Design of Adaptive Defense System for Marketing Information Management Based on Blockchain Technology

Lin Liu(✉)

School of Management and Economics, Taishan University, Taian, Shandong, China
sophiachina12@126.com

Abstract. With the advent of Internet and information era, enterprises are facing more and more opportunities and challenges. In the fierce market competition environment, how to use advanced science and technology to improve their core competitiveness is a question that every enterprise needs to think about. At present, most enterprises in China still use traditional marketing methods for product sales and customer maintenance, and this backward marketing model has been unable to meet the new requirements of modern social development. Therefore, in order to better cope with the increasingly complex and changing external business environment, enterprises must change their existing marketing concepts and means, and apply advanced computer network technology to marketing activities, so that they can obtain accurate and effective data information and make scientific and reasonable decisions in a timely manner. This paper first understands the research background of the subject and the research status of related fields at home and abroad, and then, aiming at specific problems, combining the characteristics of distributed storage, non-tampering, traceability and so on of blockchain technology, leads to a brand-new marketing information management model-adaptive defense system of marketing information management based on blockchain technology. This system can realize the functions of real-time sharing, safe and reliable transmission, and smart contract execution of marketing information; finally, the feasibility and practical value of this system are verified by specific cases.

Keywords: Blockchain technology · Marketing information management · Adaptive defense system design

1 Introduction

In the context of the current era, there is an increasing demand for data and information. In order to meet this demand, a sound and fully functional database needs to be constructed to store this data. However, the traditional data management model has certain defects, so it cannot effectively store the huge amount of data and information, which leads to the marketing activities within the enterprise to be affected. With the application of blockchain, the encryption and verification of data can be realized, thus ensuring that the data will not be tampered with or lost. At the same time, the tasks can be

K. Hemachandran et al. (Eds.): ICAID 2023, AHIS 9, pp. 62–71, 2023.
https://doi.org/10.2991/978-94-6463-222-4_6

completed by means of smart contracts, which not only improves the efficiency, but also makes the whole process more transparent and avoids unnecessary problems. In addition, the consensus mechanism in the blockchain can ensure that all nodes can participate and jointly maintain the data information on the blockchain, thus forming a complete system structure. Of course, in order to give full play to the advantages of blockchain technology, a set of scientific and reasonable operation mechanism must be established, and only in this way can the expected effect be truly achieved. This paper mainly studies how to use blockchain technology to build an adaptive defense system for marketing information management, hoping to promote the continuous improvement of China's economic development [1].

2 Application of Blockchain Technology in Marketing Information Management Adaptive Defense System

2.1 Blockchain Basics

1) Blockchain Concept

A block is composed of several different types of data, which are recorded into a specific database after verification. Blockchain is mainly used to store, manage and maintain data and information. In essence, blockchain is a decentralized distributed ledger, which can form a certain degree of alliance between independent individuals through mutual cooperation to achieve a common task or goal. Therefore, blockchain is often referred to as a "trust machine" or "trust network". In general, a blockchain needs to contain the following basic elements: (1) block header; (2) block body; (3) timestamp; (4) hash value; (5) random number; and (6) Merkle tree root. Among them, the block head is also called the Hash-Chain head, which is usually represented by a string of fixed length and must also meet the conditions that the prefix cannot be repeated and no spaces are allowed in the suffix before it can be used. The block body refers to all the transaction data corresponding to the block, which is also one of the core parts of the whole blockchain. In addition, the timestamp can effectively prove the specific time of an event, which can further ensure the authenticity and reliability of all data in the blockchain. Finally, the hash value is an important basis to determine whether a message belongs to the same transaction, and only when the user enters the correct hash value, it means that the message is really sent by the user [2].

2) Blockchain System Architecture.

When developing a system, it is necessary to understand its basic structure first. The so-called block is a kind of chain data formed by combining data blocks into a specific data structure in a chain manner according to the chronological order and on this basis. Blockchain contains a large amount of data and information, which can be verified as valid, authentic and complete by certain methods, and this also ensures that the data will not be tampered with or lost during transmission [3]. Therefore, blockchain is decentralized, unforgeable, traceable, open and transparent, etc. Blockchain is composed of multiple nodes, and each node is interconnected to form a distributed network system, and the blockchain system architecture is shown in Fig. 1.

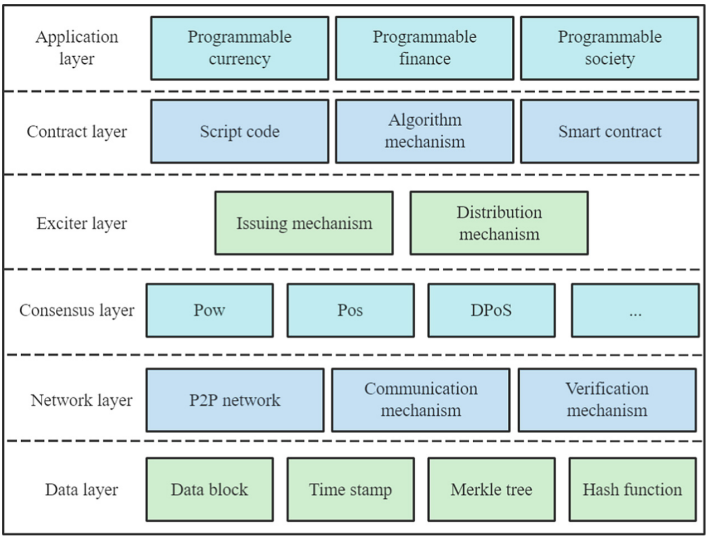

Fig. 1. Blockchain system architecture

2.2 Blockchain-Related Technologies

1) P2P Networks.

The P2P network needs to be utilized in the inspection of the system. This network is a distributed structure that connects multiple nodes to form a complete system, where the "zones" refer to the relationships between the nodes. The so-called "blocks" represent the data stored on these nodes. When a user wants to get a piece of data, he just needs to add a certain number of random numbers to it to complete the operation. At the same time, in order to ensure that there is no double counting in the whole process, a verification mechanism should be set up to ensure the accuracy of the results. P2P refers to a distributed computing model, which allows each user involved in the system to become a separate node, and the node as the main body and other nodes are interconnected to form a large information network system, p2p network topology is divided as shown in Fig. 2 [4].

2) Hyperledger Fabric.

The rapid development of blockchain has led to the emergence of many blockchain platforms, such as Hyperchain and Bit shares (Bit shares)12, as shown in Table 1.

Hyperledger Fabric is a distributed ledger consisting of several different types of blocks, each containing a certain number of transactions, timestamps and other important information that together form a link between all nodes on the blockchain [5]. When a node wants to query data or some specific information for a certain period of time, it can do so by broadcasting the blocks it owns to the whole network. Moreover, this approach can effectively prevent malicious attackers from tampering or falsifying the block contents, thus ensuring the authenticity and integrity of the information

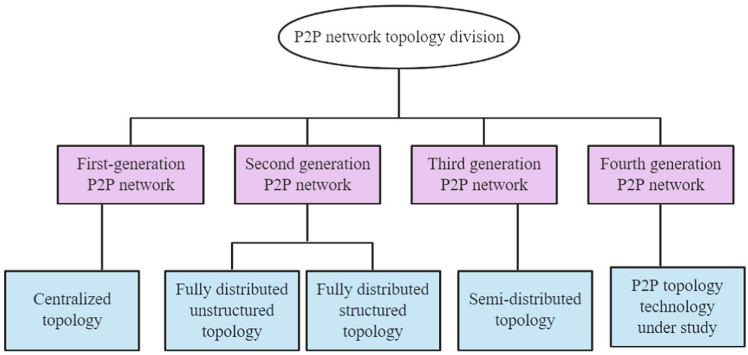

Fig. 2. p2p network topology division

Table 1. Comparison of some blockchain platforms

Blockchain platform	Consensus mechanism	category	Development language	Smart contract	TPS(transactions per second)
bitcoin	PoW	Public chain	C++	Do not support	<7
Ethereum	PoW	Public chain	Go	support	About 100
superbook	PBFT	Alliance chain	Go	support	About 3000
bitstock	DPoS	Public chain	C++	Do not support	>500
Ripple chain	RPCA	Public chain	C++	Do not support	<1000
Blockchain platform	RBFT	Alliance chain	Go	support	>10000

during data transmission. In addition, the Hyperledger Fabric can also be used to connect dispersed participants in marketing activities, allowing them to share resources and work together, thereby improving overall efficiency. The system logic architecture of Hyperledger Fabric is shown in Fig. 3.

2.3 Scenarios of Blockchain Technology Application

In practice, blockchain is mainly used in the following ways: firstly, blockchain can be used for some businesses that need to exchange and process a large amount of data; secondly, blockchain can also be used for those businesses that need to ensure security, reliability and privacy. With the continuous development of science and technology, blockchain technology has been widely used in various fields, such as the financial industry, health care and other areas have a very important role. In addition, many other

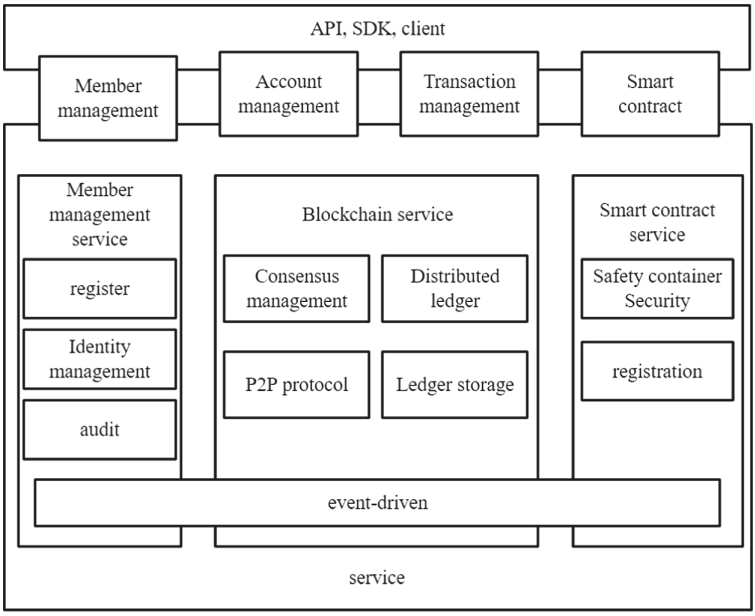

Fig. 3. System logic architecture of Hyperledger Fabric

fields have also begun to gradually introduce this new technology, and achieved good results. For example, in the current hot e-commerce platform on the emergence of such a software - "review" APP, which not only provides a platform for users to communicate and interact, but also has a certain degree of marketing functions [2]. The software collects reviews from customers and then integrates them into a complete record, which is then uploaded into a database, so that merchants can better analyze consumer needs and develop products that better meet market requirements.

3 Network Security Adaptive Defense Technology

3.1 Intrusion Detection

In the computer network, the destructive behaviors made by some illegal users or law-breakers need to be discovered through intrusion detection. And with the continuous improvement of science and technology, intrusion detection has gradually developed in the direction of intelligence and automation. At present, there are two common intrusion detection methods: one is rule-based detection; the other is packet-based detection [6]. Among them, the former is also called static detection, and the latter is called dynamic detection. There are certain differences between these two, but their purpose is to timely find and deal with various security risks and problems that occur in the network.

In the intrusion detection training process, the intrusion detection data is firstly used as the input of the ADBN algorithm, and then the data output of this layer training is completed by the RBM algorithm, which is again used as the input data of the next layer,

so as to carry out layer-by-layer learning and thus complete the pre-training process of the ADBN algorithm. The RBM can be regarded as a kind of random network based on statistical mechanics, and the introduction of energy function in the RBM is also inspired by the generalization of statistical mechanics [7]. From the statistical mechanics point of view, the model based on the energy function is also called the energy model. A temperature parameter T is added to this model so that the corresponding conditions need to be satisfied if sampling values are exchanged between different temperature chains. The joint probability of the parallel tempered RBM model at different temperatures is shown in Eq. (1):

$$P_r(v,h) = \frac{1}{Z(t_i)} \exp(-\frac{1}{t_i} E(v,h;\theta), i = 1,2,...,M) \tag{1}$$

Calculate whether the nodes (vr,hr) and (vr-1,hr-1) of the revealed and hidden layers at adjacent temperatures satisfy the exchange condition exchange condition, as shown in Eq. (2):

$$\min\{1, \exp((\frac{1}{t_r} - \frac{1}{t_{r-1}}) * (E(v_{r-1}, h_{r-1})))\} \tag{2}$$

In the process of continuous calculation, the parameters need to be updated, and the follow-up method is shown in Eq. (3):

$$\begin{cases} \Delta W_{ij} = < v_i, h_j >_{data} - < v_i, h_j >_{recon}^{t=1} \\ \Delta a_i = < v_i >_{data} - < v_i >_{recon}^{t=1} \\ \Delta b_j = < h_j >_{data} - < h_j >_{recon}^{t=1} \end{cases} \tag{3}$$

Assume that X is a network intrusion detection dataset, which can be expressed as Eq. (4).

$$X = [x^1, x^2 \cdots x^L] = \begin{bmatrix} x_1^1, x_1^2, \cdots, x_1^L \\ x_2^1, x_2^2, \cdots, x_2^L \\ \vdots \\ x_D^1, x_D^2, \cdots, x_D^L \end{bmatrix} \tag{4}$$

where L is the training set data content of the network intrusion detection data and D is the feature dimension of each intrusion detection data.

Y is the labeled dataset corresponding to the L labeled intrusion detection data, which can be expressed as Eq. (5):

$$Y = [y^1, y^2 \cdots y^L] = \begin{bmatrix} y_1^1, y_1^2, \cdots, y_1^L \\ y_2^1, y_2^2, \cdots, y_2^L \\ \vdots \\ y_C^1, y_C^2, \cdots, y_C^L \end{bmatrix} \tag{5}$$

3.2 Intrusion Prevention

The problems in the system can be detected by intrusion detection. Some advanced technical means and methods such as blocks and smart contracts need to be utilized in this process. These are popular and effective ways to help people better understand what is happening in the computer network and the data generated, and to take timely measures to solve the problems that arise. Of course, there is still a long way to go to achieve this goal, but with the continuous improvement of science and technology, I believe that the future will achieve greater breakthroughs. The block is a very important technology, which is mainly used to record transaction information, thus facilitating the follow-up work [2].

4 Design of Adaptive Defense System for Marketing Information Management

4.1 System Architecture

In this study, the B/S model will be used for the development of the system. This model has strong flexibility and scalability, and can meet the needs of different user groups. At the same time, in order to ensure safe and stable system operation, a complete network architecture needs to be established and it should be ensured that the parts can be connected with each other. In addition, it should also be noted that since blockchain is a decentralized database, it can be operated without the help of a third-party platform, which makes the whole process easier and faster.

4.2 System Function Module

After completing the construction of the system architecture and database, it needs to be applied into practice. The first thing to do is to establish a complete marketing management platform and use it to collect relevant data. Then the data is used to build the corresponding model, so that the whole system can run more efficiently [8]. The main functions are shown in Fig. 4.

5 System Testing

5.1 Set up the Network Environment

In this study, two main aspects of system functionality and performance were tested. Among them, the system function is tested by simulating the market trading process to see whether the system can achieve the expected goals; while the system performance is judged by recording the amount of data generated at each stage and the interaction between each node to see whether it meets the requirements. In order to ensure the high accuracy of the experimental results, the whole experimental period needs to be controlled in about 20 days. At the same time, since the system involves a large amount of data exchange, a MySQL database is used as the main storage tool, and the Python

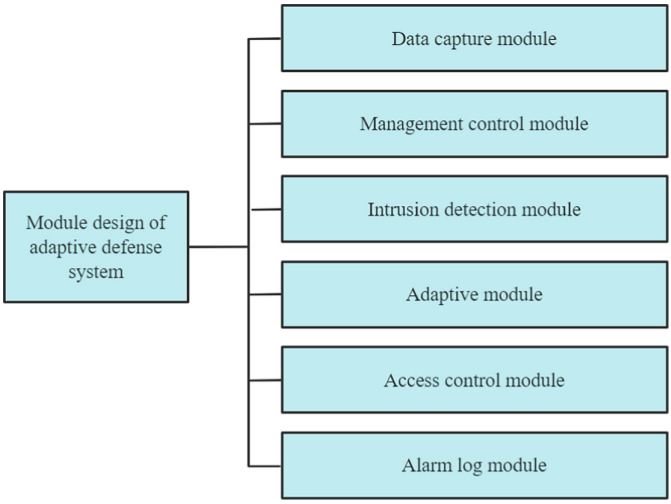

Fig. 4. Adaptive defense system module design

language is used to program the relevant operations. Specifically, the data is first imported from the MySQL database into the memory, and then processed, calculated, and saved using Python scripts. Finally, a RabbitMQ message queue is used to send a request to the blockchain network to obtain the corresponding transaction data, thus forming a complete blockchain ledger.

5.2 Verify the Performance Improvement Effect

Since the conditions are equal (same rule base, same target user), the total number of alarms is basically the same. We count the number of alarms in the interval from O to 100, and add ten alarms as a time period. The number of matches was accumulated and compared between the original snort and our system after adding the adaptive module, and the number of matches between the two systems with the same number of alarms is shown in Table 2:

Based on the data results, it can be seen that the efficiency of the system in processing packets has improved by almost fifty percent. This fully illustrates the significant performance improvement of our improved system.

Table 2. Number of matches for both systems

Alarm number	Number of times the original snort matches	Number of adaptive snort matches
10	980	510
20	1900	1005
30	2925	1423
40	4228	2019
50	4802	2446
60	5998	3060
70	7384	3406
80	8298	4229
90	8900	4609
100	10221	5054

6 Conclusion

This paper focuses on how to use blockchain technology to manage the large amount of data and information generated in the process of enterprise marketing in the era of big data. By analyzing some problems existing in the current market, a new solution is proposed - an adaptive defense system for marketing information management based on blockchain technology, which can realize the functions of collecting, organizing and storing massive data, and can effectively prevent hacker attacks or virus invasion to ensure data security It is also intelligent. It is also intelligent and automatically uploads relevant data to the cloud database when users need it, making it easy for users to query the data they need anytime and anywhere. In addition, the system adopts a distributed structure, which makes each node have the same rights and obligations, thus ensuring that the whole system operates more stably and reliably. Finally, the system is an open platform, in which anyone can participate and provide corresponding services for them, thus also greatly reducing the development cost.

References

1. Qiao Haike,Zhang Zijun,Su Qin. Blockchain technology adoption of the manufacturers with product recycling considering green consumers[J]. Computers & Industrial Engineering,2023:177.
2. Swani Kunal,Milne George R.,Slepchuk Alec N.. Revisiting Trust and Privacy Concern in Consumers' Perceptions of Marketing Information Management Practices: Replication and Extension[J]. Journal of Interactive Marketing,2021(1):56–60.
3. Zhu Shichao,Li Jian,Wang Shouyang,et al. The role of blockchain technology in the dual-channel supply chain dominated by a brand owner[J]. International Journal of Production Economics,2023:258.

4. Yap Kah Yung,Chin Hon Huin,Klemeš Jiří Jaromír. Blockchain technology for distributed generation: A review of current development, challenges and future prospect[J]. Renewable and Sustainable Energy Reviews,2023:175.
5. OrtizLizcano María Isabel,AriasAntunez Enrique,Hernández Bravo Ángel,et al. Increasing the security and traceability of biological samples in biobanks by blockchain technology.[J]. Computer methods and programs in biomedicine,2023:230–231.
6. Wenhua Zhang,Qamar Faizan,Abdali TajAldeen Naser,et al. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends[J]. Electronics,2023(3):12–16.
7. Ghode Dnyaneshwar Jivanrao,Yadav Vinod,Jain Rakesh,et al. Exploring the integration of blockchain technology into supply chain: challenges and performance[J]. Business Process Management Journal,2023(1):29–33.
8. Yong-Qiong Zhu, Ye-Ming Cai, Fan Zhang, "Motion Capture Data Denoising Based on LSTNet Autoencoder," Journal of Internet Technology, vol. 23, no. 1 , pp. 11-20, Jan. 2022.