Research on Agricultural Products Supply Chain Traceability System

- Blockchain consensus algorithm optimization

Chunrong Song
School of Information Management
Beijing Information Science and Technology University
Beijing, China
Songsongchunrong@163.com

Chen Li
School of Information Management
Beijing Information Science and Technology University
Beijing, China
lichen@bistu.edu.cn

2021 9th International Conference on Traffic and Logistic Engineering (ICTLE) | 978-1-6654-2752-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICTLE53360.2021.9525744

***Abstract*—In order to improve the authenticity and credibility of agricultural products traceability information, this paper proposes an improved blockchain consensus algorithm FPBFT for the whole process traceability system from planting to consumption of agricultural products supply chain based on blockchain, in view of the high communication overhead and low efficiency of the consensus algorithm PBFT of the coalition blockchain when the information is on the chain. The credit value of the nodes is calculated based on the behavior of each node in the consensus process, and the nodes are given different voice rights based on the credit value; then a simplified consistency protocol is proposed to reduce the time complexity by combining the node characteristics of the coalition chain. Finally, a comparison experiment is conducted to verify that the improved PBFT algorithm can reduce the communication volume and improve the efficiency.**

Keywords—Blockchain, agricultural product supply chain, traceability, Consensus algorithm

I. INTRODUCTION

Traditional traceability of agricultural products is based on a central database, the authenticity of information cannot be verified, and the information of agricultural products is not open and transparent, which makes it difficult to determine the responsible party of agricultural products. In response to the above problems, the characteristics of blockchain such as non-tamperability and traceability are applied to the supply chain to ensure the openness and transparency of supply chain information and information sharing. The traceability scheme of blockchain is shown in Fig. 1.

Starting from the source of production, production details (including production environment, soil, fertilizer, feed, etc.), quality inspection reports, certificates of origin and other information of each link of the agricultural products supply chain are packaged and uploaded onto the chain, and the information is fixed with the help of traceability codes, and these information blocks are arranged in a backward and forward order based on time stamps. Encryption operations and distributed bookkeeping guarantee that the data will not be tampered with. After consumers purchase goods, they can use cell phone applications (APP) or personal computer (PC) terminals to trace the cultivation environment, quality inspection information, origin information, processing situation and circulation process of agricultural products through the traceability code, and realize the common investigation and sharing of the whole chain.

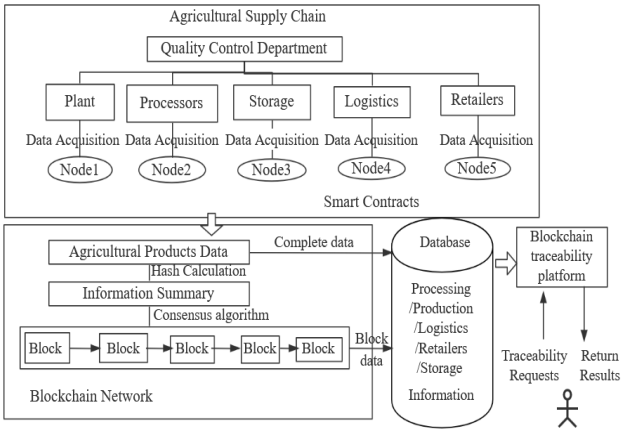

Fig. 1. Blockchain Traceability Solutions

How to establish a decentralized and credible traceability system is an important issue that government management departments, enterprises and academia need to address urgently today [1].By reading the literature [1]-[6], it is found that most traceability systems mainly focus on the optimal design of system functions, and less consideration is given to the communication volume and efficiency of the Practical Byzantine Fault Tolerance (PBFT) algorithm for blockchain.

Based on the above problems, this paper proposes an improved consensus mechanism - Food Practical Byzantine Fault Tolerance (FPBFT) based on credit score mechanism, which calculates the credit value of each node based on its behavior in the consensus process. The credit value is calculated based on the behavior of each node in the consensus process, and the nodes are given different voice rights based on the credit value, and the inertia of nodes in delaying sending messages is

reduced by rewarding and punishing the nodes with the credit value; and then the time complexity is reduced from $O(N^2)$ to 0(N) by simplifying the consistency protocol with the feature that most of the nodes on the coalition chain are honest nodes.

II. Byzantine Fault-Tolerant Algorithms

Practical Byzantine Consensus (PBFT) consists of consistency protocol, view replacement protocol and checkpoint protocol. When the information is on the chain, the nodes run the consistency protocol, each node gets the status of other nodes through peer-to-peer communication, the information is correct, the consensus is completed, and each node unifies the transaction data. In case of failure in the operation of the consistency protocol, the system replaces the failed node through the view replacement protocol to ensure stable system operation. The checkpoint protocol periodically clears the expired interaction data to reduce the node storage burden, periodically checks the system status, and synchronizes inconsistent nodes. Through analysis, PBFT also has the following deficiencies in running the consistency protocol.

A. Master Node Selection

The PBFT algorithm randomly selects the master node, which leads to an increased probability of Byzantine error nodes becoming the master node, and when the master node is wrong, the transaction process needs to be stopped and the failed node replaced by a replacement view, which reduces the system efficiency.

B. Traffic

There is a large amount of point-to-point communication between PBFT nodes, and the communication volume reaches $O(N^2)$, causing the number of node communications to increase exponentially with the number of nodes, which seriously affects the system scalability.

III. Credit Score Mechanism Consensus Algorithm

To address the shortcomings of PBFT algorithm, by reading the literature [6]-[8], we found that most scholars in the study designed credit value points only for the consideration of the node's performance in the previous consensus process, No specific application scenarios are considered. Each node in the supply chain needs to be certified by CA before it can enter the alliance chain, and it is the responsibility of each node to jointly maintain the traceability system. Optimized for the random selection of master nodes by the PBFT algorithm and the complex consensus process, the supervisory department first scores each node of the supply chain according to the usual work rating criteria, and takes the score as the initial score. After the system runs for a period of time, by taking into account the nodes' participation in consensus, the points of the nodes are correlated with the number of times they participate in consensus, and the nodes with stable performance are selected to act as consensus nodes, which can promote the system to enter a virtuous cycle. Also because most of the certified nodes are honest nodes. Therefore, this paper focuses on improving the PBFT algorithm in two aspects of node behavior credit value and simplifying the consistency protocol.

A. Node behavior Reward and Punishment Mechanism

The evaluation of consensus nodes is mainly based on three types of nodes' behaviors: normal participation in consensus, failure delay nodes, and malicious behavior nodes. The different behaviors of nodes lead to corresponding changes in credit values. The node behavior reward and punishment mechanism is the basis of master node selection and the optimization of the consistency protocol.

1) Nodal Credit Design: The credit value is calculated based on the evaluation of node behavior, which can be described from different perspectives. For example, some nodes are active and frequently participate in consensus, while some nodes are unstable and often time out, etc. These relevant factors are added to the credit value calculation to comprehensively evaluate the behavior of nodes in the consensus process.

a) Node activity: refers to the frequency of node i participating in consensus, which reflects how active the node is in the system. The node activity ρ(i) is denoted as:

$$\rho(i) = \frac{T_i}{T} \qquad (1)$$

where T is the sum of the consensus processes performed by the blockchain network in the past time, and T(i)is the total number of times node i participated in the consensus process during that active time.

b) Completing a consensus:the consensus count update T(i)' can be expressed as:

$$T_i' = T_i + 1 \qquad (2)$$

c) Inert node behavior evaluation: refers to the presence of network delay and intentional delay in sending messages by nodes. The behavior evaluation θ can be expressed as follows.

$$\theta = \frac{\Delta t}{D} \qquad (3)$$

whereΔt is the time for nodes to reach consensus and D is the fixed value of delay.

d) Credit value evaluation and update: After the consensus process of consensus nodes is completed, the system will evaluate each node based on its performance in this process. The credit value evaluation of node i can be expressed as :

- Number of consensus $\frac{T}{2} \le T_i \le T$

$$C(i) = \begin{cases} \frac{T_i}{T} * (1-\theta) + C(i) * (1+x) & (T_i \le T_i') \\ C(i) * x & (0 < T_i < T_i') \\ C(i) * z & \text{(node evil)} \end{cases} \quad (4)$$

- Number of acquaintances $0 \le T_i \le \frac{T}{2}$

$$C(i) = \begin{cases} \frac{T_i}{T} * (1-\theta) + C(i) * (1+y) & (T_i \le T_i') \\ C(i) * y & (0 < T_i < T_i') \\ C(i) * z & \text{(node evil)} \end{cases} \quad (5)$$

The model can accurately reflect the performance of nodes in the consensus process. If the nodes are active and have a short time to complete the consensus, both will submit the node credit value. On the contrary, the node credit value will decrease.

2) Pseudo code for node credit value:

First the system initializes the nodes, the initial value is the regulator score, the consensus process is sorted according to the credit value, and the node with the highest score is the master node. When the number of nodes involved in consensus is greater than half of the total consensus, the growth rate is x, otherwise the growth rate is y; when the node is evil, the node growth rate is z, where (x) y>z). The integral design pseudo-code is shown in Fig. 2.

Algorithm1 Credit Score Algorithm

```
Initialize the label of the node{n1, n2, … , nk}
Initialize the consensus number of node{T(ni)}
Initialize the activity score of the node{ac(ni)}
Initialize the power score of the node{c(ni)}
Initialize the fixed delay value D
Sort power scores from high to low;
Take out the first 2*f+1;
for all {c(ni), c(ni+t), …, c(ni+2f+1)} do
    if c(ni) and all {c(ni+t),…,c(ni+2f+1)} reach a consensus. then
     Update the consensus number T(ni) ;
     Update the credit score of the c(ni) node;
          if T/2≤T(i)≤T. then
              C(i)'=C(i)  *  (1+x)
          else
              C(i)'=C(i)  *  (1+y)
    if not participating in consensus
          if T/2≤T(i)≤T. then
              C(i)'=C(i)  *x
          else
              C(i)'=C(i)  *y
     else
              C(i)'=C(i)  *z
    Update delay score to t/D.
    Update activity score ac(ni) toT(ni) /T .
    C(i)'=t/D*T(ni)/T+C(i)'
    end
```

Fig. 2. Integral design algorithm

B. Simplified Conformance Protocol Design

1) Nodal PBFT Conformance protocol: The PBFT consistency protocol defines two types of nodes, master node and consensus node. The master node is responsible for verifying the data received by the blockchain system over a period of time that is ready to be uploaded to the chain, and after the verification is passed, the master node will pack these data into the block to initiate consensus. The slave nodes communicate two by two to confirm whether the information is correct or not, and the PBFT communication process is shown in Fig. 3.

2) Simplified Consistency Protocol Algorithm : The simplified consistency protocol firstly selects 2f+1 nodes as consensus nodes according to the points value[9], the master node with the highest points and the rest nodes as consensus nodes. After receiving the client information, the master node sends the information to the slave nodes, and the slave nodes transfer the verification process of "receive-send-receive" to the master node, which determines whether the feedback information of all consensus nodes is correct, without the need for other consensus nodes to make further judgments; the premise of the simplified consistency protocol is that all nodes in the current common blockchain network reach consensus. The process of FPBFT communication is shown in Fig. 4.

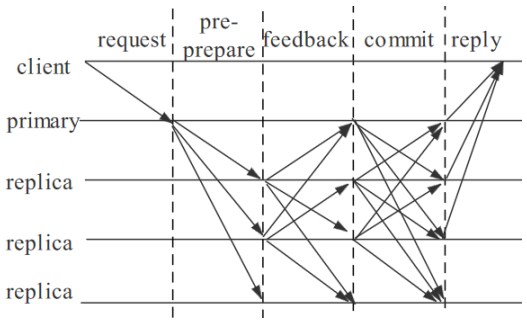

Fig. 3. PBFT communication process.

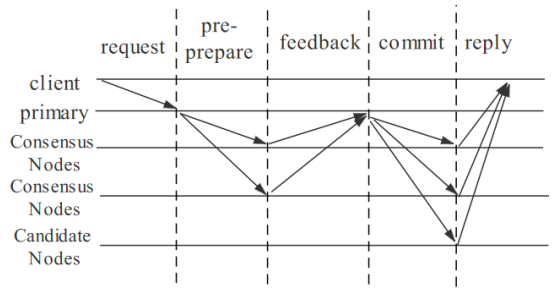

Fig. 4. FPBFT communication process.

3) Simplified Consistency Protocol Algorithm Pseudocode: The client sends the request message, the master node generates the pre-preparation message, and the consensus node executes the FPBFT simplified consistency protocol first; during the operation, the consensus node compares the pre-processing message d sent by the master node with the local message, if the content is the same, it means there is no Byzantine node, and continues to execute the simplified consistency protocol; if the content is different, it means there is a Byzantine node, stops executing the simplified consistency protocol, and Execute the complete consistency protocol. The specific algorithm process is shown in Fig. 5.

Algorithm2 Simplified consistency protocol algorithm

Input: Consistency proposal

Output: Transaction closed

```
Initialize Node;
Implementing Simplified Conformance Protocols;
Master nodes broadcast pre-preparation messages<PRE-PREPARE,v,n,d,m>;
Consensus node comparison hash;
Send master node feedback<feedback,v,n,d,i>;
  if (feedback is the same)
    then Master broadcasts to all nodes;
    Add block information<commit,v,n,d,a>;
    Node reputation points;
  else
    Stop Trade;
    Node reputation points;
    Implementing full conformance protocols;
    Node reputation points;
    Broadcast;
Update Node Points;
end
```

Fig. 5. Simplified consistency protocol algorithm.

FPBFT is a consensus algorithm proposed on the basis of the coalition chain, and nodes need CA authentication to enter, so the vast majority of them are honest nodes, so FPBFT performs a simplified consistency protocol the vast majority of the time. By introducing the reward mechanism, the node with the highest reputation score is selected as the master node, which greatly reduces the probability of failure or evil of the master node and ensures the stability of the consensus process; the method of selecting some nodes to participate in the consensus reduces the consensus time and improves the consensus efficiency.

IV. Experimental Results and Analysis

To test the operational results of the FPBFT optimization mechanism, the experiments are based on Python simulation of PBFT and FPBFT processes. The communication volume, consensus time and node reliability are compared.

A. Communication Volume Comparison

FPBFT reduces the algorithm complexity by simplifying the consistency protocol in the PBFT algorithm to reduce the time complexity from $o(N^2)$ to o(N), and compares the performance of the two algorithms in terms of communication overhead through comparative experiments.

1) PBFT traffic: Assume that there are N nodes in the blockchain network at this time, and the nodes have a two-by-two consensus, and the number of communications is N-1+(N-1)(N-1)+N(N-1). View switching, master and slave nodes broadcast messages, and the number of communications is (N-1)(N-1)+N-1. Let the system view switching probability be p. The average total number of communications for the PBFT algorithm is:

$$S = 2N(N-1) + pN(N-1) \tag{6}$$

2) FPBFT communication volume: The FPBFT algorithm shortens the consensus process of two node broadcasts, the total number of communications is 3N-2, and the view change phase is the same as PBFT with probability p. The total number of communications after the view change occurs is :

$$f = 3N - 2 + pN(N-1) \tag{7}$$

From (6)(7), the ratio of the number of communications between the FPBFT algorithm and the PBFT algorithm, r, is:

$$r = \frac{2N(N-1)+pN(N-1)}{3N-2+pN(N-1)} \tag{8}$$

3) Analysis of results: Set the number of nodes N to take the value of 4 to 15, the probability of view transformation p to take the value of 0 to 1, the use of MATLAB to derive a visualization of the formula, the results are shown in Fig. 6.

From Fig. 6, we can see that the r value is always less than 1 regardless of the values of p and N, indicating that the communication volume of the FPBFT algorithm is smaller than that of the PBFT algorithm. r value gradually decreases with the increase of the number of nodes, indicating that the communication performance of the F-PBFT algorithm is still better than that of the PBFT algorithm in a multi-node environment.

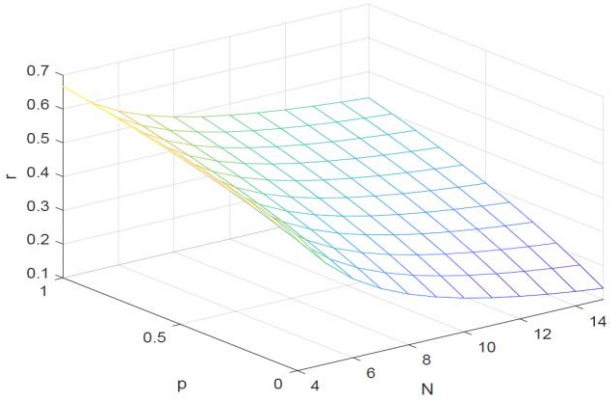

Fig. 6. Communication volume ratio

B. Consensus Node Reliability

The consensus node is the execution node of FPBFT consensus, and the consensus node reliability determines whether the consensus is successfully reached or not. The reliability of consensus nodes is tested by comparison experiments below. Two control groups are set up: integral selection and random selection, respectively. The experiments are analyzed by comparing the consensus success rate of the same number of nodes [10]. This is shown in Fig. 7.

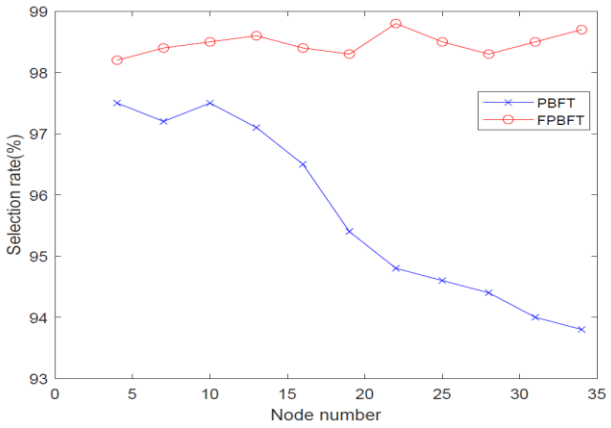

Fig. 7. Node Reliability

From the experimental results, it can be seen that the consensus success rate of the integral selection group always remains around 98.3% as the number of nodes increases, and the consensus success rate of the random selection group decreases as the number of nodes increases and the nodes are allocated fewer and fewer resources. It can be seen that the reliability of consensus nodes can be improved by adjusting the points of nodes. It is also verified that most of the coalition chains are honest and reliable nodes, and the probability of Byzantine error nodes is low. So the design of this paper has practical significance in simplifying the consistency protocol without Byzantine nodes.

C. Consensus Latency Test

Consensus latency is an important indicator of the consensus algorithm; the lower the consensus latency, the faster the transaction is confirmed and the more secure the blockchain is, as well as more practical . Consensus latency is the time consumed by a block to reach consensus, which can be expressed by equation (9).

$$delay = T_{success}\text{-}T_{submit} \tag{9}$$

where $T_{success}$is the time to successfully generate a new block and T_{submit} is the time when the transaction starts to be submitted. Experiment fixed 4 consensus nodes and the same time interval, the system sends 200, 300, 400, 500 transactions respectively for the comparison experiment, record the time delay, use MATLAB for plotting, the experimental results are shown in Fig. 8.

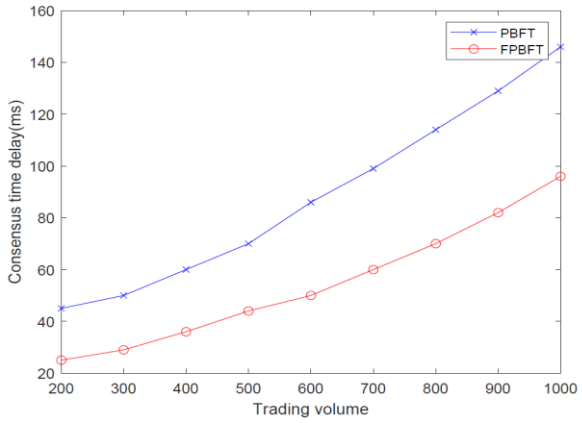

Fig. 8. Consensus delay comparison chart

As can be seen from Figure 8, when there is no Byzantine node, the FPBFT algorithm performs a simplified consistent protocol and the consensus latency is significantly lower than that of the PBFT algorithm. When the transaction volume increases, the FPBFT algorithm can reduce the latency by 31%, and the latency reduction effect is more obvious as the transaction volume increases. As can be seen from Fig. 6, in the federated chain of the traceability system, the node reliability is made stable at 98.3% according to the setting of points, which verifies that most nodes are honest nodes in the traceability system and proves that the improved FPBFT consensus algorithm research has practical significance.

V. CONCLUSION

In this paper, the blockchain-based traceability scheme for agricultural products proposes FPBFT algorithm for the shortage of PBFT algorithm, designs credit score to select consensus nodes, and cooperates with simplified consistency protocol, thus reducing system time delay and improving system speed. The whole industry chain information process design can ensure the integrity of agricultural traceability information, and combined with the decentralized, tamper-evident and traceable features of blockchain technology, it can improve the authenticity and reliability of traceability information, guarantee food safety and ensure accountability, and facilitate the supervision of government departments and improve consumer satisfaction by establishing a credible agricultural products supply chain traceability system.

ACKNOWLEDGMENT

The author is grateful to Professor Li Chen for his valuable comments and the National Natural Science Foundation of China(Grant No.61572019)for its support.

REFERENCES

[1] Ren Shouzang, He Ziming, Zhou Zhengji, Gu Xingjian, Xiong Yingjun, Yuan Peisen, Xu Huanliang. Design of crop whole industry chain information traceability platform based on CSBFT blockchain[J]. Journal of Agricultural Engineering,2020,36(03):279-286.

[2] Li HZ, Zhou SG, Tang YJ. Research on blockchain technology-enabled fruit supply chain quality and safety management.

[3] Tang Yanjun, Xu Wenhong, Li Haizhou, Zhou Xiaogang. Blockchain-based food cold chain quality and safety information platform construction[J]. Packaging Engineering,2021,42(11):39-44.

[4] Liu Ruyi, Li Jinbao, Li Xudong. Application model and implementation of blockchain in agricultural products circulation[J]. China Circulation Economy,2020,34(03):43-54.

[5] Gao YANGYANG,Lv XANGWEN,Yuan LIU,Li MENG. Research on the application of blockchain-based safe and trustworthy traceability of agricultural products[J]. Computer Application and Software,2020,37(07):324-328.

[6] Wu Xiaotong,Liu Pingzeng,Wang Zhihua. Research on blockchain-based traceability system for agricultural products[J]. Computer Application and Software,2021,38(05):42-48.

[7] Xu Governance,Feng Huamin,Liu Biao. An improved credit-based efficient consensus mechanism for PBFT [J]. Computer Application Research,2019,36(09):2788-2791.

[8] Liu Yuhong,Yang Liang,Park Chunhui,Zhang Zhiguo. Research on the key technology of railroad construction safety monitoring data sharing based on blockchain [J/OL]. Journal of Communication:1-12[2021-06-29].

[9] Fang Weiwei, Wang Ziyue, Song Huili, Wang Yunpeng, Ding Yi. An optimized PBFT consensus algorithm for blockchain[J]. Journal of Beijing Jiaotong University,2019,43(05):58-64.

[10] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair and M. Alam, Blockchain-Based Agri-Food Supply Chain:A Complete Solution[J]. IEEE .2020,8:230-234.