2020 2nd International Conference on Information Technology and Computer Application (ITCA) | 978-1-6654-0378-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITCA52113.2020.00092

Research on aerospace data transaction platform and method based on blockchain

Wu Dan[1] Li Yin [2]Wang Yeying[3] Wang Rui[4] Fan Chen[5]Zhang Zhongyang[6]Hu Dongdong[7]Guo Liang[8]
China Academy of Aerospace Systems Science and Engineering
Beijing, China
[1]wdan511@sina.com [2]10990473@qq.com [3]373755998@qq.com [4]wang_rui_185@163.com [5]fancheng@yeah.net [6]dsxyfj@163.com
[7]hudd710@163.com [8]louis8005@163.com

***Abstract*—This article authorizes all relevant participants to join the private blockchain network and form a stakeholder alliance to jointly maintain the operation of the blockchain. It not only ensures the legal compliance of the participants in the transaction system, increases mutual trust between the participants, but also provides an open and collaborative environment, and realizes the benign circulation of aerospace industry resources. The data transaction method in this article covers the entire life cycle process of data production and transaction, and uses blockchain technology to ensure data credibility, data security, and transaction traceability. It solves the problems of proof of the value of aerospace test data, data security and network transaction trust, protects the interests of both parties in the transaction, and effectively expands the application scope of aerospace industry resources.**

Keywords-blockchain; transaction;system; data; aerospace

I. INTRODUCTION

The aerospace industry investment has the characteristics of long cycle, large capital demand, difficulty in infrastructure construction, and limited space resources. In order to rationally allocate and effectively use various resources, effectively avoid repeated construction, decentralized construction, and maximize resource conservation, it is necessary to establish An open and collaborative environment activates the vitality of the entire industry chain, improves the regeneration capacity and use efficiency of state-owned assets, maximizes the utilization of industrial resources, creates greater social value, activates social innovation vitality, reduces corporate costs, and establishes sustainable development Space industry ecology.

II. NECESSITY ANALYSIS

Due to the particularity of the operating environment of the spacecraft, a large number of tests are required before the spacecraft is launched. The tests include static tests, dynamic tests, fatigue tests, flight tests, sea tests, etc. Scientific tests are what any product and system must go through. The test data is the most direct “product” of the test, and its importance and value are self-evident. Many test data are valuable wealth obtained at a huge price. For example, the flight test used for the verification of aerospace model products is very expensive for a single verification. At present, it is only used for one unit to verify one type of number. It is undoubtedly a huge waste of assets. The flight test data is collected and processed as simulation data. New product verification will greatly reduce the research and development costs of new products. With the increasing complexity of new aerospace products, challenges such as heavy test tasks, complex test procedures, long test cycles, and high costs have severely restricted the development of military products and the development of commercial aerospace. It is necessary to fully integrate test equipment, test procedures and test data Only by waiting for test resources can the test and verification capabilities of military products be improved, so as to reduce the cost of military product development and shorten the development cycle; at the same time, the rich stock assets generated by the country's large scientific research funds are used to transform results and invest Going to the trading market, revitalizing the stock assets to generate greater economic benefits will greatly promote the development of the aerospace industry. However, as an intangible asset, test data has its particularity and cannot be traded like general products. It is difficult to prove its functionality and value, and it is difficult to protect its security. Traditional data transaction methods cannot solve the problem of space test data. Issues such as value proof, data security, and online transaction trust require a brand-new transaction method to ensure test data security and asset transparency, while at the same time protecting the interests of both parties to the transaction. Blockchain uses computer technologies such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption technology for each independent node in a decentralized network structure. It has the characteristics of multi-party trust consensus, transaction traceability, and data cannot be tampered with. Therefore, the blockchain technology can be used for the credit authentication of both parties to the transaction and the management, transmission and transaction of aerospace test data to ensure credible transactions, credible data value, data security and transaction traceability.

III. SYSTEM DESIGN

A. System Framework

The aerospace industry platform ecosystem consists of five parts, namely the infrastructure layer, the resource layer, the information processing layer, the application layer, and the presentation layer.

B. Units

- The infrastructure layer includes aerospace cloud center and network layer;
- The resource layer includes service resources, equipment resources, site resources, product resources and test data resources;
- The information processing layer mainly includes big data platform, platform middleware and application container middleware;

978-1-6654-0378-8/20/$31.00 ©2020 IEEE
DOI 10.1109/ITCA52113.2020.00092

- The application layer mainly includes supporting applications such as corporate credit investigation, transaction systems, financial services, qualification certification, and blockchain identity management, as well as public applications such as intelligent research and development, intelligent production, intelligent services, and intelligent management;

- The presentation layer mainly includes the resource panorama, the design capability panorama, the production capability panorama, the mission panorama, the launch capability panorama, and the demand panorama.

C. Function Description

The block diagram of the aerospace test data transaction system described in this study. This research proposes a space test data transaction system. The data transaction system[1] is composed of user management module, data product processing module, data product generation module, test data display module, test data query module, test data transaction module, data right confirmation module, transaction after-sales processing module, etc. Among them, the user management module includes a user registration sub-module, a user trusted authentication sub-module, a blockchain authentication sub-module, and a blockchain member management sub-module.

The process and method of aerospace experiment data transaction system from user registration to becoming a member of the blockchain mainly includes the following steps.

- Step 1: User registration. Units or enterprises planning to enter the trading system upload user registration information, including user information, credit certification documents, industry-related qualifications, military qualifications, industry certifications, test-related certification materials, transaction records, loan information, etc., for user registration. User registration information is processed by data preprocessing such as denoising, missing value processing, and normalization to obtain user registration information set M.

- Step 2: Qualification certification. The blockchain central node unit reviews the materials and inquires whether the user qualification certification materials meet the requirements and whether they have the corresponding qualifications. If not, they will not be able to enter the system; users who pass the qualification review can enter the trading system.

- Step 3: Trustworthy evaluation. Inquire whether users have credit reporting problems. If there are credit reporting problems, they will not be able to enter the trading system or participate in transactions; companies or individuals that pass the first credit review review will be re-evaluated for credibility before participating in the transaction. The system establishes a credible model to make credible evaluations of enterprises or individuals, and system users with high evaluations will get trading opportunities. Ensure that both parties involved in the transaction are trusted companies.

- Step 4: Blockchain identity verification. Perform blockchain identity authentication for the settled company or individual, distribute blockchain network nodes, distribute public and private keys and digital signatures, and member information enters the blockchain member management module at the same time and joins the member group. The registration node will assign a member node to the member in the blockchain network. Users who are assigned member nodes will get corresponding blockchain permissions.

  The registration node assigns a bloom filter value from the bloom filter value set S to each member node; the registration node uses the public key of each node to encrypt the identity verification result of each node and returns it to the corresponding node; among them, return The successful result of the identity verification for the node includes: the bloom filter value assigned to the node, the identities of all member nodes, the public key PK, the bloom filter FS constructed according to the set S, and the hash function used when constructing the FS .

In step 3, the trusted model adopts the feature learning method. Construct a regression tree model, and use the square error minimization criterion for the regression tree to select features[2]. The process is to use the original feature data to train the feature model, then use the tree path learned by the tree model to construct new features, and finally add these new features to the original features to train the user data trust model[3]. The steps for establishing a trusted model are as follows:

1) The user registration information data set M obtained by data preprocessing is used as the input of the tree model. The data set M learns the data feature set $C^{(1)}$ through the first tree. The calculation formula is as follows[4]:

$$C^{(1)} = f(M,W) = \sum_{\mathrm{t}=0}^{T} a_t \mathrm{m}_t(M,W_t)$$

Among them, M is the input sample data, a is the weight of each tree, m is the classification regression tree, and W is the parameter of the classification regression tree.

$$\mathrm{W}=\begin{bmatrix} w_{11}^{(0)} & w_{12}^{(0)} & w_{13}^{(0)} & \cdots & w_{1k}^{(0)} \\ w_{21}^{(0)} & w_{22}^{(0)} & w_{23}^{(0)} & \cdots & w_{2k}^{(0)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w_{t1}^{(0)} & w_{t2}^{(0)} & w_{t3}^{(0)} & \cdots & w_{tk}^{(0)} \end{bmatrix}$$

$$C^{(1)}=\begin{bmatrix} c_{11}^{(1)} & c_{12}^{(1)} & c_{13}^{(1)} & \cdots & c_{1k}^{(1)} \\ c_{21}^{(1)} & c_{22}^{(1)} & c_{23}^{(1)} & \cdots & c_{2k}^{(1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{t1}^{(1)} & c_{t2}^{(1)} & c_{t3}^{(1)} & \cdots & c_{tk}^{(1)} \end{bmatrix}$$

Among them, K represents the dimension after the first learning.

2) Take the square difference between the learned$C^{(1)}$ *and the original real data to obtain the residual data set E. The residual calculation formula is as follows:*

$$E=\min\sqrt{\sum_{i=0}^{N}(y_i-\mathrm{m}_t(M,W_t))^2}$$

Among them, y is the label value of the data. The larger the E, the more scattered the data of the node.

$$\mathrm{E}=\begin{bmatrix} e_{11}^{(0)} & e_{12}^{(0)} & e_{13}^{(0)} & \cdots & e_{1t}^{(0)} \\ e_{21}^{(0)} & e_{22}^{(0)} & e_{23}^{(0)} & \cdots & e_{2t}^{(0)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{m1}^{(0)} & e_{m2}^{(0)} & e_{m3}^{(0)} & \cdots & e_{mt}^{(0)} \end{bmatrix}$$

3) Use E as the data training set for the next regression tree construction, and repeat steps 1) and 2) until the final residual is 0 or the number of times the regression tree is limited, and finally a tree model of q regression trees is obtained. q represents the number of trees of the feature learning model finally obtained. Save the path information of these trees to get$V^{(q)}$*, which is the final learned feature data.*

$$V^{(q)}=\begin{bmatrix} v_{11}^{(q)} & v_{12}^{(q)} & v_{13}^{(q)} & \cdots & v_{1p}^{(q)} \\ v_{21}^{(q)} & v_{22}^{(q)} & v_{23}^{(q)} & \cdots & v_{2p}^{(q)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{m1}^{(q)} & v_{m2}^{(q)} & v_{m3}^{(q)} & \cdots & v_{mp}^{(q)} \end{bmatrix}$$

Among them, p is the dimension of the feature after q times of regression tree learning.

The feature set $V^{(q)}$ extracted by deep learning is substituted into the user credibility model for training, and s trees are learned to obtain the credibility evaluation model. Then use the following function for sample prediction:

$$\mathrm{y_i}=\sum_{\mathrm{i}\in I}\mathrm{f}_s(x_i),\mathrm{f}_s\in F$$

Among them, F is the hypothesis space, f(x) is the regression tree[5]:

$$F=\{\mathrm{f}(x)=w_{q_{(x)}}\}(\mathrm{q}:R^{\mathrm{m}}\to T,w\in R^T)$$

$\mathrm{q}_{(x)}$represents the leaf node to which the sample x is assigned, w is the value of the leaf node, then $\mathrm{W}_{\mathrm{q(x)}}$ is the predicted value of the sample x. When $\mathrm{W}_{\mathrm{q(x)}}$ is close to 1, the user credibility is low, and close to 0, the user credibility is high.

IV. DATA TRANSACTION METHOD

This research provides a test data transaction method based on the space test data transaction system .

The method described in this study covers the entire life cycle process of data verification, data product right confirmation, data block storage certificate, data product transaction, transaction after-sales, transaction traceability, etc., ensuring data credibility, data security, transaction cancellation, and transaction Traceable. The method includes the following steps.

A. Data verification

Perform data processing and verification on test data packages uploaded by users, such as virus cleaning, data legality verification, and data compliance verification. The verification of the legality of data means that data containing illegal information and infringement will not be able to generate data products; only data that meets each step can be used for data product generation.

The test data package may include various test information such as test pieces, test equipment information, test tasks, test costs, test standards, test instrument information, test data, and experience knowledge. The test data in the embodiment includes: finalization test data, third-party test data, development test data, etc., such as test data such as heat protection structure, flight parameters, thermal environment data, thermal response data, and test photos.

Perform data verification before data product generation. After virus cleanup, data legality verification, and data compliance verification, data products can only be generated after verification to ensure data compliance and security .

B. Data Product Confirmation

The design unit or designer provides the identification and the certificate showing the ownership of the test data (such as: test product photos, test purpose description, test plan, test process, previous test results, test data screenshots, test data video explanation, third-party product quality Authentication materials, etc.), the system verifies and authenticates the generated data products by adding watermarks, and then generates them as data products and enters the trading system.

The method for adding a data confirmation watermark to the data product that needs to be confirmed is as follows: use the public key PK1 and the private key PK2 to add the watermark SY to the data product and perform encryption processing through the Hash operation to obtain the encrypted data confirmation watermark SY1. The public key is used to identify the node's identity, and the private key is used to encrypt data and sign.

SY= hash(C||ID||CID||DI)

SY1=hash(PK1||PK2||SY)

The encrypted digital watermark (SY1) jointly generated by data summary information (C), user ID (ID), company information (CID), database information (DI), etc. can be used as the authentication information for the copyright owner of the data product.

C. Data Block Deposit

The aerospace test data transaction system uses blockchain technology to store test data, perform multi-dimensional intelligent data authentication, and perform dual authentication of trusted timestamp and chain stamp, and generate unique identification information for each test data packet, which can be traded Provide effective evidence when tracing and attribution disputes.

D. *Data product transaction*

When conducting data product transactions, the system displays the value of the test data product information in a visual manner, and provides detailed query of the data information, and the purchaser can decide whether to purchase and data trial. The system will record the specific details of the transaction, reduce the possibility of ultra vires, and provide strong evidence when ultra vires occurs. In order to ensure the interests of both parties to the transaction, the system provides the purchaser with viewing and downloading permissions, and the system provides different keys for users with different permissions. When the transaction is submitted, the purchaser will be provided with the permission to view the data to confirm whether the purchase requirement is met. The purchaser needs to confirm whether to purchase or not to purchase within the specified time. If it does not purchase, the transaction needs to be cancelled; if it is purchased, the transaction needs to be confirmed. After the purchaser confirms the transaction, the system provides a key with download authority. If the specified time is exceeded, the transaction will default to being confirmed, the transaction can no longer be cancelled, the data cannot be returned, and the purchaser has the right to download the data. When the transaction is confirmed or cancelled, the transaction information will be written to the blockchain. Transaction information includes[6]: transaction time, transaction type, transaction name, information of both parties to the transaction, transaction quantity, data usage, data packet size, data file quantity, brief description of test data, transaction ID, transaction encryption watermark, etc.

The transaction information is written into the database watermark, and when the database is read, the corresponding transaction information can be viewed. The transaction execution steps are as follows:

1. When member node B initiates a data transaction to member node A, it will obtain the key to read data permission to check whether the data meets the requirements; the transaction type TT in this transaction information is written as the only node B's blockchain Identify SID and read status R, TT=hash(SID&R).

2. If the transaction is confirmed by the purchaser or the system defaults to the confirmed state within the specified time, the member node B obtains the key to download the data permission, can download the data, and the transaction is completed. The transaction type TT in the transaction information is rewritten as the node B's blockchain unique identifier SID and download status D, TT=hash(SID&D).

If the transaction is not completed and the transaction is cancelled, the transaction information needs to be rewritten to the canceled state, and the transaction state TT in this transaction information is restored to the initial state. Member node B cannot obtain read and download permissions unless the transaction is initiated again

E. *After-sales Transaction*

In order to protect the rights of buyers and sellers, after-sales functions are provided. When the buyer finds that the data is unavailable or the data is inconsistent with expectations, it can apply for after-sales transaction; when performing after-sales processing, the seller's data is guaranteed not to be stolen, used or transferred.

F. *Transaction traceability*

In order to protect the rights and interests of buyers and sellers, both parties in a transaction can maintain their rights through the system. After the transaction is completed, if one party to the transaction discovers that the data is infringing, it can apply for transaction details.

V. Research result

The aerospace test data transaction system proposed by the research will authorize all relevant participants to join the private blockchain network and form a stakeholder alliance to jointly maintain the operation of the blockchain. It not only guarantees the legal compliance of the participants in the trading system, increases mutual trust between the participants, but also provides an open and collaborative environment and realizes the benign circulation of aerospace industry resources;

The test data transaction method based on the aerospace test data transaction system proposed in this research covers the entire life cycle process of data product generation, data product confirmation, data block storage, data product transaction, transaction traceability, etc., using blockchain technology , To ensure data credibility, data security, and transaction traceability; to solve the problems of aerospace test data value proof, data security and network transaction trust, protect the interests of both parties in the transaction, and effectively expand the application scope of aerospace industry resources.

Refrerence

[1] Li Chao, Dai Bingrong, Zhao Xiaofeng,Wang xiaoqiang, Design and implementation of digital credit trading system based on blockchain technology[J]. Modern Computer (Professional Edition), 2018, 627(27):76-80.

[2] Yu Huan, Research on user preference based on data mining technology[D]. 2018.

[3] Deng Lifang. Research on the Cold Start Problem in Search Ads Click Through Rate Prediction[D]. 2016.

[4] Microstrong, “Deep understanding of GBDT regression algorithm”, unpublished.

[5] Anonymous,“Understanding GBDT+XGBoost from parameter space to function space”, unpublished.

[6] Huang Jiehua, Gao Lingchao, Xu Yuzhuang, Bai Xiaomin, and Hu Kai, Smart Contract Design on Crowdfunding Blockchain[J]. Information Security Research, 2017(3).