Blockchain-Based Ship Energy Consumption Data Access and Control

Shuailin Chen[1], Junbo Gao[2, *]

351589943@qq.com[1], jbgao@shmtu.edu.cn[2, *]

Shanghai Maritime University, Shanghai, China

Abstract. With the continuous development of the maritime industry and the increase in global environmental awareness, reducing carbon emissions from ships has become a global consensus. Under the current Internet environment, maritime ship energy consumption data has data access control and data traceability problems, and how to collect ship energy consumption carbon tax is also a problem. Ship energy consumption data is an important basis for assessing ship performance, optimising ship operation and reducing carbon emissions, so how to collect, store and securely access these ship energy consumption data has become a key research direction. Therefore, this paper proposes a blockchain-based scheme for accessing and controlling ship energy consumption data.

Keywords: Blockchain, Hyperledger Fabric, Access control, Smart contract.

1 Introduction

On the one hand, with the rapid development of information technology and intelligent technology as well as the rapid development of Internet technology, more and more information collection devices and intelligent devices have been widely used in the fields of smart city construction, smart medical care and smart transport. In recent years, they have also been more and more widely used in the construction of smart shipping. These devices are connected to each other through wireless networks to form a distributed network to transmit various data information. During a ship's voyage, these devices can collect a variety of data, such as the data of the ship itself, the data of the shipping company, the information of the ship's crew, the data of the ship's energy consumption, and so on. These data resources may contain state secrets, commercial secrets or personal privacy, etc. Once data leakage and other undesirable behaviours occur, it will cause different degrees of property loss or personal injury. However, these data resources sometimes need to be shared among different departments or individuals, e.g., for scientific research, business competition, ship performance monitoring, etc. Therefore, how to achieve secure data sharing and access control security has become a research hotspot in the field of intelligent shipping.

On the other hand, with the rise in global environmental awareness, reducing carbon emissions from ships has become a global consensus. To achieve this goal, governments and international organisations have introduced a series of policies and standards to encourage ship operators to adopt more environmentally friendly and efficient technologies to reduce energy consumption and emissions. For example, a carbon tax is levied on ship energy consumption. Ship energy consumption data is an important basis for assessing ship

ICBBEM 2024, March 29-31, Wuhan, People's Republic of China

DOI 10.4108/eai.29-3-2024.2347410

performance, optimising ship operations and reducing carbon emissions. Therefore, how to collect, store and securely access these ship energy consumption data has become an important research direction.

However, there are some problems with traditional data collection and storage of ship energy consumption data, such as missing, inaccurate and easily tampered data. These problems will not only affect the operational efficiency and safety of ships, but also the sustainable development of the shipping industry. Therefore, the establishment of a reliable, secure and accessible ship energy consumption data collection and management system has become an important research direction.

Blockchain technology, as a decentralised and distributed data management and exchange method, has the advantages of high reliability, good security, and tamper-proof data[6]. Therefore, applying blockchain technology to the collection, storage and management of ship energy consumption data can effectively improve the credibility and security of the data, prevent data from being tampered with and leaked, improve the accuracy and reliability of ship energy consumption data, and thus provide important support for the sustainable development of the shipping industry.

Therefore, it is of great significance to study the access and control of ship energy consumption data based on blockchain. By studying how to establish a credible, secure and traceable ship energy consumption data management system using blockchain technology, it can promote the sustainable development of the shipping industry, reduce energy consumption and emissions, collect relevant carbon taxes, and improve the efficiency and safety of ship operations, thus promoting global environmental protection and sustainable development.

2 Related Experiments and Technologies

2.1 Block Chain

Block Chain (BC) is a new type of decentralised protocol that implements peer-to-peer [1]transactions in a network where nodes don't trust each other by means of hash algorithms, digital certificates, and transaction signatures, for an example see **Fig**. 1.

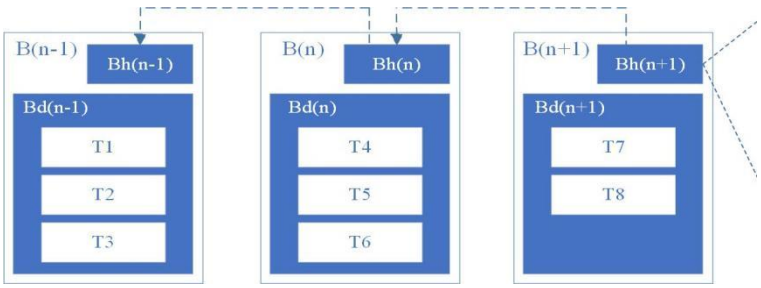

Fig. 1. Blockchain Structure.

Each block contains multiple records of transactions (Trade, T) stored in chronological order. Block (Block, B) consists of block header (Block header, Bh) and block body (Block body, Bd), in which the block header contains the Hash value (CH) of all the transactions in the

current block and the Hash value (PH) of the parent block header, and the current block and all of its sub-blocks will be affected once the transaction data in the block is altered. Therefore, blockchain has the system characteristics of information traceability and data tampering prevention:

(i) Traceability: in the chained data structure of blockchain, each block possesses the hash value of its previous block, which enables blockchain to realise data traceability through the hash value;

(ii) Anti-tampering: the data will be stored permanently after verifying the chain, unless more than 51% of the nodes in the attack system can be changed, so the reliability and security of blockchain data are extremely high.

In addition, blockchain has the technical advantages of decentralised storage, openness and transparency, system autonomy and anonymous transactions:

(iii) Decentralisation: there is no centralised hardware or management body in the blockchain network, all nodes have bookkeeping rights and work together to complete system data uploading and maintenance;

(iv) Openness: in addition to the private information of each transaction node being encrypted, the data in the blockchain network is open to all participants, and any organisation or individual can query the data through the open interface, and the whole network is highly transparent;

(v) Autonomy: the blockchain system adopts consensus contracts, which are automatically executed when the contract conditions are met, and all participating nodes are able to securely transact on their own in a de-trusted network;

(vi) Anonymity: nodes in the blockchain network are addressed based on a fixed algorithm, and both parties to a transaction can execute the transaction without disclosing each other's identity.

2.2 Hyperledger Fabric

The network architecture of Hyperledger Fabric[2] mainly includes Certificate Authority (CA), Client (CLI), Peer node (Peer), and Order node (Order).The Fabric transaction flow is shown in **Fig. 2**, CA node is responsible for carrying out the certificate of identity for all members of the network management and provides PKI (Public Key Infrastructure) services; CLI nodes are mainly used to create transactions and broadcast transaction requests to Order nodes after receiving sufficient transaction endorsements; Peer nodes are mainly responsible for maintaining the state and ledger, and are divided into Endorser nodes and Confirmation nodes (Committer): The Endorser node invokes the smart contract according to the specified strategy, endorses the transaction result and returns it to the CLI node, while the Committer node is responsible for checking the legitimacy of the transaction, and at the same time updating and maintaining the local ledger, the state database LevelDB; the Order node is responsible for sorting the transactions submitted by the CLI, and after that generates a new block and broadcasts it to the Committer node broadcast to the Committer node.

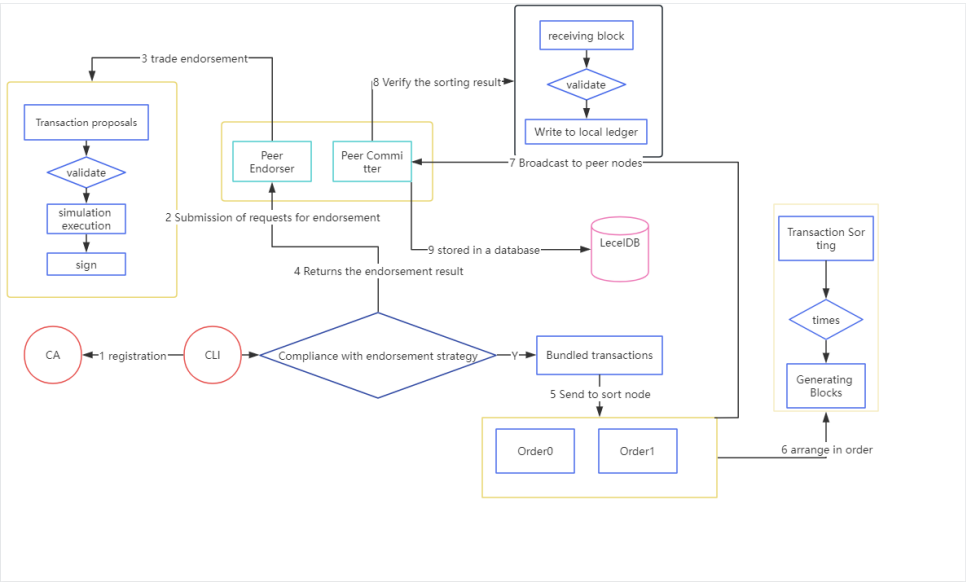

Fig. 2. Hyperledger Fabric Transaction Flow.

Hyperledger Fabric realises complex queries of data through an immutable distributed ledger, and compared with public chain platforms such as Bitcoin and Ethereum, Fabric has the advantages of high throughput, strong security, and efficient consensus algorithm, which is more suitable for enterprise-level applications and facilitates users' commercial development. Considering the sensitivity of ship energy consumption data and the needs of ports and ships for privacy protection and data security[5], this paper adopts the Fabric platform to complete the design and development of the ship energy consumption system, which provides users with high transaction throughput performance and low transaction confirmation latency, and at the same time ensures the privacy and confidentiality of information related to ship energy consumption.

2.3 Smart Contract

Smart contracts are programmed contracts compiled by programming languages with complete Turing to avoid user default situations[3]. In the Fabric platform, smart contracts, also known as chaincode, can be implemented in a variety of programming languages such as Java, Go, Nodejs, etc., and are installed on each user node to verify the correctness of transactions, as well as to be invoked by external programs when they transact with the ledger. Smart contracts are not only a key mechanism for encapsulating information and keeping it simple throughout the network, they are also a key mechanism that can be written to allow participants to automate the execution of transactions. Many of the proposed solutions based on blockchain are implemented with simulations done through smart contracts.

The smart contract in Hyperledger Fabric, i.e., Chaincode (CC), can run independently in a Docker container with security attributes, and the gRPC protocol enables interaction with the designated Peer node, so as to carry out the corresponding operations on the ledger data and complete the client's command requests.

The interaction process of the chain code is shown in **Fig. 3**, firstly, the Peer node registers locally for the chain code and completes the initialisation work, after which the client CLI calls the chain code CC through Docker, and the chain code receives the transaction request and then processes it according to the pre-defined business logic, and returns the result of the processing to the Peer.

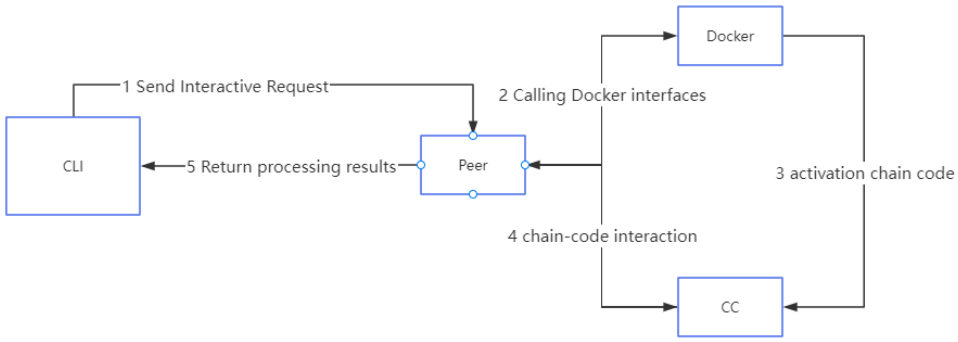

Fig. 3. Chain-Code Interaction Procedure.

2.4 Attribute-Based Access Control Schemes

Traditional access control is identity-based access control, in which a user controls the permissions to perform operations on data resources through the role or group assigned to the user by the system. In identity-based access control the user's role is associated with the permission to perform operations, and this type of access control is more cumbersome to manage. In real-world access control policies, user requests need to be approved or denied based on arbitrary attributes of the user and selected attributes of the object, as well as the environmental conditions under which the current policy is enforced, an approach commonly referred to as attribute-based access control.

Ship energy consumption data in an open network environment such as blockchain, attribute-based access control methods are more responsive to the needs of data access control. Attribute-based access control (ABAC)[4] is a flexible fine-grained access control method that controls access to data resources by evaluating the attributes of the relevant entities (subjects and objects), operational privileges, and environments of the requested data. Attribute-based access control methods can formulate an access control policy for a data requester in relation to a data resource. This policy does not need to specify a separate relationship between each data requester and each data resource, and determines the access control privileges of a data requester to a data resource mainly by determining whether the data requester has the correct attributes.

ABAC evaluates attributes of subjects, objects, operations, and environments to control access to objects, defined as A ∈ {S,O,P,E}.The meaning of each field is explained as follows: A stands for attributes, each of which has the format of a key-value pair, i.e. A={key: value}.S represents the attributes of the subject, i.e., the identity and characteristics of the entity that initiates the access request, such as the requester's ID, identity, public key, etc. O represents the attributes of the object, i.e., the attributes of the data resource, such as the type of the data resource, the data owner of the data resource, and the data owner's signature on the data resource, etc.P denotes the attribute of privilege, i.e., the executable operations of the subject on the object, such as read, write, etc. E denotes the attribute of environment, i.e., the environment information when generating the access request, such as the IP address, the time of the request, etc. An access control policy is formed by pairing and setting the attributes to realise the subject's access control to the object.

Here, according to the characteristics of blockchain with ABAC can dynamically carry out access control as well as fine-grained access control, using smart contract-based access control mechanism. With the trusted computing characteristics of the blockchain, users transform their access control policies into smart contract codes uploaded to the blockchain, and when the accessing subject meets the pre-set conditions of the contract, it is automatically granted access to the object and stored on the blockchain in the form of transactional transactions. To further expand, the user can use the smart contract to control all the data interaction processes between the access subject and the object, and realise the supervision and management of all the data such as the attribute states of the subject and the object, the traceability information of the permission granting, and the history of the policy updating.

2.5 Blockchain-based Data Access and Control Model for Ship Energy Consumption

The blockchain-based data access and control model for ship energy consumption is shown in **Fig. 4**.

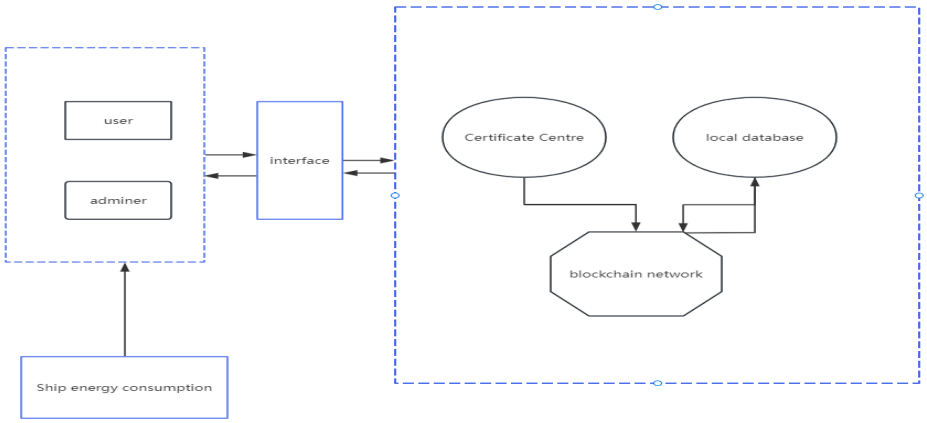

Fig. 4. Ship Energy Access Control Model.

The model includes the entities listed below:

(1) ship energy consumption

Ship's energy consumption data includes the ship's own attributes, port information, energy consumption information, and so on.

(2) user

Users have two identities, data owners and data requesters, and some data owners are also data requesters. Data owners are able to upload data resources on the blockchain network and manage the access control policies associated with the data resources, process requests from data requesters and respond to them. Data requesters, who can send requests to data owners, access private data resources through access control policies.

(3) manager

The administrator is responsible for managing the entire blockchain system. The administrator does not have the authority to change and delete the data resources and access control policies stored in the blockchain network, but only has the authority to start the blockchain network and install the chain code of the nodes. At the same time, the installation of the chain code requires that all legitimate endorsement nodes agree to install it, otherwise the transactions related to the installation of the chain code will be rejected, so as to prevent the administrator from illegally changing the chain code and causing damage to the blockchain network.

(4) certificate Centre

The Certificate Centre is the certificate issuing authority within the blockchain system, promulgating the relevant certificate to the new node as the unique identification. Each user needs to use the certificate issued by the CA to call the chain code directly using the client to achieve the operation of the blockchain system.

(5) blockchain network

The blockchain network consists of multiple nodes, which are subdivided into ORDERERER nodes and PEER nodes to implement functions such as validation, endorsement, and ordering of transactions. The blockchain network is a key component of the proposed scheme for data storage and authentication of the access control system.

This experiment has a total of 5 smart contracts as follows:

(1) User Contract: User smart contracts, user creation, login and other operations.

(2) Attribute Contract: Attribute smart contracts that dynamically generate access control policies based on attributes.

(3) User Attribute Contract: User attribute smart contracts, based on user attributes, determine whether it is legal to access the data.

(4) Energy Consumption Contract: Ship energy smart contract to query the relevant ship energy consumption and other related data.

(5) EC Policy Contract: Policy smart contracts that dynamically create access policies through attributes.

3 Conclusions

This paper proposes a blockchain-based access and control scheme for ship energy consumption data, which combines blockchain technology and ABAC model to solve the storage security as well as access control problems of ship energy consumption data. Firstly, for the energy consumption data generated by ship navigation, it is stored to the blockchain platform. Second, according to the definition of ABAC model, a dynamic access control scheme is proposed, which combines access request, visitor's attributes, environment and other factors to achieve the access control of ship energy consumption data. Moreover, based on the energy consumption data, it carries out the collection of carbon tax of relevant countries, responding to the concept of low carbon and environmental protection, which has a strong practical value.

References

[1] Liang W, Zhang D, X Lei, et al. Circuit Copyright Blockchain: Blockchain-based Homomorphic Encryption for IP Circuit Protection [J]. IEEE Transactions on Emerging Topics in Computing, 2020(99): 1-1.

[2] Liang W, Tang M, Long J, et al. A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things [J]. IEEE Transactions on Industrial Informatics, 2019:1-1.

[3] Abdullah S, Rothenberg S, Siegel E, et al. School of block-review of blockchain for the radiologists. Academic Radiology, 2020, 27(1):47–57.

[4] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. V oas, “Attribute-based access control,” Computer, vol. 48, no. 2, pp. 85–88, 2015, doi: 10.1109/MC.2015.33.

[5] Ahmad R W, Hasan H, Jayaraman R, et al. Blockchain applications and architectures for port operations and logistics management [J]. Research in Transportation Business and Management, 2021(4):100620.

[6] Botcha K M, Chakravarthy V V, Anurag . Enhancing Traceability in Pharmaceutical Supply Chain using Internet of Things (IoT) and Blockchain [C]. 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT). IEEE, 2019: 45-48.