Application research of smart logistics based on blockchain technology

Haidi Tang *

Jiangsu Navston Technology Co., Ltd, Zhangjiagang 215600, China.

Publication history: Received on 22 March 2020; accepted on 27 March 2020

Article DOI: https://doi.org/10.30574/gjeta.2020.2.3.0020

Abstract

Aiming at the problems of difficulty in accountability and difficult to trace information in the current logistics system, this article optimizes the permission control scheme in the blockchain system and designs a smart logistics platform based on blockchain. The platform effectively solves the problem of the decline of the credibility of the blockchain caused by abnormal data and poor compatibility without increasing the computational complexity. Through strict and efficient authority control, the intelligent logistics platform can ultimately ensure that the performance requirements of logistics application scenarios are met under the premise of high security.

Keywords: Blockchain; Authority control; Smart logistics

1. Problems in the current logistics system

Logistics is a comprehensive industry involving multiple fields, and product competition is the norm. How to make the logistics industry orderly compete, reduce costs, improve quality and efficiency has become the main content of the development of the logistics industry. Although, about 90% of world trade volume is carried out by the international shipping industry each year. However, the logistics behind global trade is extremely complicated, and its sharp contradictions are mainly reflected in the following three aspects [1-4]:

1.1. Lack of risk control

Most modern logistics adopt a centralized management model of resources and services. The problems caused by large-scale logistics service transactions are highly concentrated, the coordination capabilities between various flow systems are poor, the processing process is tedious, the storage space is large, and data cannot be traversed quickly. Once the files are lost, the risks are uncontrolled and traceability investigations are not possible.

1.2. Unbalanced development of logistics enterprises

The logistics information platform is costly and is not suitable for the overall layout of small and medium-sized logistics enterprises. Although large logistics enterprises can effectively improve the logistics service transaction experience, the logistics trade involved cannot cover all the goods on the market. Therefore, the development of the entire logistics industry is severely uneven, and the resource sharing rate is extremely low, which ultimately leads to low logistics efficiency.

1.3. Loose supervision of logistics industry

Logistics is a typical service industry. Due to the imbalance in the development of the logistics industry, many logistics companies have neglected the quality of services while seeking to maximize their benefits, and their default and illegal costs are extremely low. Therefore, an intelligent supervision mechanism is urgently needed to realize high-quality logistics transactions under the supervision of the whole process. At the same time, non-standardized companies can respond quickly and force them out of trading.
According to an estimate by the World Economic Forum (WEF), reducing the logistics barriers caused by the above issues will increase global domestic product (GDP) by nearly 5% and increase global trade volume by 15% [5-7]. Blockchain is currently the technology direction most likely to break through the development bottleneck of the logistics industry. Blockchain is a distributed database system, which is not easy to tamper with, difficult to forge, and traceable. The blockchain records all the information about the transactions that occur. Once the data enters the blockchain, it is difficult for even insiders to make any changes in it without being discovered. For the logistics industry, since each company has its own main logistics system, which belongs to a separate supply chain, it is necessary to design a smart logistics platform based on the blockchain. Under the requirements of ensuring compatibility and security, solve the disadvantages of traditional blockchains, such as low compatibility, weak system throughput, and abnormal data, make it meet the needs of practical application scenarios in the logistics and express delivery industry.

2. Permission Control in Blockchain

In the new generation of blockchain, the control of data access rights is the basis for ensuring the credibility of the blockchain. The blockchain that the logistics industry belongs to is a typical multi-source, heterogeneous and complex chain system. This complex system is prone to problems such as data anomalies and version compatibility, which reduces the credibility of the logistics blockchain. Therefore, logistics blockchains need to use various fast and efficient encryption algorithms, use different role nodes to form identity protection, permission settings, internal transactions, security audits, and bad block removal mechanisms, and build a complex block system of channels, organizations, and member nodes under multiple levels of authority control. However, in the context of logistics, the high throughput of the blockchain system leads to a linear increase in the number of encryption and authentication operations performed. The blockchain permission control scheme proposed in this paper can effectively solve the above problems. First, when ordinary nodes write content to the blockchain ledger, the content area is encrypted by the SHA256 algorithm to obtain an encrypted block. Second, the encryption key, transaction hash, and sensitive state are recorded in the blockchain management ledger, and the first 20 bytes of the area are encoded by the SHA256 hash algorithm and the Base58 algorithm to obtain a fixed-length address identifier. Finally, the sensitive state of the encrypted block address identification is calculated using the Secp256k1 algorithm. If it is determined that the address identifier is in a sensitive state, the content of the encrypted block is added to the ordinary node, otherwise the smart contract mechanism is used to seal the encrypted block to a separate storage area and prompt an exception. The relevant code is as follows:

```java
import java.security.MessageDigest;

public class StringUtil
{
    // Applies Sha256 to a string and returns the result.
    public static String applySha256(String input)
    {
        try
        {
            MessageDigest digest = MessageDigest.getInstance("SHA-256");

            // Applies sha256 to our input,
            byte[] hash = digest.digest(input.getBytes("UTF-8"));

            StringBuffer hexString = new StringBuffer();

            // This will contain hash as hexadecimal
            for (int i = 0; i < hash.length; i++)
            {
```

68
3. Design of smart logistics platform based on blockchain

As shown in Fig. 1, this article designs a smart logistics platform architecture based on the blockchain, which enhances the credibility and operational efficiency of the logistics blockchain by strengthening system identity management and access control. The user management module includes customers, logistics companies, and other related goods and cargo carriers. These entity roles obtain product information from a designated logistics source and use it to run the required logistics tasks. The task scheduling module analyzes business rules and commodity processes, divides the business into basic tasks and dynamic tasks, and rationally maps the correspondence between assigned roles and tasks. At the same time, you can prevent the same entity from performing the same task by setting rules for mutual exclusion.
of tasks and roles. The authority scheduling module includes smart contract and authority allocation functions. By applying the permission control scheme proposed in this paper, the user roles and tasks in the logistics blockchain are hierarchically and regionally managed, and many logistics providers and logistics-related resource owners are integrated into a unified and efficient management platform.

The logistics platform enhances the trust in the system through strict identity control, offloads the work of message verification and data security to the outer layer of the logistics blockchain, simplifies the system’s internal verification and security mechanism, and uses more lightweight level encryption mechanism to improve performance and reduce costs. For industry-level information platforms, the logistics blockchain designed in this article will not be disturbed by external factors at the demand level, and fully takes advantage of the advantages of blockchain technology in data that cannot be tampered with, easy to trace to the source, and multi-party verification and maintenance. To improve system performance and efficiency.

4. Summary
Blockchain technology, as the integrator of computer and information technology, has the advantages of decentralization and trust, data tamper resistance, and easy traceability. It fundamentally breaks through the bottleneck brought by the centralized management of logistics enterprises and improves traditional logistics scenarios. There are inherent problems such as liability tracing, privacy leakage, and opaque data. Aiming at this goal, the intelligent logistics platform designed in this article optimizes the authority control problem to ensure that the system meets the performance requirements of logistics express application scenarios on the premise that the security performance is not lower than that of the traditional blockchain system.

References
[1] Nakamoto S. (2008). Bitcoin: A peer to peer Electronic Cash System [EB/OL]. Switzerland: Nakamoto S.
[2] Shor PW. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM review, 41(2), 303-332.
[3] Karame G, Androulaki E and Capkun S. (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin[J]. IACR Cryptology ePrint Archive, 248.
[4] Eyal I and Sirer EG. (2018). Majority is not enough: Bitcoin mining is vulnerable [J]. Communications of the ACM, 61(7), 95-102.
[5] Garay J, Kiayias A and Leonardos N. (2015). The bitcoin backbone protocol: Analysis and applications[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 281-310.
[6] Kiayias A, Russell A, David B, et al. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol[C]. Annual International Cryptology Conference. Springer, Cham, 357-388.
[7] King S and Nadal S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake [J]. Self-published paper, 19.
[8] Mobile payment forum, Ltd, mobile payment forum white paper [N], http://www.mobilepaymentforum.org.
[9] Seema Nambari, Lu CT and Liang L.R. (2004). Analysis of payment transaction security in mobile commerce[R], Information Reuse and Integration, IRI. Proceedings of the 2004 IEEE International Conference 475-480.
[10] Oto Kolsi and Teemupekka Virtanen. (2004). MIDP2.0 Security Enhancements[R]. Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE, 217-222.

How to cite this article
Haidi T. (2020). Application research of smart logistics based on blockchain technology. Global Journal of Engineering and Technology Advances, 2(3), 67-70.