EasyChair Preprint

№ 9700

Blockchain-Based Cloud Resource Allocation Mechanism for Privacy Preservation

Nihar Ranjan Nayak, Akhilesh Kumar, Samrat Ray and Ashish Kumar Tamrakar

February 14, 2023

Blockchain-Based Cloud Resource Allocation Mechanism for Privacy Preservation

[1]Dr. Nihar Ranjan Nayak, [2]Dr. Akhilesh Kumar, [3]Samrat Ray,

[4]Dr Ashish Kumar Tamrakar

[1]Assistant professor Department of MCA, Sri Venkateswara College Of Engineering & Technology(Autonomous), Chittoor, 517127,Andhra Pradesh

[2]Assistant Professor, Department of Information Technology, Gaya College, Gaya, Bihar

[3]Assistant Professor, Marketing management, Sunstone CIEM campus

[4]Assistant Professor, CSE, Bhilai Institute of Technology(BIT) Raipur Chhattisgarh.

Email: [1]nayak.niharranjan0@gmail.com,[2]getaky123@gmail.com, [3]samrat.ray@sunstone.edu.in, [4]ashish.tamrakar1987@gmail.com

Abstract: In the cloud manufacturing platform, virtualized manufacturing resources are complex to ensure the authenticity and security of transaction data during the transaction process and rely on the unified deployment of cloud manufacturing platform operators (CPOs). This centralized framework is prone to a single point of failure and risks leakage of private data. Because of these problems, combined with the advantages of decentralization and immutability of blockchain, we innovatively explore the application of blockchain technology in cloud manufacturing and propose a blockchain-based cloud manufacturing resource allocation method. Firstly, a blockchain-based decentralized cloud manufacturing trading platform framework is presented. The Elliptic Curve Digital Signature Algorithm (ECDSA) in manufacturing resource/demand release is studied, and the matching mechanism between manufacturing resources and demand is analyzed. Then, a manufacturing resource verification contract and a manufacturing resource transaction contract for cloud manufacturing are designed using smart contracts (SC). The experimental tests in the Remix platform are completed using Solidity. The test results show that the proposed method can provide a safe and reliable guarantee for virtualized manufacturing resource transactions. Finally, the game problem of supply-demand balance between manufacturing resource suppliers (MRS) and demanders (MRDs) under the decentralized architecture is explored, and simulation is carried out on MATLAB R2021b. The simulation

results show the manufacturing resource supply and demand. The fair game can reach the Nash equilibrium and has a faster convergence rate than the existing research.

Keywords: Blockchain; Cloud; Resource Allocation; Digital Signature

I. INTRODUCTION

Cloud manufacturing [1, 2] relies on advanced technologies such as cloud computing, the Internet of Things, big data, and virtualization to provide a new production model for the manufacturing industry. Based on the cloud manufacturing platform, the physical world's manufacturing resources and manufacturing capabilities are abstracted into virtual resources that can be used for consumption through digital twin technology [3]. It is still possible to break the constraints of geographical conditions. Cloud manufacturing aims to provide users with various flexible and customizable manufacturing services throughout the product life cycle [4].

As a frontier issue of common concern in academia and industry, research work on cloud manufacturing mainly focuses on reliability, resource allocation, and service quality. Literature [5] constructed an evaluation index system to effectively characterize cooperation trust by monitoring historical service evaluation data, quantified service satisfaction and proposed a trust evaluation model based on service satisfaction. Reference [6] studies the credibility of manufacturing resources in cloud manufacturing platforms and evaluates the credibility of manufacturing resources in terms of credibility and reliability. To solve the ambiguity and uncertainty of preference information in the process of matching complex product manufacturing tasks on the cloud manufacturing platform, literature [7] proposed a bilateral matching model based on double hesitant fuzzy preference information. Reference [8] offers a resource allocation method based on energy consumption perception for the energy consumption of cloud manufacturing platforms in manufacturing resource allocation. Authority [9] proposes a resource bidding mechanism based on the resource scheduling problem with complex characteristics of cloud manufacturing, which ensures the fairness of the cloud manufacturing market. In [10], considering that different manufacturing cloud services have similar functions and different service qualities, a context-aware manufacturing cloud service description model is proposed to describe the dependence of a single service on other related services. Reference [11] studied the impact of disturbances on service quality in the cloud manufacturing process and used discrete Markov hopping systems to achieve dynamic optimization of resources. The above-mentioned theoretical research and exploration of cloud manufacturing have made some progress in reliability, resource allocation and service quality. However, the underlying system architecture it relies on is still a centralized framework system. Under this framework, the operator operates the cloud manufacturing platform, and the platform operator deploys both the supplier and the demander of manufacturing resources. Its most prominent feature is that the decision-making in the system depends on a small number of nodes, so it is inherently unable to avoid a single point of failure. The single issue of failure problem is mainly solved through the redundant backup, but it requires expensive maintenance costs. It cannot fundamentally solve the single point of failure. In addition, a small number of nodes in the system have too much authority, which is easy to become the target of hacker attacks, and there is a risk of leakage of confidential data.

Blockchain technology is a new decentralized infrastructure and distributed computing paradigm [12]. In the public chain, all nodes have the same status, and only when certain conditions are

met can they obtain accounting rights. Other nodes are responsible for verifying and updating the local data after the warranty. The blockchain network stimulates the enthusiasm of nodes to mine by issuing rewards. Therefore, even if there is no central node scheduling in the network, the blockchain network can still ensure the integrity and consistency of data storage. At the same time, blockchain technology is a technology for creating trust. In a network with weak faith, nodes can be recognized by most nodes according to objective criteria, such as computing power and coinage. It provides a secure way to exchange any goods, services or transactions. The data on the blockchain cannot be tampered with. The data stored in the block is uniquely encoded by hash operation, and the blocks are connected in a chain structure, strengthening the security of the stored data.

Blockchain technology has broad application prospects. Weng Xiaoyong designed a double-chain structure to protect the shared data in the cloud platform by taking advantage of the decentralization and non-tampering properties of the blockchain [13]. Author used the data traceability of blockchain to design a food traceability system [14]. To solve the expired data in the blockchain, author proposed a delectable blockchain based on an improved threshold ring signature scheme and a consensus mechanism based on proof of space [15]. Reference [16] made a systematic review of the application of blockchain in manufacturing and engineering. Reference [17] pointed out that blockchain technology can meet the needs of distributed systems with high reliability and high data security and proposed the establishment of a system platform for trusted management and control of industrial resources. Reference [18] explores the non-zero-sum rational pricing strategy and the impact of different load levels on the benefits of all parties in the platform in a blockchain-based cloud manufacturing platform. References [19-20] mainly aim at the trust problem in the cloud manufacturing platform and combine the blockchain to design a credible service transaction method. Authorities propose a distributed peer-to-peer network architecture for the centralized architecture and trust issues of third-party platforms to improve the security and scalability of the system. Reference proposed a blockchain-based workflow management system to centrally share heterogeneous logistics resources of different customers. Authority offers a service composition model based on blockchain technology. As a novel manufacturing architecture, the centralization mechanism is overcome by dividing the original service composition problem into multiple sub-problems, each containing a portion of the service/task pool.

Blockchain technology can provide an effective solution to the problems of trust and data security in cloud manufacturing systems. However, relatively few studies use the decentralization and data immutability properties of blockchain for cloud manufacturing. Therefore, this paper proposes a blockchain-based decentralized cloud manufacturing trading platform framework. The workload and innovation points of this paper are as follows:

1. A blockchain-based decentralized cloud manufacturing trading platform framework is proposed. The elliptic curve digital signature algorithm in manufacturing resources/demands is studied, and the matching method of manufacturing resources and needs.

2. The manufacturing resource verification contract and the manufacturing resource transaction contract for cloud manufacturing are designed using smart contracts, and the experimental test in the Remix platform is completed.

3. Explored the game problem of supply and demand balance between manufacturing resource suppliers and demanders under the decentralized architecture and conducted MATLAB simulation. The simulation results show that the game between manufacturing resource suppliers and demanders can reach Nash equilibrium and has a faster convergence rate than existing research.

II. BLOCKCHAIN

Blockchain is a decentralized distributed ledger with the advantages of common maintenance, non-tampering, openness, transparency, security and anonymity. The core components are smart contracts and consensus mechanisms, and their structure is shown in Figure 1. The block header stores data items related to consensus and the current block hash value is the unique identifier of the block. The block body mainly stores the transaction records packaged by the nodes.

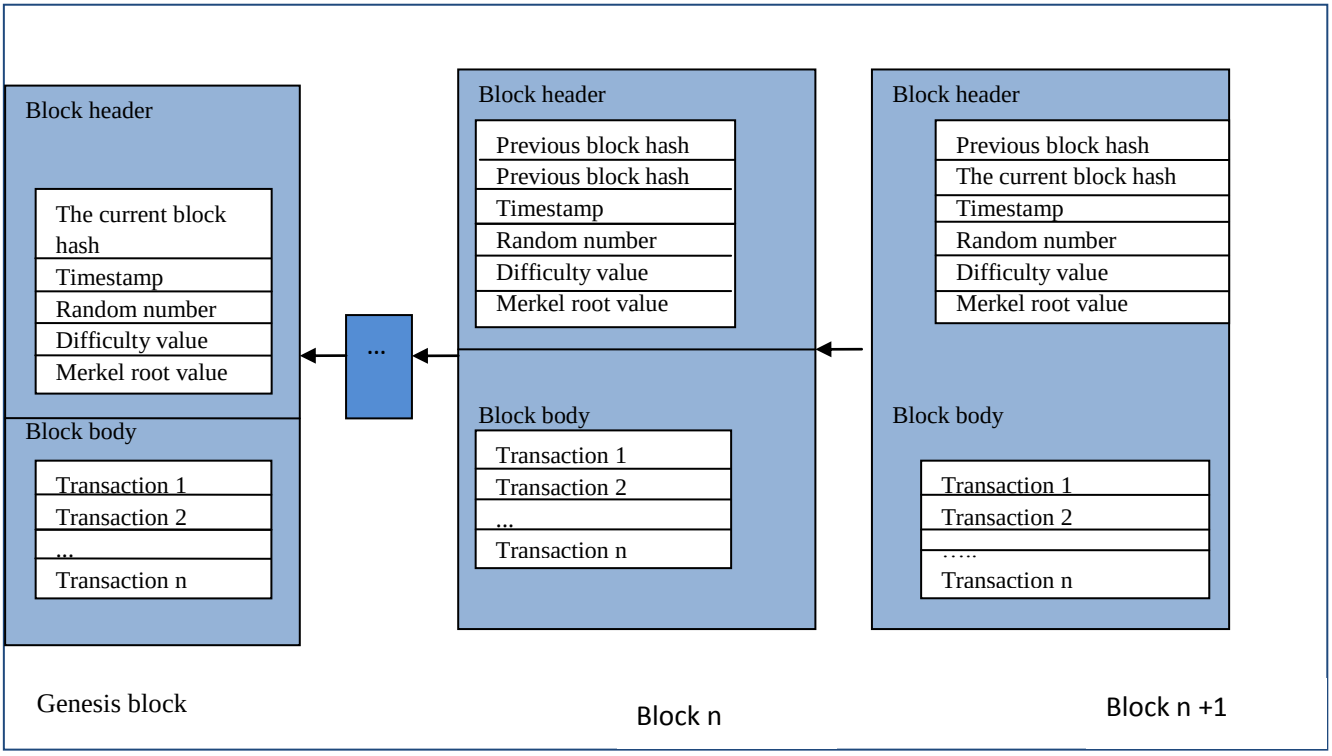

Fig.1 Blockchain structure

Blockchain can be divided into public, alliance, and private chains [26]. The public chain is a completely decentralized network. Nodes in the network have equal status and can join or leave the network at any time, represented by Bitcoin and Ethereum. The consortium chain is a multi-centralized network. The consortium chain's initial members determine the number of centers. The joining of nodes requires the approval of a specific institution, represented by Hyperledger. Finally, a private chain is a centralized network suitable for smaller groups.

A smart contract (SC) is a code embedded in hardware and can be executed automatically. Broadly speaking, a smart contract is a computerized transaction protocol that does not require an intermediary, self-verifies, and self-enforces the terms of the contract. Smart contracts endow the blockchain with greater scalability and flexibility, allowing developers to develop business logic in the blockchain network. Smart contracts use the immutability of the blockchain as the underlying support, and the entire life cycle includes contract creation, contract deployment, contract invocation, and status update. During the entire life cycle of the contract, each link is recorded in the blockchain in transactions.

Consensus algorithms are a necessary part of a blockchain system, and the consensus is the process of agreeing on data or states in a blockchain network. A blockchain system as a distributed network cannot satisfy consistency, availability and partition fault tolerance simultaneously, so a mechanism is needed to compromise between consistency and availability based on satisfying partition fault tolerance. At present, consensus algorithms in blockchain systems can be roughly divided into proof-based and voting-based algorithms. Famous proof-based consensus algorithms include workload proof, equity proof, delegated equity proof, etc. The voting-based consensus algorithm is mainly a Byzantine fault-tolerant algorithm.

III. BLOCKCHAIN-BASED CLOUD MANUFACTURING RESOURCE ALLOCATIONS

The traditional cloud manufacturing platform participants can be divided into manufacturing resource suppliers (manufacturing resource suppliers, MRSs), manufacturing resource demanders (manufacturing resource demanders, MRDs), cloud platform operators (cloud platform operators), platform operators, CPOs. The MRSs register the available resources with the CPOs. The CPOs coordinate the allocation of manufacturing resources according to the needs of the MRDs, as shown in Figure 2, which is a centralized architecture. The blockchain-based cloud manufacturing platform proposed in this paper can realize the allocation of manufacturing resources through smart contracts without the direct participation of a third party. As shown in Figure 3, after MRSs and MRDs agree on resource price and resource supply, they sign a smart contract and save the contract in the blockchain to ensure that the contract data is not tampered with. CPOs is responsible for overseeing the trading behavior of MRSs and MRDs and verifying the manufacturing resources used for trading by checking SCs. When the two parties have a transaction dispute, they can determine the object of the dispute through CPOs and viewing SC.

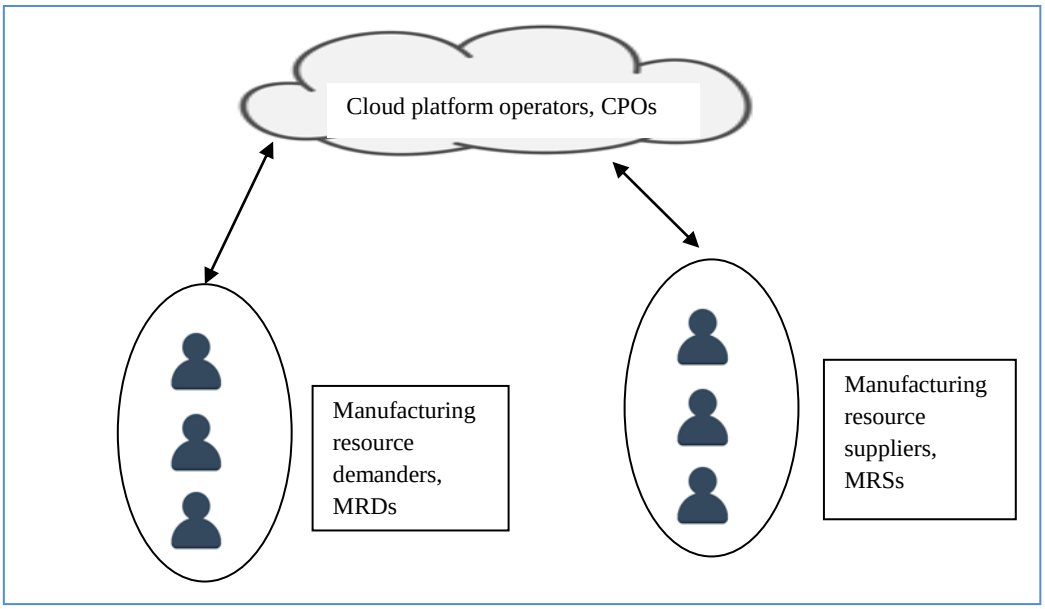

Fig.2 Traditional cloud manufacturing platform architecture.

The introduction of blockchain technology can strengthen the trust between MRDs and MRSs, realize direct transactions between the two parties, and weaken the role of third parties in traditional cloud manufacturing platforms, greatly reducing the cost of credit relyFurthermore, relyingasymmetric digital encryption and communication technology, MRSs and MRDs can grasp the usage of manufacturing resources in real-time.

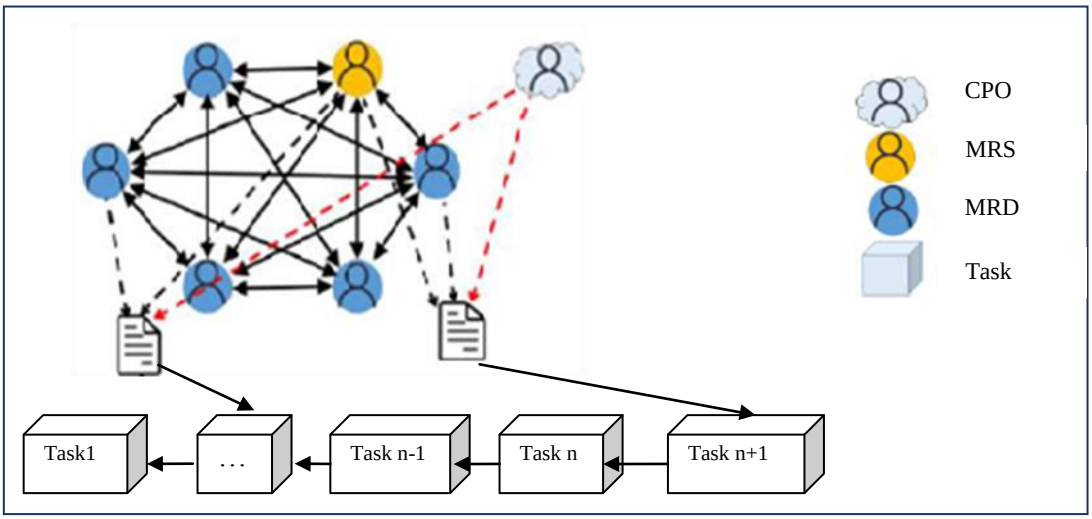

Fig.3 Blockchain-based cloud manufacturing platform architecture

5.1 Manufacturing Resource/Requirement Release

To enhance the security of manufacturing resources/requirements distribution, this paper uses an elliptic curve digital signature algorithm (ECDSA) to ensure that the data transmission between MRSs and MRDs is not tampered with. Taking the MRD sending the resource request message M to the MRS as an example, the specific steps are as follows:

MRD determines an elliptic curve E(a,b) of order p over a finite field HF(q), where a and b are curve parameters, and determines the base point H on the elliptic curve C(a,b). HF(q) ={0,1,2,..., q -1}, q is prime, and $q \in M$. p in the following is the same as here. Without loss of generality, this paper selects the curve $C(0,17) = y^3 - x^3 + 17 = 0$.

MRD selects a random number L_{TD} as the private key, 1< L_{TD} < q, and calculates the public key L_{QD} :

$$L_{QD} = L_{TD} * H \quad (1)$$

Select a secure hash function, perform a hash operation on the request information O, and obtain the information digest m:

$$O = SHA1(O) \quad (2)$$

Randomly choose an integer c, 1<c < q. Compute the coordinates (y_1, x_1) that map c to the elliptic curve:

$$(y_1, x_1) = c * H \quad (3)$$

Still get the first part s of the digital signature:

$$s = y_1 \quad (4)$$

If smod q =0 is the modulo operation, perform this step again. Otherwise, perform the next step.

MRD uses the private key L_{TD} to calculate another part r of the digital signature:

$$r = c^{-1} (o + s * L_{TD}) mod\ q \quad (5)$$

If r = 0, go back to the second step, otherwise go to the next step.

The MRD sends the resource request message O, the signature (s, r), the MSD's public key L_{QD}, the elliptic curve C(a, b) and the base point H to the MRS.

MRS verifies the received message O^* using MRD's public key L_{QD} and signature information calculate:

$$O^* = \frac{o*H+s*L_{QD}}{r} \quad (6)$$

If O^* = c * H, the verification passes, otherwise the verification fails.

5.2 The matching process of manufacturing resources and manufacturing requirements

Consider the following scenario: MRD needs to produce a batch of products, and the product processing task can be decomposed into n sub-tasks Task = {$Task_1$, $Task_2$, $Task_3$,..., $Task_n$ } . Each subtask requires different processing equipment and processing time. Therefore, MRD needs to encrypt the manufacturing demand information MMRD through the ECDSA proposed in the previous section and publish it in the blockchain network to ensure the anonymity of MRD's identity. A hash function encrypts the address information of MRD to obtain MRD_{ad}.

$$MRD_{ad} = HASH(L_{QD}) \quad (7)$$

$$O_{MRD} = \{E, Q_1, U_{MRD}, MRD_{ad}, [C_{MRD}(a,b), H], L_{QD}\} \quad (8)$$

Among them, E = [d_1,d_2,d_3,..,d_n] represents the manufacturing resource demand of MRD's sub-tasks, Q= [q_{11},q_{12},q_{13},q_{1n}] represents the MRD a round is willing to give the purchase unit price of the manufacturing resources of each sub-task, U_{MRD} ={U_{MRD}, U_{MRD1}, U_{MRD2}, U_{MRD3}, U_{MRDn}} represents the increase of each sub-task

Working time period, MRD_{ad} represents the address information of [C_{MRD}(a,b), H] represents the information data used by MRD for signature, C_{MRD}(a,b) represents elliptic curve, H is the base point; L_{QD}

Step 1: MRD uses ECDSA to digitally sign the manufacturing requirement information O and broadcast the signature and the required information to the network.

Step 2: After receiving the manufacturing resource request message M'_{MRD} from MRD, MRS first verifies the message's validity and verifies whether the message is a message sent by MRD through the public key L_{QD} provided by MRD. If the message is invalid, it will not respond; if the message is valid, the MRS will check the request information M'_{MRD}, and reply to the manufacturing resource information O_{MRS} that can be provided to the MRD to the MRD.

$$O_{MRS} = \{R, P_1, U_{MRS}, MRS_{ad}, [C_{MRD}(a,b), H], L_{QD}\} \quad (9)$$

Where R = {R_1, R_2, R_3,.., R_n} represents the manufacturing resources that MRS can provide, P = {p_{11},p_{12},p_{13},..,p_{1n}} represents the number of resources that MRS can provide for each requested resource. The unit price of one round of selling, U_{MRD} ={U_{MRD}, U_{MRD1}, U_{MRD2}, U_{MRD3}, U_{MRDn}} represents the available time period of the resource.

Step 3: After receiving the manufacturing resource supply message 'MMRS' from MRS, MRD first verifies the message's validity and verifies whether the message is a message sent by MRS through the public key KPS provided by MRS. If the message is invalid, it will not respond; if

the message is valid, MRD will check the reply message 'MMRS, and negotiate the disputed place, such as price, to send the message to MRS.

$$O_{MRS} = \{Q_2, MRS_{ad}, [C_E(a,b), H], L_{QD}\} \quad (10)$$

$Q_2 = \{q_{21}, q_{22}, q_{23}, .., q_{2n}\}$ represents the second round of offers for MRD. The price negotiation may last for several rounds, and the game between MRS and MRD will eventually reach an equilibrium point. If both parties can accept the price at the equilibrium moment, the transaction reaches a consensus and proceeds to the next step; if at least one party cannot accept the price at the equilibrium point, the transaction fails, and MRD re-publishes the resource request message to the network.

Step 4: Both MRS and MRD sign the smart contract for the transaction.

In the process of matching manufacturing resources and demand, according to the price, both parties to the transaction independently complete the matching and transaction. After the contract is signed, it is stored in the blockchain to ensure that the transaction record is not tampered.

IV. SMART CONTRACT DESIGN FOR CLOUD MANUFACTURING

Smart contracts are an important part of the blockchain. They are stored in a specific location on the blockchain and can be called and automatically executed by other nodes, giving the blockchain the characteristics of intelligence. Due to the openness and transparency of the blockchain, all nodes can judge the output of the contract according to the input before running the contract formally, so there is no fraud through smart contracts. Despite the advantages of smart contracts, few studies have applied this advantage to actual production. Literature combined smart contracts with data in the Industrial Internet of Things, studied data package contracts and data analysis service contracts, and realized the transaction of data commodities. Inspired by this, this paper proposes a blockchain-based cloud manufacturing framework. In the process of resource allocation, the security and credibility of transactions are guaranteed by signing manufacturing resource verification contracts and manufacturing resource transaction contracts.

4.1 Manufacturing Resource Verification Contract

The manufacturing resources stored in the cloud manufacturing resource pool are the digital version of the manufacturing resources in the physical world. In the process of virtualization, to obtain greater benefits, MRSs may falsify virtual resources by some means, such as deliberately exaggerating the number of resources. Although the blockchain can guarantee the immutability of the data on the chain, it cannot guarantee the authenticity of the original data in uploading the data to the chain. Therefore, the introduction of a regulatory mechanism is critical. Therefore, when introducing blockchain technology, this paper does not completely abandon the supervision function of CPOs due to its decentralization characteristics. The supervision function of CPOs only exists in the first uploading of manufacturing resources. This paper mainly relies on CPOs and SC to complete the verification of data uploading. If the manufacturing resources reported by MRSs exceed the range of manufacturing resources counted by CPOs, the reporting process will be intercepted to improve the data reliability of the system. Once the data of the

manufacturing resource is uploaded to the blockchain network, the system will judge the legality of the manufacturing resource based on the historical records. Therefore, retaining the supervision function of CPOs will increase the reliability of the data, although it will add a verification link and reduce the efficiency of data uploading.

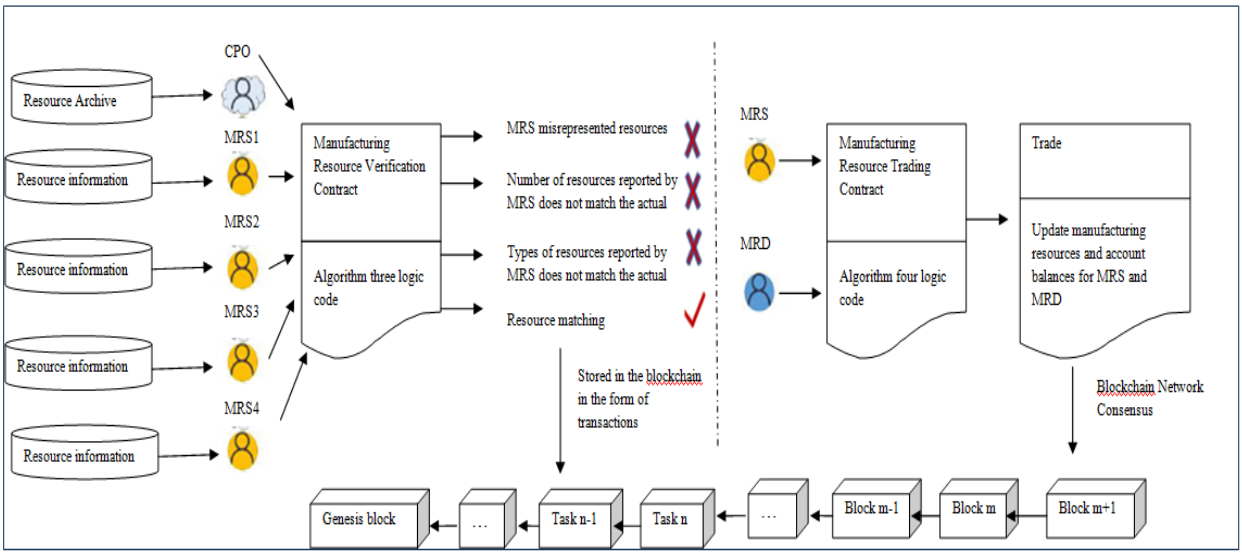

Fig.4 Smart contract design process for cloud manufacturing

The manufacturing resources stored in the cloud manufacturing resource pool are the digital version of the manufacturing resources in the physical world. In the process of virtualization, to obtain greater benefits, MRSs may falsify virtual resources by some means, such as deliberately exaggerating the number of resources. Although the blockchain can guarantee the immutability of the data on the chain, it cannot guarantee the authenticity of the original data in uploading the data to the chain.

Therefore, the introduction of a regulatory mechanism is critical. Therefore, when introducing blockchain technology, this paper does not completely abandon the supervision function of CPOs due to its decentralization characteristics. However, the supervision function of CPOs only exists in the first uploading of manufacturing resources. Therefore, this paper mainly relies on CPOs and SC to complete the verification of data uploading. If the manufacturing resources reported by MRSs exceed the range of manufacturing resources counted by CPOs, the reporting process will be intercepted to improve the data reliability of the system. Once the data of the manufacturing resource is uploaded to the blockchain network, the system will judge the legality of the manufacturing resource based on the historical records. Therefore, retaining the supervision function of CPOs will increase the reliability of the data, although it will add a verification link and reduce the efficiency of data uploading.

4.2 Manufacturing Resource Trading Contract

After MRS and MRD reach a consensus on the resource price, type and quantity through the blockchain communication network, the authenticity and validity of the transaction are guaranteed by signing a smart contract. The price Q in the contract is the price agreed upon by

both parties. The MRS displays the type r_i.name and $r_i.num, r_i \in R$ of all manufacturing resources R in the contract. MRD selects the relevant manufacturing resource type d j .name and quantity $e_j.num, e_j \in E$ according to the purchase demand E. During the transaction process, the manufacturing resource smart contract calculates the payment amount according to the MRD demand; MRS supply and resource price, and sends the amount to the MRS account balance[MRS]. At the same time, adjust the number of resources corresponding to MRS and the account balance[MRD], as shown in Figure 4. Once the smart contract runs on the blockchain, all transaction records will be permanently stored and cannot be tampered with, thus ensuring the authenticity and reliability of the transaction.

4.3 The game of supply and demand of manufacturing resources

The blockchain-based cloud manufacturing resource allocation framework enables MRSs and MRDs to communicate in real-time and bi-directionally through the blockchain network and enables both parties to keep abreast of each other's manufacturing resource demand/supply situation. Therefore, MRDs can determine the purchase amount of resources according to the unit resource price and supply provided by MRSs and their own demand. MRSs can also adjust the supply of manufacturing resources and resource price according to the resource demand of MRDs. There are m MRDs and 1 MRS in the cloud manufacturing platform for a certain manufacturing resource S. Each MRD publishes the demand du of resource S through the blockchain network. MRS determines the supply W_s of the resource after summarizing all demand information and can provide a sufficient amount of resource S to obtain the optimal income. Therefore, the two parties have a time sequence when making decisions, which is a dynamic process with complete information. Therefore, this paper adopts the related theory of the Stackelberg game to solve the problem of resource income between MRDs and MRS, in which MRDs is the leader, MRS is the follower, and MRS determines the resource supply according to the resource demand of MRDs, forming a multi-leader-follower issuer.

First, MRDs collect and publish the manufacturing resource demand V_d , V_d ={v_{d1},v_{d2},v_{d3},..,v_{dm}} through the blockchain network. v_{dj} is the resource requirement of each MRD, j∈{1,2,...,m}. After MRDs obtain manufacturing resources, they can benefit by processing and producing products. The benefit of converting manufacturing resources into product benefits is Y, Y = {y_1, y_2, y_3, .., y_m} denotes the benefit of each MRD, j∈{1,2,...,m}. The price paid per unit of manufacturing resource S is Q_s = [q_s], and the production cost D_d, D_d= [c_{d1},c_{d2},c_{d3}, .., c_{dm}] represents the production cost of each MRD, j∈{1,2,...,m}. Therefore, the profit of MRDs is:

$$I = V_d\{Y - Q_s - D_d\} \qquad (11)$$

After MRD understands the manufacturing demand, it determines the supply of manufacturing resources W_s= [w_s] . The price of manufacturing resources is affected by supply and demand, which is positively correlated with demand and negatively correlated with supply. Therefore, the resource selling price is defined as:

$$Q_s = b \sum_{j=1}^{m} v_{dj} - cv_s \qquad (12)$$

b>0 , c>0 is the influence coefficient of demand and supply on price. The MRS is responsible for the routine maintenance of the manufacturing resource S, and the maintenance cost per unit resource is recorded as $D_s = [d_s]$ So the profit for MRS is:

$$G = W_s\,(Q_s - D_s\,) \qquad (13)$$

The purpose of the game is to maximize the profit for the participants. Therefore, the objective function is:

$$\begin{cases} \max\limits_{v_{dj}} I \\ \max\limits_{w_s} G \\ s.t.\, v_{dj} \geq 0, w_s > 0 \end{cases} \qquad (14)$$

4.4 Stackelberg balance of resource supply and demand

The Stackelberg game is the dominant game. In this paper, MRDs are the dominant players, and the resource demand is determined first, and then the MRS determines the supply according to the demand. The ultimate goal of both sides of the game is to gradually adjust their own strategies under the constraints of the other party's strategies to maximize their own interests. When the interests are maximized, the strategy sets of both parties will reach a relatively stable state; that is, the Nash equilibrium will be reached.

Lemma 1 For the resource price $\alpha=[\alpha_1,\alpha_2,\alpha_3,...,\alpha_k,...,\alpha_m]$, m is the number of players in the game, and the difference between it and the profit $\beta(\alpha)$ Stackelberg game, if conditions I and II are satisfied, there is a Nash equilibrium.

The condition I: α is a nonempty bounded closed convex subset on Euclidean space.

Condition II: $\forall\beta_j \in \beta\,, \beta_j$ is continuous and concave concerning α_j .

Theorem 1 For the Stackelberg game of supply and demand of manufacturing resources described by equations (11)-(14), there is the Nash equilibrium.

Proof because for $\forall j \in \{1,2,..m\}, v_{dj} > 0\; w_s > 0$. So the policy set is a nonempty bounded closed convex subset on Euclidean space. So condition (I) is established also because:

$$i_j = y_j v_{dj} - (b\sum_{j=1}^{m} v_{dj} - cw_s + d_{dj}) \qquad (15)$$

$$g = w_s(b\sum_{j=1}^{m} v_{dj} - d_s) - cw_s^2 \qquad (16)$$

It is known from equations (15) and (16) that i_j is continuous concerning v_{dj} , and g is continuous concerning w_s .

$$\frac{e^2 i_j}{e v_{dj}^2} = -2a < 0 \,, \forall j \in \{1,2,..m\} \qquad (17)$$

$$\frac{e^2 g}{e w_s^2} = -2b < 0 \qquad (18)$$

It is known from equations (17) and (18) that i_j is concave concerning v_{dj} , and g is concave concerning w_s . So condition (II) holds.

Using the reverse induction method, assuming that MRS has reached the equilibrium point, resource supply $W_s = W_s^* = [w_s^*]$substitute into equation (15), take the derivative of equation (15) concerning v_{dj} , and set the derivative function equal to zero to get:

$$v_{dj}^* = \frac{y_i - D_{dj} + C W_s^* - b \sum_{i=1, i \neq j}^{m} v_{dj}}{2b} \qquad (19)$$

Substitute Equation (19) into Equation (16), and derive Equation (16) concerning w_s , and set the derivative function equal to zero to obtain:

V. EXPERIMENT AND RESULT ANALYSIS

5.1 Smart Contract Testing and Result Analysis

The test of the smart contract uses Remix as the test environment. A remix is a browser-based compiler and IDE that allows users to build Ethereum contracts and debug transactions using the solidity language.

In the manufacturing resource verification contract, MRS and CPO upload manufacturing resource information in the contract, respectively. Then, deploy the contract into the Ethereum blockchain network. To verify the contract's validity, four tests are performed on the manufacturing resource on-chain verification contract, and the test input data is shown in Table 1.

Tab.1 Input data of contract test

	MRS resource name	MRS resource quantity	CPO funding source name	CPO funding number of sources
Test 1	m1,m2	10,20	m1,m2	10,30
Test 2	m1,m2 ,m3	10,20,30	m1,m2	10,30

Test 3	m1,m2	20,30	m1,m2	10,30
Test 3	m1,m3	10,20	m1,m2	10,30

In Test 1, the types of resources reported by the MRS were consistent with the types assessed by the CPO, and the number of resources was within the scope of the assessment. Therefore, the resource information is successfully uploaded to the chain, a transaction is created in the blockchain network, and the hash value of the transaction is generated. In test 2, MRS maliciously reported the type and quantity of resources, in test 3, MRS exaggerated the number of resources and in test 4, MRS falsely reported the type of resources, which were intercepted by the blockchain network, interrupted the execution of the transaction, and rolled back to the chain. To maintain the authenticity and credibility of the data in the cloud manufacturing platform, the original data that has been tampered with is kept on the chain. Therefore, the blockchain-based cloud platform architecture can effectively supervise the operation records in the platform, facilitate tracing the origin of disputes, and maintain the openness and transparency of the platform.

5.2 **Game Simulation and Result Analysis**

Under the cloud manufacturing resource allocation framework based on blockchain, resource prices are affected by supply and demand, MRDs lease relevant manufacturing resources according to production needs, and MRS formulates relevant supply strategies according to resource demand maximum profit under the constraints of the strategy. The experiment uses MATLAB2019b to carry out the real supply and demand game between 3 MRDs and 1 MRS. The coefficients of the price function are a = 0.8, b = 0.2. This paper assumes that the impact of price demand is greater than that of supply.

Table 2: Comparison over Cloud parameter

Evaluation Parameter	**Speed of Game**			
	MRD1	**MRD2**	**MRD3**	**MRS**
Converge speed	52	54	50	45
Load overhead	48	45	55	59
Converge cost	58	60	65	70
Supply demand balance	78	82	71	65

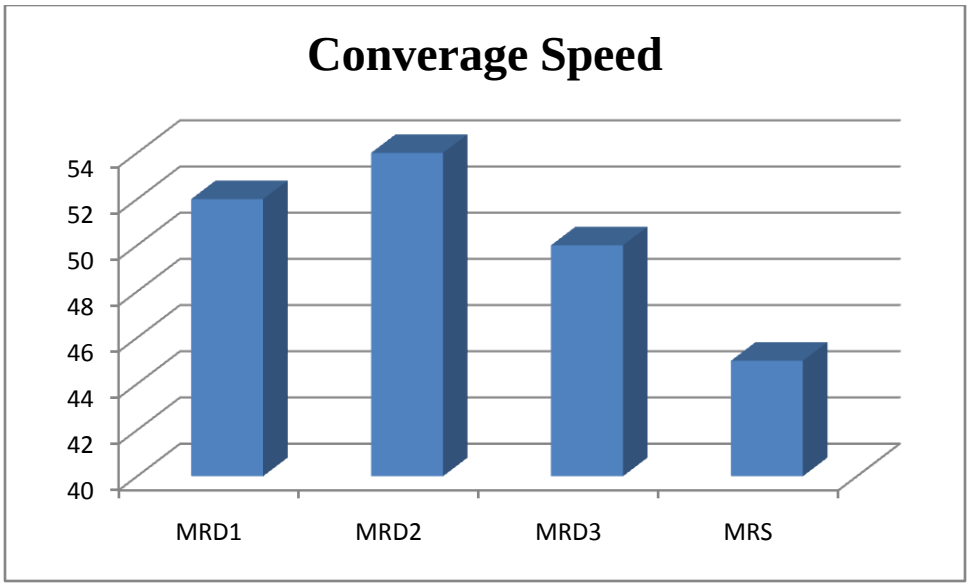

Fig.5 Comparison of convergence speed of games

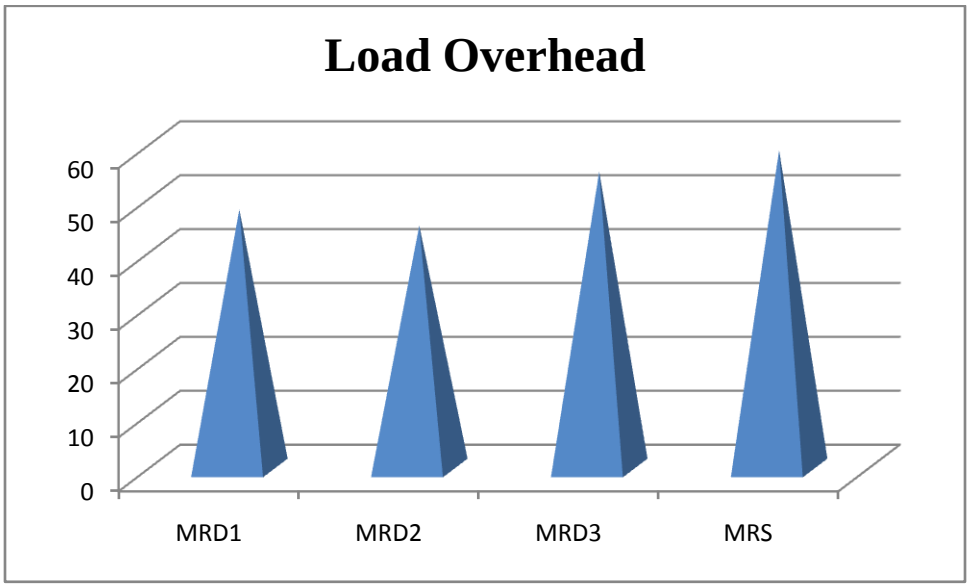

Fig.6 Comparison of Convergence Load Of Games

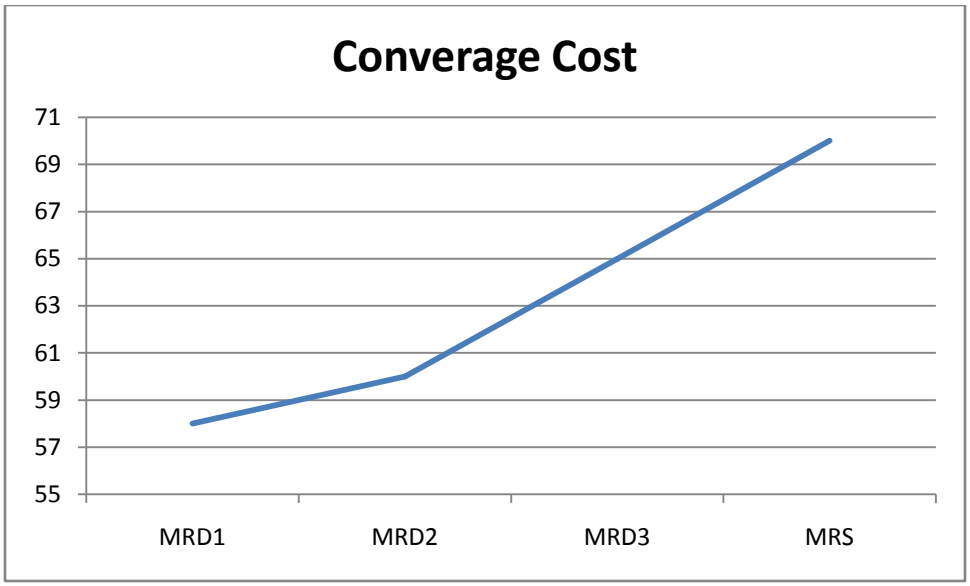

Fig.7 Comparison of convergence Cost of games

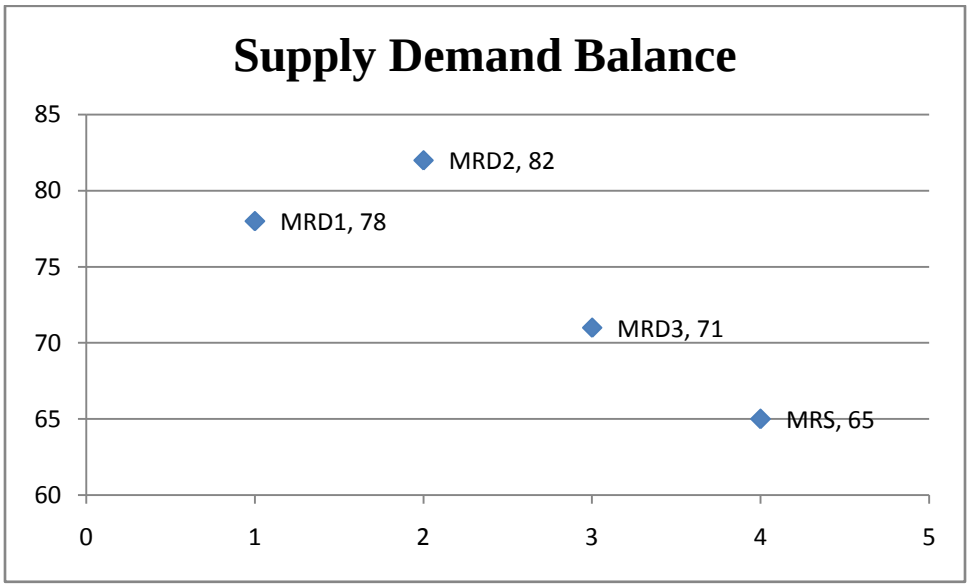

Fig.6 Comparison of convergence Supply Demand balance of games

Y =[100,200,200] , D_d =[45,45,15] , D_s =[10]. The initial demand V_d =[100,100,100] and the supply W_s=[200]. The manufacturing resource game model proposed in this paper is compared with the power grid supply and demand game model proposed in . Although the research objects are different, both study the problem of Stackelberg equilibrium convergence, so there is certain comparative research significance. According to the parameter settings in the literature, this paper makes a real comparison in MATLAB 2019b. It can be seen from Figure 6 that this paper is close to convergence after about 15 iterations. In comparison, the literature is close to convergence after 35 iterations, and the convergence speed is increased by 57%. About Figure 5-8 The impact of the increase in MRD3 demand on the balance of supply and demand After the balance of supply and demand, MRD3 privately increased the demand to obtain higher returns,

breaking the balance of supply and demand. The increase in demand led to increased resource prices, which brought a greater impact to MRS. Profit. It also increases the purchase cost of MRD3 and MRD2. Therefore, MRS gains more profit by hoping to increase the supply, while MRD2 and MRD3 are forced to reduce resource demand. Still, the price is balanced. Ultimately 3 1 MRDs and 1 MRS return to the original supply and demand balance, as shown in Figure 5-8.

VI. CONCLUSIONS

This paper mainly studies the application of the integration of blockchain technology and cloud manufacturing platforms and proposes a blockchain-based cloud manufacturing resource allocation framework. At the same time, the Stackelberg supply and demand game problem between the resource demander and the supply side under the decentralized framework is studied. Under this framework, the participants of the cloud platform use the elliptic curve digital signature algorithm to complete the distribution of resources through the blockchain network and complete the matching and transaction of resources through smart contracts. Through the test of intelligent contracts through Remix, the results show that the transaction data of the blockchain-based cloud platform can be safely stored in the blockchain, and the immutability of the blockchain can enhance the credibility of cloud manufacturing data. In the multi-leader-follower game model, the manufacturing resource supplier and the resource demander can obtain the Nash equilibrium. The results show that this model's Nash equilibrium convergence speed is greatly improved compared with the existing research, and it has certain robustness. In the future, we will study the optimization of the consensus algorithm of blockchain, reduce its consensus loss, and explore how to improve the throughput of its application in the cloud manufacturing platform.

VII. REFERENCES

[1] B. Kaynak, S. Kaynak and Ö. Uygun, "Cloud Manufacturing Architecture Based on Public Blockchain Technology," in *IEEE Access*, vol. 8, pp. 2163-2177, 2020, doi: 10.1109/ACCESS.2019.2962232.

[2] T. M. Hewa, A. Braeken, M. Liyanage and M. Ylianttila, "Fog Computing and Blockchain based Security Service Architecture for 5G Industrial IoT enabled Cloud Manufacturing," in *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2022.3140792.

[3] J. Leng *et al.*, "ManuChain: Combining Permissioned Blockchain With a Holistic Optimization Model as Bi-Level Intelligence for Smart Manufacturing," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 182-192, Jan. 2020, doi: 10.1109/TSMC.2019.2930418.

[4] Y. Liu, J. Zhang, L. Zhang and H. Liang, "IoT - and blockchain-enabled credible scheduling in cloud manufacturing: a systemic framework," *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)*, 2020, pp. 488-493, doi: 10.1109/INDIN45582.2020.9442088.

[5] J. E. Kasten, "Engineering and Manufacturing on the Blockchain: A Systematic Review," in *IEEE Engineering Management Review*, vol. 48, no. 1, pp. 31-47, 1 Firstquarter,march 2020, doi: 10.1109/EMR.2020.2964224.

[6] A. Bhattacharjee, S. Badsha and S. Sengupta, "Blockchain-based Secure and Reliable Manufacturing System," *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, 2020, pp. 228-233, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00052.

[7] G. Volpe, A. M. Mangini and M. P. Fanti, "An Architecture for Digital Processes in Manufacturing with Blockchain, Docker and Cloud Storage," *2021 IEEE 17th International Conference on Automation Science and Engineering (CASE)*, 2021, pp. 39-44, doi: 10.1109/CASE49439.2021.9551633.

[8] C. Esposito, F. Palmieri and K. -K. R. Choo, "Cloud Message Queueing and Notification: Challenges and Opportunities," in *IEEE Cloud Computing*, vol. 5, no. 2, pp. 11-16, Mar./Apr. 2018, doi: 10.1109/MCC.2018.022171662.

[9] R. Li, T. Chen, P. Lou, J. Yan and J. Hu, "Trust Mechanism of Cloud Manufacturing Service Platform Based on Blockchain," *2019 11th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, 2019, pp. 15-19, doi: 10.1109/IHMSC.2019.10099.

[10] P. Ruf, J. Stodt and C. Reich, "Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud," *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, 2021, pp. 192-199, doi: 10.1109/WorldS451998.2021.9514058.

[11] A. Adhikari and M. Winslett, "A Hybrid Architecture for Secure Management of Manufacturing Data in Industry 4.0," *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 973-978, doi: 10.1109/PERCOMW.2019.8730717.

[12] C. Yang, S. Lan, Z. Zhao, M. Zhang, W. Wu and G. Q. Huang, "Edge-cloud Blockchain and IoE enabled Quality Management Platform for Perishable Supply Chain Logistics," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2022.3142095.

[13] M. Wang, C. Xu, X. Chen, L. Zhong, Z. Wu and D. O. Wu, "BC-Mobile Device Cloud: A Blockchain-Based Decentralized Truthful Framework for Mobile Device Cloud," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1208-1219, Feb. 2021, doi: 10.1109/TII.2020.2983209.

[14] M. Soni and D. K. Singh, "Blockchain Implementation for Privacy preserving and securing the Healthcare data," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021, pp. 729-734, doi: 10.1109/CSNT51715.2021.9509722.

[15] S. Leivadaros, G. Kornaros and M. Coppola, "Secure Asset Tracking in Manufacturing through Employing IOTA Distributed Ledger Technology," *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*, 2021, pp. 754-761, doi: 10.1109/CCGrid51090.2021.00091.

[16] Z. Xiong, J. Kang, D. Niyato, P. Wang and H. V. Poor, "Cloud/Edge Computing Service Management in Blockchain Networks: Multi-Leader Multi-Follower Game-Based ADMM for Pricing," in *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 356-367, 1 March-April 2020, doi: 10.1109/TSC.2019.2947914.

[17] Y. Wang, X. Sun, F. Zhu, F. Zhang, M. Zhang and H. Cao, "Chain FileSynch: An Innovate File Synchronization for Cloud Storage with Blockchain," *2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM)*, 2019, pp. 552-556, doi: 10.1109/AIAM48774.2019.00115.

[18] Q. Chen, Q. Xu and C. Wu, "Optimal Sharing Strategies of Idle Manufacturing Resource Considering the Effect of Supply-Demand Matching," *2019 International Conference on Industrial Engineering and Systems Management (IESM)*, 2019, pp. 1-6, doi: 10.1109/IESM45758.2019.8948199.

[19] E. Shaikh, A. Bashar and N. Mohammad, "Recent Applications of Computing and Mobility Technologies to Modern Manufacturing," *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2021, pp. 1-6, doi: 10.1109/ICCSPA49915.2021.9385756.

[20] Shobanadevi, A., Tharewal, S., Soni, M. et al. Novel identity management system using smart blockchain technology. Int J Syst Assur Eng Manag (2021). https://doi.org/10.1007/s13198-021-01494-0