IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

Production Industry Supply Chain Management Based On the Ethereum Blockchain

Sandesh Walunj[1], Akshay Gupta[2], Anuradha Sonone[3], Saurabh Yadav[4], Puja Gholap[5]
Students, Department of Computer Engineering[1,2,3,4]
Assistance Professor, Department of Computer Engineering[5]
Sharadchandra Pawar College of Engineering, Pune, Maharashtra, India

Abstract: *Currently, the composition and structure of the production industry's supply chain is becoming increasingly complex. The loss and untimely transmission of supply chain information exacerbated the bullwhip effect. At the same time, due to the lack of a reliable repository of information, difficulties in traceability and accountability have also made supply chain management difficult. Blockchain has the characteristics of supporting distributed networks, synchronization of information between nodes, digital encryption, traceable information and unforgeable block content, which is suitable for use in supply chain and can provide a solution for it. In this paper, a design scheme of an integrated platform for information services provided by supply chain participants and based on the Ethereum blockchain is proposed. Using Ethereum smart contracts, the regular trade involved in the supply chain is realized using blockchain technology, and key information about the production and circulation of the supply chain is stored on the blockchain to ensure that the information cannot be falsified. At the same time, a reputation evaluation method based on smart contracts is used to evaluate the reputation of enterprises in the supply chain, which can provide references for supplier selection among enterprises.*

Keywords: Supply Chain Management, Information Platform, Blockchain, Smart Contract

I. INTRODUCTION

The following bottlenecks exist in the supply chain information management process of the traditional production industry. First, as the control system of information flow, logistics and capital flow of enterprises, the supply chain has many participants who form a network, so the timeliness of information transmission and sharing is affected to some extent, causing a bullwhip effect of supply. the chain itself. Second, although centralized data management can also establish a system of collaborative management, it suffers from the problems of data vulnerability to illegal manipulation and difficult accountability. Finally, for consumers and regulators, when they want to know the production history of the products they buy or regulate, or if they want to see if the implementation of each link is compliant, it can take one to two weeks or more to trace. information within a traditional supply chain surveillance system.

Blockchain, as a cryptographic and interconnected storage structure, has the basic characteristics of supporting multi-party maintenance, non-tamperable data, easy traceability, and so on. These characteristics coincide with the multi-party collaboration characteristics of the production industry's supply chain management and the demand for better information sharing and transparency, so they are considered key technical solutions to supply chain management problems [1]. The use of blockchain in the supply chain can track all links of the supply chain and improve its overall security. At the same time, blockchain can break the information islands in the supply chain, strengthen the information connection between supply chain members, improve the efficiency of cooperation between participants, and facilitate information traceability and supervision due to the consistency of node information in the blockchain.

At the same time, the Internet of Things can be combined with blockchain and used in industrial applications, especially in the supply chain management of the production industry. On the one hand, blockchain technology can increase the security of supply chain data collected from the Internet of Things in industrial applications; on the other hand, industrial supply chain IoT data can act as input to smart contracts on the blockchain to manage supply chain processes.

Ethereum Blockchain is the first blockchain platform that supports on-chain programming, i.e. smart contract. Smart contracts running on the Ethereum Blockchain can be designed to complete many logical services. Its official

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

recommendation language, Solidity, is a Turing Complete programming language that can meet the needs of many functions. Therefore, some agreed rules can be written into smart contracts, deployed on the blockchain, and then used by users, providing a convenient business support channel for all parties in the supply chain who need to cooperate with each other.

This paper aims to design a comprehensive production supply chain management system based on the Ethereum blockchain, using smart contracts and Node.js technology to provide ordering, trading, information and inquiry tracking, and other services for various kinds of supply chain participants.

II. RELATED WORK

Since the birth of blockchain technology in the last ten years, research on its application has been constantly developing and deepening. Blockchain has gone through phase 1.0 represented by digital currency and2.0 represented by smart contracts and financial transactions such as stocks and bonds. Now it has reached3.0 phase [2], where all social layers are actively involved.

Research on the application of blockchain in the supply chain mainly focuses on the tracking of product information. One use case of blockchain in the pharmaceutical supply chain was shown in [3], a new blockchain-based product ownership management system to combat counterfeiting in the post supply chain was proposed in [4], and a set of contracts for supply chain traceability are proposed in [5].

The main focus of current research is the traceability of product information. The main idea is to store information about each link in the blockchain. There are fewer proposals for other functions involved in supply chain operations. Based on existing research, this paper will propose a more comprehensive management system for supply chain business based on blockchain and other related technologies to meet the needs of various supply chain participants. The more complex and larger the supply chain is, the longer and more unpredictable its delivery time will be, and the less transparent its process will be to the upstream and downstream companies. One consequence of this, it's that a small delay in any link of the supply chain may lead to an excess or insufficient inventory in other links of the supply chain, which is what usually call the bullwhip effect of the supply chain[6].

III. SYSTEM ARCHITECTURE

The content of this part is the presentation of the physical architecture and the logical architecture used in the development of the system. It clarifies the system design, operating mode, and calling rules between logical components. This paper improves the conventional architecture of decentralized applications according to the actual needs of the system.

3.1 Physical System Architecture

Consortium chain is a type of blockchain that is not fully decentralized. It allows the authorized nodes to join the network and participate in consensus. Nodes in the consortium chain can register and leave the chain themselves. They can inquire about any information about the blockchain. Since the system needs administrative nodes to regulate the registration process of the various participants in the supply chain, a chain of consortia is a suitable solution for this scenario.

The system adopts an overall distributed blockchain-based architecture, and each participant is responsible for the operation of the Ethernet blockchain consensus node. When enterprises plan to join the consortium chain, they must submit an application offline, and then the governing organization will issue unified blockchain initialization data for the system. Each enterprise can use this initialization information to join the consortium chain with a different specific configuration on its own node. After that, businesses can register accounts through the system according to their own blockchain addresses and business information. As a unique identification of a business in the system, an Ethereum address is tied to a business entity. The physical operating model of the system is shown in Fig. 1.

System administrators and supply chain members such as manufacturers, processors, logistics providers and distributors form a blockchain consensus network. Every organization runs an Ethereum node. The database server is managed by administrators. Consumers do not participate in the consensus of the blockchain network, but can access the system when performing query operations. The above system architecture can meet reasonable system design needs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

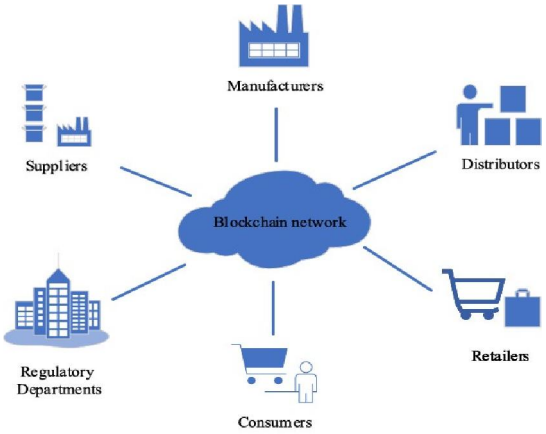

Fig. 1. Physical system architecture diagram

The main working routine of a distributed network is as follows:

1. A node for each entity generates new transaction data, and disseminates the data through a peer-to-peer network.
2. all nodes generate new blocks according to the Ethereum consensus mechanism.
3. all nodes calculate the signature and hash, and the first one to complete the calculation and send the result can get the right to record this transaction; transaction information, previous hash, timestamp, difficulty and other fields would be wrapped in a new block.
4. a node that gets the right to record a transaction broadcasts a new block to the entire network.
5. all other nodes that receive the new block will verify the information and place the new block at the tail of the local blockchain.

3.2 Logical Architecture of the System

A DAPP architecture typically includes HTML pages, browser-side JavaScript, the web3.js library, and the Ethereum blockchain. Although this conventional DAPP architecture can meet the basic requirements of a blockchain application, the system has poor scalability and needs more front-end logic processing. Therefore, this paper optimizes it and proposes a four-layer overall architecture as shown in Fig. 2.

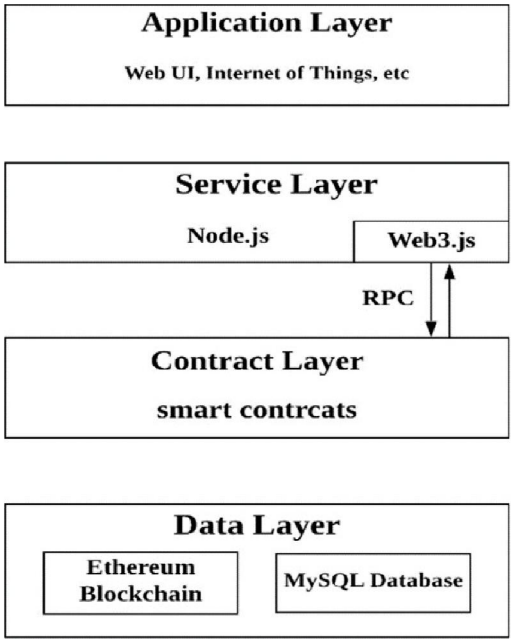

Fig. 2. System logic architecture diagram

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

The system is divided into four layers: application layer, service layer, contract layer and data layer. The application layer provides the user interface and the service layer provides the Node.js web services needed by the system. The contract layer complements the management of business logic and the control of access to blockchain data and database data using smart contracts. The data layer is responsible for storing blockchain data and database data. The invocation connection between the service layer and the contract layer is implemented through the RPC interface exposed by the Ethereum workshop.

The design and implementation of the service layer, contract layer and their interaction are quite important for this control system. A node in the service layer is the main service delivery mechanism that supports the entire application. The server part has a rather complex logic. Node.js is used here to ensure better compatibility with the web.js interface, which is recommended by the Ethereum development team. The Ethereum blockchain can be contacted directly with in-browser scripts, but this solution is hardly scalable. Adding a service layer brings better extensibility and maintainability.

Smart contracts reside on the contract layer, which is mainly responsible for interacting with the Ethereum blockchain. A smart contract developed with the Solidity programming language can retrieve some data, such as timestamp and block information, from the blockchain. Cryptographic functionality provided by the language itself can facilitate processes such as data authentication.

Since huge numbers of direct blockchain queries can have a slow response, this document includes database storage. The database combined with blockchain can realized massive storage with responsible resource consumption and better access efficiency.

3.3 Organization of System Modules

The system has a total of 4 modules. They are System management, Tracing, Process management and Reputation management. The System Management module includes member registration, authorization management, information editing, member deletion and information publishing functions; the Tracing module includes the functions of recording information, querying information and adding and verifying signatures in all links of the supply chain, realizes the traceability of goods in the system and ensures the trustworthiness of information using a digital signature; the Process Management module meets the functional requirements of joint supply chain cooperation for businesses. It includes order management, receipt and delivery management, balance and funds management. Finally, the reputation management module includes order ranking, reputation calculation and reputation query functions. It can perform sound and reliable credit evaluations for businesses by analysing transaction data and historical scores. Their organizational relationships are Shown in Fig. 3.

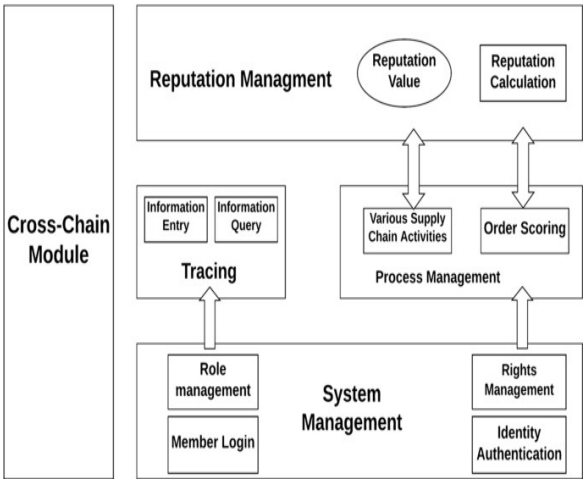

Fig. 3. Organizational chart for the system module

It can be seen that the authentication of members and the management of rights of various roles in the system management module are an important basis for the normal operation of the entire system. Members can use specific features only after registration. They can register for the corresponding traceability module link and use the services provided by the process control module only after they are identified as having these specific role rights. The reputation

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

management module can calculate enterprise reputation values based on accumulated data in the process management activities, which in turn provides a reference for process management activities.

IV. SYSTEM DESIGN

This section will show the details of the system design and provide solutions to some of the critical design issues.

4.1 Basic System Functions

In this system, the core functions include authority control, tracking, trading and reputation calculation. Tracking is a relatively independent function. The process of transaction is buyer publishing an order request – seller taking the order– buyer choosing a service provider – both parties reaching an order agreement – seller delivering the order – buyer receiving the order - the transaction completed.

When choosing, requesters must check the reputation of the service providers. Reputation comparisons can influence the choice of request issuers. The reputation calculation is designed to be performed in real-time, providing the most recent results when queries are executed. In this way, not only can the latest data be obtained, but the storage pressure can be relieved to some extent.

4.2 Main Technical Solutions

A. The Tracing Process

The tracking process is of great importance in this supply chain management system. Here we depend on the Ethereum blockchain to ensure that reliable and unaltered information can be obtained. Information has two repositories: the database and the blockchain. We put traceable original information into a database and put a verifiable signature into the blockchain to ensure verifiability. To ensure that the information to be retrieved later is reliable, supply chain participants must sign their information at the information registration stage. In this paper, we propose a method for generating and verifying signature. The detailed method is shown as follows:

a. Storage of Information

Suppose we have the original information ***I***; we can obtain signature information ***S*** with the help of following functions:

$$H = \text{sha3}(I) \quad (1)$$

$$S = \text{Sign}(H, \text{default Account}) \quad (2)$$

In equation (1), H means the intermediate result after applying the SHA algorithm to the original information. The parameters passed to the signature function in equation (2) are the hash result from the first step and the account information of the current entity. Hash and signature functions can be provided by the web3.js library. Results can be obtained off-chain.

Here the original information is stored in a database for quick retrieval and later comparison.

b. Verification of Information

The Ethereum address of the ***A*** subject about which the information would be verified is stored in the smart contract. Information retriever should first retrieve the original information ***I'*** from the database over the network and use the ***keceack256*** function to calculate the new hash ***H'***.

$$H^r = \text{keceack256}(I^r) \quad (3)$$

The three cryptographic parameters ***r***, ***s*** and ***v*** can be separated from ***S*** in the smart contract. By passing these three parameters with ***H'*** to the ***ecrecover*** function provided by Solidity, we can get the Ethereum address of the information provider ***A'***. The validity of the message can be tested by equation (4).

$$A = A' \quad (4)$$

The signature and keceack256 is calculated using JavaScript and the signature verification is performed using Solidity.

c. Information Display

There is a mapping between the contract address and the business name stored in the smart contract. with this the business name mapping can be displayed to the end user.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

Each item will be identified by an ID and its component ID is recorded in the combination. In the blockchain, the signature and timestamp are stored together and mapped to the item ID. When querying by item id, users can get the process from production to its circulation.

B. Reputation Management

The reputation rating mechanism we set up for supply chain businesses is actually a relatively simple index rating system. The system can dynamically evaluate the supplier's reputation and calculate the reputation value that will be displayed to the requester when making an inquiry.

When studying of complex evaluation with multiple indices, the prerequisite of scientific evaluation is to construct a reasonable index evaluation system. In general, the principles followed in the design of the rating system are "comprehensive indicators", "non-overlapping" and "easily obtainable", while having "scientific", "rational" and "applicable". A specific evaluation method can be designed and modified according to the specific requirement of the management system.

a. Timestamp Dependency

The allowable time error for the verification and generation of an Ethereum block is 900s, which means that a block can be generated if the time difference between the timestamps of two nodes for the same block is less than or equal to 900s. If there is a judgment based on accurate timestamps in the smart contract , the results of the programs would be affected by the current timestamps. This means that the results may be unstable and this fact could even be manipulated by malicious nodes to affect the execution results. This phenomenon is called timestamp dependency in the Ethereum blockchain. To avoid errors in smart contracts due to different timestamps in different nodes, this paper implements a timestamp-based system and proposes a method to avoid timestamp dependency. The detailed method is shown as follows:

When the user enters a date in a human-readable format into the browser, the JavaScript engine convert the date into a UNIX timestamp, which has unit of millisecond and contains 13 digits. Then the first 10 digits are reserved using equation (5).

$$t^r = \frac{\checkmark\ h\ h.\ \text{Priority 1}}{1000} \qquad (5)$$

The essence of equation (5) is to convert a millisecond to a second using the truncation method. t' is then passed to the smart contract. This article uses block.timestamp as a factor for assessment. It uses a solution provided by the Ethereum blockchain to depend on the timestamp. The basis of this solution is that the program allows a maximum time error of 900 s, or that when smart contracts run on EVMs of different nodes, the results are the same when the time stamp difference between them is less than or equal to 900 s.

More specifically, ***block. Timestamp*** is used to set when the command requests expire and whether commands are executed on time. This should guarantee a time difference tolerance of 900s Some judgements should in smart contracts should be adjust. For example, equation (6) should be modified as equation (7), and equation (8) should be modified as equation (9).

$$t_{current} \leq t_{expiration} \qquad (6)$$

$$t_{current} \leq t_{expiration} - 900 \qquad (7)$$

$$t_{current} < t_{agreed} \qquad (8)$$

$$t_{current} < t_{agreed} - 900 \qquad (9)$$

In this way, the assessment of the program will not be affected even if there is some time difference between different local systems.

4.3 Design of Smart Contracts

A smart contract contains data and methods. In Solidity, storage-type data can be permanently stored in blockchains by defining data structures to store the necessary data. A function is an important way to complete logical execution. The defined function waiting to be called. There are two kinds of functions: those that change the state of blockchain and those that don't. This part mainly presents the design of some key contract data structures and methods in the system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

- Authorization of user rights. We do this by defining a member structure that contains Boolean values indicating whether the current user has access to some link information. Initial values are false. When administrators grant permissions to different parties, they modify the corresponding values of a particular user's structure variables so that permission checking is implemented.
- Information recording. Each item is distinguished by an ID; hash values of the registration information are entered; a cryptographic signature is generated; timestamps are collected automatically; and all information is saved.
- Receiving orders. First, we need to make sure that the requests are not stale and have not been accepted (the request issuer should not select a service provider for the current request). Then enter the promised arrival time and price, generate a receipt record, and enter an order receipt record by its corresponding ID.
- Choosing a service provider. Enter the ID of the selected service provider; changes the selected tag value in the receipt to 1; and the tag values of other service providers for the current order will be set to 2. Then update the cooperation partner records for the specified order. Finally, the contract generates an order record that contains order receipt information and requirements information.
- Reputation calculation. By retrieving the values of necessary storage-typed variables from the blockchain and incorporating an applicable algorithm, the reputation calculation can be performed in real-time

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed an Ethereum-blockchain- based management system design scheme for production industry supply chain We introduced architecture and operating mode of the system and described the functional modules in it. We have designed several smart contracts for supply chain participants.

In the future, our work could further develop in some ways as follow:

- Develop better consensus mechanisms that are compatible with Ethereum so that we can improve the performance of the system at the blockchain consensus level.
- Expand system functionality. We can add business functions related to supply chain finance and take full advantage of blockchain while meeting larger user needs.
- Design a reasonable and applicable evaluation method or algorithm for different suppliers in the supply chain.
- Strengthen the connection with the Internet of Things. We can develop communication mechanisms that can directly send messages from the IOT sensor to the blockchain. It would be more convenient for direct collection of reliable and objective data, which further reduces the possibility of human intervention and manipulation.

VI. ACKNOWLEDGMENT

The First and foremost, we would like to express our gratitude to our Mentor, Prof. Gholap Puja, who was a continual source of inspiration. He pushed us to think imaginatively and urged us to do this homework without hesitation. His vast knowledge, extensive experience, and professional competence in Data Science enabled us to successfully accomplish this project. This endeavor would not have been possible without his help and supervision. We could not have asked for a finer mentor in our studies. This initiative would not have been a success without the contributions of each and every individual. We were always there to cheer each other on, and that is what kept us together until the end.

I'd like to thank The University of Savitribai Phule Pune University for providing me with the opportunity to work on the project (Production Industry Supply Chain Management Based On the Ethereum Blockchain). Last but not least, I would like to express my gratitude to my family, siblings, and friends for their invaluable assistance, and I am deeply grateful to everyone who has contributed to the successful completion of this project.

REFERENCES

[1]. Zhijun Xu, Yichen Liu , Jun Zhang, Zhaoxiong Song, Jun Li, Jihua Zhou "Manufacturing Industry Supply Chain Management Based on the Ethereum Blockchain ondren Library Rice University: DOI 10.1109/IUCC/DSCI/SmartCNS.2019.00124.

[2]. Swan, Melanie. Blockchain: Blueprint for a New Economy. Blockchain: blueprint for a new economy.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

O'Reilly, 2015.

[3]. Bocek, Thomas, et al. " [IEEE 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - Lisbon, Portugal (2017.5.8-2017.5.12)] 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - Blockchains everywhere - a use-case of blockchains in the pharma supply-chain." Integrated Network & Service Management IEEE, 2017:772-777.

[4]. Toyoda, Kentaroh, et al. "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain." IEEE Access (2017):1-1..

[5]. Kim, Henry M., and M. Laskowski. "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance." (2016).

[6]. Shi-Min, Sun, C. Hui-Ying, and L. Zhao-Yun. "Study on Comprehensive Evaluation Index System for Pig Form in High Quality Pork Supply Chain." Operations Research and Management Science (2007).

BIOGRAPHY

Mrs. Gholap Puja has done her Masters in Computer Engineering from Sharadchandra Pawar College of Engineering, Pune University, and Maharashtra, India in the year 2017. She is currently working as Assistant Professor in the Department of Computer Engineering, at Sharadchandra Pawar College of Engineering, Pune University. She is pursuing PhD in Computer Science from Sandip University Nashik. Her research interests are in Machine Learning, Artificial Intelligence, Cloud computing