Hindawi
Mobile Information Systems
Volume 2023, Article ID 9780671, 1 page
https://doi.org/10.1155/2023/9780671

Retraction

Retracted: Blockchain Technology in the Management of Scientific and Technological Achievement Transformation in Chinese Universities

Mobile Information Systems

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Wang and Q. Ni, "Blockchain Technology in the Management of Scientific and Technological Achievement Transformation in Chinese Universities," *Mobile Information Systems*, vol. 2022, Article ID 1801037, 17 pages, 2022.

Hindawi
Mobile Information Systems
Volume 2022, Article ID 1801037, 17 pages
https://doi.org/10.1155/2022/1801037

Research Article

Blockchain Technology in the Management of Scientific and Technological Achievement Transformation in Chinese Universities

Yu Wang[1] and Qing-Ting Ni[2]

[1] *Department of Science & Technology Industry, Jiangsu University of Technology, Jiangsu, Changzhou 213001, China*
[2] *School of Chemical and Environmental Engineering, Jiangsu University of Technology, Jiangsu, Changzhou 213001, China*

Correspondence should be addressed to Qing-Ting Ni; nqt@jsut.edu.cn

Received 10 May 2022; Revised 6 June 2022; Accepted 20 June 2022; Published 1 July 2022

Academic Editor: Imran Shafique Ansari

The article uses blockchain technology to design and develop a blockchain-based management system for the transformation of scientific and technological achievements in universities, which solves the problems of difficulty in promoting information of scientific and technological achievements, low trust of both parties in the process of transformation, and lack of corresponding service platform. It solves the problems such as low trust between the two parties and lack of a corresponding service platform. The main research work of the article is as follows: first, it conducts demand analysis, proposes the overall architecture of the system, and designs the scientific research results management module. The system is divided into two parts, namely, user information management module and result information management module. Second, the data protection module is designed. A trust-optimised consensus algorithm C-DPOS is introduced to provide basic technical support for the operation of the blockchain-based university science and technology results trading and knowledge sharing system, thereby reducing the probability of malicious nodes committing mischief in the blockchain network environment during the operation of knowledge sharing, and comparing the probability of malicious and normal nodes participating in consensus. Third, system implementation and testing. By comparing the difference in consensus latency between DPoS and the improved C-DPoS, it is concluded that C-DPoS has a greater operational speed advantage over DPoS. The implementation of the C-DPoS consensus algorithm can further ensure that blockchain-based result trading and knowledge sharing can operate stably. According to the Law on Promoting the Transformation of Scientific and Technological Achievements (2015 revised version), the transformation of scientific and technological achievements of universities refers to the activities of subsequent testing, development, application, and promotion of scientific and technological achievements until the formation of new technologies, new processes, new materials, and new products and the development of new industries to improve the productivity level. Through the development of the transformation management system of scientific and technological achievements, the research data can be summarised in real time and comprehensively, and the blockchain can be used to achieve data protection, which has the characteristics of comprehensive management functions and strong security and effectively improves the efficiency and information security of the transformation of scientific and technological achievements.

1. Introduction

Blockchain has become one of the most important strategic technologies in China. Blockchain has been elevated to the height of national science and technology strategy with its characteristics of "decentralization, enhanced trust, distributed accounting, and nonmanipulation," and the management system of university science and technology achievement transformation should be designed and coordinated with benefit-sharing type and risk management mechanism. Blockchain technology is an electronic transaction proof generated and recorded in chronological order by a peer-to-peer timestamp server. That is, through various ways to obtain various scientific research projects, carry out scientific and technological research and development activities, complete the transformation from abstract scientific theoretical knowledge into concrete scientific and technological achievements, and then through the confirmation of rights and market-oriented, commercial operation, to realize the value of the achievements.

1.1. Blockchain Technology Research Status. Blockchain originated from the study of Bitcoin technology, (2008, Satoshi Nakamoto) proposed an electronic cash system that does not need to go through a third-party financial institution to achieve payment through peer-to-peer, which is also known as Bitcoin, which is the initial application of blockchain technology. (2018, Liu Sen, Hu Yanan, Yang Dan) [1] proposed that blockchain is a technology that does not need to rely on intermediaries to achieve credit consensus. Decentralization is the main feature of blockchain. (2009, Kingombe) [2] found that the main factors for the high cost of remittances in Africa are inefficient payment systems and opaque market information and proposed that cost reduction and efficiency can be achieved by applying blockchain technology to build a system that does not require the involvement of financial intermediaries like Bitcoin. The decentralized advantage of blockchain can bring more opportunities to the digital plan business field, (2017, Banafa) [3] found that the reliability and scalability of IoT technology platforms have different degrees of deficiencies, which can be improved and effectively compensated in terms of privacy protection if applied in combination with blockchain technology. (2017, Lei Jun) [4] argued that the public chain is the original idea of blockchain technology, i.e., everyone can participate in it and that the application of the public chain can unleash productivity in terms of data mining and sharing in addition to saving transaction costs compared to traditional transaction systems. (2019, Zhang Liqing, Wu Tong) [5] argued that smart contracts designed based on blockchain technology have the feature of automatic enforcement and can improve the accuracy of contract execution because the hash of the code and the digital signature are copied to the smart contract at the same time when the smart contract is executed.

1.2. Current Status of Research on Transformation of Scientific and Technological Achievements in Universities. At present, Chinese scholars have conducted some research on the transformation of scientific research achievements in universities. (2012, Cheng Yuan) analyzed the characteristics of transformation of scientific and technological achievements in universities in the region and the main functions of universities in the process of transformation in "Research on the Promotion Mechanism of Transformation of Scientific and Technological Achievements in Universities" and proposed the mechanisms to promote the transformation of scientific and technological achievements in universities such as organization optimization mechanism, resource integration mechanism, and benefit-sharing mechanism [6]. (2002, Liu Haiyan) in "Research on the Mechanism of Transformation of Scientific and Technological Achievements in Colleges and Universities" proposed that the reason for the low efficiency of the transformation of college achievements is the imperfection of three major mechanisms of input, evaluation, and incentive. It is believed that optimizing mechanism is the key to solve the problem of fruit transformation, among which establishing an effective intellectual property incentive mechanism is the most important [7]. (2005, Yang Jingjing, Liu Mingjun) argued that the backwardness of the transformation mechanism of scientific and technological achievements in colleges and universities is an important reason for the low transformation rate of achievements and used the theory and method of mechanism theory to study the motivation mechanism, constraint mechanism, and target mechanism of the transformation of scientific and technological achievements in colleges and universities, as well as the operation principle of each transformation mechanism [8].

1.3. Analysis of the Situation. At present, many scientific research achievements and performance transformation processes in China are difficult to get financial support, financing channels are not fully open, and it is difficult to transform a large number of "semifinished products" from universities and research institutes. The current situation of transformation of scientific research achievements in Chinese universities has the following four characteristics: first, the national innovation system lacks effective integration of scientific and technological innovation resources invested by universities. Second, the process of transformation of scientific and technological achievements in universities lacks effective supervision and control. In some links, there are still problems such as disconnection between demands and achievements, poor communication, and various resources are not effectively integrated. Third, there is a lack of a strong system guarantee in the distribution of innovation results in universities. The key to the transformation of scientific and technological achievements in colleges and universities is the distribution of achievements. Therefore, it is important to discuss the attribution and benefit distribution of scientific and technological achievements in the management system of transformation of scientific and technological achievements in universities to solve the problem of the low transformation rate of scientific and technological achievements in China. At present, there is no special intellectual property protection department in Chinese universities, let alone a professional institution for the transformation of scientific and technological achievements. Scientific and technological achievements are managed by the Ministry of Science and Technology. This leads to the lack of standardization and specialization in the management of scientific and technological achievements in universities. The declaration and management of scientific and technological achievements are still carried out according to project acceptance or title evaluation, resulting in the achievements cannot continue to produce value. Fourth, the investment in the transformation of scientific and technological achievements in colleges and universities is insufficient. The investment of scientific research funds in colleges and universities mainly comes from the state fund allocation, but the risk of engaging in pilot tests and promotion of scientific and technological achievements needs to be borne by colleges and universities themselves, and most of the social capital and scientific and technological manufacturing enterprises do not bear the risk of transformation of scientific and technological achievements and are not actively willing to invest.

2. Detailed Design of the User Information Management Module

The main functions of each functional module are designed and implemented in detail with the detailed requirement analysis and overall architecture. In the detailed design of each functional module, the business process is analyzed first, followed by the front and back-end interaction analysis with the timing diagram, and the attribute fields of the objects in the specific smart contract and their descriptions are given; the implementation of the functional module mainly includes the key implementation code and explanation, and the corresponding system screenshots are attached.

2.1. Business Process of User Information Management Module. The users of the User Information Management module are mainly university teachers. The module requires users to register and undergo identity verification before they can log in to use the system. When registering, the user needs to fill in the front-end page with information that meets the format requirements, mainly including name, work number, telephone number, university affiliation, login password, etc., and needs to choose the type of user, which is classified as general teachers or professional leaders Reference [9].After the user submits the information, the system will first make a logical judgment on the data filled by the user through the front-end JavaScript function, if there are two different passwords, required fields are empty, the format does not meet the requirements, etc., the user will be directly given information error prompt, and no user data will be sent to the back end. After the data filled in pass the logical judgment of the front end, the system will call the smart contract User at the back end to determine whether the user has ever registered in the system [10]. If the user has not yet registered, personal information will be stored for the user and recorded on the blockchain of EtherChannel. After the above process, the user information will be sent to the efficient administrator for review, and after passing the review, the user can get the corresponding role authority and use the corresponding system functions according to the filled-in user type. The business process of user registration is shown in Figure 1.

The front end of the system is combined with MetaMask wallet plug-in, which enables users to interact with the Ethereum blockchain with the front-end interface through the web3.js library. Combined with this wallet plug-in, the system implements the function that users can sign data transactions through their private keys and can ensure the security of this process. Therefore, users use MetaMask plug-in during registration, which enables the smart contract to verify and record information such as user account number and address. MetaMask plug-in also plays a great role in the subsequent transaction operation.

When logging in, the user needs to fill in the password filled in the front-end page and then confirm the login, and after the front-end judge the password format, the system also calls the back-end user smart contract. [11] MetaMask can get the information of the currently logged-in user, and after confirming that the user is a registered user, the user's password will be checked. After passing the password check, the system provides feedback that the user has successfully logged in, gets the user's identity type and other information from the back end, and renders the corresponding front-end page according to the user type authority. The business process of user login is shown in Figure 2.

2.2. Timing Diagram of User Information Management Module. The business process of the user information management module is split into front and back ends, and the service invocation timing diagrams of user registration and login are derived, respectively. The user registration timing diagram is shown in Figure 3.

After the teachers fill in the information required for registration in the front-end page named Register.vue, the front-end page first calls checkData() to judge the information filled in, and then the front end transmits the registration-related data by signup() to call User, a smart contract deployed on the blockchain [12]. User will first call several internal function modifiers to uniquely verify key information data such as registration account, e-mail, and contact number and then call the function create(); first, create() will encrypt the user's password data, then process and store the data according to the user's identity type at the time of registration, and then call Register() to uniquely verify the registration time and registration information. After completing the registration record, the smart contract User returns the data to Register.vue, which calls checkUserType() to send the prompt information to the checkUser.vue interface and wait for the administrator to conduct identity audit.

After the administrator checks the user's information and approves or rejects the identity type, the front-end page checkUser.vue calls the back-end smart contract User using checkUserType(), and after receiving the call, the smart contract User calls the function modify() to modify the user's data being manipulated and calls Register() to record the changed information data. After the operation is completed, the User returns the information to the checkUser.vue page and Register.vue page, giving the user relevant hints.

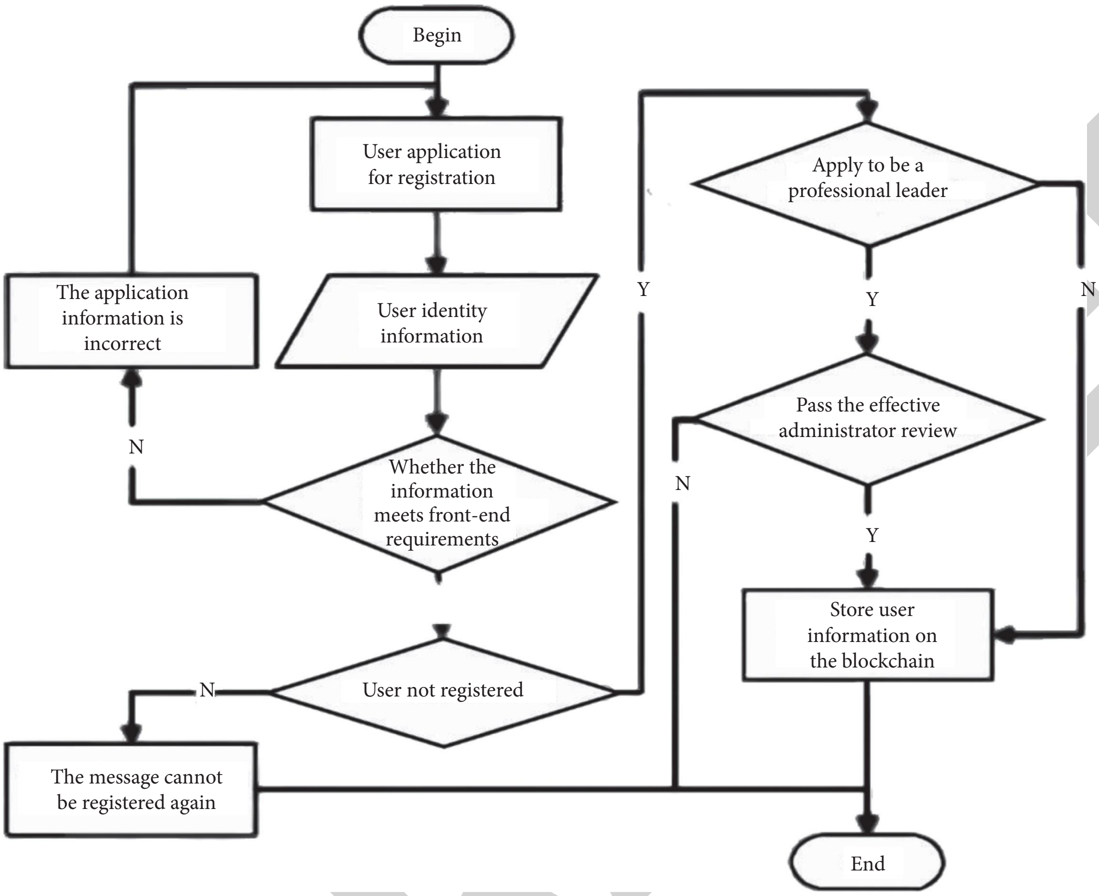
Begin
User application for registration
User identity information
The application information is incorrect
N
Whether the information meets front-end requirements
User not registered
N
The message cannot be registered again
Y
Apply to be a professional leader
Y
N
Pass the effective administrator review
N
Y
Store user information on the blockchain
End

Figure 1: User registration business flow chart.

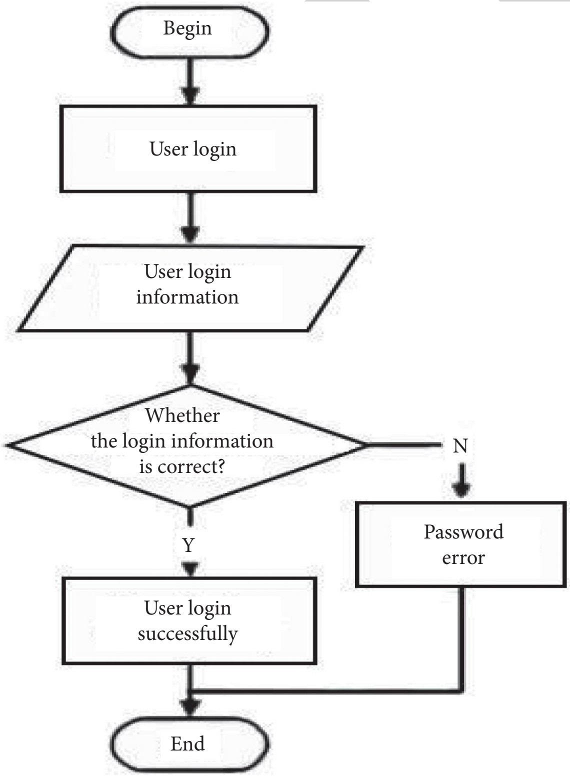

Figure 2: User login business flow chart.

In solidity, it is easy to change the behavior of functions with function modifiers. For example, they can automatically check certain conditions before executing the function. In case there are multiple modifiers called by the same function in the system, just separate them with spaces and the modifiers will be checked in turn. [13] Eventevent is an abstraction on top of the EVM logging functionality. Applications can subscribe and listen to these events through the RPC interface of the Ethernet client. When an event is called, its parameters are stored in the transaction log, which is a special data structure in the blockchain. These logs and addresses are associated with each other and are stored permanently in the blockchain and remain there for as long as the block is accessible. The user login timing diagram is shown in Figure 4.

The login call service is much simpler compared to the registration process. The user needs to fill in the correct password on the front-end page loginIn.vue and confirm the login; first, the front-end will make a null operation on the password and then call the signIn() method to send the entered user password to the back-end smart contract User. The user calls the function login() to query the current login user account, encrypt the input password and compare it with the password data stored in the blockchain, and then return the information about the user or a hint of a password error to the loginIn.vue page to perform a page jump or user hint operation.

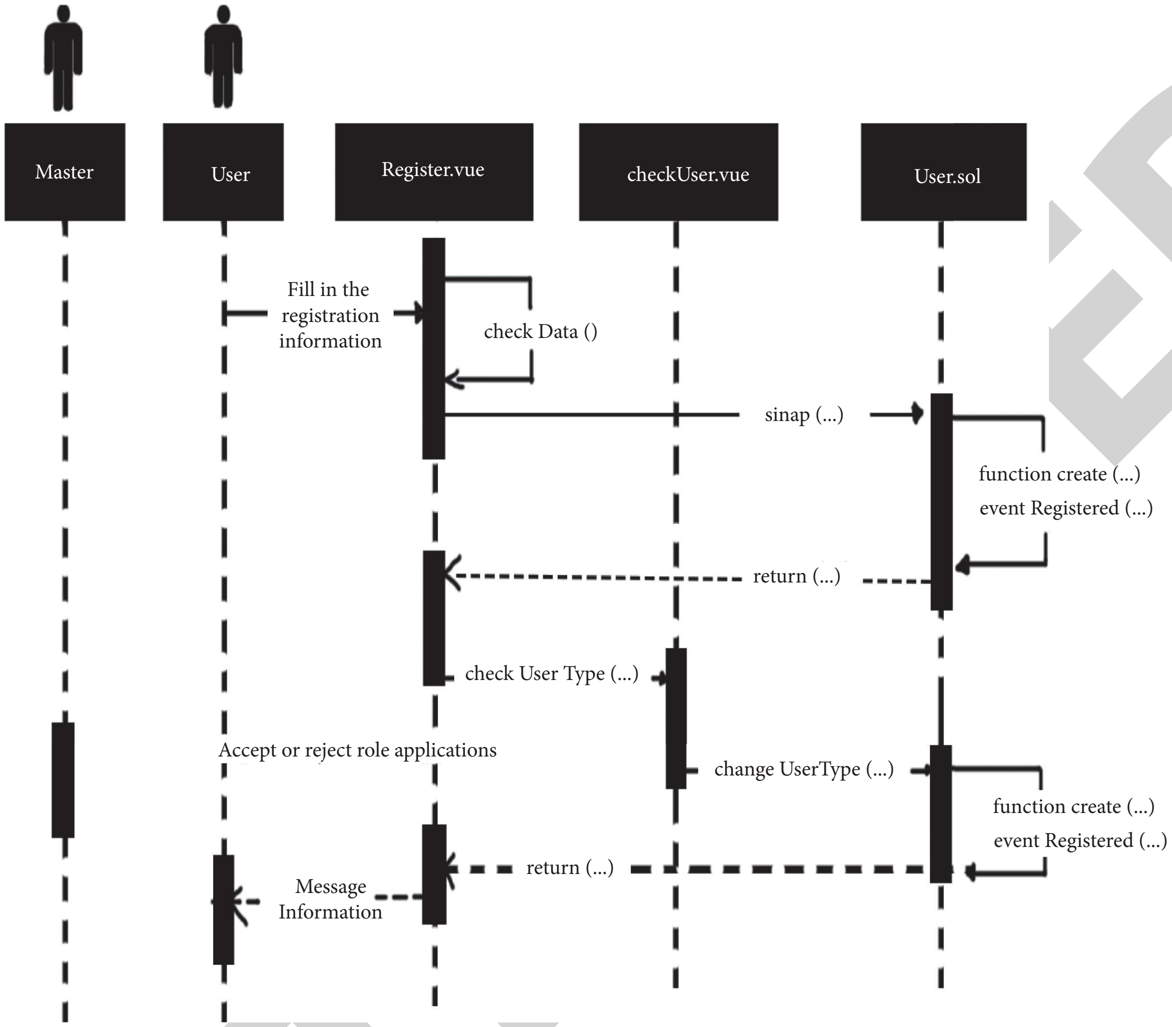

Figure 3: User registration timing diagram.

3. Detailed Design of Result Information Management Module

3.1. Business Processes in the Results Information Management Module. The main function of the Results Information Management module is to improve and review results information. The corresponding users are university teachers and university professional leaders, and the functions of this module also include the query of results information for all users who have completed registration in the system [14]. The uploading and downloading of result information involves IPFS service, and it is more appropriate to store large volume files such as pictures, videos, and compressed packages in the off-chain IPFS service than the flatter blockchain data storage. The process of patent result information improvement is shown in Figure 5.

There are two entry points for users on the front page, the “View Details” in each row of the results information list and the cards on each of the university results in information display pages. Only those who meet the system’s identity requirements can download and view the details of the patent results, while other users can only see part of the results. When the system requests the result information, it will first call the smart contract PatentInfo to return the information of each field, and then download the detailed additional information of the relevant patent result from the IFPS service cluster according to the IPFS hash address for viewing. Figure 6 shows the flow of patent result information query.

3.2. Time-Series Diagram of the Results-Based Information Management Module. Based on the analysis of the result information refinement and the query process, the corresponding service call timing diagrams are designed respectively, as shown in Figure 7.

The results information needs to be reviewed by both the head of the university and the administrator before it can be accessed and traded. The front-end operations and back-end processing of the two reviews are similar, so only one review process is shown in the timing diagram, and only one is described in this section. In addition, the teacher who adds a

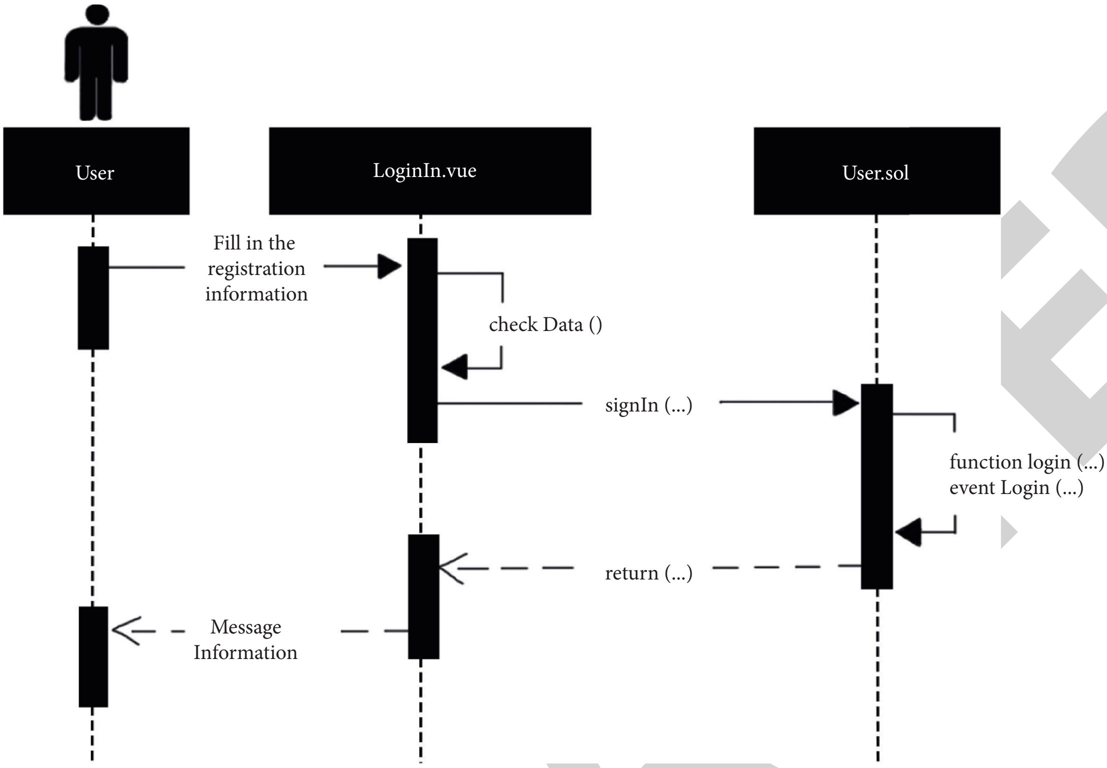

Figure 4: User login timing diagram.

new result is automatically recorded as the person responsible for the result, and any subsequent modifications or transactions can only be carried out by the person responsible for the result.

The results query timing diagram is shown in Figure 8 and focuses on the services involved in querying the list of results information and details of a particular result.

When searching for details of a result, the user selects a result in the front-end page checkInfo.vue or index.vue and then enters the result details page patentInfo.vue. The front-end page calls the back-end smart contract PatentInfo with getDetail(), and then the smart contract PatentInfo calls getPatentDetail() to get the data for each field of the result, which is returned to the patentInfo.vue page for rendering. The detailed force includes the IPFS address of the uploaded data, which can be clicked to download the previously uploaded and approved details.

4. Introduction of the Trust-Optimised Consensus Algorithm C-DPoS

4.1. C-DPOS Design Principles and Implementation Steps. The purpose of designing C-DPoS is to prevent the emergence of malicious nodes in DPoS because the DPoS consensus is formed by the participation of elected super nodes, if the super node itself is a malicious node, then the new area generated by the blockchain network will no longer be trusted, which will lead to the common interests of all nodes in the blockchain network. Therefore, to address the problems of traditional DPoS, we propose a C-DPoS consensus algorithm that introduces a node trust value, which dynamically calculates the trust value of a node based on its historical participation in consensus, and punishes malicious nodes to reduce their participation in consensus, thus ensuring the stability of the blockchain network that supports knowledge sharing.

4.1.1. Design Principles of the C-DPOS Consensus Algorithm

(1) The number of voting nodes and the number of campaign nodes in the blockchain network are preset and initialized in the consensus system. Each voting node gets its number of votes, and then the voting nodes vote and determine the set of supernodes based on the voting results. The super nodes can perform trust value initialization, and the process of node trust value initialization gives the initial trust value to the nodes participating in the consensus, and if the trust value is negative, the node is defined as a malicious node. All nodes based on the blockchain in the knowledge sharing are nodes of the knowledge sharing subject and consist of the knowledge sharing subject.

(2) The super nodes take turns to obtain the bookkeeping rights among themselves, and after successful bookkeeping, the node will increase its trust value according to its node's trust value, and the

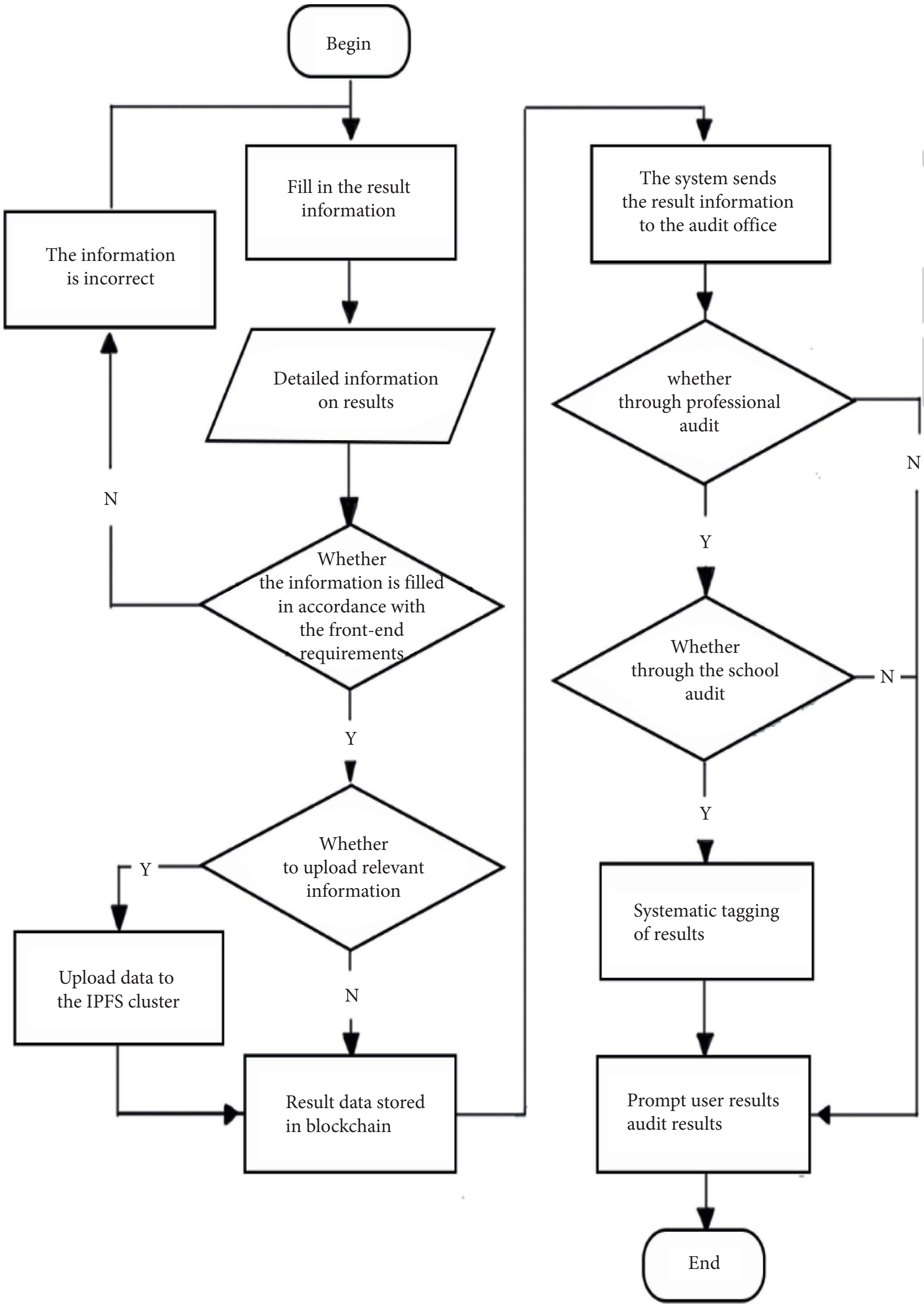
Begin
Fill in the result information
The information is incorrect
Detailed information on results
N
Whether the information is filled in accordance with the front-end requirements
Y
Y
Whether to upload relevant information
Upload data to the IPFS cluster
N
Result data stored in blockchain
The system sends the result information to the audit office
whether through professional audit
N
Y
Whether through the school audit
N
Y
Systematic tagging of results
Prompt user results audit results
End

Figure 5: Flow chart for improving results information.

result of the vote obtained is associated with the trust value. A new block is created after the super node has obtained the bookkeeping rights.

(3) Set penalties for malicious nodes and dynamically adjust node rewards and penalties according to changes in node trust values.

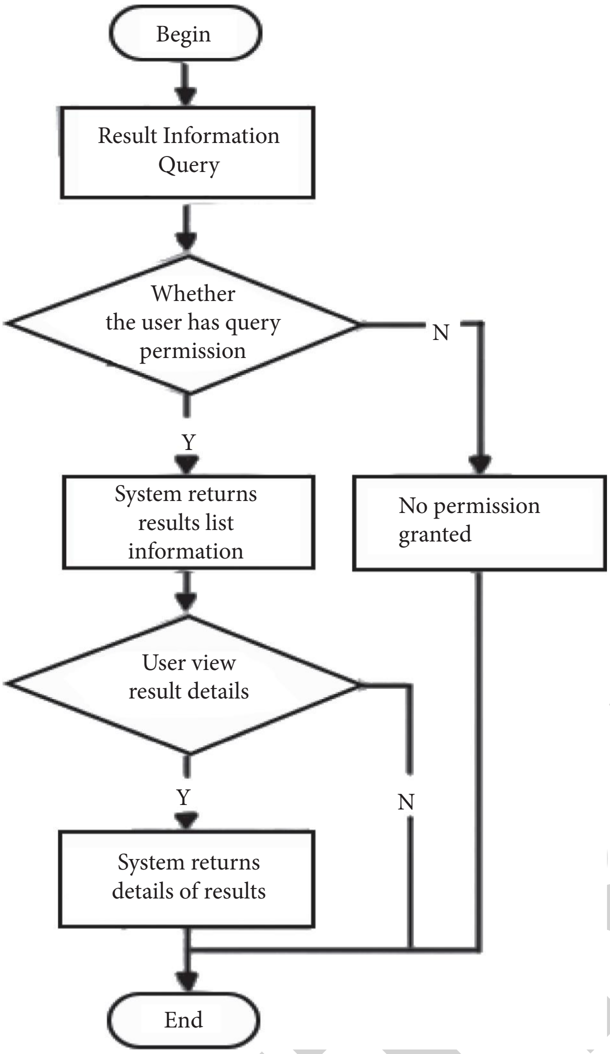
Begin
Result Information Query
Whether the user has query permission
N
Y
System returns results list information
No permission granted
User view result details
Y
N
System returns details of results
End

Figure 6: Flow chart of results information search.

The overall flow of the design C-DPOS implementation is shown in Figure 9.

4.1.2. Steps for Implementing the C-DPOS Consensus Algorithm

(1) Set up a pool of voting nodes to participate in the poll, and determine the number of voting nodes to participate in the poll based on the initial number of nodes set. This experiment sets up 100 voting nodes.

(2) Set up a pool of campaign nodes, and determine the number of campaign nodes (aka super nodes) to participate in the campaign based on the number of campaign nodes set. In this experiment, 10 campaign nodes are set up.

(3) Initialize the voting node pool and the campaign node pool, where each voting node will have a certain number of votes to vote for the campaign node, but the campaign node is just initialized, and each campaign node has the same rights, and the campaign node generates a consensus super node after the voting node has finished voting. The voting node and the campaign node of this experiment are generated by this step.

(4) The voting nodes in the voting node pool conduct independent random voting on the campaign nodes in the campaign node pool, count the number of votes for each campaign node after voting, select the top five campaign nodes in terms of votes, initialize their trust values, and complete the trust value initiation for the super nodes to participate in the blockchain consensus.

(5) A node participates in consensus, and usually, its trust value increases when it participates in consensus once. If the node is found to be a malicious node, its trust value will decrease, thus affecting its likelihood of participating in consensus. To encourage malicious nodes to participate in the correct consensus, their trust value will also increase if they participate normally, but the increase in trust value will be much smaller than for normal nodes.

(6) Consensus is reached among the super nodes to generate new blocks.

4.2. C-DPOS Consensus Algorithm Implementation

4.2.1. Algorithm 1. Algorithm 1 defines and initializes the initial number of voting and active nodes in steps 1, 2, and 3. The initialization process includes the generation of Genesis blocks. The structure of all blocks in the blockchain network is the same as the structure of the Genesis blocks in the blockchain network. After initialization, voting nodes and active nodes will be stored in the voting node pool and active node pool respectively. Algorithm 1 implements the initialization of voting nodes and campaign nodes, and the node initialization is shown in Table 1.

4.2.2. Algorithm 2. Algorithm 2 implements Step 4 voting, and the core code of the voting algorithm, Algorithm 2, is shown in Table 2. When Algorithm 2 is run, each voting node randomly votes its votes to the campaign nodes in the campaign node pool. Finally, the number of votes received by each campaign node in the campaign node pool is counted and ranked. The five campaign nodes with the most votes are selected as the blockchain consensus super nodes.

Unlike traditional DPoS, the experiment introduces node confidence as a criterion for determining whether a node is normal or malicious. A node penalty mechanism is also introduced, where the trust value increases by 0.2 for every time a node participates in consensus when it is a normal node, and due to the increase in trust value, the node dynamically increases its chances of participating in consensus. On the other hand, if a node is found to be malicious, its chances of participating in consensus are reduced.

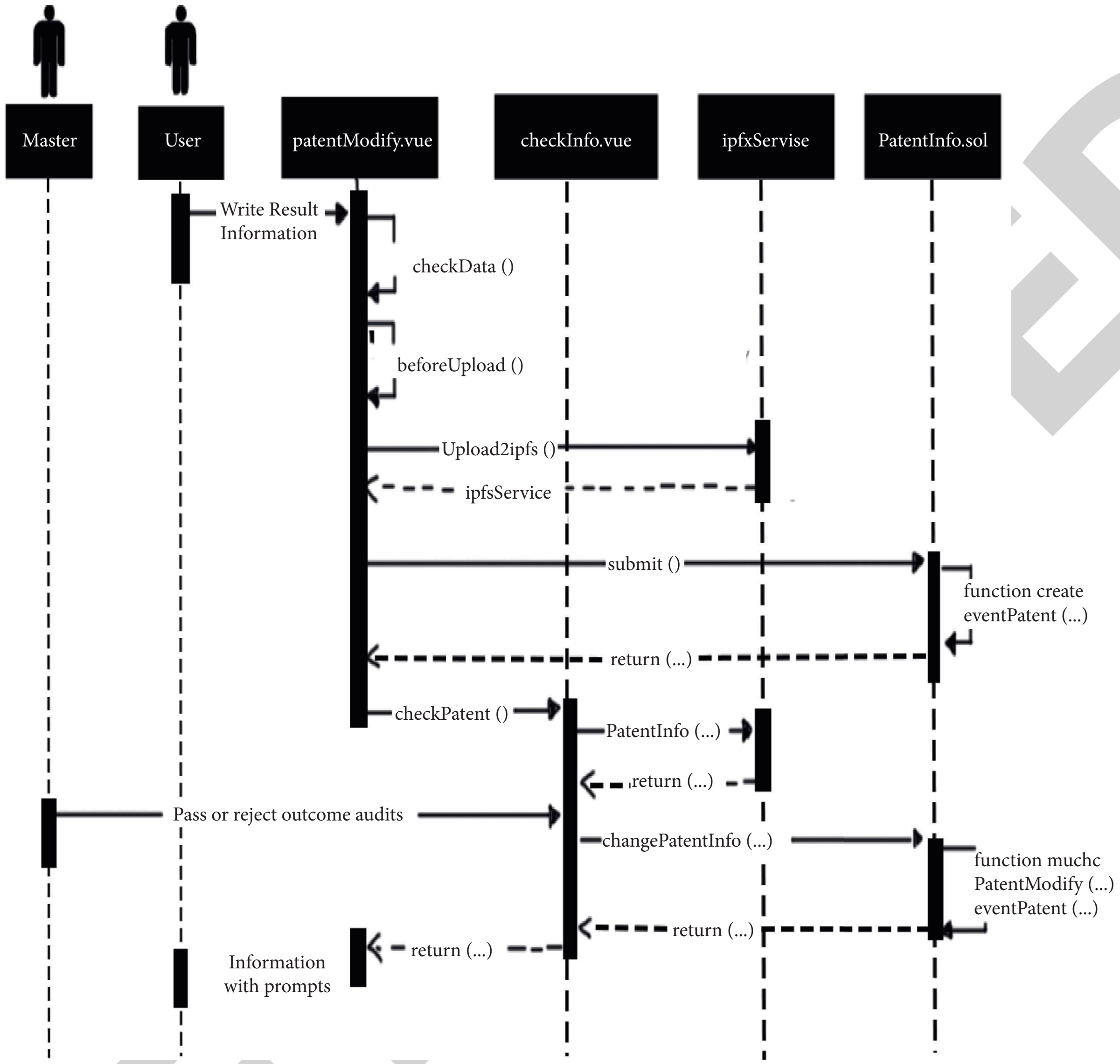

Figure 7: Timeline for refinement of results information.

In this experiment, the node comes to perform the penalty mechanism by setting the following threshold: the demarcation line between the node's normal and malicious trust values is 0. If the node's trust value is below 0, then it is judged to be a malicious node; if the node's trust value is above 0, then it is judged to be a normal node.

When the node is a malicious node, divided into different nodes' specific threshold levels under the specific penalty: Node trust value in [−20,0), when this knot is a super node involved in blockchain consensus because this is a malicious node, so this opportunity to participate in blockchain consensus is judged invalid, then the opportunity will be randomly assigned to other normal nodes in the super node pool, after this operation, the node trust value will be increased by 0.05. When the node trust value is in [−20,0), for every 1 unit increase in trust value, it takes 20 times for its random selection to participate in consensus, and this penalty mechanism increases the cost of malicious nodes to do evil.

When a node's trust value falls below −20, the strength of punishing the node increases due to its high level of evil. Just like the step of selecting nodes to participate in the consensus when the trust value is at [−20,0), the trust value increases by 0.01 after completing a selection of nodes as participating nodes and randomly assigning this opportunity to other nodes in the supernode pool. When the trust value increases to the interval [−20.0), the increase in trust value after each operation is the same as the increase in trust value within the interval [-20.0), both being 0.05. This also indicates that when the trust value of a node is less than −20, each increase in trust value by 1 unit requires 100 random selections to participate in consensus, which makes it more costly for the

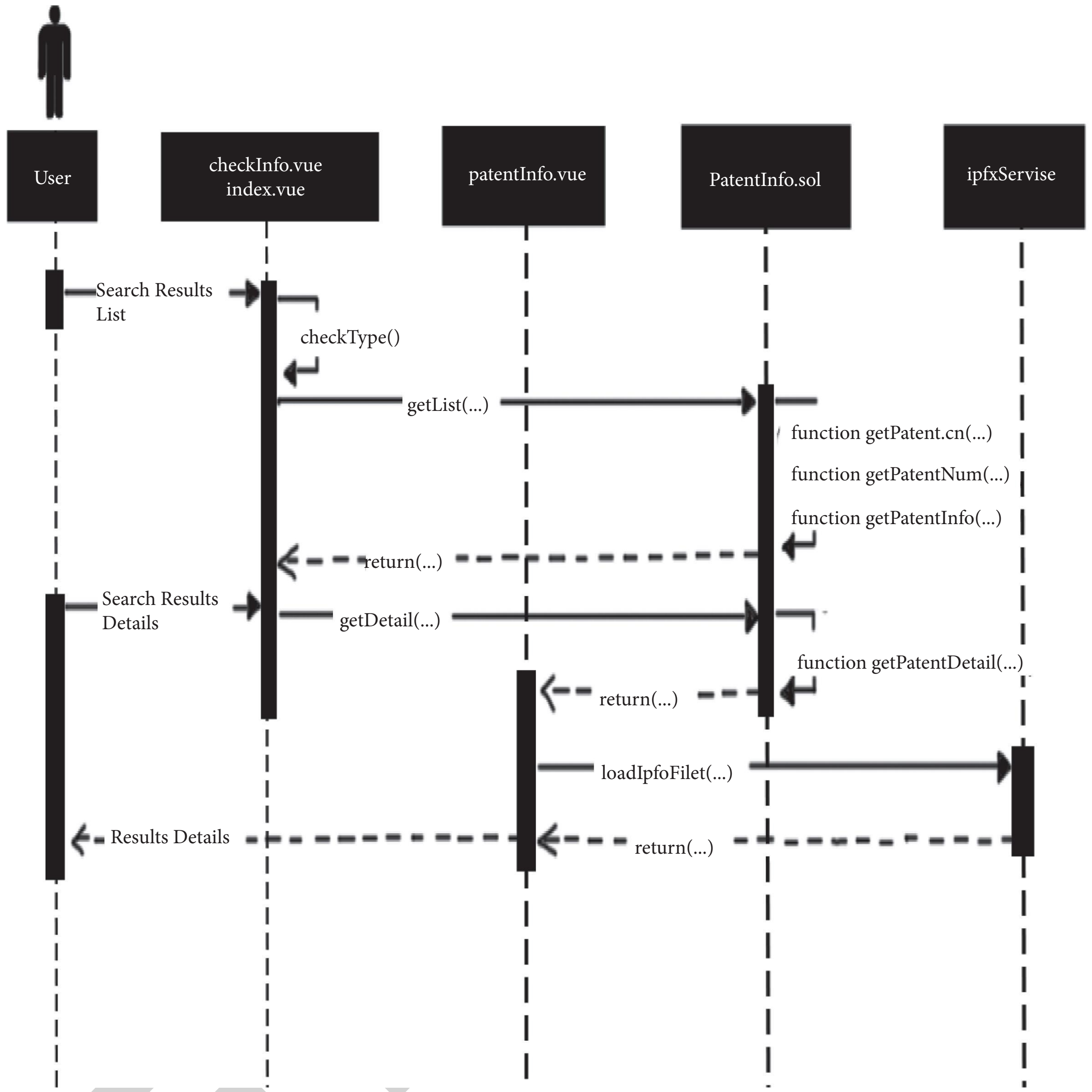

Figure 8: Time-series diagram for querying results information.

node to do evil. (1) Dynamic adjustment of the node trust value after the node has acquired the right to bookkeeping once.

$$\text{credit} = \begin{cases} \text{credit} + 0.2\ \text{credit} \geq 0, \\ \text{credit} + 0.05 - 20 \leq \text{credit} < 0, \\ \text{credit} + 0.1\ \text{credit} < -20. \end{cases} \tag{1}$$

After the dynamic adjustment of node trust value is introduced in the penalty mechanism, it will increase the cost required for nodes to be evil, so nodes try to participate in consensus normally and do not choose to be evil. Because C-DPOs are elected as super nodes, the way to participate in consensus becomes super node polling, which means that the nodes in the super node pool need to participate in consensus once in order, and when a malicious node is found, a super node (which should be a normal node) will be randomly selected among the remaining super nodes for consensus. Because the trust value of a normal node increases by 0.2 after each consensus, it ensures a dynamic balance among the nodes participating in the consensus, so there will not be any super node with a significantly higher trust value than other nodes, and the trust values of all super nodes remain in a reasonable balance.

4.2.3. *Algorithm 3.* Algorithm 3 is the core code of the C-DPOS consensus algorithm after the introduction of trust optimization, as shown in Table 3.

Algorithm 1, Algorithm 2, and Algorithm 3 introduce the core steps of the C-DPoS consensus algorithm after the introduction of trust optimization. Based on the above

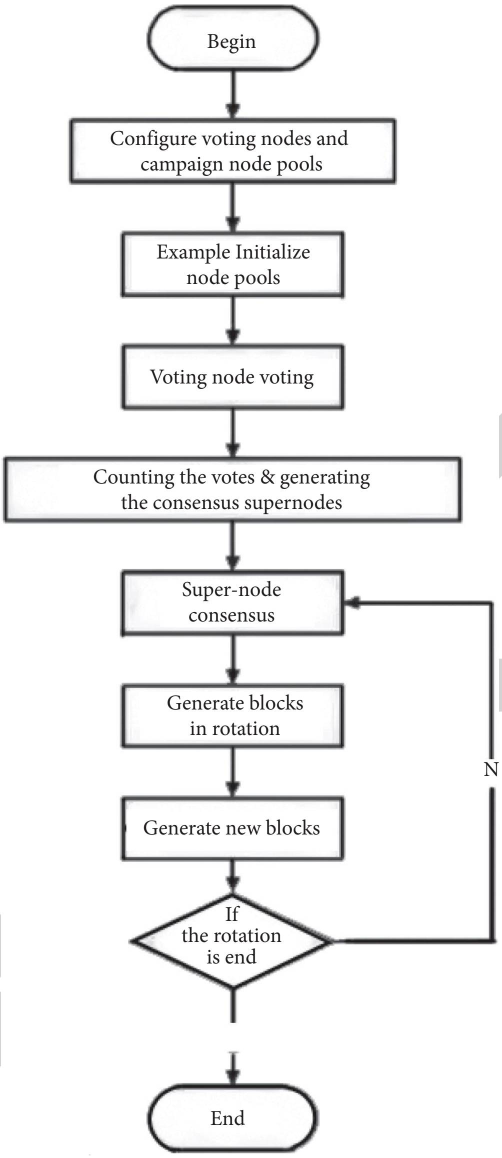
Begin
Configure voting nodes and campaign node pools
Example Initialize node pools
Voting node voting
Counting the votes & generating the consensus supernodes
Super-node consensus
Generate blocks in rotation
Generate new blocks
If the rotation is end
N
End

Figure 9: Flow chart of the C-DPOS algorithm.

algorithms, the core execution flow of C-DPoS is shown in Figure 10.

4.3. Experimental Analysis. Performance analysis of the proposed consensus algorithm C-DPOS is performed and compared with the traditional DPoS algorithm. The algorithm counts votes for the campaign nodes as follows:

$$\begin{aligned} &\text{Number of votes received} \\ &\quad = * \text{number of votes cast} + * \text{trust value}, \end{aligned} \tag{2}$$

In (2): α denotes the vote gain coefficient, β denotes the trust coefficient, $\alpha + \beta = 1$, and the values are closely related to the trust values of the campaign nodes, and the variation relations of α and β are as follows:

$$\alpha = \begin{cases} 0.25, & \text{credit} \geq 0, \\ 0.5, & -20 \leq \text{credit} < 0, \\ 0.75, & \text{credit} < -20, \end{cases} \tag{3}$$

$$\beta = \begin{cases} 0.25, & \text{credit} < -20, \\ 0.5, & -20 \leq \text{credit} < 0, \\ 0.75, & \text{credit} \geq 0. \end{cases} \tag{4}$$

The initial trust value of the campaign node is obtained randomly during the initialization process. The confidence interval is [−100, 100]. After initialization, it can be determined whether a node is a normal node based on the magnitude of its trust value. If a node's trust value is greater than or equal to 0, the node is identified as a normal node for this experiment. If a node's trust value is less than 0, then it is

Table 1: Algorithm 1 Init().

```
Input: voteNodeNum, superNodeNum
Output: voteNodePool, superNodePool
input voteNodeNum = 100‖Define the number of voting nodes as 100
input campaignNodeNum = 10‖Define the number of campaign nodes as 10
input mineSuperNodeNum = 5 define the number of super nodes for consensus to be 5 per round
type node struct{//Structure of the nodes
    votes float64‖Number of votes
    address string‖Address
    credit float64&par;Trust value
}
type superNode struct{ ‖Structure of super nodes inherit node structure
    node &par;Node type
}
var voteNodePool[]node‖Define a voting node pool variable of type as []node
var superNodePool[]superNode‖Define the superNode pool variable type as []superNode
func init(){‖Node initialization
    for i = 0; i ≤ voteNodeNum: i++{
        VoteNodePool[i].votes = random()‖Each node randomly obtains the number of votes
    }
    for i = 0; i ≤ super NodeNum; i++{‖Super node initialization
        superNodePool[i] = Supernode{node{0,0,0}}
    }
}
return
end‖End of algorithm
```

Table 2: Algorithm 2 voting().

```
Input: voteNodesPool'votes
Output: mineSuperNode
for i = 0; i ≤ superNodeNum; i++{
    starNodePool[i].votes = 0‖All votes received by the super node are initially 0
    for_, v: = range voteNodesPool{‖Loop through the pool of polling nodes to get them to get votes
        rInt, err: = rand.Int(rand.Reader, big.NewInt(superNodeNum))
        if err! = nil{
            log.Panic(err)
        }
        superNodesPool[ int(rInt.Int64o) votes + votes each node votes randomly and gives its votes to the super node it voted for
‖Ranking of campaign nodes by number of votes
func sortCampaignNodes() {
    sort.Slice(campaignNodesPool, func(i,j int)bool {‖Sorting functions
        retum campaignNodesPool[i].votes > campaignNodesPoolj].votes
    })
    superCampaignNodesPool = campaignNodesPool[:mineSuperNodeNum]
    ‖mineSuperNodeNum = 5, Select the top five campaign nodes to become super nodes for consensus
    return
    end
}
```

a malicious node. The number of super nodes defined for this experiment is 10 and the number of super nodes that reach consensus is 5, i.e. 5 super nodes reach consensus in each round. Each node of the experiment is a node of the knowledge commons.

Since the blockchain network uses the C-DPOS consensus algorithm, which does not involve the arithmetic power of PoW, etc., consensus between nodes can be achieved quickly [15]. For example, if the system runs 10,000 consensus runs, first the system will initialize 100 voting nodes, each with the initial number of votes to be cast at initialization. Then, the system initializes 10 campaign nodes. All campaign nodes are randomly assigned confidence values at initialization. The initial confidence interval is set to [−25,25]. After initializing the 10 campaign nodes, each campaign node will randomly vote for the campaign node in the campaign node pool. The voting process is random, and all campaign nodes have the same chance of receiving a vote as any other normal node. The trust value will have a significant impact on the super node when it participates in consensus later on. After the first round of voting operation is completed, the number of votes received

Table 3: Algorithm 3 C-DPos.

```
Input: block information
Output: new block
init()‖First initialize each node
var blockchain []block
creat genesisBlock ≤ block {prehash, hash, timest amp,data, height,address}‖Create a Genesis block
blockchain = append(blockchain.genesisBlock) ‖Link new blocks after each block
for{‖Calculate the trust value and votes after one round of consensus based on the current trust value of the super node
    if superNode's credit<0&& > = −20{
        this credit = credit+0.05
        superNode's votes < −0
        this consensus opportunity - > other normal superNode
    } else if superNode's credit < −20{
        this credit = credit+0.01
        superNode's votes < −0
        this consensus opportunity - > other normal superNode
    }else{
        this credit = credit+0.2
        this superNode consensus success‖The super node consensus is successful
    }
}
return
```

by each super node in the campaign node pool is calculated according to equations(2), (3), and (4), and the initialization of each node is shown in Table 4.

From Table 4, the top five selected nodes after the first round are: Super Node 2, Super Node 4, Super Node 5, Super Node 6, and Super Node 7. That is to say, the first five rounds of consensus will be conducted by these five super nodes because the initial trust values of Super Node 2, Super Node 4, and Super Node 5 are all less than 0, so the first five rounds of consensus will be randomly selected among Super Node 6 and Super Node 7 whose initial trust values are greater than or equal to 0. The first five rounds of consensus will be randomly selected among the Super nodes 6 and 7 with initial trust values greater than or equal to 0. If the super node with a trust value less than 0 is selected for consensus, then the bookkeeping right will be randomly assigned to the super node with a trust value greater than or equal to 0, and its trust value will be accumulated according to the interval described in equation(1). When a normal node acquires bookkeeping rights, its trust value will also be increased according to the description of equation (1).

This experiment uses every 1000 rounds as a split point to count the change in trust value of the 10 super nodes in the campaign node pool, and after 10,000 rounds of consensus, the change in trust value of the 10 super nodes is shown in Figure 11.

From the above figure, it can be seen that the overall change of trust value of normal nodes is even, and the change curve of trust value of each normal node is almost parallel, which indicates that the probability of nodes acquiring bookkeeping rights is almost equal and there is no large gap, which also proves that C-DPOS can make normal nodes acquire bookkeeping rights more fairly. The probability of each super node obtaining the bookkeeping right after completing 10,000 times of consensus is shown in Figure 12.

Combining the analysis in Table 4 and Figure 12, it can be seen that there is no significant difference in the probability of a normal successful node successfully obtaining a bookkeeping right and completing the bookkeeping, again demonstrating that C-DPoS enables normal nodes to obtain bookkeeping rights more equitably. In contrast to traditional DPoS with no node trust value, DPoS participates in the full consensus process regardless of whether the node is normal or malicious and does not penalize malicious nodes. The probability of each node participating in consensus after 10,000 rounds of the traditional DPoS consensus algorithm is shown in Figure 13.

From the figure, the probability of each node successfully participating in the consensus and completing the bookkeeping after 10,000 times of consensus fluctuates around 10%, and the overall gap is small. The probability of each node is distributed more evenly, and the probability of a

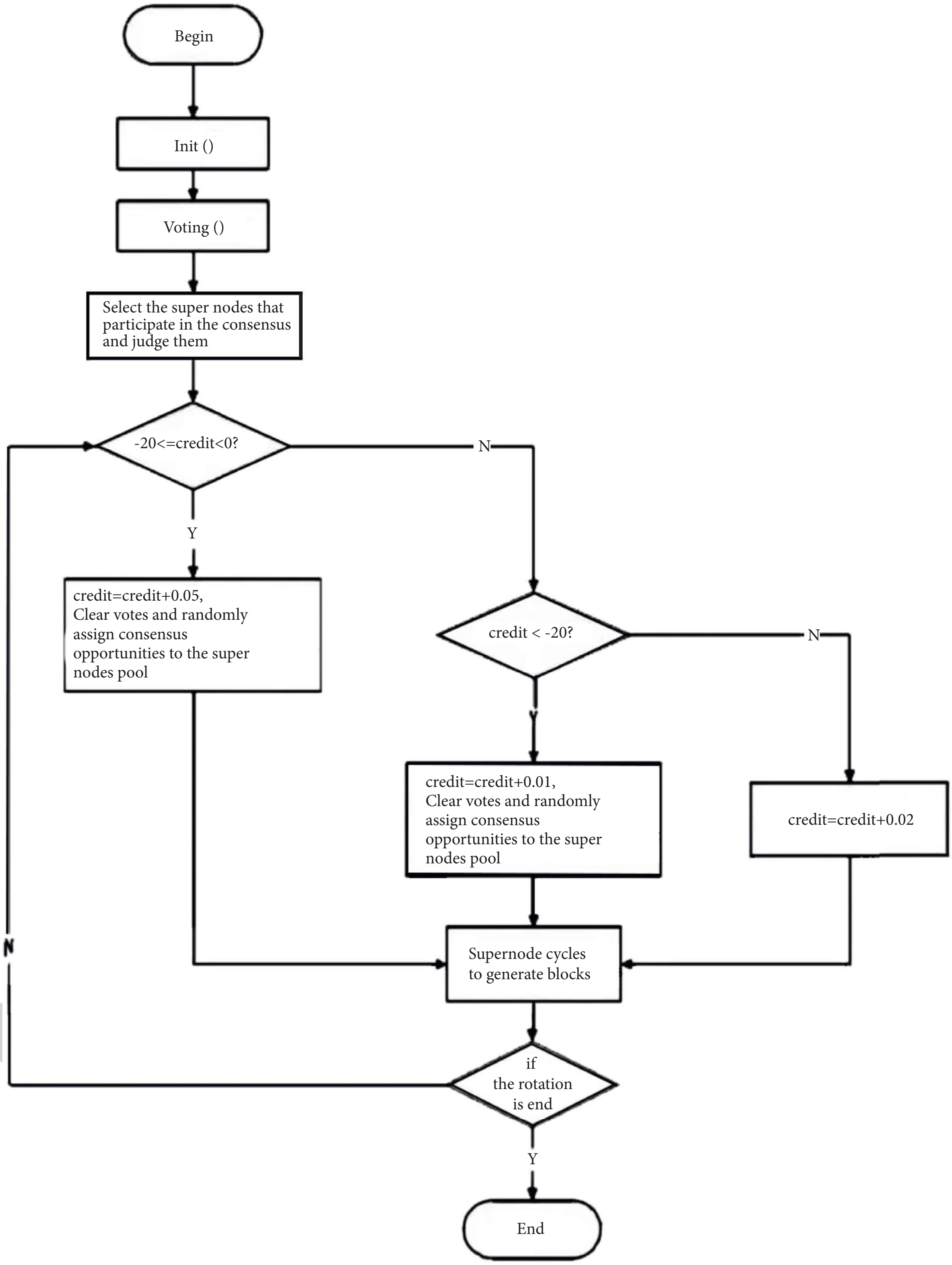
Begin
Init ()
Voting ()
Select the super nodes that participate in the consensus and judge them
-20<=credit<0?
N
Y
credit=credit+0.05,
Clear votes and randomly assign consensus opportunities to the super nodes pool
credit < -20?
N
Y
credit=credit+0.01,
Clear votes and randomly assign consensus opportunities to the super nodes pool
credit=credit+0.02
N
Supernode cycles to generate blocks
if the rotation is end
Y
End

Figure 10: C-DPoS core execution flow chart.

Table 4: Initial super node situation.

SuperNodeNum	Votes	Credit
SuperNode 0	336	9
SuperNode 1	317	23
SuperNode 2	694	−7
SuperNode 3	489	9
SuperNode 4	47	−25
SuperNode 5	190	−15
SuperNode 6	537	14
SuperNode 7	533	0
SuperNode 8	342	20
SuperNode 9	219	6

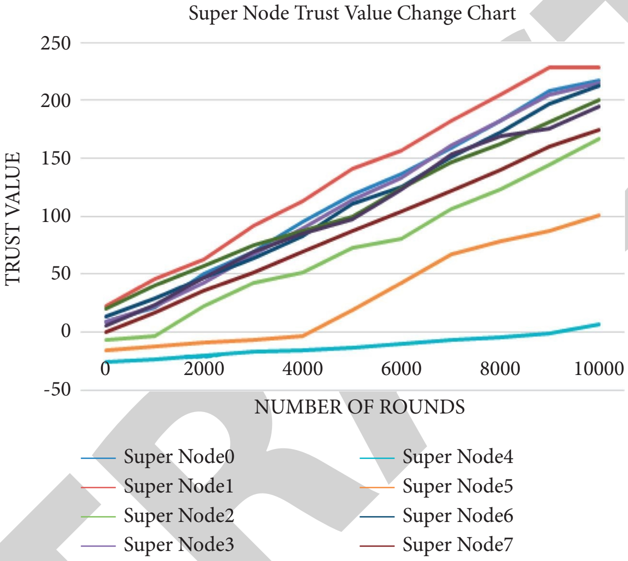

Figure 11: Graph of super node trust value change.

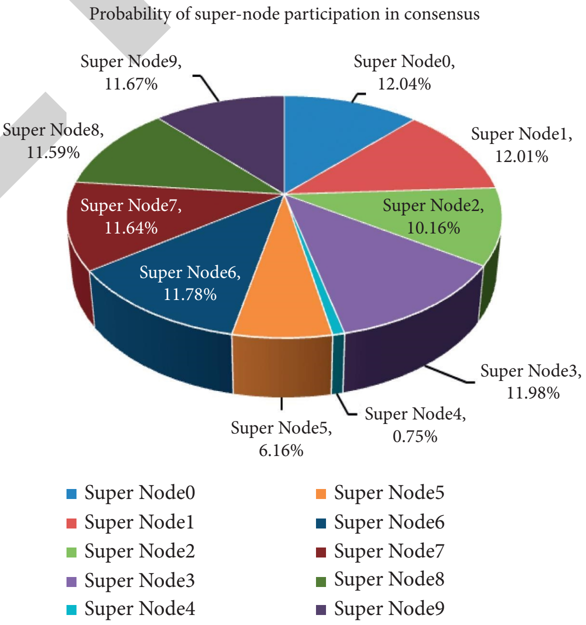

Figure 12: Probability graph of super node participation in consensus.

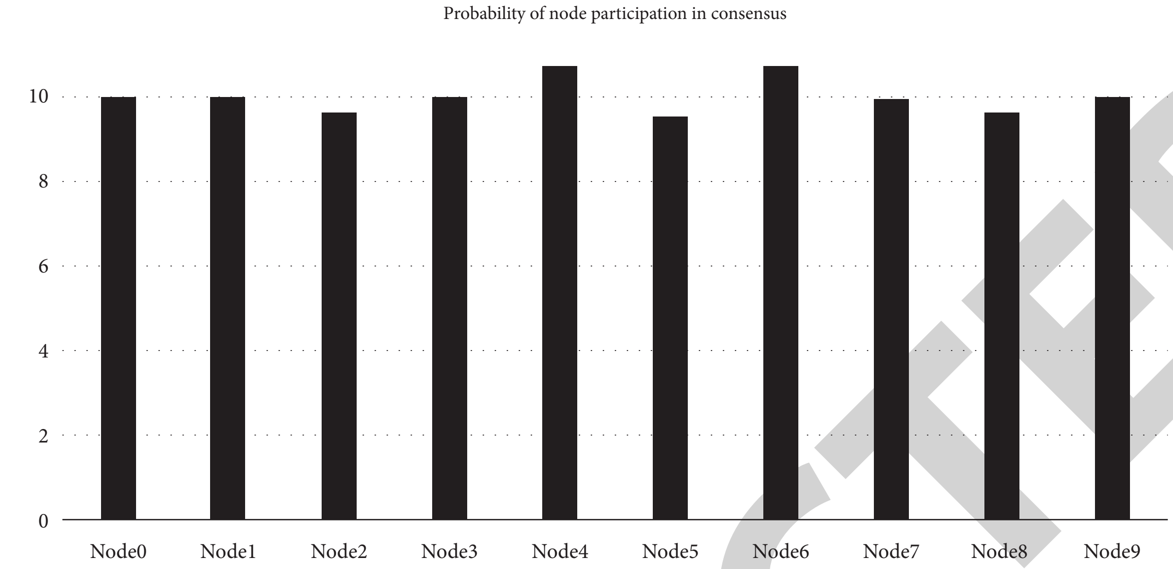

Figure 13: Probability graph of traditional DPoS nodes participating in consensus.

node completing its participation in the consensus and bookkeeping is not reduced because it is a malicious node, which will cause the malicious node to still be able to agree normally, thus affecting the fairness of the whole system.

5. Conclusion

The transfer and transformation of scientific and technological achievements is a complex and systematic project. In addition to the complexity of the achievements themselves, there are more identities of the participating subjects, including universities, research institutes, technology transfer agencies, enterprises, law firms, finance companies, and fund companies. [16] With the rapid improvement of scientific research level in universities, the types and quantity of scientific research are increasing, which has put forward higher requirements for the transformation of scientific and technological achievements. Currently, the application of computer systems for the transformation of scientific and technological achievements has become a development trend, and universities have also developed their systems for the transformation of scientific and technological achievements. Blockchain technology can achieve decrediting and redefine the way credit is generated in the network. [17]

(1) The use of blockchain technology can reduce the transaction costs of both parties. Based on the demand for university scientific research results management, blockchain technology is used to design and develop the university scientific research results management system, so as to realize the promotion of scientific and technological results information and scientific and technological results transaction between universities and enterprises, reduce the transaction cost of both parties and improve the transformation rate of university scientific and technological results. According to the result of the requirement analysis, the module is divided into three parts: system login, comprehensive management, and scientific research results management, and the detailed design of each part is carried out, in which the management functions in the scientific research results management part are designed into seven categories: scientific research projects, thesis statistics, scientific research results, academic exchange, student exchange, academic activities, and teaching results, and the detailed management contents are designed under each category. The functions of querying, adding, modifying, and verifying the research results are then designed.

(2) The use of blockchain technology to write smart contracts to protect data and information. According to the characteristics of blockchain, which is highly tamper-proof and has low data access performance, the data protection scheme combining private blockchain and private IPFS (Inter Planetary File System) network is proposed, and the private chain is built by Ether, and the consensus mechanism of Po A (Proof of Authority) is adopted to reduce the time required to reach consensus. The private chain stores the hash value of research data and IPFS address, and the private IPFS network stores data and files.

(3) The use of blockchain technology to enhance the trust of cooperation. The article introduces the trust-optimised consensus algorithm C-DpoS, blockchain technology that provides a secure data tracking and information anti-counterfeiting system for our information sources and databases. As the data in the blockchain are connected backwards and forwards to communicate a timestamp that cannot be tampered with, it will be possible to affix a set of nonfalsifiable and authentic records for all participants and trajectories, so that falsified information and channels in the process of transferring and transforming

technological achievements can be identified, and participants' information sources, intervention times and results resulting from interventions can all be recorded through the blockchain. If problems arise during the process, the problem can be traced back to the point of problem, so that every participant is in awe, avoiding abuses and underhand operations, and facilitating the smooth promotion of technology transfer and transformation.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Acknowledgments

This work was supported by Changzhou Science and Technology Planning Project "Yuying's innovation Space of Jiangsu University of Technology with Technology Service Capacity Improved" (no. CM20176011)".

References

[1] Y. Xue, M. Z. Li, X. Ran, and Y. H. Feng, "Reform and practice of transforming scientific and technological achievements in colleges and universities to promote innovation and entrepreneurship education of college students," *Journal of Luoyang Normal College*, vol. 41, no. 02, pp. 88–92, 2022.

[2] X. Xi, "Jinping stresses blockchain as an important breakthrough in independent innovation of core technologies during the 18th collective study of the Central Political Bureau to accelerate the development of blockchain technology and industrial innovation," 2019, http://www.xinhuanet.com/politics/201910/25/c_112553665.htm2019-10-25/2020-02-13.

[3] Standing Committee of the National People's Congress, "Law of the People's Republic of China on Promoting the Transformation of Scientific and Technological Achievements," 2021.

[4] Department of Science and Technology, *Ministry of Education of the People's Republic of China 2017 Compilation of Science and Technology Statistics of Higher Education Institutions*, Higher Education Press, Beijing, China, 2018.

[5] China Academy of Information and Communication Research, *Blockchain white Paper*, China Academy of Information and Communication Research and Trusted Blockchain Promotion Program, Beijing, China, 2019.

[6] S. Yadav and S. P. Singh, "Blockchain critical success factors for sustainable supply chain," *Resources, Conservation and Recycling*, vol. 152, Article ID 104505, 2020.

[7] A. Banafa, "How to Secure the Internet of Things(IoT) with Blockchain," 2014, https://www.datafloq.com/read/securinginternet-of-things-iot-with-blockchain/2228,2017-O1-O7.

[8] P. F. Wong, F. C. Chia, M. S. Kiu, and E. C. W. Lou, "Potential integration of blockchain technology into smart sustainable city (SSC) developments: a systematic review," *Smart Sust. Built Envir*, vol. 13, p. 3334, 2020.

[9] V. G. Venkatesh, K. Kang, B. Wang, R. Y. Zhong, and A. Zhang, "System architecture for blockchain based transparency of supply chain social sustainability," *Robotics and Computer-Integrated Manufacturing*, vol. 63, Article ID 101896, 2020.

[10] E. Safapour, S. Kermanshachi, and S. Kamalirad, "Analysis of effective project-based communication components within primary stakeholders in construction industry. Built," *Environ. Proj. Asset. Manag*, vol. 11, no. 17, pp. 157–173, 2020.

[11] S. Kurpjuweit, C. G. Schmidt, M. Klöckner, and S. M. Wagner, "Blockchain in additive manufacturing and its impact on supply chains," *Journal of Business Logistics*, vol. 42, no. 1, pp. 46–70, 2021.

[12] S. K,.ohler and M. Pizzol, "Technology assessment of blockchain-based technologies in the food supply chain," *Journal of Cleaner Production*, vol. 269, Article ID 122193, 2020.

[13] S. Ghosh, C. Wölper, A. Tjaberings, A. H. Gröschel, and S. Schulz, "Syntheses, structures and catalytic activity of tetranuclear Mg complexes in the ROP of cyclic esters under industrially relevant conditions," *Dalton Transactions*, vol. 49, no. 2, pp. 375–387, 2020.

[14] R. Petrus and P. Sobota, "Magnesium and zinc alkoxides and aryloxides supported by commercially available ligands as promoters of chemical transformations of lactic acid derivatives to industrially important fine chemicals," *Coordination Chemistry Reviews*, vol. 396, pp. 72–88, 2019.

[15] D. M. Palm, A. Agostini, V. Averesch et al., "Chlorophyll a/b binding-specificity in water-soluble chlorophyll protein," *Nature Plants*, vol. 4, no. 11, pp. 920–929, 2018.

[16] W. Gruszka and J. A. Garden, "Advances in heterometallic ring-opening (co)polymerisation catalysis," *Nature Communications*, vol. 12, no. 1, p. 3252, 2021.

[17] T. Rosen, J. Rajpurohit, S. Lipstman, V. Venditto, and M. Kol, "Isoselective polymerization of rac -lactide by highly active sequential {ONNN} magnesium complexes," *Chemistry - A European Journal*, vol. 26, no. 71, Article ID 17189, 2020.