IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 19, 2019, accepted April 3, 2019, date of publication April 16, 2019, date of current version April 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2911265

Food Safety Supervision System Based on Hierarchical Multi-Domain Blockchain Network

QI TAO[1], XIAOHUI CUI[1], XIAOFANG HUANG[2], ANGELLA M. LEIGH[1], AND HEHE GU[1]

[1]Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

[2]School of Computer Science and Technology, Southwest University of Science and Technology, Sichuan 621010, China

Corresponding author: Xiaohui Cui (xcui@whu.edu.cn)

This work was supported by the National Key R&D Program of China under Grant 2018YFC1604000.

ABSTRACT The traditional food supervision system has problems such as lack of industry chain and data fragmentation, which has caused the phenomenon of field regulation to be uncomprehensive in the existing regulatory system and the disposal of response lag. Combining the characteristics of blockchain such as distribution, transparent, and collegiality with the actual needs of regional autonomy, we propose the hierarchical multi-domain blockchain (HMDBC) network structure and the secondary-check mechanism, which can support timely correction and replacement of the malicious supervision nodes by regional nodes co-governance, auxiliary verification of supervision nodes, and arbitration of superior regions. In order to optimize the supervision nodes election, we proposed fuzzy comprehensive evaluation model of credibility, which can be used to objectively and fairly evaluate the comprehensive reputation of each node in that region by considering various influencing factors of node performance indicators. Furthermore, we designed the data block structure model, which can support the supervisor node replacement. Our system can perform automatic food quality detection and warning of substandard food in the entire industrial chain, with the use of smart contracts combined with the food industry standards. Finally, comparing the complexity of the traditional blockchain system with PBFT consortium, our system is more secure, with lower broadcast complexity.

INDEX TERMS HMDBC network, supervision, credit evaluation, smart contract, food safety.

I. INTRODUCTION

The food industry has over recent years, experienced food quality related incidents both domestically and internationally. Examples of such incidences are the Sudan red, Melamine, and Horsemeat, which not only threatens the health of consumers, but also affects the stability of social order and causes huge losses to the national economy. There is about 90% of the total production of fresh meat and 80% of the total production of vegetables and fruits are under the poor logistics which result in huge waste and increased cost [35]. All these and more are issues that need to be addressed in the food safety field.

Establishing an effective food quality traceability system is one of the main measures to protect food quality and safety. The traditional food safety traceability system has the following problems: 1) a small number of central database institutions master most of the valuable information, which is easy to form a high-cost and inefficient operation status. Also, the information providers can selectively shield or even tamper with information that is not favorable to them, while the consumer can hardly identify with the naked eye. 2) Food industry chain links are increasingly refined, involving many links, elements, and participants, with huge communication cost. 3) Sharing information between different links in the food industry is a serious challenge. Without information sharing and management, the industry data is fragmented [33]. However, if the food industry data is shared, development of the food industry will experience great benefits which will be of use to research been carried out on optimization of the industry chain, and also improve food quality supervision and anti-counterfeit. It is necessary to call for attention on how to innovate and energize ICTs in order to best assist all nations to achieve the SDGs by 2030 [41]. The blockchain technology can build a trusted way with different organizations to support information sharing. The mathematical method feature of blockchain makes possible the establishment of a trust relationship between nodes,

The associate editor coordinating the review of this manuscript and approving it for publication was Jinsong Wu.

This work is licensed under a Creative Commons Attribution 3.0 License. For more information, see http://creativecommons.org/licenses/by/3.0/

eliminating third-party participation. It also helps avoid the risk of centralized server crashes [11], and its smart contract feature used to protect user's privacy and automatic information processing [13], [14].

In 2008, Nakamoto first proposed the blockchain architecture of distributed, tamper-proof and social governance, which was successfully applied in financial filed likely Bitcoin and Ethereum [1], [3], [8]. Recently, blockchain technology application has broken through the boundary of the financial field. [2], [16] It proposed a method for data security and sharing of health records in the medical sector based on blockchain technology. [9], [15], [34] Blockchain technology also offers benefits to energy system operations, markets, and consumers, and has the potential to improve customer services along with current and internal practices of energy companies. [10] Blockchain can be used to establish a secure and trusted autonomous ITS ecosystem, optimizing utilization of ITS infrastructure and resources. [5], [17] With the characteristics of the distributed ledger and consensus protocol, blockchain can be used to ensure the security of data stored in the cloud. [39] Mapping and scheduling workflows in a multi-cloud environment speeds up the processing and allows for a better big data management. [40] With data sets collected by the IoT and sent to the edge cloud, real-time data analysis can be facilitated. [42] With higher bandwidth, greater reliability and lower latency to the IoT data transmission, the 5G era will enhance the usability and reliability of the IoT. [47] The greening big data has several research challenges on data acquisition, storage and processing. [4] Blockchain has a potential to increase the autonomy and security of IoT devices. [41] Granting all this, the actual coverage of sensor networks is, however, still low because there has been a lack of mature solutions for the deployment and management of large-scale sensor network. [6], [7] Blockchain application in the food supply chain can not only reduce agricultural losses by optimizing product logistics, but it can also provide improved efficiency in food supply chain tracking and supervision. That is, all these features introduce the establishment of a whole blockchain network environment. It does not, however, satisfy the hierarchical management system of companies, because each city is autonomous and supervised by superiors. In order to avoid the disadvantages of effectively managing the traditional traceability system, and satisfying the needs of social institutions, we have designed new blockchain system architecture to optimize the traditional food industry processes, overcome the present obstacles, by building a transparent food safety supervision system and a full chain consensus that cannot be tampered with.

The remainder of this work is as follows: Section II introduces the blockchain architecture, the $\boldsymbol{\lambda}$ level set, a concise overview of Consensus mechanism, with the demonstration of the PBFT consensus arithmetic principles and processes. In Section III, a detailed construction of food safety supervision system based on HMBC network, the comprehensive evaluation model of node reputation, the Secondary-Check mechanism, and the Main-Sub chain structure. Section IV describes the system analysis, security, and performance, while the conclusion is presented in section V.

II. PRELIMINARIES

Definitions and notations employed in this work are defined below.

A. BLOCKCHAIN ARCHITECTURE

According to the application field, the blockchain can be divided into three types, including public blockchain, consortium blockchain, and private blockchain [12].

1) PUBLIC BLOCKCHAIN

It allows any node to freely join or quit the network. All nodes have equal rights in the chain, with a collective maintenance of one chain by the whole network making it a decentralized network. Regardless of the adoption of PoW and PoS algorithms, the performance is quite slow due to the transaction verification requirements across the entire network. A typical example is Bitcoin.

2) CONSORTIUM BLOCKCHAIN

Any node can join or exit the blockchain network after being authorized by the entity organization. Each node can have different functions in the network. The entire network is organized as a unit forming a alliance to mutually maintaining the operations of the blockchain network. The transaction speed is faster than the public chain, and each node has low accounting costs and can be regulated. A typical example is Hyperledger Fabric.

3) PRIVATE BLOCKCHAIN

It only service to individuals or single entities. The number of nodes is small and the permissions of each node are controlled internally. The entire network is easy to maintain and has excellent privacy.

Compared to public blockchain or private blockchain, the consortium blockchain can satisfy multi-scene applications and have several advantages as: 1) A better performance than the public blockchain. 2) It supports the identity certificate service, which can provide higher security and better controllability. 3) It can be independent of tokens, has high scalability, and is easy to apply to the expansion of various fields. It not only meets the needs of the food industry but also fulfills the regulatory requirements of the management agencies for food safety. Only enterprise nodes authorized by certificates can join the blockchain network, which guarantees the reliability of each node in the network and the security of inter-enterprise transactions. Based on these features mentioned, the consortium blockchain was used in the construction of our food safety and supervisory system.

B. THE λ LEVEL SET

Assume the set U and fuzzy set is $F(U) = \{T|T : U \rightarrow [0,1]\}, \boldsymbol{\lambda} \in [0,1], A \in F(U), \boldsymbol{\lambda}$ level set of A is $A_\lambda = \{u \mid u \in U, A(u) \geq \lambda\}$, where $A(u) \geq \lambda$ means $u \in$

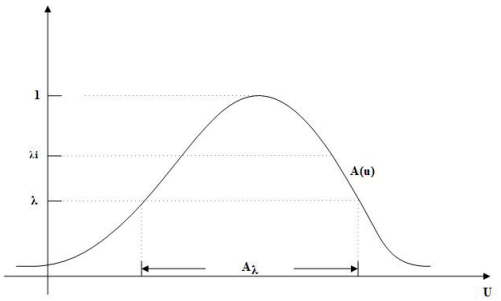

FIGURE 1. Relationship between fuzzy Set A and λ level set A_λ. With the value λ from 1 to 0, A_λ gradually expands outward.

A_λ *and* $A(u) < \lambda$ *means* $u \notin A_\lambda$. The figure 1 showed relationship between A and λ level set A_λ. It possesses the follow properties [46]:

- If $\{A_t | t \in T\} \subseteq F(U)$, then $(\bigcup_{t \in T} A_t)_\lambda = \bigcup_{t \in T} (A_t)_\lambda, (\bigcap_{t \in T} A_t) = \bigcap_{t \in T} (A_t)_\lambda$;
- If A∈F(U), then $A = \bigcup_{\lambda \in [0,1]} (\lambda A_\lambda)$.

C. CONSENSUS MECHANISM

The consensus mechanism would directly impact the performance and security of the blockchain network. Many foreign and domestic scholars devote themselves to consensus algorithm research. Satoshi *et al.* proposed the decentralized consensus scheme, based on adaptive difficulties and Sybil attack prevention, by building a completely decentralized computation that is difficult to verify but easy to implement [1], [19]. The PoW algorithm is quite difficult for a wider application due to resource density character. It is completely based on workload to determine the 'correct' chain during the competitive block-chains, which is possible to cause transaction uncertainty with probabilistic factor of workload proof [20]. The PoS algorithm determines whether the account can create data blocks at a specified time through the statistics of virtual assets of the account, and can easily cause Cartel problems resulting in financial oligopoly [21]. The traditional BFT algorithm can effectively solve the abnormal behaviors, such as malicious attack and network congestion interruption, allowing no more than 1/3 of the host node fault tolerance ability. Its lack of clock synchronization mechanism and the complexity however increases exponentially with the increase in nodes. The PBFT algorithm can reduce this complexity from exponential to polynomial, and it typically consists of three phases: pre-prepare, commit and reply [18], [22]–[24].

As the PBFT workflow showed that the C denotes task client, P0-P3 shows the server nodes in blockchain network, and the P3 server shows the broken. The PBFT algorithm works as follows. (Assume that there are $3f + 1$ server nodes in blockchain network and set $f = 1$. The honest nodes

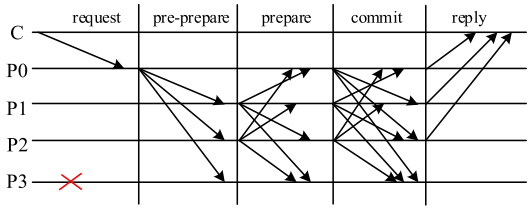

FIGURE 2. The PBFT workflow.

can follow the same instructions and broadcast messages truthfully.)

1) REQUEST PERIOD

The task client C encapsulates the tag C task O and timestamp T into the following: Request (C, O, T) , and submit to the master node P0, then wait for the server nodes verification results Reply(V, T, C, Pi, R). According to the PBFT fault-tolerant mechanism, the request is completed only when the Client receives more than f replies during one time slice from different server nodes Pi with the same timestamp T and check result. PBFT would however, reselect the primary node and resend the request in cases of timeout.

2) PRE-PREPARE PERIOD

After Request(C, O, T) has been received, the P0 gets the request view V and sets the sequence number n, then encapsulate to the Preprepare(V, n, D(Request), Request) and finally broadcast it to other nodes $Pi|_{i=1,2,3}$. D (Request) is the digital signature of Request(C, O, T).

3) PREPARE AND COMMIT PERIOD

The Commit period is mainly ensure that the node Pi receives the Preprepare response from the other nodes within the valid time slice. If the P3 is broken, $Pi|_{i=1,2}$ would receive Preprepare and send Replica(V, n, D (Request) , Request,$Pi|_{i=1,2}$) to other nodes for verification. $Pi|_{i=1,2,3}$ Would enter the *Reply* period only when it receives more than 2f Replica with the same (V, n, D (Request)).

4) REPLY PERIOD

Reply(V, T, C, Pi, R) would be given as the result by $Pi|_{i=0,1,2,3}$ to Client, upon receiving more than 2f Replica with the same parameters (V, n, D (Request)).

III. FOOD SAFETY SUPERVISION SYSTEM BASED ON HMDBC NETWORK

The following literature gives a detail description of the HMDBC network architecture, Two-Level Verify Mechanism, comprehensive evaluation model of node reputation; block construction, and the Main-Subchain Structure.

A. HMDBC NETWORK ARCHITECTURE

In order to satisfy the current social status that the lower-level regional autonomy and the upper-level supervision, we propose the HMDBC network architecture based on PBFT

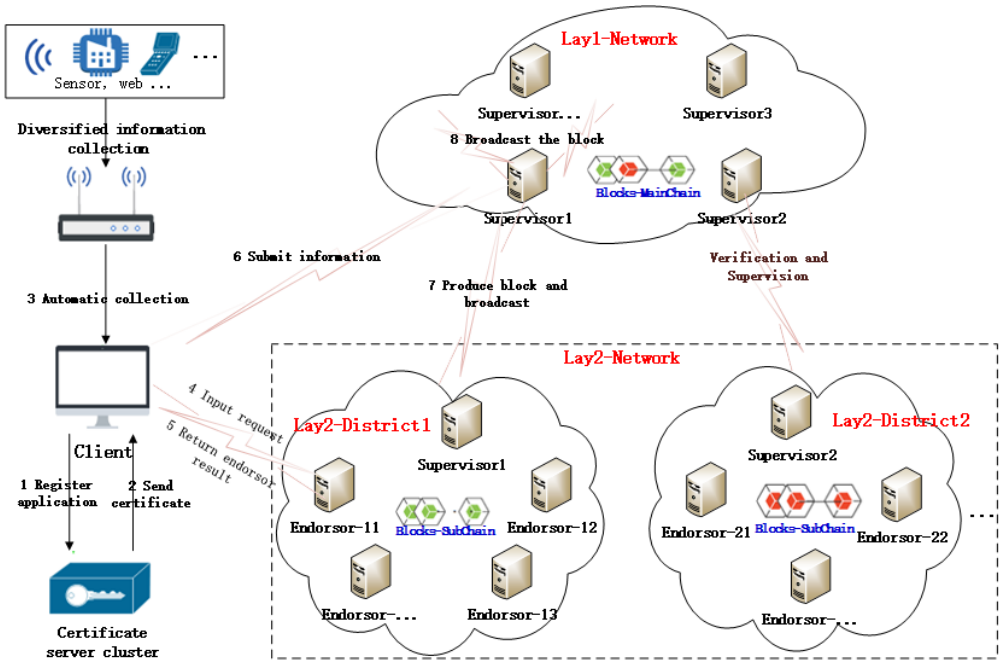

FIGURE 3. HMDBC network architecture.

algorithm by combining with Fabric underlying architecture [25]. As shown in figure 3, the whole architecture of the system includes application layer, upper-level blockchain network (Lay1-Network) and lower-layer blockchain network (Lay2-Network).

The application can support functions including customer service, Certification Authority (CA), and information collect.

The upper-level blockchain network is composed of the supervision nodes of regional elections from different regions in lower-layer network, and it can support verification of (block) transaction information, timestamp and block generation.

The lower-layer network is divided into multiple regions based on various factors (time, region, etc.), and each region constitutes a separate blockchain network system. Each region includes two types of role nodes: supervision node and endorsement node. The supervision nodes are elected by PBFT algorithm and node reputation mechanism (detailed in section B) in the region, and are responsible for recording and verifying the latest blocks. After successful recording, block information is broadcasted in the region. The endorsement node is the node responsible for verifying the digital signature of client and invoking the smart contract execution. In addition, each node within the network is responsible for recording block information into the ledger.

The combination of blockchain technology and the whole food industry chain not only overcomes many pain points in the food industry, but also changes a variety of business processes such as food information collection, food quality inspection, food supply and marketing. It also support functions as automatic information process, automatic inspection and screening of food quality in whole industrial chain. The process is as follows:

1) The CA servers provide authorization and certification function to enterprise clients, and generate the public/private key pairs and issue certificates.
2) Electronic identification technology (bar code technology, wireless sensor technology, etc.) is adopted to automatically collect data of all links of the food industry chain (quality inspection, processing data, etc.), so as to reduce the originality of human factor intervention information and avoid human error.
3) The collected information is sent to endorsor-11 of the local area network through Client.
4) Endorsor-11 verifies and filters the food information by calling the loaded intelligent contract to generate the node signature and return the endorsement result to the Client;
5) Client for signature verification, will contain the food of endorsed the result information sent to the area Supervisor1, and the Supervisor1 validate the effectiveness of food information, sorting, and generate a new block.
6) Supervisor1 packaged the food information into a new block and broadcast in the area (Lay2 - District1 and Lay1 - Network).
7) The nodes receives block, updates the ledger and synchronizes ledger in the region network. So the nodes in Lay1-Network will back up the whole Lay2-Netork data blocks.

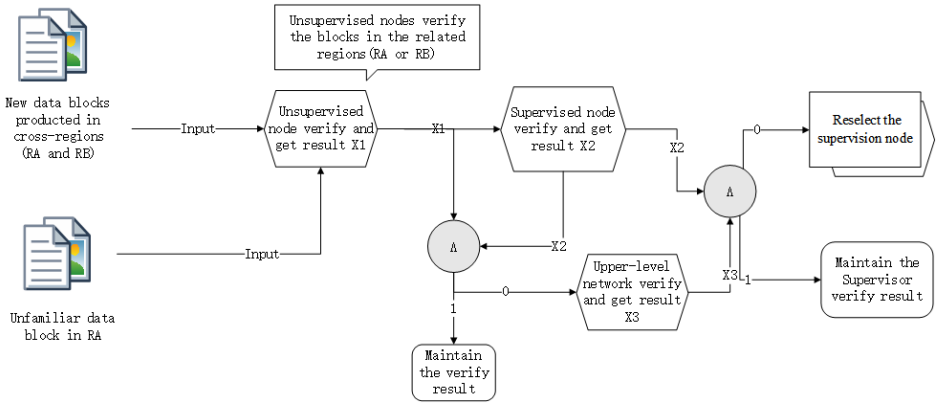

FIGURE 4. Two-level verify mechanism workflow.

TABLE 1. Comprehensive Evaluation Algorithm Analysis.

Algorithm	Features	Main Application
Fuzzy comprehensive evaluation algorithm	By using fuzzy logic, it can deal with multi-factors, fuzziness and subjective judgment problem of information system, and it has great expandability; But the determination process of subordinate function need to be further investigated.	Performance evaluation, Competitiveness evaluation, Innovative evaluation.
BP artificial neural network evaluation algorithm	With the character of self-learning, self-adaptation and nonlinear mapping, it used to deal with the complex systematic problem(nonlinear or non-locality); But slow convergence rate, low precision, local minimum problem and need huge number of samples.	Comprehensive assessment for the development level of the urban infrastructure.
Factor analysis algorithm	Comprehensiveness, objectivity and comparability; But subjective influence exists in some major arithmetic process, non-quantitative analysis and need huge number of samples.	Analysis of customer survey and market segmentation
Linear weighted sum algorithm	Comprehensiveness, quantification and used to solve multi-objective comprehensive evaluation problems; But usually use the subjective weight, poor objectivity, huge amount of computation, and it can't be used for fuzzy evaluation.	Evaluation and decision for optimizing system

Two-Level Verify Mechanism

New or unfamiliar block verification in this region is done by unsupervised nodes in Lay2-Network regions based on the PBFT algorithm, and result X1 submitted to the supervisor. Block results submitted to supervisor are properly checked and the result X2 is produced.

1) If X1 = X2, the system maintains the verified result and broadcasts it in the region.

2) It would be arbitrated by upper-level network containing the regional supervisor and determined if the monitoring node is attacked. If arbitration result equals the supervisor result, then it would maintain the supervisor result and broadcast the result in the region. Otherwise, it indicates that the supervisor abuses power or is captured, lower the evaluation level of the supervisor by one level (detailed in section B) and reselect the regional supervision node.

B. THE SUPERVISOR NODES ELECTIONS AND REPLACEMENT MECHANISMS

The PBFT algorithm is widely used by researchers [22], [36], and it is eminent that these methods do introduce the supervisor node selected sequence, thereby influencing the performance of the entire network. Few of the methods used to comprehensively evaluate node performance are mentioned in the table 1 and we proposed fuzzy comprehensive evaluation model of credibility to optimize the supervision nodes election based on the analysis of existing evaluation algorithms and actual needs.

1) COMPREHENSIVE EVALUATION MODEL OF NODE REPUTATION

We proposed the fuzzy comprehensive evaluation algorithm based on entropy weight to build the quantitative credit evaluation system of nodes in the regional network. It can contribute to reduce the human factors influence on the index weight and make the evaluation results more objective [27]–[30]. The algorithm is detailed as follows:

1) Set up the evaluation factor set There is a set of influencing factors $S = (S_1, S_2, \ldots, S_i)$ and $s_i = (s_{i1} s_{i2} s_{i3}, \ldots, s_{im})$ is the collection of different influencing factors. We analyze the key influencing factors of supervisor election in regional network:

- The hardware factors S_1 include CPU, Memory, queue buffer size and performance, etc.
- The network factors S_2 include server bandwidth, network latency, server vulnerability trace, data set backlog, etc.
- The reputation factors S_3 include the server current reputation, etc.

Thus, constructed evaluation index element set of the influencing factors:

$$S^T = (s_{i1}, s_{i2}, s_{i3}, \ldots, s_{im}) \tag{1}$$

2) Determine evaluation grade standard By combining China's network security level standards [31], and setting the evaluation grade standard to be

$$V = (v_1, v_2, v_3, v_4) \tag{2}$$

This can be used to represent (excellent, good, qualified, poor) respectively.

3) Construct fuzzy evaluation matrix Combined with the network QoS performance index change rule [32] and the change rule of equipment performance [37], we choose the normal distribution subordinate functions in fuzzy comprehensive evaluation model, which can screen out more information with low membership degree [38]. In terms of the 3σ criterion, we choose 6σ as the domain of the subordinate function. Combined with the features of λ level set, so the subordinate function for evaluation grade standard v_i is:

$$p_1 = \begin{cases} 0 & x \le v_1 \\ 1 - e^{\left(-\frac{1}{2\delta_1^2}(x-v_1)^2\right)} & v_4 > x > v_1, \quad \sigma_1 = \dfrac{v_2 - v_1}{3} \end{cases} \tag{3}$$

$$p_2 = \begin{cases} 1 - e^{\left(-\frac{1}{2\delta_{20}^2}(v_2-x)^2\right)} & v_1 \le x \le v_2, \ \sigma_{20} = \dfrac{v_2 - v_1}{3} \\ 1 - e^{\left(-\frac{1}{2\delta_{21}^2}(x-v_2)^2\right)} & v_4 \ge x > v_2, \ \sigma_{21} = \dfrac{v_4 - v_2}{3} \end{cases} \tag{4}$$

$$p_3 = \begin{cases} 1 - e^{\left(-\frac{1}{2\delta_{30}^2}(v_3-x)^2\right)} & v_2 \le x \le v_3, \ \sigma_{30} = \dfrac{v_3 - v_2}{3} \\ 1 - e^{\left(-\frac{1}{2\delta_{31}^2}(x-v_3)^2\right)} & v_4 \ge x > v_3, \ \sigma_{31} = \dfrac{v_4 - v_3}{3} \end{cases} \tag{5}$$

$$p_4 = \begin{cases} 1 - e^{\left(-\frac{1}{2\delta_4^2}(x-v_1)^2\right)} & v_4 > x > v_1 \\ 1 & x \ge v_4, \quad \sigma_4 = \dfrac{v_4 - v_3}{3} \end{cases} \tag{6}$$

We can get the subordinate functions set $P_{ij} = [p_{i1}\ p_{i2}\ p_{i3}\ p_{i4}]$, the normalized process P_i, get the result $R_i = [r_{i1}\ r_{i2}\ r_{i3}\ r_{i4}]$, and

$$r_{ij} = \frac{p_{ij}}{\sum_{j=1}^{4} p_{ij}} (0 \le r_{ij} \le 1).$$

4) Calculate the weight of index influencing element ii
Using it standardized process with the index element among the influencing factors $Y_{ij} = \frac{(s_{ij} - \min(s_i))}{(\max(s_i) - \min(S_i))}$ where the expert score, and compute i influencing factor's weight:

$$w_i = \frac{1 - E_i}{k - \sum_{i=1}^{k} E_i}, \quad \text{and } E_i = -\frac{\sum_{j=1}^{m} \gamma_{ij} \ln \gamma_{ij}}{\ln m},$$
$$\gamma_{ij} = \frac{Y_{ij}}{\sum_{i=1}^{m} Y_{ij}}.$$

5) Calculate the comprehensive evaluation index of node reputation
Constructed the fuzzy comprehensive evaluation matrix of reputation to be $Z = W^*R = [w_1 w_{2\ldots} w_i]^* \begin{bmatrix} r_{11} & \cdots & r_{14} \\ \vdots & \ddots & \vdots \\ r_{i1} & \cdots & r_{i4} \end{bmatrix}$ and then compute the comprehensive evaluation index of node reputation, given as $CER = Z^* V^T$.
Each node calculates the credibility CER and broadcasts in its own region. According to the CER magnitude of the node in the regional network, the maximum value of the CER is selected as the regional supervisor, and the information of the new supervision node is broadcasted to the upper-level network nodes.

C. THE DATA BLOCK STRUCTURE

To meet the needs of HMDBC network, the block structure model design is shown in Figure 5 below, with detail of each element in the block.

The Version Number is used to save version information for this block. The Front Block Hash is used to save the hash value of the previous block and lead the blocks to chain order by the timestamp. The Time Stamp is used to store the block generation time and the Hierarchy mark stores the hierarchy information about the block generated. The Merkle Root is hash value by the layer-by-layer hashing of records.

Support the supervisor nodes replacement

Assume that the honest node can elect the best reputation node as the supervisor. When the new supervisor is elected, the blockchain network will perform the following steps:

1) The local region information updates (Fig.3 Lay2-Network): The new supervisor gets the former supervisor information from the latest block, and sends the verification information to it. The former supervisor receives and verifies the information and then actively pushes the outer region of data blocks to the new supervisor who is lacking.

2) The superior region information update: At the same time, the new supervisor sends a request to neighbor node in the supervisor node network (Fig.3 Lay1-Network), which

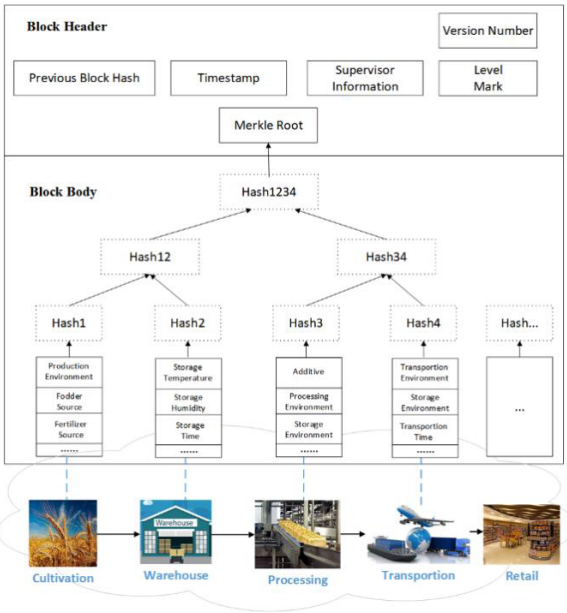

FIGURE 5. The block structure model.

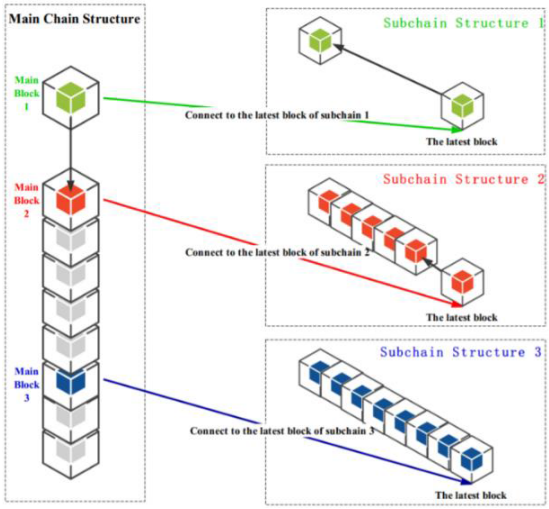

FIGURE 6. The main-subchain structure.

includes block synchronization information, node authentication information and time stamp T. After the request is received and the identity verified, the neighbor node records it and actively synchronizes all data blocks that the time stamp T have received so far.

So after update finish, the new supervisor node will get the full information.

D. THE MAIN-SUBCHAIN STRUCTURE

The key to food safety supervision is the effective traceability of food information in the whole industry chain, and the chain structure of blockchain would affect this traceability performance. In view of the contradiction between full backup and storage capacity of blockchain, we proposed a main-sub chain structure (as shown in Figure 6), which includes a main chain, and multiple sub chain structures. The Front Block Hash in the main chain blocks includes the previous block hash and the latest block hash of the Subchain. Each region has an independent Subchain.

When a new region is established or a Subchain generates a new data block, the main chain will generate a block and point to the end of the sub-chain. Compared with the traditional single-chain architecture, the main-Subchain architecture has significant advantages in terms of information traceability and storage capacity. It can satisfy the society requirement of cross-regional (department, enterprise, etc.) supervision and reduce audit costs. The tamper-proof feature protects the reliability of information and ensures the accuracy and integrity of traceability information.

E. INTELLIGENT SUPERVISION

Smart contract is an intelligent, self-executing logic code without third-party intervention. The smart contract can automatically execute the agreement between the two parties without the participation of any intermediary, thereby eliminating transaction costs. Multi-nodes automatically execute and generate endorsements based on pre-established smart contracts. Only when the endorsement results of multi-node transactions are consistent, can data be added to the

Protocal 1 Autodetect Whether Food Additive/Main Heavy Metal Content Satisfy for the National Food Standards

Input : Food information
Output: Success or Alarm

```
1 : function Verify(Food_Information)
2:   Feedback<-null
3:   if Food_Information.additive> standard.additive then
4:     Feedback<-"Additive Error\n"
5:   end lf
6:   if Food_Infonnation.metalcontent> standard.
      metalcontent then
7:   Feedback<- Feedback +"metal content overproof
      Error\n"
8:   end if
9:   if Food_Information.temperature> standard.
      temperature then
10:     Feedback<- Feed back +"temperature Error\n"
11:  end if
12:  if Feedback==null then
13:     writeblockchain(Food_Information)
14:     Authorize(nextstep)
15:     return true
16:  else
17:     writeblockchain(false)
18:     alarm(Feedback )
19:     return false
20:  end if
21: End function
```

TABLE 2. Performance comparison of POW and PBFT.

	POW	PBFT
Throughput	Bitcoin：7TPS, 1 block/10 min Ethereum：20-30TPS，1 block/12-15 sec	200-2000TPS (Fabric 0.6)
Cost of Transaction Confirmation	Bitcoin：60min,Ethereum：3min	Millisecond level
Fault Tolerance	<50% computing power	<33% untrusted nodes
Resource Consumption	Hash computing	Broadcast

blockchain. Smart contract is written in accordance with national food additive targets and quality standards. Smart contract automatically inspects and screens food processing materials, and those that do not meet the national food standards will be rejected. This approach ensures limited occurrence of food safety accidents from the source, and makes up for the defects of manual inspection.

The Smart contract case protocol 1 shows that it can be used to automatically detect whether food additive/main, heavy metal, and content information satisfies the national food standards.

IV. ANALYSIS

A. SECURITY ANALYSIS

We proposed a HDMBC network food safety supervision model. Based on the PBFT consensus algorithm, the regional node consensus verification is implemented and each region can still validate the data block consensus when no more than 33% of the untrusted nodes exist. This paper proposed the Two-Level Verification Mechanism and Arbitration scheme to enhance the accuracy of block verification achieve the regulation of supervisor and timely discover the supervisor's abused power. Its objective is the fair election of reliable supervisory nodes in a region, with the comprehensive evaluation model of node reputation. Established smart contracts based on the national food industry standards can automatically screen out substandard circulating products in the whole industrial chain and give warnings to ensure food quality and safety in the industrial chain.

B. PERFORMANCE ANALYSIS

From our compared and analyzed performance of PBFT algorithm with the POW consensus algorithm, performance results are as shown in table 2 [43]–[45].

As shown in table 2, the bottleneck of PBFT efficiency is broadcast consumption. We proposed a hierarchical domain design scheme, assuming that the network hierarchy is n, each layer has m regions, each region contains x nodes, and all nodes under the condition of no transmission losses, so our scheme's blocks broadcast validation complexity is $O(m^2 + x^2)$, but the Fabric 0.6 block consensus broadcast complexity $O(m^2x^2)$ with all nodes Shared the same domain. Our scheme thus shows higher throughput efficiency.

V. CONCLUSION AND FUTURE WORK

This paper proposed HMDBC network architecture and the Two-Level Verification Mechanism. It can supervise the regional supervision nodes, correct the errors and replace the supervision nodes in time if the supervision nodes abuse power or have been attacked, achieve protect the system security and improve the overall performance. It can tolerate no more than 33% broken nodes. The comprehensive reputation evaluation model is proposed to evaluate the credit of nodes and ensure the reliability of regional nodes. The smart contract design is used to auto-detect whether or not the transportation product satisfies the national food standard. The comparison analysis demonstrates the performance and the cost of this system reduced to $1/m2$.

Future research will explore optimizing the performance of the proposed system via implementation using in a real-world setting.

ACKNOWLEDGEMENTS

The authors would like to thank anonymous reviewers and the Editor for their valuable comments which helped them to improve the quality and presentation of this paper.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[3] W.-T. Tsai, E. Deng, X. Ding, and J. Li, "Application of blockchain to trade clearing," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Lisbon, Portugal, Jul. 2018, pp. 154–163.

[4] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[5] I. Mohiuddin, A. Almogren, M. Al Qurishi, M. M. Hassan, I. Al Rassan, and G. Fortino, "Secure distributed adaptive bin packing algorithm for cloud storage," *Future Gener. Comput. Syst.*, vol. 90, pp. 307–316, Jan. 2019.

[6] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Singapore, Dec. 2017, pp. 1357–1361.

[7] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Jun. 2016, pp. 1–6.

[8] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Future Internet*, vol. 9, no. 3, p. 25, 2017.

[9] M. Andoni *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[10] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2663–2668.

[11] P. Rafael and S. Elaine, "FruitChains: A fair blockchain," in *Proc. ACM Symp. Princ. Distrib. Comput. (PODC)*, New York, NY, USA, 2017, pp. 315–324.

[12] W. D. Cai *et al.*, "Research on development method of application system based on blockchain," *J. Softw.*, vol. 28, no. 6, pp. 1474–1487, 2017.

[13] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Inform.*, vol. 35, no. 8, pp. 2337–2354, 2018.

[14] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.

[15] C. Plaza, J. Gil, F. de Chezelles, and K. A. Strang, "Distributed solar self-consumption and blockchain solar energy exchanges on the public grid within an energy community," in *Proc. IEEE Int. Conf. Environ. Elect. Eng., IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Eur.)*, Palermo, Italy, Jun. 2018, pp. 1–4.

[16] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for eHealth data access management," in *Proc. 4th Int. Conf. Adv. Biomed. Eng. (ICABME)*, Beirut, Lebanon, Oct. 2017, pp. 1–4.

[17] D. Tosh *et al.*, "CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, San Francisco, CA, USA, Jul. 2018, pp. 302–309.

[18] M. Castro, "Practical byzantine fault tolerance and proactive recovery," in *Proc. Symp. Oper. Syst. Design Implement.* Berkeley, CA, USA: USENIX Association, 1999, pp. 173–186.

[19] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[20] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 1992, pp. 139–147.

[21] I. Bentov, R. Pass, and E. Shi. (2016). Snow white: Provably secure proofs of stake. IACR Cryptol. ePrint Arch. [Online]. Available: http://eprint.iacr.org/2016/919

[22] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. 3rd USENIX Symp. Oper. Syst. Design Implement. (OSDI)*, New Orleans, LA, USA, 1999, pp. 173–186.

[23] B. Christian and P. R. Hans, "Scaling Byzantine consensus: A broad analysis," in *Proc. 2nd Workshop Scalable Resilient Infrastruct. Distrib. Ledgers (SERIAL)*, New York, NY, USA, 2018, pp. 13–18.

[24] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Changshu, China, Jun. 2018, pp. 280–285.

[25] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, 2016. [Online]. Available: https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf

[26] Z. J. Wang *et al.*, "Research on deterministic delay calculus theory of control network," *J. Electron.*, vol. 34, no. 2, pp. 380–384, 2006.

[27] H. J. Wu *et al.*, "Research on fuzzy comprehensive evaluation model of network public opinion early warning based on entropy weight method," *Inf. Sci.*, vol. 36, no. 7, pp. 58–61, 2018.

[28] G. F. Wang and M. Li, "Research on public opinion early warning model of mobile social network based on AHP-fuzzy comprehensive analysis," *J. Mod. Inf.*, vol. 37, no. 1, pp. 41–44, 2017.

[29] F. Y. Nie and Y. Zhang, "Construction of public opinion early warning index system for mobile social networks," *Inf. Stud., Theory Appl.*, vol. 38, no. 12, pp. 64–67, 2015.

[30] Q. Y. Cheng, "Structural entropy weight method for determining weights of evaluation indicators," *Syst. Eng. Theory Pract.*, vol. 7, pp. 1225–1228, 2010.

[31] *National General Emergency Plan for Public Emergencies*, State Council, China Legal Publishing House, Beijing, China, 2006.

[32] L. Qinghua *et al.*, "Deterministic upper bounds on QoS performance about wireless ad hoc network based on network calculus," *J. Commun.*, no. 9, pp. 32–39, 2008.

[33] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: How to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, pp. 283–287, Feb. 2001.

[34] C. Burger, A. Kuhlmann, P. Richard, and J. Weinmann, "Blockchain in the energy transition,"İ in *A Survey Among Decision-Makers in the German Energy Industry*. Berlin, Germany: DENA German Energy Agency, 2016.

[35] H. J. Sun, "Analysis on agricultural products cold chain logistics," *Logistics Technol.*, vol. 28, no. 3, pp. 158–159, 2009.

[36] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya. (2018). "YAC: BFT consensus algorithm for blockchain." [Online]. Available: https://arxiv.org/abs/1809.00554

[37] J. Wu, Z.-X. Cai, C.-C. Hu, and J.-D. Cao "Status evaluation of protective relays based on the membership function in fuzzy normal distribution," *Power Syst. Protection Control*, vol. 40, no. 5, pp. 48–52, 2012.

[38] P. Z. Wang and H. X. Li, *Fuzzy Systems Theory and Its Applications*, 1st ed. Beijing, China: Science Press, 1996, pp. 92–128.

[39] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, "Big data meet cyber-physical systems: A panoramic survey," *IEEE Access*, vol. 6, pp. 73603–73636, 2018.

[40] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2389–2406, 3rd Quart., 2018.

[41] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Big data toward green applications," *IEEE Systems J.*, vol. 10, no. 3, pp. 888–900, Sep. 2016.

[42] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 1, pp. 49–54, 2017.

[43] R. Wattenhofer, *The Science of the Blockchain*, 1st ed. Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2016, pp. 5–37.

[44] Y. Yuan *et al.*, "Blockchain consensus algorithms: The state of the art and future trends," *Acta Automatica Sinica*, vol. 44, no. 11, pp. 2011–2022, 2008.

[45] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data (SIGMOD)*, Chicago, IL, USA, 2017, pp. 1085–1100.

[46] L. B. Yang and Y. Y. Gao, *Fuzzy Mathematics: Principles and Applications*, 4nd ed. Guangzhou, China: South China University of Technology Press, 2006, pp. 3–22.

[47] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Greening big data," *IEEE Syst. J.*, vol. 10, no. 3, pp. 873–887, Sep. 2016.

QI TAO received the master's degrees from the School of Computer Science and Technology, Southwest University of Science and Technology, in 2016. He is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Wuhan University. His research interests include information security, blockchain technology, and food safety.

XIAOHUI CUI received the Ph.D. degree in computer science and engineering from the University of Louisville, Louisville, KY, USA, in 2004. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University. His main research interests include big data, cluster intelligence theory, blockchain technology, food safety, and high-performance computing.

XIAOFANG HUANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2010. She is currently a Professor with the School of Computer Science and Technology, Southwest University of Science and Technology, China. Her main research interests include information security, cloud computing, and blockchain technology. She got the information Security Leading Talent Award of the District Level, in 2015.

ANGELLA M. LEIGH received the bachelor's degree in electrical and electronics engineering from the Fourah Bay College, University of Sierra Leone, in 2013. She is currently pursuing the master's degree with the School of Cyber Science and Engineering, Wuhan University. Her current research interests include blockchain technology provided solution to challenges faced in civil registration, and intellectual property systems in Africa.

HEHE GU received the B.S. degree from Nantong University, in 2018. He is currently pursuing the M.S. degree with Wuhan University, China. His research interests include information security, cryptographic algorithm, and blockchain.