Journal of Business and Technology Management Vol.2, No.1 (2021), pp.17-28
http//dx.doi.org/10.46410/jbtm.2021.2.1.03
Received: March 9, 2021 Reviewed: May 10, 2021 Accepted: June 17, 2021

Research on Commercial Data Sharing Model Based on Blockchain Consensus Mechanism

Chung Xuan Nhien[1]

[1] Hanoi University of Technology, Hanoi, Vietnam; cx_nhein@gmail.com

Abstract: Blockchain is a popular public ledger technology based on a consensus mechanism. In this paper, a blockchain-based commercial data sharing model is designed based on blockchain-related technologies and the Interplanetary File System. This model realizes basic operations such as the safe sharing of commercial data and the protection of commercial data and can ensure the safe sharing of commercial data at a lower economic cost. Compared with the existing model, it has more advantages in terms of security, scalability and cost. This model considers the basic operations of business data sharing and protection and does not do too much research on other aspects of business data applications. Through the establishment of the model in this article, the model can be extended to more fields and include more functions and will conduct more in-depth research on the blockchain consensus mechanism of business data management.

Keywords: *Commercial Data Center; Smart Contract Technology; Blockchain; Data Sharing*

1. Introduction

To maximize the benefits of commercial data, combining the current hot big data, data mining, and blockchain to mine the value of commercial data has become a research hotspot in recent years [1-2]. The existing commercial data management system relies on the commercial information management system [3]. Although it is more convenient than traditional commercial data management, there are still some problems. In the process of using commercial data, such as the process of data management and transmission, it is easy to be modified. For each business center, all business data is an island of information. Each business center cannot effectively share each other's data, and cannot maximize the value of the data. Existing commercial data security measures rely on technologies such as digital signatures and watermarks, which cannot be recovered when encountering extreme conditions such as data destruction and tampering. The authenticity of commercial data cannot be guaranteed. If the data in the commercial center is invaded or the relevant personnel are involved, the authenticity and security of the commercial data will be threatened.

Blockchain is a popular public ledger technology based on a consensus mechanism, which is decentralized and does not require a trusted third party [4]. Anyone who wants to change data needs to pay a huge cost, which leads to difficulties in implementation, is tamper-proof, and has features such as traceability. These high-quality characteristics of the blockchain make the research of the blockchain in various fields a hot topic, especially the application of the blockchain to privacy protection [5], such as the application of the blockchain to the protection of personal credit reporting systems [6], File data protection [7], medical data privacy protection [8-9], personal privacy, etc. The application of blockchain technology in data security protection is not only a theoretical study but also applied to real-life scenarios by many companies. For this article, these characteristics of blockchain help to solve the problems of poor security and ineffective sharing in current business data management. This paper proposes a commercial data sharing model based on technologies such as blockchain, cryptography and inter-planetary file system (IPFS) [10]. Propose solutions from the following aspects:

(1) Build alliance chains between commercial data centers and jointly maintain the operation of the system on this basis. Commercial data copies are linked to the public chain, which can reduce data maintenance costs and ensure data security.

(2) The original data is stored in encrypted form through the private interplanetary file cluster

system, combined with the blockchain smart contract technology, to store the summary information of the data, including the unique fingerprint sequence of the stored data, so as to realize the safe management of commercial data.

(3) With the help of blockchain technology and interplanetary file system, historical data can be traced, thus solving the problem of unrecoverable commercial data.

2. Basic Concepts

2.1. Blockchain technology-related knowledge

Blockchain stores data in units of data blocks. It is a non-central database that combines consensus algorithms and cryptography technology [11] so that each data block contains transaction information in the bit network, which can be anti-counterfeit and generate a new block. According to the open authority of the blockchain, the blockchain is divided into a public chain, a consortium chain, and a private chain. The public chain [12] means that the blockchain is completely open, and any node can participate in consensus. The alliance chain [13] is for alliance nodes to participate, and the consensus mechanism requires all alliance nodes to make joint decisions. The private chain [14] is used internally by the organization, and the access rights are not open.

The consensus mechanism [15] is to solve the consensus problem of all nodes in the blockchain. How to determine the validity of node data, all nodes share the same standard, which guarantees fairness and data security, and node data cannot be tampered with at will. The consensus mechanism of the blockchain requires that all nodes are equal and that the minority obey the majority. Only in this way can the security of the data be guaranteed. Here the minority obeys the majority does not necessarily refer to the number of nodes, it may be workload, computing power, time, and so on. According to a different basis, a variety of consensus mechanisms have been proposed, such as Proof of Work[16] algorithm, Proof of Stake[17] algorithm, Proof of Space[18] algorithm, Proof of Luck[19] algorithm, Proof of Elapsed Time [20] Algorithm, Delegated Proof of Stake[21] algorithm, Proof of Useful Work[22] algorithm, alliance chain Quorum[23], etc.

Smart contracts [24] are some special agreements for the decentralization of blockchains, which meet different needs and include all agreed terms. Only when all agreements are satisfied can they take effect, ensure fairness, and eliminate the possibility of human operation. Sex. The blockchain that supports smart contracts is represented by Ethereum, and smart contracts can be developed on this basis.

2.2. Knowledge of Interplanetary File System

The interplanetary file system (IPFS) is a network transmission protocol for distributed storage and file sharing [25]. Each file and data block on the system has a unique encrypted hash called a fingerprint, which has the characteristics of version tracking, addressability, non-tampering, and decentralization. The IPFS system is based on content addressing [26], all content has a unique fingerprint, and is divided into public cluster system and private cluster system according to different permissions to join the network: public cluster system is that any node can join the interplanetary file system freely; Private clusters are authorized nodes or organizations to join the system.

3. Models

3.1. System model

As shown in Figure 1, the commercial data sharing model proposed in this paper is composed of five modules: commercial data center, service center, alliance center, public blockchain, and private interplanetary file cluster system.

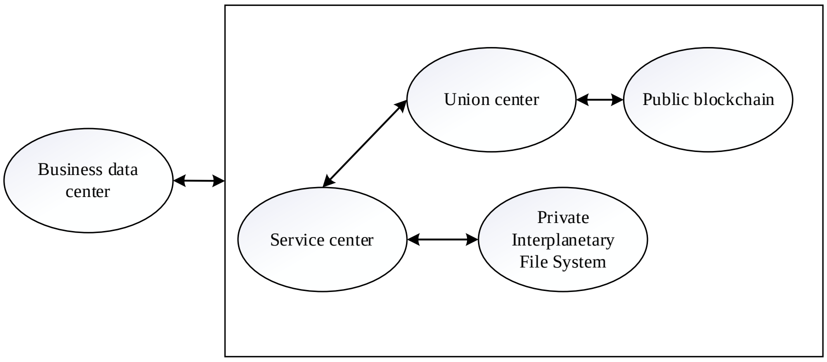

Figure 1. System model

As an important node of the commercial data sharing model, the commercial data center directly participates in the alliance blockchain center and has functions such as data protection, verification, and sharing.

The service center itself does not store data, it is a decentralized structure, and provides smart contracts and interplanetary file system interfaces for commercial data sharing models in the form of interfaces.

The alliance center is the Ethereum alliance chain. The data information of the commercial data center is stored through smart contracts, including the digital identity and summary information of the commercial data center, which is used to realize the registration, restoration, protection, and sharing of the identity of the commercial data center. Operate and interact with the public chain regularly to ensure data security.

The public blockchain is the Ethereum blockchain, which regularly stores the mirror image of the database copy of the alliance center to ensure the authenticity of the data in the alliance center.

The private interplanetary file cluster system stores the original information of commercial data. With the support of technologies such as distributed hash tables and block exchanges, it realizes node identity authentication and guarantees data security. The message flow of the above parts is shown in Figure 2.

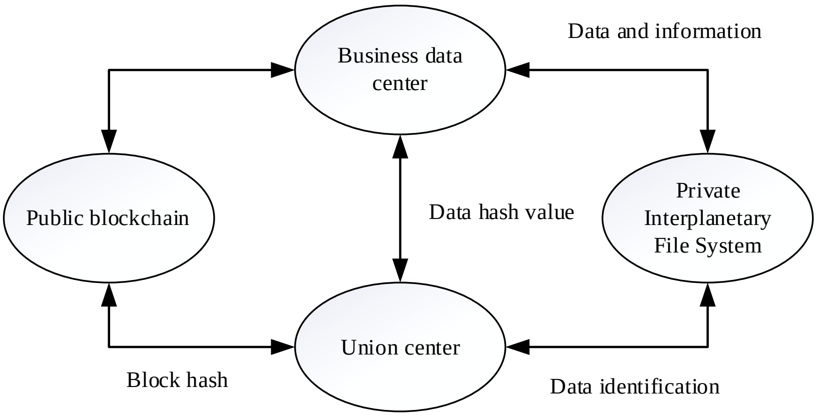

Figure 2. Message flow

3.2. Contract structure

The smart contracts involved in the model in this article are mainly used to manage the identities of commercial data centers, that is, to confirm the identities of these nodes, and also to manage commercial data. The modules involved in smart contracts mainly include public blockchain modules and alliance center modules. There is an alliance data protection contract in the public blockchain, which is mainly used to ensure the authenticity of the data in the alliance center. The smart contract in the alliance center module mainly completes the two tasks of identity authentication and business data management for commercial data center nodes. The smart contracts of the alliance center include node information storage contract (NISC), node information management contract (NIMC), commercial data management contract (CDMC), etc. As shown in Figure 3.

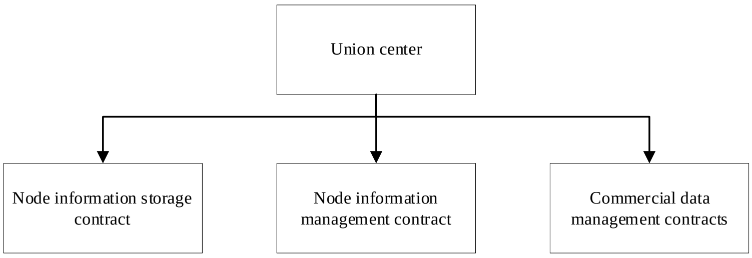
Union center
Node information storage contract
Node information management contract
Commercial data management contracts

Figure 3. The contract structure of the alliance center

The node information storage contract is mainly used to store the node identity information involved in the model for identity recognition. Therefore, the contract records the identities (data center identity, dcID), public keys, and public keys of all commercial data centers in the alliance center. The node information management contract and commercial data management contract corresponding to this node.

The node information management contract realizes the internal autonomy of commercial data center nodes based on democratic voting technology, and consists of a new node contract and a node reset contract. Among them, the node creation contract creates a dcID for the newly added commercial data center node through voting. The node reset contract is used to reset the key of the commercial data center to prevent the risk of the private key leakage of the commercial data center.

Commercial data management contracts are mainly used to manage commercial data, including verification, restoration, sharing and protection of commercial data, and are composed of commercial data information storage contracts, commercial data authority control contracts, and commercial data sharing management contracts. The structure of the commercial data management contract is shown in Figure 4.

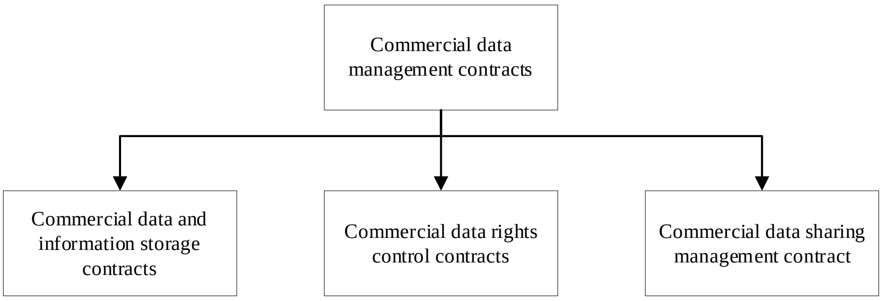
Commercial data management contracts
Commercial data and information storage contracts
Commercial data rights control contracts
Commercial data sharing management contract

Figure 4. Business data management contract structure

The commercial data information storage contract (CDSC) mainly records the digital summary information of the commercial data center, including the interplanetary file system address, number, hash value, creation time, modification time and so on of the commercial data object.

A commercial data control contract (CDCC) is mainly used to control the permissions of commercial data centers.

The commercial data sharing management contract (CDMC) mainly records the data information shared by the commercial data center, including the data number, the identity of the commercial data center to which it belongs, the sharing time, and so on. A data number can be shared to multiple commercial data centers for access. When the ID of the commercial data center corresponding to the data number is -1, it means that the data is completely open and all users can directly obtain the information; if the identifier is 0, it means that the data is conditionally open and all members of the alliance center can access; If the identifier is not less than 1, it means that the data is private and only the data center with the specified authority can access it.

3.3. Method design

The commercial data center node does not directly participate in the alliance center, but only replaces it with an identity. Therefore, identification is very important for commercial data centers, and a majority of votes are required to authorize registration. Its operation is shown in Algorithm 1:

Algorithm 1: Registration of commercial data center identity

Input: Commercial data center request

Output: Generate business data center identity

The commercial data center that needs to join the alliance center generates a key pair $\langle K_{pub}, K_{pvi} >$, based on a certain encryption algorithm. For example, the model in this paper adopts the elliptic curve algorithm [15], and the private key is kept properly.

The public key K_{pub} and basic information are disclosed to the alliance center. The basic information includes the address of the commercial data center. At the same time, a node is randomly entrusted to create a voting contract, and the nodes in the alliance center participate in voting;

If the number of votes is more than half, the commercial data information storage contract saves the public key information of the commercial data center, and then generates the dcID of the commercial data center and creates a commercial data information storage contract and a commercial data authority control contract, which are represented by triples (dcID, CDSC, CDCC).

Since the private key is kept by the commercial data center itself, there is a situation of internal personnel stealing it, and there is also a risk of being stolen. Once it is stolen, the person who obtains the private key can forge the identity of the commercial data center to operate on the data. Therefore, the commercial data management center needs to properly keep the private key. In addition, this article designs a key reset contract. Once the key is discovered, you can start the dcID reset contract to reset the key. The specific operation is as algorithm 2:

Algorithm 2: Reset the key

Input: Reset request

Output: Generate a new public key

The commercial data center generates a pair of keys $\langle K_{pubnew}, K_{prinew} >$, and the private key$K_{prinew}$ saves itself;

The new public key is disclosed to the alliance center, the secret key is reset, the commercial data center identity has been registered, so the commercial data center identity is also attached, and the node is randomly entrusted to create a reset voting contract;

All the alliance centers vote again. If the votes are more than half, the node information management contract resets the public key of the commercial data center and replaces $\langle K_{pub}, K_{pvi} >$ with $\langle K_{pubnew}, K_{prinew} >$

Taking into account the security risks of the private key of the commercial data center, the reliance on the public key of the operation is relieved through the consistent recognition of the node's identity. Since the operations of the commercial data designed above are based on the node identity, even if the dcID reset contract resets the public key of the commercial data center, as long as the node identity is consistent, the identity of the commercial data center can still be verified.

The protection of commercial data refers to the protection of data when adding and updating commercial data objects. Based on the private cluster technology of the Interplanetary File System, the data is stored on the blockchain and cooperated with the alliance center and the public blockchain. Smart contracts protect data, prevent data from being destroyed, and support basic operations such as verification and recovery.

The newly added data object is to store the commercial data object in the private interplanetary file cluster system, and the data object number is stored in the commercial data information storage contract; the updated data object is to protect the object and data time the data object is updated.

The structure of a commercial data object (commercial data object, represented in JSON form in this article, so abbreviated as cdJSON) is shown in Figure 5, including information such as object number, version number, creation time, operator, and summary.

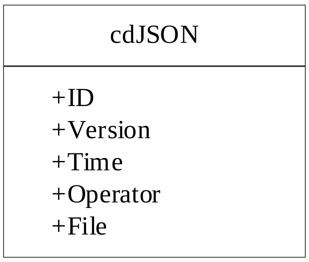

Figure 5. Business data object structure

New data object operation steps

The commercial data center generates a pair of random keys $randkey(K_{pubr},K_{prir})$, which is mainly used to encrypt commercial data abstracts and commercial data objects.

Use the private key K_{prir} to encrypt the commercial data digest, save it to the interplanetary file cluster system after encryption, and sign the hash value, the serial number of the encrypted attachment, and the serial number of the encrypted commercial data object. Send to the smart contract through the service center to wait for subsequent processing;

The commercial data information storage contract receives a request for a new data object, calls the commercial data authority control contract to recover the public key from the signature, and compares the recovered public key with the key in the node information storage contract. If the verification is passed, a mirror image of information such as the commercial data object number and summary is added to the contract.

The process of adding new objects is shown in Figure 6.

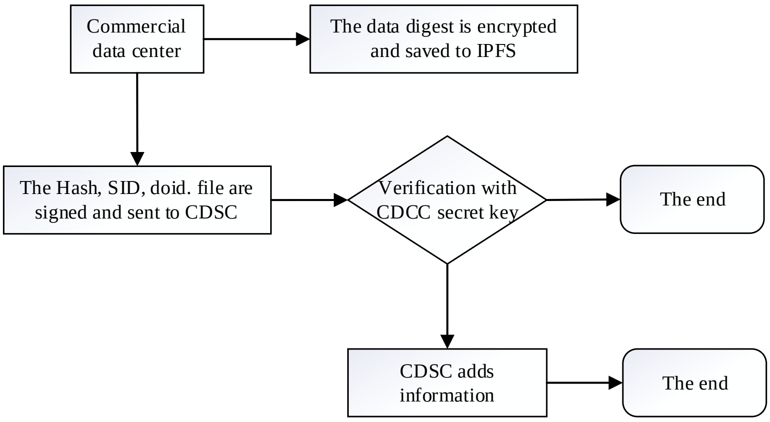
Commercial data center
The data digest is encrypted and saved to IPFS
The Hash, SID, doid. file are signed and sent to CDSC
Verification with CDCC secret key
The end
CDSC adds information
The end

Figure 6. New object process

The operation of updating a data object is similar to that of adding a new data object, except that the commercial data center will not generate a key pair, but directly use the original key pair; the commercial data center will use the commercial data information storage contract and interplanetary according to the commercial data object number. The commercial data object information is extracted from the file system, and then new commercial data objects are generated according to the updated commercial data information. After encryption, they are saved back to the commercial data information storage contract and the interplanetary file system, and the original information is also updated.

The verification of commercial data objects includes the verification of data on the blockchain of the alliance center by the public blockchain, the verification of the data in the interplanetary file system by the alliance center, and the verification of data by the commercial data object in the commercial data center. The specific verification process is shown in the following algorithm:

Algorithm 3: Data verification of the blockchain of the alliance center by the public blockchain

Input: Data verification request

Output: verification result

The commercial data center signs the dcID and data number to get sign(dcID, dataID), and sends the result to the service center;

After receiving the message, the service center obtains the latest copy image of the alliance data block from the alliance data protection contract in the public blockchain;

It is verified by comparison with the block information in the alliance center; if the verification is passed, the signature is sent to the smart contract for the next step; if the verification fails, the data exception in the alliance center is returned.

Algorithm 4: verification of data in the interstellar file system by Alliance Center

Input: Data verification request

Output: verification result

The commercial data information storage contract receives the verification request, confirms the identity of the commercial data center through the commercial data authority control contract, and finds the summary information of the corresponding data from the contract according to the data ID;

After the commercial data center obtains the required information from the commercial data information storage contract, it obtains the data objects in the cluster from the interplanetary file system according to the obtained data objects;

Verify whether the obtained hash value is the same as the former, if the verification is passed, proceed to the next step; if the verification fails, return to the Interplanetary File System data exception.

Commercial data object's data verification of commercial data center: The method of obtaining data object information is the same as above, except that the data object information is compared and verified with the data object information of the commercial data center. If the verification is passed, the next step will be entered normally, otherwise, return to business The data in the data center is abnormal.

In response to the above-mentioned abnormalities, this article proposes the following recovery methods:

Data anomaly in the alliance center: After an anomaly is found, it can be traced back, and the alliance block information can be compared with the previous block information to find the location of the abnormal block, and the newly created block on this basis;

Interplanetary file system data anomaly: The commercial data information storage contract stores each historical version of the data block. If an abnormality is found, the correct version of the previous period can be restored;

Business data center data exception: the tampered data information of the business data center can be reset according to the historical records on the alliance chain.

Commercial data sharing refers to data sharing between alliance center nodes and external nodes. With the support of smart contracts, interplanetary file systems, and hybrid encryption mechanisms, the secure sharing of data is ensured. The following takes commercial data center A to share commercial data with commercial data center B as an example to introduce the data sharing process of the solution in this paper. The commercial data center identity of commercial data center A is recorded as dcIDA, and the commercial data center identity of commercial data center B is recorded as dcIDA. It is dcIDB, see Algorithm 5 for details:

Algorithm 5: Sharing of business data

Input: Data sharing request

Output: shared data or failure prompt

Commercial digital center A uses the private key AK_prir to sign the data ID、dcIDA of the data object that needs to be shared to obtain $\mathrm{sign}_a(\mathrm{dataID}, dcID_A)$, and then send $\mathrm{sign}_a(\mathrm{dataID}, dcID_A)$ to the commercial data sharing management contract through the service center. After receiving the request, the commercial data sharing management contract first calls the commercial data permission control contract to check $dcID_A$, and writes it into the sharing sequence of the contract data object data ID after passing the check;

The commercial data center B uses the private key BK_{vrir} to sign the data ID、dcIDB to obtain the signb (data ID, dcIDB), and then sends the signb (data ID, dcIDB) to the commercial data sharing management contract through the service center. After receiving the request, the commercial data sharing management contract first calls the commercial data permission control contract to check the permission of the commercial data center B. Passing the check means that B has the permission to read the data object and read the hash value of the corresponding data object. And the fingerprint of the data object; commercial data center B obtains the encrypted data object from the interplanetary file cluster system according to the obtained data object fingerprint and sends the data ID and dcIDB to the commercial data center A to obtain the decryption key of the data object;

After A receives B's request, the commercial data sharing management contract checks the shared record of the commercial data based on the received information. If the shared record is incorrect, the sharing failure is returned; otherwise, the sharing is true and correct, and dcIDB is obtained from the node information management contract. The corresponding public key BK_{vrir} is sent to B after asymmetric encryption of the decryption key;

B uses the private key BK_{vrir} to decrypt the received message to obtain the original decryption key and uses the decryption key to decrypt the encrypted data object to obtain the original information of the data object.

4. Program analysis

4.1. Safety performance analysis

Since the copies of the data blocks of the alliance chain are mirrored in the public chain, the heights of each other cannot be the same, there must be a height difference, here the height difference is recorded as h. If a hacker wants to attack, then the attack process needs to recalculate all the content of the current block height of the public chain and pass the entire network verification. Assuming that the computing power of the node is a hash per second, and the computing power of the hacker is bhash per second, there will be no abnormal situations. If a large number of nodes join the attack, the calculation difficulty of the new block is generally not much different. Here, assuming there is no abnormal situation, ordinary nodes The probability of the clock generating a new block is p, and the probability of a hacker node generating a new block is q. Then there are three situations in which the height difference h changes every second, which are larger, smaller and unchanged. Each probability is expressed as P1, P2, P3. Then in t seconds, there are t times of changes, and n is used to mark the number of times of becoming larger, m is the number of times of becoming smaller, then the number of constants is t-n-m times, where the height difference changes satisfy multiple distributions. If within t seconds, the hacker attacking the node successfully needs to satisfy m∈ [0, (t-h-1)/2], n=m h c, where 1≤c≤t-2 m-h, the probability of occurrence is as follows

$$P_h(t) = \sum_{m=0}^{(t-h-1)/2t-2m-h} \sum_{c=1}^{t!} \frac{t!}{m!n!(t-m-n)} P_1^m P_2^n P_3^{t-m-n}$$

Where $P_1 = q(1-p)$ 是 is the probability that the height difference becomes larger, $P_2 = p(1-q)$ is the probability that the height difference becomes smaller, and $P_3 = 1 - P_1 - P_3$ is the probability that the height difference does not change.

If the computing power of a hacker attacking a node is less than that of an ordinary node, the probability of success is smaller. Therefore, the case of equivalent computing power is discussed here. According to the above formula, the probability distribution of a successful hacker attack is shown in Figure 7, where the y-axis is the probability of successful hacker attack P, the x-axis is time T, and the unit is the unit time of computing power.

From Figure 7, we can see that the probability of a hacker being able to successfully attack and tampering with data decreases as the height difference increases. Calculated with a height h=20, the probability of success is also 15% under a long-term attack. In practical applications, the block height difference will be in the order of tens of millions. In this case, the probability of successful tampering is almost zero. Moreover, Ethereum has an incentive mechanism. If it has such large computing power, it is better to be an ordinary node, and the reward is far greater than the benefit of attacking and tampering. Therefore, through analysis, this model is reliable in terms of security and cannot be tampered with.

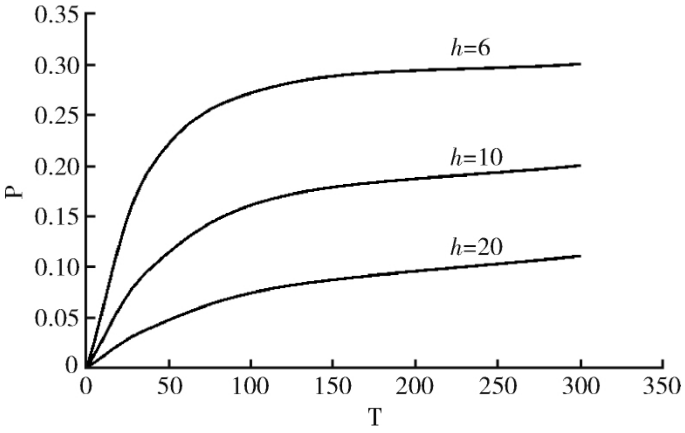

Figure 7. Attack success probability distribution

4.2 Economic Cost Analysis

This model is mainly used for the sharing and protection of commercial data. Assuming that the number of times of protection required per day is m, the number of shares times is n, and the number of identity information management times is 1, then the cost of deploying smart contracts on the public blockchain on Ethereum is $\text{Cos}\,t_1 = m\text{Cos}\,t_2 + n\text{Cos}\,t_3 + l\text{Cos}\,t_4$, where $\text{Cos}\,t_1$ is the cost of Ethereum, $\text{Cos}\,t_2$ is the cost of protection operations, $\text{Cos}\,t_3$ is the cost of sharing operations, and $\text{Cos}\,t_4$ is the cost of identity information management.

The model in this article combines the public chain and the alliance chain. Smart contracts in the public chain can be deployed in the alliance chain. Therefore, the call cost in the alliance chain is almost negligible. You only need to consider the operating cost of the alliance center and the net cost of the alliance center. Marked as s, the alliance chain does not need to access the public chain every time it runs. Assuming that the alliance center has performed t data operations and needs to access the public chain, then the cost of the model in this article will be $\text{Cos}\,t = \frac{m+n+l}{.}\text{Cos}\,t_1 + s, s > 1$, as the scale of the alliance center becomes larger, the interaction between the alliance center and the public chain will become less and less, that is, t will become larger and larger, so the cost of the model will become lower and lower. In the actual operation process, the network operating costs is negligible compared to other costs. Here, for the convenience of explanation, it is ignored. Then under this model, the economic cost will become the original $u = \frac{m+n+l}{.}$, and here t Is much larger than $m + n + l$, so u<1, it can be seen that the model in this paper does reduce the economic cost.

4.3. Comparative analysis

This article is to establish a model for the protection and sharing of commercial data by combining the alliance chain and the public chain. Combined with the interplanetary file system, the functions of safe sharing, protection and recovery of commercial data are realized, and the alliance chain is used alone. The performance comparison of the public chain is shown in Table 1. The security of the model proposed in this paper is higher than that of the alliance chain, and the security of the public chain is equivalent, but the cost is lower than that of the public chain; in terms of scalability, the model of this paper is higher than the two. This shows that the model in this paper is better.

Table 1. Performance comparison

Program	Safety	Cost	Scalability
Paper model	High	Lower	Good
Alliance chain	Higher	Low	Bad
Public chain	High	High	Bad

5. Conclusion

In this paper, a blockchain-based commercial data sharing model is designed based on blockchain-related technologies and the Interplanetary File System. This model realizes basic operations such as the safe sharing of commercial data and the protection of commercial data and can ensure the safe sharing of commercial data at a lower economic cost. Compared with the existing model, it has more advantages in terms of security, scalability and cost. This model considers the basic operations of the sharing and protection of business data but does not do too much in the application of other aspects of business data. In future work, the model can be expanded to more fields and include more functions. More in-depth research will be conducted on the blockchain consensus mechanism of business data management.

Reference

[1] Majumdar J, Naraseeyappa S, Ankalaki S. Analysis of agriculture data using data mining techniques: application of big data[J]. Journal Of Big Data, Vol. 4, No. 1, pp. 20, (2017)

[2] Shadroo S, Rahmani A M. Systematic Survey of Big Data and Data Mining in Internet of Things[J]. Computer Networks, No.139, pp. 19-47, (2018)

[3] Banyal R K.; Jain V K.; Jain P. Data Management System to Improve Security and Availability in Cloud Storage[J]. IEEE, 2015.

[4] Perez I J.; Cabrerizo F J.; Alonso S, et al. A New Consensus Model for Group Decision Making Problems With Non-Homogeneous Experts[J]. IEEE Transactions on Systems Man & Cybernetics Systems, Vol. 44, No. 4, pp. 494-498, (2017)

[5] Oh S J.; Fritz M.; Schiele B. Adversarial Image Perturbation for Privacy Protection A Game Theory Perspective[C]// IEEE International Conference on Computer Vision. IEEE Computer Society, 2017.

[6] Durkin T A.; Elliehausen G. New Evidence on an Old Unanswered Question: Why Some Borrowers Purchase Credit Insurance and Other Debt Protection and Some Do Not[J]. Finance & Economics Discussion, 2017.

[7] Boyd A.; Woollard M.; Macleod J, et al. The destruction of the 'Windrush' disembarkation cards: a lost opportunity and the (re)emergence of Data Protection regulation as a threat to longitudinal research[J]. other, Vol. 3, (2018)

[8] Sivaprakash A.; Rajan S N E.; Selvaperumal S. Privacy Protection of Patient Medical Images using Digital Watermarking Technique for E-healthcare System[J]. Current Medical Imaging, 2019.

[9] Nandhini K, Jayanthi S. Privacy Protection and Interruption Avoidance for Cloud-Based Medical Data Sharing. 2019.

[10] Patsakis C.; Casino F Hydras; IPFS. A Decentralised Playground for Malware[J]. International Journal of Information Security, Vol. 18, No. 6, pp. 787-799, (2019)

[11] Mary A J.; Palanisamy D V. File Security Using Hybrid Cryptography[J]. Artificial Intelligent Systems & Machine Learning, 2011.

[12] Blockchain Encyclopedia. Credit union and ten cent cloud reached strategic cooperation to build blockchain industry ecology [EB/OL]. [2020-09-17].

[13] Benet J. IPFS—Content addressed, versioned, P2Pfile sys-tem [EB/OL]. [2020-09-17]. https://raw.githubusercon-tent.com/ipfs/papers/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf, 2018.

[14] Lazar, Fred. Antitrust Immunity for Joint Ventures Among Alliance Airlines[J]. Journal of Air Law & Commerce, 2018.

[15] Kim S K. The Trailer of Strategic Alliance for Blockchain Governance Game[J]. Computers &, Vol. 136, pp. 373-380, (2019)

[16] Vukoli M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication[C]// International Workshop on Open Problems in Network Security. Springer International Publishing, 2016.

[17] Pass Rafael; Seeman L; Shelat A. Analysis of the blockchain protocol in asynchronous networks [C]//Annual International Conference on the Theory and Applications of CryptographicTechniques, pp. 643-673, (2017)

[18] Azais J M.; Mourareau S.; Castro Y D. A rice method proof of the null-space property over the Grassmannian[J]. Annales De Linstitut Henri Poincare, Vol. 53, No. 4, pp. 1821-1838, (2017)

[19] Alexander Chepurnoy; Tuyet Duong; Lei Fan, et a l. Twins Coin: A cryptocurrency via proof-of-work and proof-of-stake[C]//IACR Cryptology ePrint Archive, pp. 232-253, (2017)

[20] Badertscher C.; Gazi P.; Kiayias A, et al. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 913-930, (2018)

[21] Dziembowski S.; Faust S.; Kolmogorov V. et al. Proofs of space [C]//Annual Cryptology Conference, pp. 585-605, (2015)

[22] Mitar Milutinovic; Warren He. Proof of luck: An efficient blockchain consensus protocol [C]//Proceedings of the 1stWorkshop on System Software for Trusted Execution, pp. 201-219, (2017)

[23] Singh P K.; Schaefer A L.; Parsek M R, et al. Quorum-sensing signals indicate that cystic fibrosis lungs are infected with bacterial biofilms. [J]. Nature, Vol. 407, No. 6805, pp.762-764, (2000)

[24] Larimer D. Delegated Proof-of-stake white paper [EB/OL]. [2020-09-17].https://bitsharestalk.org/index.php?topic=4009.60,2014.

[25] Buterin V.A next-generation smart contract and decentralize dapplication platform [EB/OL]. [2020-09-17]. https://www.mendeley.com/catalog/nextgeneration-smart-contract-decentralized-application-platform/,2013.

[26] Stebalien. Experimental features of Go-IPFS [EB/OL]. [2020-09-17].https://github.com/ipfs/go-ipfs/blob/master/docs/experimental-features.md#private-networks,2018.