IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 September 2023, accepted 26 October 2023, date of publication 1 November 2023,
date of current version 7 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3329126

RESEARCH ARTICLE

Blockchain-Based Multidimensional Trust Management in Edge Computing

YAN WANG[1] AND ZENAN WU[2]
[1]Institute of Robotics, Ningbo University of Technology, Ningbo 315211, China
[2]College of Computer Science, Zhongyuan University of Technology, Zhengzhou 450007, China

Corresponding author: Zenan Wu (rayoo0127@sina.com)

This work was supported by the Open Fund of Key Laboratory of Flight Techniques and Flight Safety, CAAC, under Grant FZ2022KF17.

ABSTRACT Due to the resource limitations of Internet of Things (IoT) terminals and the distributed characteristics of edge computing architecture, trustworthy services management in dynamic edge computing is a very large challenge. A general and extensible blockchain-based multidimensional trust management (BMDTM) model suitable for edge computing is proposed in this paper. First, probabilistic linguistic terms sets (PLTSs) are adopted as a trust scaling method to integrate the multicriteria evaluation data of the whole domain to measure the performance of the service provider, and the stability degree of each attribute performance is calculated based on information entropy theory, which enables us to measure the dynamic performance accurately and precisely. Second, the dual characteristic of the associated criteria is utilized to filter out malicious or unprofessional evaluation information of requesting nodes and avoid malicious user collusion, ensuring the credibility of trust management. Third, blockchain technology and smart contracts (SCs) are adopted to store trust evidence, share trust information across domains, and execute multisource trust fusion automatically, avoiding the problems of information opacity and the single point of failure of the traditional centralized trust model. The experimental results demonstrate that our model can well manage trust problems in a dynamically hostile edge computing environment. The first finding is that the introduction of the domain trust value significantly improves the quality of service (QoS) compliance ratio due to an accurate description of the dynamic performance of services. The second finding is that our model performs better in attack resistance by leveraging blockchain technology and the dual characteristic of the associated criteria.

INDEX TERMS Blockchain, edge computing, trust evaluation, smart contract, probabilistic linguistic terms set.

I. INTRODUCTION

In the era of 5Ga and with the rapid development of IoT technology, the number of terminal devices has sharply increased, and the types have also become diversified, reflecting the characteristics of great dispersion [1]. The application of cloud computing technology to the IoT inevitably leads to service delays and potential concentration risk. To solve these issues, edge computing is proposed as a new paradigm, where the processing is completed at the local edge computing layer without handing over to the cloud [2]. This will undoubtedly greatly ameliorate the processing efficiency and alleviate the load on the cloud. However, the security protection measures of edge computing are not as strong as those of cloud computing, increasing the security risk and privacy exposure of access terminal nodes [3]. Therefore, trust management in edge computing has become a key focus to achieving a secure and trusted resource-sharing computing environment, and is also the critical factor to promote edge computing from concept to application [4].

The existing trust evaluation model [5], [6], [7], [8] can be divided into centralized and decentralized models. In the decentralized trust evaluation mechanism, terminal devices evaluate the trust value of the nodes they interact with, increasing the burden on resource-constrained nodes. The centralized trust management model usually relies on a third-party trust management center to assess and store the trust value of end nodes in the whole network, which may

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

lead to delay, congestion, and even a single point of failure. In addition, the evidence of trust is not open to all users, and trust evaluation results are not fully trusted by all participants due to a lack of transparency and traceability in a centralized trust framework. To circumvent this issue, blockchain, as a new distributed computing paradigm, provides a completely decentralized platform, which provides tamper-proof, verifiable, and traceable functions [9], [10]. For example, distributed storage can help persistently record user behaviors, encryption/decryption algorithms can help protect user privacy data and ensure data ownership, and the SC mechanism can help realize various automatic evaluation and authentication services. However, blockchain integrated with the SC can only ensure the security, autonomy, and integrity of the data on the chain executed by the business logic defined in the SC, and it cannot guarantee the QoS performance of the target service providers [11]. In the edge computing environment, the terminal node can request low-latency services from service providers in the vicinity [12]. Nevertheless, service providers may not maintain committed QoS due to various factors, such as dynamic network environment, service cost, energy usage, application characteristics, and malicious behavior of other entities. Thus, it is essential to construct a multifaceted trust evaluation model based on blockchain, specifically, the trustworthiness of a service provider can be evaluated on various facets, such as QoS, competence, integrity, honesty, and benevolence.

Due to the resource restrictions of terminal nodes and the dynamics of the network environment, trust management in edge computing is not well implemented [13], [14], [15]. The authors in [16], [17], and [18] proposed novel trust evaluation methods suitable for the IoT edge computing environment, but they did not measure the dynamic performance of the service providers, so they cannot accurately evaluate the trust value of the service providers. The researchers in [19] utilize probabilistic linguistic elements (PLEs) to measure the overall performance of the trustee, which is a very suitable tool to depict the trustor's feedback information when they are uncertain about their judgments and prefer to describe their evaluation information using several linguistic terms with corresponding probability. We adopt the PLTS method to integrate the evaluation data of the requesting nodes in each domain, which utilize the linguistic terms with the corresponding probability to measure the dynamic performance of the service provider in each domain. Many researchers have proposed a blockchain-based trust evaluation model in the IoT or vehicular environment, where the trust value corresponds to a binary experience, (i.e., either positive or negative), which may produce unrealistic and inaccurate results in many instances, ad does not account for the dynamic network environment [20], [21], [22]. Therefore, building a multidimensional trust evaluation model suitable for the dynamic edge computing environment is a huge challenge under the condition of accurate trust requirements and resource constraints, which is of great significance for risk prevention, service selection, recommendation, and decision-making.

In the edge computing environment, different types of services lead to the diversity of evaluation attributes, which is a huge workload to build a trust evaluation model covering multiple attributes. To fulfill these challenges, the terminal nodes with similar locations are divided into a domain, and the domain is taken as a whole to evaluate the trust value of the service provider in the BMDTM framework. Each domain selects a node with strong resource capability as the domain administrator (DA), who is responsible for collecting subjective and objective feedback information from the requesting nodes within the domain, and then converts them into a vector of PLEs that simultaneously considers the qualitative variables and their distribution property. On this basis, we calculate the corresponding performance degree and stability degree, which can better reflect the dynamics and uncertainty of service performance. Then, the trust value of the service provider in each domain is fused to obtain the reputation value. Four different SCs on the blockchain are employed in the BMDTM framework: (1) identity registration smart contract (IRSC), (2) QoS capability smart contract (QCSC), (3) reputation evaluation smart contract (RESC), and (4) data integrity smart contract (DISC) for storing identity information and QoS capabilities and realizing automatic calculation of reputation value and verification of data integrity. In addition, the concept of associated criteria that possess dual characteristics is introduced for filtering malicious subjective feedback of the requesting nodes to avoid inaccurate results caused by malicious user collusion.

Due to the accuracy requirement of trust assessment, insufficient security protection of edge nodes, limited resources of terminal nodes, and dynamic instability of a large-scale network environment, this paper studies the optimization problem suitable for the actual constraints in an edge computing environment, focusing on the realization of an accurate, lightweight, traceable and tamper-proof multidimensional trust evaluation optimization model.

The main contributions of the proposed model are as follows:

- BMDTM takes the domain as a whole to evaluate the service provider, and the trust evidence data collection, processing, and fusing are handed over to each DA to ensure accuracy and reduce the workload of the terminal nodes.
- The dual characteristic of associated attributes is employed to filter out malicious or nonprofessional evaluation information and avoid malicious user collusion. Furthermore, each DA endows each attribute weight according to the attribute feedback proportion of users within the domain to accurately reflect the performance of the service provider.
- Measuring the trust of service providers in terms of performance degree and stability degree, and adopting PLTS as a trust scaling method enabled measuring the dynamic performance of the service providers in the whole domain.

•Four different smart contracts are introduced to store the trust data and related evidence data, and multisource trust fusion is executed automatically.

The remainder of this paper is organized as follows: Section II outlines works related to trust management. Section III introduces essential knowledge and system design. Section IV provides a detailed introduction to our proposed trust management based on blockchain technology. Section V provides technical solutions and implementation, and verifies the effectiveness and accuracy of our proposed model. Section VI provides a general summary of the whole paper.

II. RELATED WORKS

This section reviews existing works on trust management in the edge computing environment and blockchain-based trust management framework.

A. TRUST SYSTEM IN EDGE COMPUTING

Edge computing aims to provide services in a trustless environment, where neither party can be fully trusted [23]. Obviously, this faces complex security and trust issues. End users may communicate with dishonest or malicious nodes. Under this circumstance, trust becomes crucial because it facilitates subsequent service selection and decision-making. Owing to the mobility and resource-constrained characteristics of terminal nodes, it is very difficult to evaluate trust accurately and establish trust relationships among nodes in the IoT edge computing environment. The authors in [24] proposed an architecture pattern that supports trusted orchestration for edge clouds which describes the basic processing of choreography activities and is supported by blockchain to achieve trusted choreography management. The architecture coordinates communication between sensors and cloud services by introducing fog and edge architecture, and addresses the data from sensors and clouds. The authors in [5] noted that cloud computing cannot provide effective and direct management for end nodes due to the relatively large distance between them. In addition, we presented a trust evaluation model based on trust transitivity on a chain assisted by mobile edge nodes, which can ensure the reliability of nodes in the IoT and resist malicious attacks. The authors in [18] proposed a reputation-based trust evaluation management method in mobile edge computing networks, which combines identity trust, capability trust, and behavior trust to ensure that the edge nodes that join the network system for service interaction are qualified, capable, and reliable. The authors in [13] considered the (QoE) of requesting nodes to optimize the edge computing system, and realized the indicator mapping from QoS to QoE, Meanwhile, they presented that the comprehensive trust evaluation system should include the identity trust, behavior trust, and capability trust to support resource sharing and scheduling. The researchers in [25] proposed a trust evaluation model suitable for the edge computing environment in which the complex and huge trust relationship between edge devices was abstracted into a directed weighted graph. However, it cannot perform accurate multiple attribute evaluation and does not solve the problem of node load balancing. Therefore, trust evaluation optimization issues suitable for the actual constraints in the edge computing environment are studied in this paper.

B. BLOCKCHAIN-BASED TRUST MANAGEMENT FRAMEWORK

In the trust evaluation model of edge computing, there is a lack of a centralized party to perform information collection, data aggregation, and trust calculation. For this reason, trust evaluation in edge computing should be conducted in a decentralized way without relying on any trusted parties. The authors in [26] proposed an AI-enabled trust management system for vehicular networks using the blockchain technique, which utilized a deep learning method to evaluate the trust of nodes (including both vehicles and roadside units (RSUs)) as well as data (such as messages) automatically and dynamically, and applied blockchain technology to ensure that both the identity of both vehicles and RSUs and the authenticity of messages sent in the vehicular networks could be validated, thereby remarkably enhancing the security of vehicular networks. The authors in [21] presented a novel distributed trust management mechanism combining the advantages of active detection and blockchain. Active detection can filter the surrounding malicious nodes, and blockchain technology can ensure the consistency of trust data in different regions. The authors in [27] noted that trust awareness can reduce the risk of violating QoS, improve the confidence in operating QoS across multiple domains, develop QoS compliance verification and trust quantification mechanisms, and efficiently leverage the tamper-proof and decentralized properties of blockchain to store and exchange different kinds of trust information required to provision and verify E2E QoS compliance of the domains.

Therefore, blockchain has emerged as a new and promising technology that will change the way we share information. Its unique features regarding operating rules and traceability of records ensure the integrity, undeniability, and security of transaction data. The security of blockchain mainly relies on a consensus mechanism rather than the trust of the centralized party. With the motivation to address the above-discussed problem, the specific objective of this work is to present an accurate blockchain-based trust evaluation model suitable for the edge computing environment.

III. PRELIMINARIES AND SYSTEM DESIGN

A. PRELIMINARIES

The definitions of probabilistic linguistic term set (PLTS) are shown as follows.

Definition 1 ([28]): Let $S = \{s_\alpha | \alpha = 1, 2, \ldots, \tau\}$ be a linguistic term set (LTS). A PLTS is defined as: $L(p) = \left\{ s^l(p^l) | s^l \in S, p^l \geq 0, l = 1, \ldots, \#L(p), \sum_{l=1}^{\#L(p)} p^l \leq 1 \right\}$, where $s^l\left(p^l\right)$ is the linguistic term s^l associated with the probability p^l, and $\#L\,(p)$ is the number of all the different

linguistic terms in $L(p)$. For convenience, $L(p)$ is also called the probabilistic linguistic element (PLE).

Definition 2 ([28]): $S = \{s_\alpha \,|\, \alpha = 1, 2, \cdots, \tau\}$ be an LTS, for a PLTS $L(p) = \{s^l(p^{(l)})|s^l \in S, l = 1, ..\#L(p)$,the expected value function of $L(p)$ is

$$E(L(p)) = \sum_{l=1}^{\#L(p)} \left(\frac{f^l}{\tau} p^{(l)}\right) \Big/ \sum_{l}^{\#L(p)} p^{(l)} \qquad (1)$$

where f^l is the subscript of the linguistic term s^l.

Definition 3: Trust value is a metric that measures the trust of the service provider in each domain by verifying its objective QoS compliance and other subjective attribute performance.

Definition 4: Reputation value is an overall measure of the service performance of a service provider, which denotes a weighted sum of the service provider's trust value in each domain.

B. SYSTEM DESIGN

1) BLOCKCHAIN HIERARCHICAL STRUCTURE

Considering a distributed IoT edge computing architecture, there are many terminal devices and a limited number of edge servers. Nodes communicate with each other through overlay network protocols or underlying network protocols. In addition, multiple domains are defined based on geographic location. As shown in Figure 1, the BMDTM framework mainly consists of two layers, namely, the edge server layer and the domain node layer, including four elements (i.e., edge servers, domain nodes, domain administrator, and blockchain). The role of each component is described below.

a: DOMAIN NODES

also known as requesting nodes, refer to fixed or mobile nodes that request services within a certain domain. Due to resource restrictions, these domain nodes act as the clients of the blockchain. Each domain node is equipped with monitoring devices that can monitor the actual performance of service providers during the interaction process. After interactions, the domain node provides the subjective feedback ratings and monitored QoS performance of the service provider to the DA, and submits the corresponding digests to blockchain for storage and verification.

b: DOMAIN ADMINISTRATOR (DA)

refers to a fixed node in the domain that has strong computing power and storage capacity. As the administrator of the whole domain, it periodically collects the feedback information and objective QoS value within the domain, then handles this information and submits it to the blockchain for further processing. It also acts as the full node of the blockchain, responsible for mining blocks and maintaining the normal operation of the blockchain. It is assumed that each DA is a trusted authority in this paper.

c: EDGE SERVERS

also known as service providers. Oftentimes, these servers are located at the edge of the network, which can provide services to other requesting nodes. Meanwhile, they are responsible for submitting QoS capabilities negotiated with the requesting node to the QCSC and the corresponding hash value to the DISC.

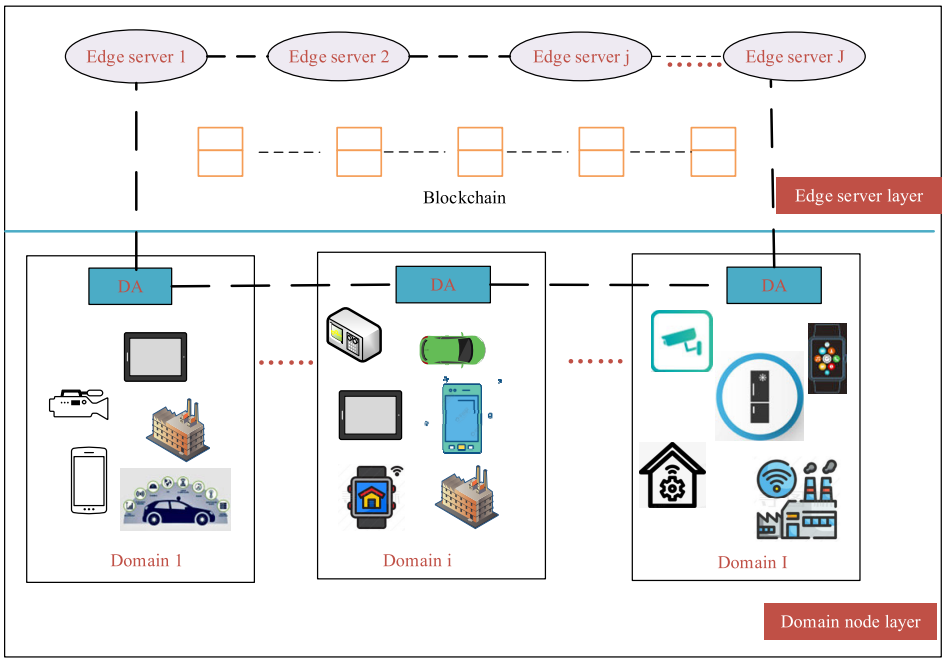

FIGURE 1. The system architecture.

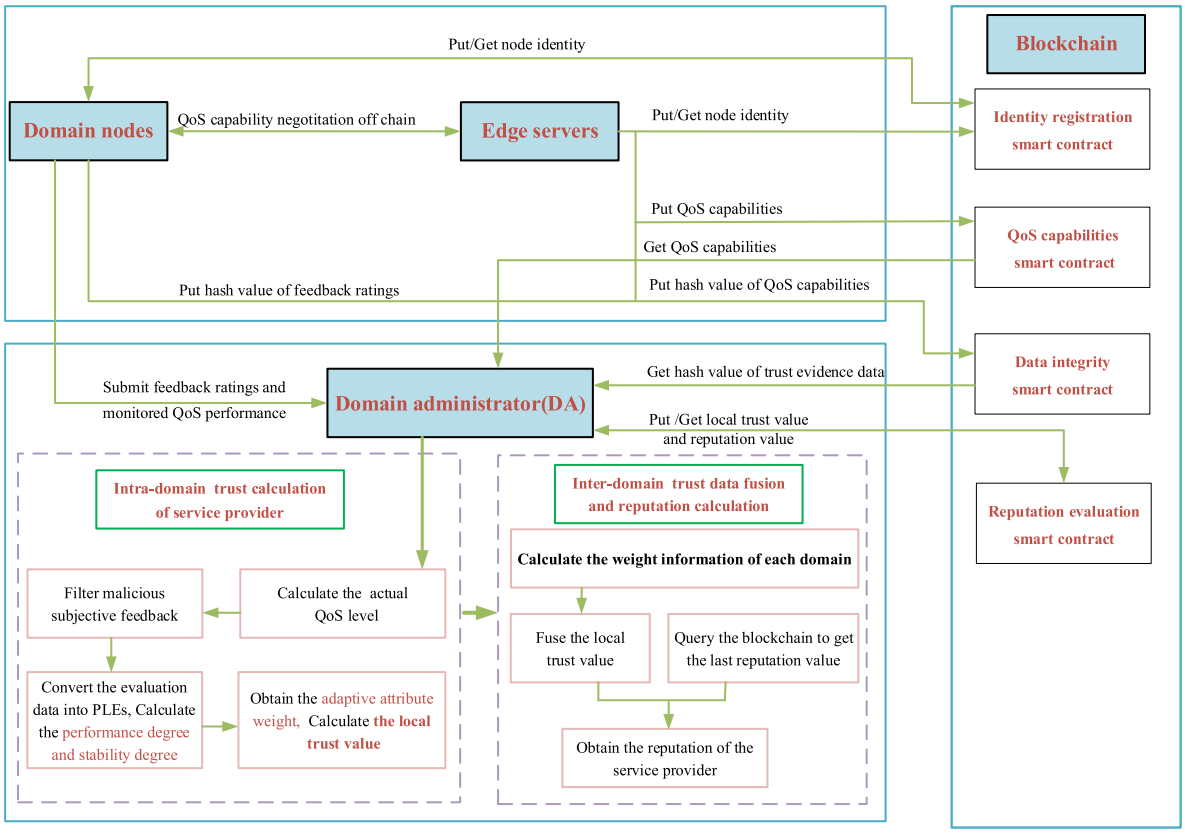

FIGURE 2. The BMDTM framework.

d: BLOCKCHAIN

blockchain possesses the advantages of high security and reliability due to its consensus mechanism and identical distributed-storage copies, and has been extensively studied and deployed. Blockchain is leveraged to achieving the functions such as identity registration, QoS capabilities, automated evaluation, calculation and storage of reputation value, and data integrity verification.

2) HIGH-LEVEL ARCHITECTURE OF BMDTM

The BMDTM framework is shown in Figure 2. Trust management of BMDTM is divided into two sub-modules, one is **intra-domain trust evaluation**, consisting of performance degree and stability degree calculation, and the other is **inter-domain trust data fusion and reputation evaluation**.

Specifically, we fuse the trust value of the service provider in each domain in the hth time window $T^h(i,j),(i = 1,\cdots,I)$, query the blockchain to obtain the reputation value R_j^{h-1}, and subsequently calculate the reputation value R_j^h. The details of the major functionalities of BMDTM are illustrated as follows:

Local Trust Calculation: Each DA adopts probabilistic linguistic term sets (PLTS) as a trust scaling method to integrate multicriteria evaluation data of all requesting nodes in the domain, which enables evaluation from two perspectives: performance degree and stability degree. The attribute weight is set based on the preference of user feedback attributes in the domain. Then, we obtain the local trust value of the service provider in the current time window.

Reputation Calculation: The local trust value of the service provider in the current time window is aggregated. It is worth noting that the weight of each domain is positively related to the number of interactions of the service provider in the domain. Then, the blockchain is queried to obtain the reputation value of the service provider in the last time window and they are aggregated to obtain the reputation value of the service provider in the current time window.

Trust Evidence Data Storage and Verification: The requesting node submits the subjective feedback ratings and monitored QoS performance of the service provider to the DA after interactions and submits the corresponding hash value signed with its private key to the DISC to avoid malicious DA tampering. The service provider submits the QoS capabilities to the QCSC and submits the corresponding hash value signed with its private key to the DISC.

Identity Registration: When the fixed or mobile node in the domain requests service for the first time, it needs to call the IRSC to implement node identity registration, node address, and public key distribution, and determines which domain the node belongs to.

TABLE 1. Symbol definition.

Symbol	Definition	Symbol	Definition
es_j	The jth edge server	dm_i	The ith domain
s^l	Feedback rating s^l	p^l	The proportion of s^l to all feedback ratings in the whole domain
ω_q^h	The weight of the qth attribute in the hth time window	$i(k)$	The kth node in dm_i
δ_i^h	The weight of dm_i in the reputation calculation in the hth time window	V_q	The actual QoS level of the qth attribute
Q_q^m	Monitored QoS value of the qth attribute	Q_q^c	The promised QoS value of the qth attribute
$ap^h(i,j)$	Attribute performance vector of es_jin dm_i in the hth time window	$ap_q^h(i,j)$	The qth attribute performance of es_j in dm_i in the hth time window
$pd_q^h(i,j)$	The qth attribute performance degree of es_j in dm_i in the hth time window	$st_q^h(i,j)$	The q th attribute stability degree of es_j in dm_i in the hth time window
$T^h(i,j)$	The trust value of es_j in dm_i in the hth time window	$R^h(j)$	The reputation value of es_j in the h th time window

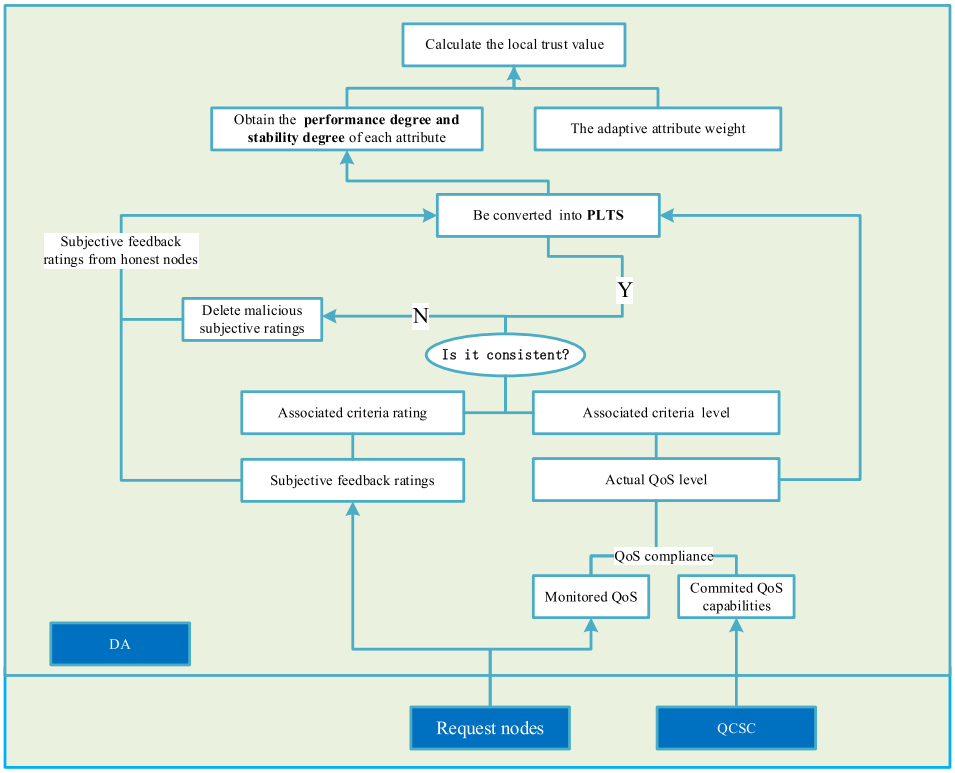

FIGURE 3. The procedure of intradomain trust calculation.

IV. BMDTM SYSTEM DESIGN

Trust management in the BMDTM framework is divided into two submodules, intradomain trust evaluation and interdomain trust data fusion, and reputation evaluation. The symbols and their definitions in this paper are shown in **Table 1**.

A. INTRADOMAIN TRUSTN CALCULATION

To measure service performance more accurately, in addition to the performance degree evaluation, the stability degree evaluation is introduced, which focuses on measuring the dynamics and stability of each attribute's performance. Therefore, two indicators were constructed to evaluate the trust of service providers. The first is the **performance degree,** which can measure the performance of each attribute. The second is the **stability degree,** which can measure the dynamics and uncertainty of each attribute. The procedure of local trust value calculation is shown in Figure. 3

Due to the diversity of service types and the difference in users' attribute preferences, it is inappropriate to adopt the same attributes to evaluate different services.

In the BMDTM framework, the requesting node can submit feedback information about their preferred attributes. The DA assigns the corresponding weight to each attribute which is positively related to the attribute feedback times of the service provider in the domain. In addition, to avoid the requesting nodes providing malicious subjective feedback ratings, the associated criteria with dual characteristics are proposed, which can filter malicious or biased subjective feedback ratings.

1) FILTERING MALICIOUS OR BIASED SUBJECTIVE FEEDBACK RATINGS

In the traditional trust evaluation model, attributes are generally divided into subjective and objective attributes. For example, attributes such as honesty and privacy protection are subjective attributes, while attributes such as throughput, response time, and task failure rate are objective attributes. The researchers in [29] proposed the definition of associated criteria and noted that some subjective attributes and objective attributes can be regarded as the same performance aspect under some circumstances. For example, the throughput of the service can be quantitatively measured through monitored tools, and thus can be considered objective criteria. Meanwhile, consumers can also present their subjective ratings (e.g., ''good'', ''bad'' and ''perfect'') of the throughput performance of the service and thus are deemed subjective criteria. Those that can be considered both subjective criteria and objective criteria are defined as associated criteria. Assume that there are Q subjective and objective criteria, and b associated criteria. Figure. 4 illustrates the relationship between these criteria.

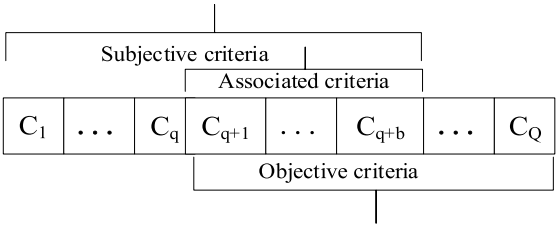

FIGURE 4. The relationship between subjective, objective, and associated criteria.

After the interaction with the service provider, the requesting node provides subjective feedback ratings (i.e.,1-5) to the DA. The objective evaluation data are used as a benchmark to eliminate the subjective feedback information of the requesting nodes whose subjective ratings are inconsistent with the objective evaluation data concerning an associated criterion. The auditability of objective QoS implementation results forms an important source for verifying QoS compliance and subsequently evaluating the credibility of the service provider. The DA queries the service commitment performance in the QCSC and compares it with the monitored QoS performance to obtain the actual QoS level. The equation is shown as follows.

$$diff_q(ij) = \begin{cases} Q_q^m / Q_q^c & postive\ attribute \\ Q_q^c Q_q^m & negative\ attribute \end{cases} \tag{2}$$

$$V_q = \begin{cases} 5 & diff_q(ij) \geq 2 \\ 4 & 1 \leq diff_q(ij) < 2 \\ 3 & 0.8 \leq diff_q(ij) < 1 \\ 2 & 0.5 \leq diff_q(ij) < 0.8 \\ 1 & diff_q(ij) < 0.5 \end{cases} \tag{3}$$

Q_q^m denotes the monitored value of the qth attribute of the service provider in the interaction with the requesting node. Q_q^c indicates the qth attribute value promised by the service

2) CALCULATE MULTIATTRIBUTE PERFORMANCE DEGREE AND STABILITY DEGREE

Each DA integrates the feedback information to obtain each attribute performance of the service provider in the whole domain, which is expressed by PLEs. PLEs simultaneously consider the qualitative variables and their distribution property, which can effectively aggregate the feedback information of each requesting node within the domain. For example, suppose that ten requesting nodes in a domain provide 10 feedback records on the ''Availability'' attribute of the target provider, with three good performances, five medium performances, and two bad performances. The performance degree using the PLEs method is denoted as

$$L(p) = \{good(0.3), medium(0.5), bad(0.2)\},$$

which better reflects the performance of the service provider in the whole domain. Therefore, each attribute performance of the service provider in the whole domain is expressed as

$$L(p) = \{s^l(p^{(l)})| \sum_{l=1}^{l=5} p^{(l)} = 1, \quad l = 1, \ldots 5.$$
$$p^l = \frac{|s^l|}{\sum_{l=1}^{5} |s^l|} \quad l = 1, \ldots 5. \tag{4}$$

$|s^l|$ represents the number of feedback rating s^l in the domain in terms of a certain attribute performance of the service provider.

a: CALCULATE THE ATTRIBUTE PERFORMANCE DEGREE

The attribute performance vector of es_j $(j = 1, 2, \ldots, J)$ in dm_i in the hth time window is

$$ap^h(i,j) = \left(a\, p_1^h(i,j)\ ap_2^h(i,j)\ \cdots ap_Q^h(i,j) \right) \tag{5}$$

$ap_q^h(i,j) = \left\{ s^l\left(p^l\right) \right\}, l = 1, \ldots, 5.$ represents the qth attribute performance of es_j in dm_i in the h th time window. For the convenience and simplicity of the subsequent aggregation process, we convert the linguistic terms in the PLEs to a crisp number in the range of [1, 0] based on eq. (1). The expected value of $ap_q^h(i,j)$ is

$$pd_q^h(i,j) = E\left(ap_q^h(i,j)\right) \tag{6}$$

b: CALCULATE ATTRIBUTE STABILITY DEGREE BASED ON INFORMATION ENTROPY

We utilized information entropy as the measurement tool because it is suitable for measuring the uncertainty of the evaluation information formulated in terms of the probability, and the information expressed in PLTS happens to satisfy such conditions exactly. Information entropy denotes a measure of the degree of system order. The greater the uncertainty of the variables, the greater the information entropy.

Definition 5: Suppose a PLTS is denoted as: $L(p) = \{s^{(l)}(p^{(l)})|l = 1, 2 \ldots \#L(p), \sum_{l=1}^{L(p)} p^{(l)} = 1\}$.

The information entropy of $L(p)$ is defined as follows.

$$H(L(p)) = -\log z \sum_{l=1}^{\#L(p)} \left(p^{(l)}\right) \log \left(p^{(l)}\right) \tag{7}$$

where z is a constant that is set to 1.28.

Afterward, the **stability degree** can be obtained through

$$st(L(p)) = \tau * (1 - H(L(p))) \tag{8}$$

$$\tau = \beta + (1 - \beta) * e^{\frac{E(L(p))-1}{\Delta}} \tag{9}$$

where τ is an adaptive adjustment factor depending on the value of $E(L(p))$, which can prevent some services with a high stability degree but poor performance degree from obtaining higher trust values. $0 \leq \beta \leq 1$ is utilized to control the minimum value of τ. When β is fixed, the closer $E(L(p))$ is to 1, the greater the value τ is. $\Delta > 0$ denotes the preset constant that is utilized to adjust the falling rate of the function curve of τ. Therefore, we obtain $st_q^h(i,j)$ which denotes the stability degree of the qth attribute of es_j in dm_i in the hth time window.

3) CALCULATE THE TRUST VALUE OF THE EDGE SERVER IN EACH DOMAIN

The trust value of es_j in dm_i in the hth time window is calculated by equation (10)

$$T^h(i,j) = \sigma_1 \sum_{q=1}^{Q} \omega_q^h \cdot pd_q^h(i,j) + (1 - \sigma_1) \sum_{q=1}^{Q} \omega_q^h \cdot st_q^h(i,j) \tag{10}$$

$\sigma_1, 1 - \sigma_1$ denotes the weight of the performance degree and stability degree respectively. ω_q^h denotes the weight of the qth attribute, which is calculated by eq. (11). The basic idea is that the more times the requesting nodes in a domain evaluate a certain attribute, the higher the importance of the attribute.

$$\omega_q^h = \frac{k_q^h(i,j)}{\sum_{q=1}^{Q} k_q^h(i,j)} \tag{11}$$

$k_q^h(i,j)$ indicates the number of evaluation data for the qth attribute of es_j by dm_i in the hth time window.

B. INTERDOMAIN TRUST DATA FUSION AND REPUTATION EVALUATION

The reputation value of es_j in the hth time window is calculated using the following equation.

$$R_j^h = \mu_1 \sum_{i=1}^{I} T^h(i,j) \cdot \delta_i^h + (1 - \mu_1) \cdot R_j^{h-1} \tag{12}$$

$$\delta_i^h = \frac{|j \to i|^h}{\sum_{i=1}^{I} |j \to i|^h} \tag{13}$$

where δ_i^h denotes the weight of dm_i in the hth time window and $|j \to i|^h$ denotes the number of interactions between dm_i and es_j in the hth time window. $\mu_1, 1 - \mu_1$ represent the weight of the trust in the current time window and the weight of the reputation value in the previous time window, respectively. The interdomain trust data fusion and reputation evaluation algorithms are shown in Algorithm 1.

Algorithm 1 Interdomain Trust Data Fusion and Reputation Evaluation

Input: Previous reputation value $R^{h-1}(j)$.
Interaction times $|j \to i|^h, (i = 1, \cdots, m)$.
The trust value of es_j in each domain $T^h(i,j), (i = 1, \cdots, I)$.

Output:
Reputation value $R^h(j)$.

Preset parameters
$R^0(j) = 0.5$; In case there is no prior transaction, $R^{h-1}(j)$ is set to $R^0(j)$
$min_{R(j)} = 0$; $max_{R(j)} = 1$; Reputation value is normalized in the range [0-1].

Begin:
while $i \leq I$
do $K+ = |j \to i|^h$;
end while
while $i \leq I$
do $\delta_{A(x_i)}^h = |j \to i|^h / K$;
end while
Obtain the reputation value : $R^h(j) = \mu_1 \sum_{i=1}^{I} T^h(i,j) \cdot \delta_i^h + (1 - \mu_1) \cdot R^{h-1}(j)$

V. IMPLEMENTATION AND EXPERIMENTS

This section provides a real-world demonstration for the proposed decentralized blockchain-based trust system, and conducts experiments. It is mainly divided into three parts. The first part introduces the blockchain data structure. Technical solutions and implementation are provided in the second part. Finally, the third part conducts the experiment evaluation to assess the performance of our trust management model.

A. BLOCKCHAIN DATA STRUCTURE

The requesting node encapsulates the trust source data according to the canonical data format, sends transactions to the blockchain, and then transmits the transaction to any full node for verification. If it is legal, it will continue to broadcast

to nearby full nodes; otherwise, propagation will be stopped. After receiving the transaction, each full node puts it into a transaction waiting queue. After receiving all transactions in the hth time window, they will be packaged into a block and the block will be broadcast to the whole network, where the full nodes will verify the legitimacy of the block. If it is legal, add the block to the tail of the local blockchain; otherwise, stop propagation.

The structure of a block is exhibited in Figure. 5, which consists of the block head and block body. The blockhead contains the hash of the previous block, difficulty, timestamp, nonce, and the state root. The block body consists of trust evidence records, SCs, and some related trust data.

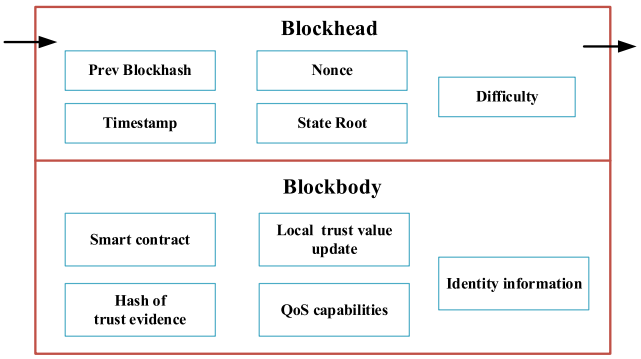

FIGURE 5. The structure of the block.

B. TECHNICAL SOLUTIONS AND IMPLEMENTATION

The proposed decentralized trust evaluation system is deployed on Ganache, which is a private Ethereum-based blockchain system. Ganache is a customizable blockchain that utilizes Node.js and Web3 to operate the interactions between the blockchain and the clients. Many researchers utilize ganache to test and develop the proposed blockchain-based application model. In our implementation, four SCs are programmed in Solidity language which is the primary language on Ethereum.

1) REPUTATION EVALUATION SMART CONTRACT (RESC)

Necessary information about service providers' reputation value and trust value in each time window are permanently recorded on-chain using two state variables **repv** and **trvalueh,** which are defined in RESC. These two state variables act as a public distributed ledger that can permanently record the complete history of the trust state transition of service providers. It is convenient to obtain the latest trust information of service providers because Ethereum supports key-value pair format storage. The RESC fuses the trust degree of service provider es_j in each domain and subsequently queries the blockchain to obtain the previous reputation value $R^{h-1}(j)$. Then, the reputation value $R^h(j)$ can be obtained by calculating their weighted sum.

2) QoS CAPABILITY SMART CONTRACT (QCSC)

The QoS capability SC defines the service provider's QoS commitments to the requesting nodes. The state variable QoS_capabilities acts as the role of a public distributed ledger that can permanently record service providers' commitment to QoS performance. The DA needs to query the blockchain to obtain the QoS performance commitments when calculating the difference degree $diff_q(ij)$ between the monitored and promised performance of service providers.

3) IDENTITY REGISTRATION SMART CONTRACT (IRSC)

The identity registration smart contract implements the functions of node identity registration, node address, and public key distribution, and determines which domain the node belongs to. The state variable node_values serves as a publicly distributed ledger for recording the node's identity information.

4) DATA INTEGRITY SMART CONTRACT (DISC)

DISC can realize data integrity verification, which prevents malicious nodes from tampering with trust evidence information. Ensuring the authenticity and reliability of the source data and the accuracy of subsequent trust evaluation. For example, the requesting node can provide feedback information to the DA and submit the corresponding hash value to DISC for storage. Similarly, the service provider can also provide QoS capabilities to the DA and store the corresponding hash value in DISC.

The smart contract source code is publicly available at "https://github.com/panggeda/sc_test".

C. EXPERIMENTS

BMDTM requires a time-series QoS dataset to measure the dynamic service performance more accurately. There is no appropriate edge computing QoS dataset supporting BMDTM. Therefore, we process the existing real-world web QoS dataset [30] published by the Chinese University of Hong Kong (CUHK) to generate a new dataset to meet the characteristics of the edge computing environment. This dataset consists of QoS data of service invocations on 4532 services from 142 users around the world in 64 timeslots. We select 60 services randomly, extracted 12 QoS values for each service, and constructed a $142*60*12$ user-service-time submatrix to verify the performance of BMDTM. To capture the characteristics of the edge computing environment, users with similar time-series QoS are regarded as domain nodes from the same domain by employing the K-means method. In addition, 60 services are identified as services from 30 edge servers. We configure the location of the service provider according to the following principles, that is, the shorter the average response time of the service provider in the domain, the closer it is. We use NetLogo software to simulate and verify our model and then export the data to MATLAB for data analysis. NetLogo is a programmable modeling environment used to simulate natural and social

phenomena and is particularly suitable for modeling complex systems evolving. We build a simulation environment consisting of 10 domains and 30 edge servers covering an area of 1.9 square kilometers. Each domain contains an average of 12 terminal nodes, among which the node with strong capabilities is selected as the DA. Suppose there are four common criteria, including 3 objective criteria, namely, response time, throughput, and task failure rate, and 2 subjective criteria, namely, confidentiality and response time. Among these, response time is an associated criterion.

1) REPUTATION VALUE COMPARISON

In this experiment, the impact on reputation value is verified by setting the ratio of malicious services provided by the service provider. Malicious service refers to the service provider failing to meet the service quality specified in the agreement when providing services. We divide 30 service providers into three groups, with 10 providers in each group. The services provided by the first group always comply with the service commitment. The services provided by the second group are 30% malicious and the other 70% comply with the service commitment. The services provided by the third group, 50% of the services are malicious, and the other 50% of the services comply with the service commitment. It is worth noting that complying with the service commitment mean V_q is assigned as 4 or 5 by equal opportunity, and the malicious services means V_q is assigned as 1, 2, or 3 by equal opportunity. In addition, we randomly generate the subjective ratings for the target service concerning ''confidentiality''. To ensure the consistency of the experiment, each group employs the same feedback data concerning ''confidentiality''. After 10 rounds of interactions, the average reputation value under different malicious service proportions is shown in the figure below. It can be seen from Figure. 6(a) that the average reputation value of different groups changes with the number of transaction rounds. In the first group, it rises slowly with the increase of the transaction rounds, in the second group it rises and falls while presenting an overall upward trend, and it shows a slow downward trend in the third group. This illustrates that BMDTM is feasible and effective in dealing with malicious attacks from service providers.

Compared with most other trust evaluation models, we introduce the concept of stability degree, which is an indicator to measure service dynamics and uncertainty. In this experiment, we will test the impact of the stability degree on the reputation value in our model. We simulate the stability of service performance caused by busy network status or random malicious behavior of service providers. The experimental parameter settings are the same as those in Experiment 1. Figure. 6(b) and Figure. 6(c) demonstrate the comparison curves of the reputation value with and without considering the stability degree when the malicious service ratio is 0 and 30%, respectively. The weight σ_1 is assigned as 0.5 when considering the stability degree. β is set to 0.5 by default. It can be seen that when the service providers do not provide malicious services, the two curves are essentially close to whether or not stability is considered. However, when the service providers provide 30% malicious services, considering the stability degree can inhibit the growth of reputation value to a certain extent.

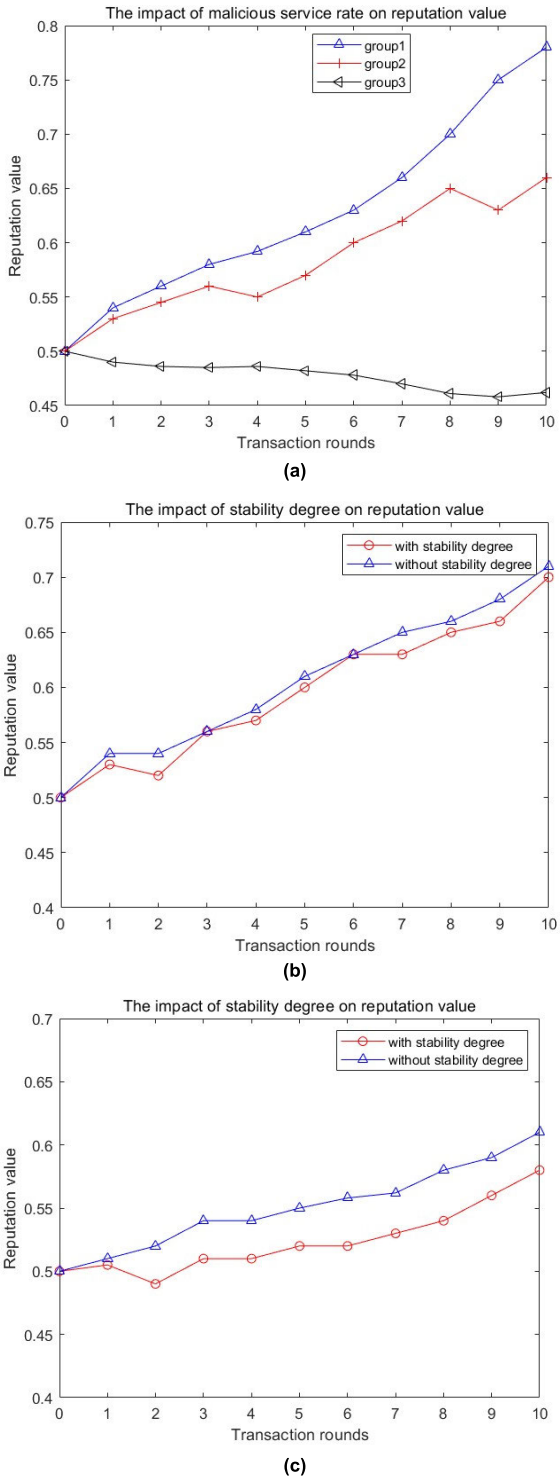

FIGURE 6. (a) The impact of malicious service rate on reputation value. (b) The impact of stability degree on reputation value when the malicious service ratio is 0. (c) The impact of the stability degree on the reputation value when the malicious service ratio is 30%.

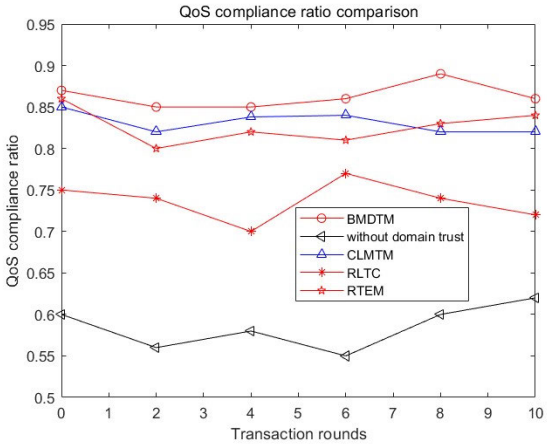

FIGURE 7. QoS compliance ratio comparison curves.

2) QoS COMPLIANCE RATIO COMPARSION

In the BMDTM framework, two indicators are introduced to measure the trustworthiness of service providers, namely, reputation value $R^h(j)$ and domain trust value $T^h(i, j)$. We randomly selected some service providers from group 1 and group 2 for testing, and compared the QoS compliance ratio in the following cases.

Case 1 (BMDTM): The requesting node considers both the reputation value and domain trust value when selecting services. Suppose that when the requesting node selects a service provider, it follows two principles. First, the reputation value of the service provider should be higher than the threshold. Second, the average local trust values of the service providers in the past 3 time windows in the domain where the requesting node is located are sorted, and the one with the highest trust value is selected.

Case 2 (Without Domain Trust): Only consider the reputation value in service selection. The requesting node prioritizes selecting service providers with high reputation value.

Case 3 (CLMTM): The overall trust is designed as the minimum of the capability trust and the weighted summation of the direct trust and indirect trust in this model [16]. The requesting node prioritizes selecting service providers with high overall trust value.

Case 4 (RLTC): The authors in [17] argued that the proposed trust scheme significantly outperforms existing approaches in both attack resistance and reliability, where the global trust of the node is aggregated by the two trust factors, namely, D-to-D direct trust and B-to-D feedback trust. The D-to-D direct trust is a subjective evaluation after the interaction with the service provider, and the B-to-D feedback trust is an aggregation of subjective evaluations of the service provided by other nodes in the domain. The requesting node prioritizes selecting service providers with high global trust values.

Case 5 (RTEM): The authors in [18] proposed a three-tier trust evaluation framework (identity trust, capability trust, behavior trust) to ensure the edge nodes participating in the network system for service interaction are qualified, capable, and reliable, and put forward the local reputation calculation model and overall reputation calculation model. The requesting nodes prioritize selecting service providers with high local reputation value.

The comparison curves of the QoS compliance ratio are demonstrated in Figure. 7. It can be seen that the QoS compliance ratio of the BMDTM model is the best, because our trust management model can measure the dynamic performance of services more accurately and precisely, and the dual characteristics of the associated criteria can filter malicious or biased feedback ratings effectively, ensuring that the trust evaluation results are more reliable. Although dynamic time series evaluation information is considered in the RLTC model, the QoS compliance ratio is relatively low because the evaluation data only contains subjective feedback information which cannot comprehensively reflect the service performance. The QoS compliance ratio in Case 2 is the worst because it only involves reputation value and does not consider the domain trust value. The domain trust value is obtained by aggregating the evaluation information of nodes with the same context as the requesting node, which has a great reference value for the service selection of the requesting node.

3) THE INFLUENCE OF MALICIOUS FEEDBACK RATIO ON THE DOMAIN TRUST CHANGING RATE

In this experiment, the influence of the malicious feedback ratio on the domain trust changing rate is tested and compared with the other two methods. (1) The overall trust value is designed as the minimum of the capability trust and the weighted summation of the direct trust and indirect trust in the CLMTM framework, coupled with a dual filtering design based on the K-means clustering algorithm, which can effectively filter feedback with low similarity in the current task context and feedback from malicious devices, making the trust evaluation mechanism more reliable [16]. (2) The authors put forward an adaptive trust model based on the recommendation filtering algorithm for the IoT environment, which divided the nodes into multiple groups and each group selects a trusted third party (TTP) responsible for assisting the trust evaluation in the ATM model [31]. The TTP utilizes the feedback and its trust evaluation module to evaluate the direct trust, recommendation trust, and synthesis trust of the trustee. It is worth noting that the trust value calculated in the above two methods is equivalent to the domain trust in the BMDTM model.

The comparison curves of the domain trust changing rate are demonstrated in Figure. 8. It can be seen that compared with the other two models, the domain trust value changing rate of our model is lowest under different malicious feedback ratios. This is because the dual characteristics of association attributes are utilized to filter out malicious or unprofessional evaluation information of the requesting nodes by comparing subjective and objective data in our model, which can effectively avoid malicious user collusion and ensure the

credibility of trust management. While, the other two models filter malicious data by comparing evaluation data provided by the requesting node with the data provided by the nodes with the same text or neighboring recommenders, lacking certain accuracy.

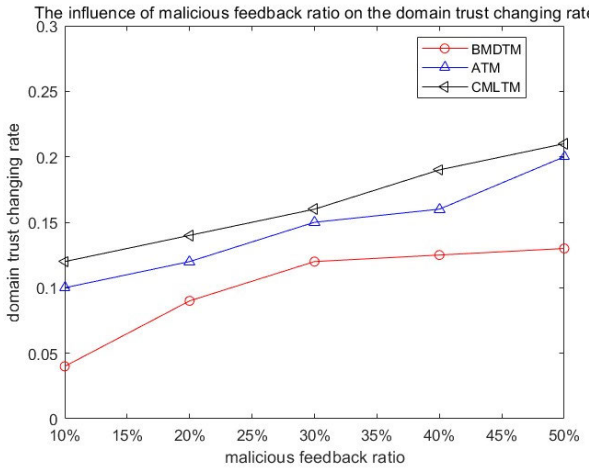

FIGURE 8. Domain trust changing rate comparison.

4) ROBUSTNESS OF BMDTM AGAINST GENERIC ATTACKS

In this paper, defending against generic attacks mainly considers two methods: one is the trust evaluation model, and the other is the traceability and tamper resistance of blockchain.

a: BAD-MOUTHING BY MALICIOUS FEEDBACK NODES

Bad-mouthing by malicious feedback nodes means that the nodes are dishonest and provide malicious or biased feedback ratings to the trustee. In our model, the associated criteria are introduced to filter out malicious subjective feedback ratings. In this experiment, we test the malicious node detection success rates of different models. The first comparison model [32] employs the K-means method (labeled KM) to filter malicious subjective feedback information, and the second comparison model [33] (labeled AM) argues that the opinions of dishonest or malicious users are usually less consistent with the majority of the other users' opinions than those of honest users. The comparison figure is shown in Figure. 9.

It is seen that BMDTM maintains a relatively high detection success rate with the increase in the proportion of malicious nodes, whereas the other two models show a significant downward trend. This is because as the proportion of malicious feedback nodes increases, it becomes increasingly difficult to distinguish between normal and malicious nodes using KM and AM methods. When the proportion increases to a certain extent, the evaluation data of normal nodes will even be overpowered. While BMDTM utilizes objective attribute performance as the benchmark to identify malicious subjective feedback ratings, it is not affected by the proportion of malicious nodes.

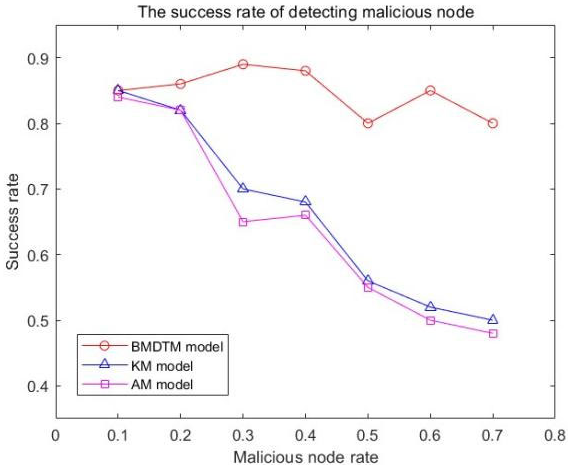

FIGURE 9. Comparison of malicious node detection success rate.

b: BAD-MOUTHING BY MALICIOUS SERVICE PROVIDERS

Bad-mouthing by malicious service providers refers to the service providers submitting mendacious QoS capabilities to the DA. This is entirely avoidable. The DA can calculate its hash value, and then query the hash value of QoS capabilities in DISC for comparison and verification, or ask domain nodes for the hash value of the QoS capabilities negotiated offline by both sides for comparison.

c: IMPERSONATION ATTACK

An impersonation attack refers to an attacker stealing the identity of edge servers or domain nodes and attempting to update information (i.e., QoS capabilities, trust evidence data, or trust value) to the blockchain. Our proposed model can effectively prevent this attack because all the transactions implemented using its blockchain account address are officially signed by its private key. Generally, as a property of systems involving blockchain, private keys are considered highly secure and difficult for attackers to steal.

VI. CONCLUSION

In this paper, we propose multidimensional trust management in edge computing based on blockchain technology. The BMDTM differs from existing work in several ways. First, take the domain as a whole to evaluate the service provider and adopt the PLTS method as a trust scaling method to integrate the evaluation information within the domain, which can describe the dynamic performance of services and avoid information loss to a certain extent. Second, the associated (objective) attribute value is taken as a benchmark to filter corresponding subjective evaluation information; subsequently, two indicators are utilized to evaluate the trust of the service provider in each domain. Third, blockchain technology is combined to realize automated reputation value calculation, trust evidence storage, verification, and data sharing. The experimental results demonstrate that our model can well manage trust problems in dynamically hostile edge computing.

REFERENCES

[1] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, Aug. 2019.

[2] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: A survey," *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, Sep. 2020.

[3] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020.

[4] R. Latif, M. U. Ahmed, S. Tahir, S. Latif, W. Iqbal, and A. Ahmad, "A novel trust management model for edge computing," *Complex Intell. Syst.*, vol. 8, no. 5, pp. 3747–3763, Oct. 2022.

[5] T. Wang, H. Luo, X. Zheng, and M. Xie, "Crowdsourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–19, Nov. 2019.

[6] C. Esposito, A. Castiglione, F. Palmieri, and M. Ficco, "Trust management for distributed heterogeneous systems by using linguistic term sets and hierarchies, aggregation operators and mechanism design," *Future Gener. Comput. Syst.*, vol. 74, pp. 325–336, Sep. 2017.

[7] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, May 2020.

[8] T. Wang, P. Wang, S. Cai, X. Zheng, Y. Ma, W. Jia, and G. Wang, "Mobile edge-enabled trust evaluation for the Internet of Things," *Inf. Fusion*, vol. 75, pp. 90–100, Nov. 2021.

[9] T. Xiao, C. Chen, Q. Pei, and H. H. Song, "Consortium blockchain-based computation offloading using mobile edge platoon cloud in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 17769–17783, Oct. 2022.

[10] N. Truong, G. M. Lee, K. Sun, F. Guitton, and Y. Guo, "A blockchain-based trust system for decentralised applications: When trustless needs trust," *Future Gener. Comput. Syst.*, vol. 124, pp. 68–79, Nov. 2021.

[11] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4000–4015, May 2020.

[12] Z. Xiong, J. Kang, D. Niyato, P. Wang, and H. V. Poor, "Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based ADMM for pricing," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 356–367, Mar. 2020.

[13] X. H. Deng, P. Y. Guan, Z. Wan, E. Liu, and Z. Zhao, "Integrated trust based resource cooperation in edge computing," *J. Comput. Res. Develop.*, vol. 55, no. 3, pp. 449–477, 2018.

[14] J. Al Muhtadi, R. A. Alamri, and F. A. Khan, "Subjective logic-based trust model for fog computing," *Comput. Commun.*, vol. 178, pp. 221–233, Oct. 2021, doi: 10.1016/j.comcom.2021.05.016.

[15] L. Zhang and X. Y. Wei, "Trust evaluation algorithm of IoT edge server based on cooperation reputation and device feedback," *J. Commun.*, vol. 43, no. 1, pp. 118–130, 2022, doi: 10.11959/j.issn.1000-436x.2022024.

[16] Z. Gao, W. Zhao, C. Xia, K. Xiao, Z. Mo, Q. Wang, and Y. Yang, "A credible and lightweight multidimensional trust evaluation mechanism for service-oriented IoT edge computing environment," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2019, pp. 156–164.

[17] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018.

[18] X. Deng, J. Liu, L. Wang, and Z. Zhao, "A trust evaluation system based on reputation data in mobile edge computing network," *Peer Peer Netw. Appl.*, vol. 13, no. 5, pp. 1744–1755, Sep. 2020.

[19] Y. Wang, L. Tian, and Z. Wu, "Trust modeling based on probabilistic linguistic term sets and the MULTIMOORA method," *Expert Syst. Appl.*, vol. 165, Mar. 2021, Art. no. 113817.

[20] D. Wang, X. Chen, H. Wu, R. Yu, and Y. Zhao, "A blockchain-based vehicle-trust management framework under a crowdsourcing environment," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1950–1955.

[21] F. Li, Z. Guo, C. Zhang, W. Li, and Y. Wang, "ATM: An active-detection trust mechanism for VANETs based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4011–4021, May 2021.

[22] Y. Zhang, X. Xu, A. Liu, Q. Lu, L. Xu, and F. Tao, "Blockchain-based trust mechanism for IoT-based smart manufacturing system," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1386–1394, Dec. 2019.

[23] J. Zhang, C. Lu, G. Cheng, T. Guo, J. Kang, X. Zhang, X. Yuan, and X. Yan, "A blockchain-based trusted edge platform in edge computing environment," *Sensors*, vol. 21, no. 6, p. 2126, Mar. 2021.

[24] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[25] R. Z. Du, K. Q. Xu, and J. F. Tian, "Optimization scheme of trust model based on graph theory for edge computing," *Adv. Eng. Sci.*, vol. 52, no. 3, pp. 9–17, 2020.

[26] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.

[27] P. Podili and K. Kataoka, "TRAQR: Trust aware end-to-end QoS routing in multi-domain SDN using blockchain," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103055.

[28] X. Wu, H. Liao, Z. Xu, A. Hafezalkotob, and F. Herrera, "Probabilistic linguistic MULTIMOORA: A multicriteria decision making method based on the probabilistic linguistic expectation function and the improved Borda rule," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3688–3702, Dec. 2018.

[29] L. Qu, Y. Wang, M. A. Orgun, L. Liu, H. Liu, and A. Bouguettaya, "CCCloud: Context-aware and credible cloud service selection based on subjective assessment and objective assessment," *IEEE Trans. Services Comput.*, vol. 8, no. 3, pp. 369–383, May 2015.

[30] Y. Zhang, Z. Zheng, and M. R. Lyu, "WSPred: A time-aware personalized QoS prediction framework for web services," in *Proc. IEEE 22nd Int. Symp. Softw. Rel. Eng.*, Nov. 2011, pp. 210–219.

[31] G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107952.

[32] K. Su, B. Xiao, B. Liu, H. Zhang, and Z. Zhang, "TAP: A personalized trust-aware QoS prediction approach for web service recommendation," *Knowl.-Based Syst.*, vol. 115, pp. 55–65, Jan. 2017.

[33] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Gener. Comput. Syst.*, vol. 74, pp. 302–312, Sep. 2017.

YAN WANG received the Ph.D. degree from the School of Computer Science and Technology, Qinghai Normal University, in 2021. She is currently a Lecturer with the Ningbo University of Technology. Her current research interests include cloud computing, edge computing, service performance evaluation, network security, and the IoT.

ZENAN WU received the Ph.D. degree from the School of Computer Science and Technology, Qinghai Normal University, in 2022. He is currently a Lecturer with the Zhongyuan University of Technology. His current research interests include cloud computing, user behavior analysis, network security, the IoT, and stochastic game net.