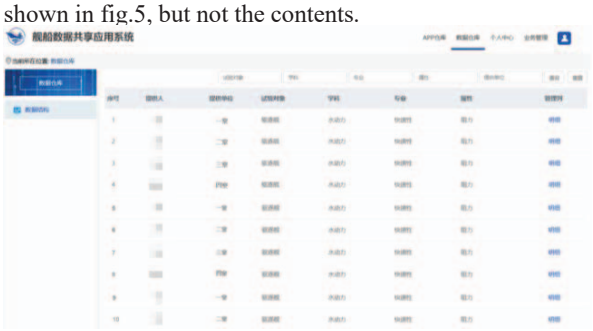

Figure 5. Data information list on the blockchain

Data stored on the blockchain is then available for users to apply through the demo program. User enters the necessary information for prediction on GUI, then the program gets data from blockchain, train the surrogate model and predict the resistance of target ship.

Figure 6. GUI of the demonstration program

The usage log of data will be saved on the blockchain when the prediction in done. The data provider could check the usage log as shown in fig.7, including the identity of users, time and program applied.

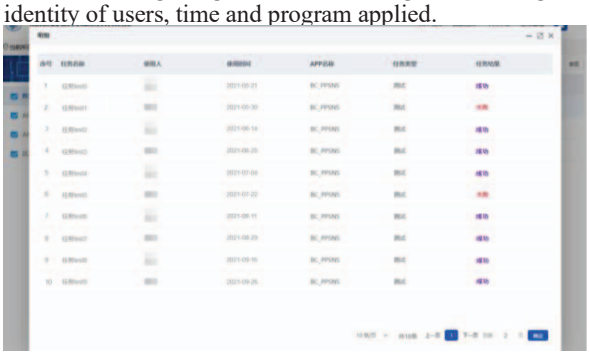

Figure 7. Data usage log on the blockchain

VI. CONCLUSIONS

The technical features of blockchain applicable for authentication, sharing and application of data, and provided an available way for the application of R&D data in ship industry. With the help of blockchain, data as well as other intellectual properties could be applied sufficiently and safely. According to the requirement of data application, a method for data sharing and application is introduced in this paper, and its function is verified with a

demonstration, showing this method available for practical application. Data has already become an essential source of technology and engineering innovation, and the implement of blockchain could effectively solve the problems in the new mode of cooperation and sharing, boosting the development and innovation of ship industry.

REFERENCES

[1] Zhao Feng, Chen Weizheng, Wei Xizhong, Chen Yihong. A system engineering based approach to enhance ship general performance [J]. Ship Building of China, 2021, 62(2): 275-283.

[2] China's blockchain technology and application development white paper 2016[EB/OL]. Ministry of Industry and Information Technology, 2016

[3] HUAWEI Blockchain R&D team. The technology and application of blockchain [M]. Beijing: Tsinghua University Press, 2019

[4] Hou Jiabin, Li Jun. Prospect of blockchain's military application [J]. China Information Security, 2019(2): 108-111.

[5] Wang Xiuli, Jiang Xiaozhou, Li Yang. Model for data access control and sharing based on blockchain [J]. Journal of Software, 2019, 30(6): 1661-1669.

[6] Wu Daiyue, Yu Xiang, Wang Chao, Li Qiang. Data protection technology for information systems based on blockchain [J]. Journal of Command and Control, 2018, 4(3): 183-188.

[7] Guo Naiwang, Ni Weidong. Privacy protection data sharing based on blockchain [J]. Communications Technology, 2019, 52(8): 1982-1986.

[8] Xia Junjie, Sun Ye, Yang Haitao, Chen Chang. Research and application of data asset protection and trading platform based on blockchain [J]. Design Technology of Posts and Telecommunications, 2019(9): 5-9.

[9] Liu Yansong, Xia Qi, Li Zhu, Xia Hu, Zhang Xiaosong, Gao Jianbin. Research on secure data sharing system based on blockchain [J]. Big Data Research. 2020, 6.
https://kns.cnki.net/kcms/detail/10.1321.G2.20200622.1046.002.html

[10] China Classification Society. CCS builds a new ecology of data together with the ship industry [EB/OL]. 2020, 8.
https://www.ccs.org.cn/ccswz/articleDetail?id=20200811084976492

[11] Zhang Zhao, Tian Jixin, Jin Cheqing. On-chian witness and off-chain transmission trustworthy data sharing platform [J]. Big Data Research, 2020, 6(5): 106-117.

[12] Liu Zixiang. A new method for ship hydrodynamic performance prediction based on test data of scaled models [D]. China Ship Scientific Research Center, 2019.