Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8864533, 12 pages
https://doi.org/10.1155/2020/8864533

Research Article

Wireless Communications and Mobile Computing Blockchain-Based Trust Management in Distributed Internet of Things

Fengyin Li,[1] **Dongfeng Wang**,[1] **Yilei Wang**,[1] **Xiaomei Yu**,[2] **Nan Wu**,[3] **Jiguo Yu**,[4,5] **and Huiyu Zhou**[6]

[1]*School of Computer Science, Qufu Normal University, Rizhao 276826, China*
[2]*School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China*
[3]*Science and Technology Department, Qufu Normal University, Qufu 273165, China*
[4]*School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China*
[5]*Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250014, China*
[6]*School of Informatics, University of Leicester, Leicester LE1 7RH, UK*

Correspondence should be addressed to Yilei Wang; wang_yilei2019@qfnu.edu.cn

Received 10 September 2020; Revised 18 November 2020; Accepted 1 December 2020; Published 19 December 2020

Academic Editor: Shaohua Wan

The development of Internet of Things (IoT) and Mobile Edge Computing (MEC) has led to close cooperation between electronic devices. It requires strong reliability and trustworthiness of the devices involved in the communication. However, current trust mechanisms have the following issues: (1) heavily relying on a trusted third party, which may incur severe security issues if it is corrupted, and (2) malicious evaluations on the involved devices which may bias the trustrank of the devices. By introducing the concepts of risk management and blockchain into the trust mechanism, we here propose a blockchain-based trust mechanism for distributed IoT devices in this paper. In the proposed trust mechanism, trustrank is quantified by normative trust and risk measures, and a new storage structure is designed for the domain administration manager to identify and delete the malicious evaluations of the devices. Evidence shows that the proposed trust mechanism can ensure data sharing and integrity, in addition to its resistance against malicious attacks to the IoT devices.

1. Introduction

Mobile Edge Computing is a new technology which provides an IT service environment and cloud-computing capabilities at the edge of the mobile network. In recent years, with the widespread implementation of the Internet of Things, the number of edge services running on mobile devices has exploded [1]. It is estimated that by 2025, the number of global IoT connections will reach 25.1 billion, and the market size will exceed 10 trillion Chinese yuan. Emerging technologies such as data mining [2], artificial intelligence [3], 5G technology, and natural language processing are also increasingly being extended to IoT applications [4–6]. For example, in the Internet of vehicles [7], we can build a smart city traffic system [8]. Through the use of intelligent abnormal event monitoring for electric vehicles [9] and the use of deep learning to preanalyze road conditions [10], the occurrence of traffic jams can be effectively reduced [11]. Therefore, the need for cooperation between IoT devices has been significantly increased [12]. However, the performance of IOT devices in the process of cooperation is uncertain [13]. The focus of the recent research is how to measure the availability and privacy of data [14, 15] and how to measure the performance of devices through trust data to understand the recent performance of IOT devices [16].

The blockchain technology is essentially a distributed and secure ledger that records all the transactions into a hierarchically expanding chain of blocks. Edge computing brings the cloud capabilities closer to the computation tasks. The convergence of blockchain and edge computing paradigms can overcome the existing security and scalability issues [17]. An IoT device is expected to cooperate with the devices

of high reliability. Before that, it is necessary to ensure the performance of the other devices and the trustworthiness of them, which is the criterion to examine the reliability of the devices before cooperation [18, 19]. However, existing trust mechanisms heavily rely on the trusted third parties or additional trust assumptions; there are hidden security risks such as malicious modifications to the trusted data [20]. Moreover, most distributed trust systems have not considered the malicious evaluation on the IoT devices [21, 22]. Wang et al. proposed a trust management method using environment awareness [23]. From nodes' historical behaviors in different cooperation types, they obtained a comprehensive trustrank to handle any new task, but this process relies on a reliable trust management institution. By caching previous interaction summaries, Liu et al. proposed a verifiable method to solve the hierarchical trust problem of IoT systems [24], but this method needs to establish additional trusted third parties over different domains.

Benkerrou et al. proposed an IoT trust evaluation method based on trust and honesty [25], but they assumed that all master nodes in the domain were completely trusted. Chi et al. proposed an algorithm $SR_{\text{Amplified-LSH}}$ can ensure a good balance between the accuracy and efficiency of recommendation and user privacy information [26]. Based on blockchain technologies, Ren et al. proposed a trust management method suitable for distributed Internet of Things, but they did not consider the irresponsible malicious evaluation problems between malicious devices [27].

Blockchain is a new application of distributed data storage, point-to-point transmission [28], consensus mechanism [29, 30], and encryption algorithms [31, 32]. Blockchain has the characteristics of distributed trust [33], openness, and unforgeability [34], in which the intelligent contract ensures the traceability and irreversibility of transactions. The adoption of multiparty computation and measurement method can guarantee the user to derive results from multiple data sources [35, 36]. Therefore, data sharing and integrity can be guaranteed, and reliable trustworthiness can be established among parties that are blind to each other. Blockchain can realize the sharing and synchronization of trusted data in the distributed Internet of Things, so as to ensure that the data will not be forged or modified by malicious entities [37, 38].

By introducing the theory of blockchain and risk into trust management, we propose a trust management method for distributed IoT. The new mechanism does not rely on any trusted third party; the process of trust establishment and management is entirely independent maintained by each IoT domain manager. The main contributions of our method are as follows:

(1) Aiming at the dependence of trusted third party, a trust mechanism of Internet of Things based on normative trust and risk trust is proposed. This trust mechanism does not rely on any trusted third party, and all trust establishment and trust management are completely managed and maintained by IOT domain administrators and IOT devices

(2) Aiming at the phenomenon of malicious evaluation of devices by existing mechanisms, a trust data storage scheme based on blockchain is proposed. In order to ensure the reliability of the trust mechanism, a storage structure and identification method are designed for domain manager to identify and filter a large number of malicious evaluations of devices

2. Trust Management Model in Distributed Internet of Things

2.1. The Structure of System. According to the characteristics of IoT, we design a decentralized distributed IoT architecture (as shown in Figure 1). Each management domain consists of a domain manager and all subordinate IoT devices. The domain manager manages all IoT devices in the domain. IoT devices can communicate and cooperate with other devices in any management domain. The domain manager can collaborate with others to exchange data.

Each cooperation between the domain manager and the device will be evaluated in both directions based on each other's performance. The gist for evaluation includes the device's communication success rate, data processing capability, transmission range, and network stability. The device can be evaluated based on the other party's overall performance. The communication success rate between the devices is considered as the main indicator of the devices' performance in this paper.

In Figure 1, x represents the IoT domain identifier, x_1, x_2, x_3 represent different IoT domain identifiers, $H(x)$ represents the domain manager of IoT domain x, and $D(x, \mathrm{y}_i)$ represents different IoT devices in the domain x, which is managed by $H(x)$, where $y_i \in N^*(i = 1, 2, \cdots, n)$.

2.2. Trust Model. In order to describe the trustworthiness of IoT devices, this paper uses normative trust and risk measures to quantify trustrank. Normative trust defines the ability of a specific entity to earn credit by other entities, and the risk measure defines the stability level of a specific entity's credit performance in the past period. The concrete definition of the trust model is as follows.

Definition 1. Evaluation value.

The evaluation value of $D(x_i, y_m)$ is denoted as $\delta(x_i, y_m, x_j, y_n, l)$, which refers to the evaluation of a given IoT device $D(x_i, y_m)$ by another IoT device $D(x_j, y_n)$. It is defined as follows.

$$\delta(x_i, y_m, x_j, y_n, l) = \begin{cases} 1, & \text{Good performance,} \\ 0, & \text{Ordinary performance,} \\ -1, & \text{Poor performance,} \end{cases} \quad (1)$$

where l indicates the serial number of the evaluation currently received by $D(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the evaluation value represents the evaluation value of $H(x_i)$,

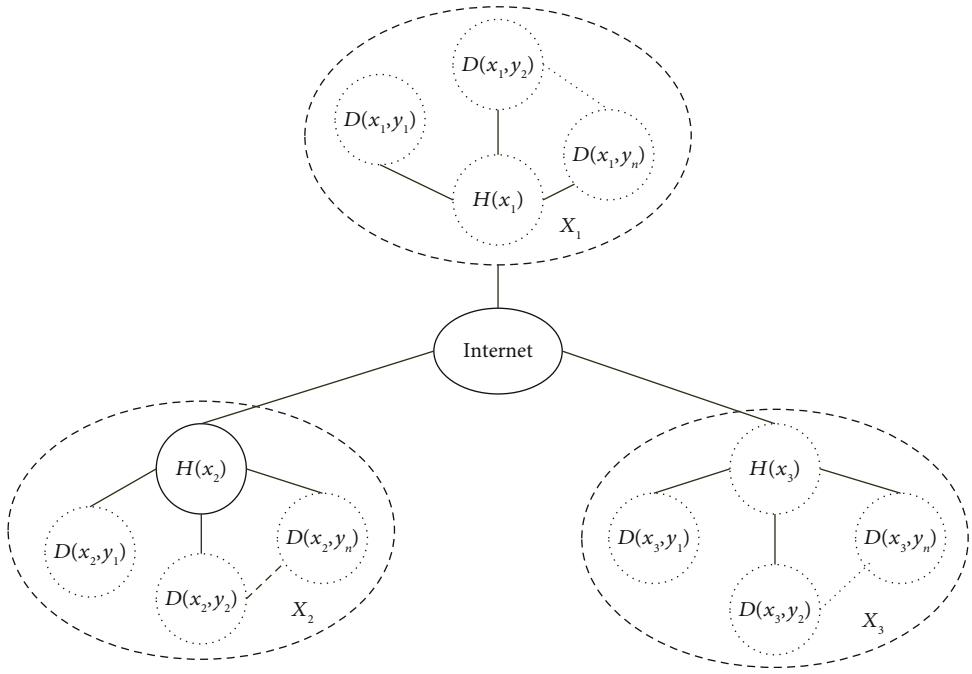


Figure 1: Architecture of distributed IoT.

which refers to the evaluation of a domain manager $H(x_i)$ by another domain manager $H(x_i)$.

Definition 2. Trust scale.

When receiving the kth evaluation, the trust scale of $D(x_i, y_m)$ is denoted as $\mathrm{TC}(x_i, y_m, k)$, and it is iterated according to the evaluated value $\delta(x_i, y_m, x_j, y_n, l)$ given by other evaluators. It is defined as follows.

$$\mathrm{TC}(x_i, y_m, k) = I + \sum_{l=1}^{k-1} \delta\left(x_i, y_m, x_j, y_n, l\right), \tag{2}$$

where I is a trust initial value (we suppose $I = 50$ in our experiments for simplicity) and $k \in N^*$ represents the maximum serial number of the current evaluation received by $D(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the trust scale represents the trust scale of a domain manager $H(x_i)$, and it is iterated according to its evaluation value given by another domain manager $H(x_i)$.

Definition 3. Normative trustrank.

The normative trustrank of $D(x_i, y_m)$ is denoted as $\mathrm{NT}(x_i, y_m, k)$, which represents the standardized trustrank of device $D(x_i, y_m)$. It is defined as follows.

$$\mathrm{NT}(x_i, y_m, k) = f(\mathrm{TC}(x_i, y_m, k)) = \frac{1}{\left(1 + e^{(-\mathrm{TC}(x_i, y_m, k))}\right)}, \tag{3}$$

where $x_i, x_j (i \neq j)$ represent different IoT domain identifiers, $y_i, y_j (i \neq j)$ represent different IoT devices, and $k \in N^*$ represents the maximum serial number of the current evaluations received by $D(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the normative trustrank represents the normative trustrank of a domain manager $H(x_i)$.

Definition 4. The mean value.

The mean value of the trust of $D(x_i, y_m)$ is denoted as $\mathrm{MT}(x_i, y_m, k, r)$, which represents the average value of the latest r normative trust of $D(x_i, y_m)$. It is defined as follows.

$$\mathrm{MT}(x_i, y_m, k, r) = \frac{\sum_{k'=k-r+1}^{k} \mathrm{NT}\left(x_i, y_m, k'\right)}{r}, \tag{4}$$

where $k \in N^*$ represents the maximum evaluation serial number received by $H(x_i)$ and $r \in N^*$ represents the number of $CD(x_i, y_m, k')$ included in the risk assessment.

If the device numbers y_m and y_n are not given here, this value represents the mean value of a domain manager $H(x_i)$, which represents the average value of the latest r normative trust of $H(x_i)$.

Definition 5. Risk value.

The risk value of $D(x_i, y_m)$ is denoted as $\mathrm{RV}(x_i, y_m, k, r)$, which is used to measure the risk of the credit performance of $D(x_i, y_m)$ in the history. Up to the maximum evaluation serial number k, the most recent r normative trustranks are taken into consideration, and the risk measure of definition $D(x_i, y_m)$ is as follows.

$$\mathrm{RV}(x_i, y_m, k, r) = \sqrt{\frac{\sum_{k'=k-r+1}^{k}\left[\mathrm{NT}\left(x_i, y_m, k'\right) - \mathrm{MT}(x_i, y_m, k, r)\right]^2}{r}}, \tag{5}$$

where $k \in N^*$ represents the maximum evaluation serial number received by $D(x_i, y_m)$, and $r \in N^*$ represents the number of $\mathrm{NT}(x_i, y_m, k')$ included in the risk assessment.

If the device numbers y_m and y_n are not given here, this value represents the risk value of a domain manager $H(x_i)$, which is used to measure the risk of the credit performance of $H(x_i)$ in the past.

Definition 6. Harmonic trustrank.

The harmonic trustrank of $D(x_i, y_m)$ is denoted as $\mathrm{HT}(x_i, y_m, k, r)$, which is used to represent the comprehensive trust evaluation of $D(x_i, y_m)$. Considering the normative trustrank and risk measure of $D(x_i, y_m)$, we define $\mathrm{HT}(x_i, y_m, k, r)$ as follows.

$$\mathrm{HT}(x_i, y_m, k, r) = \frac{\mathrm{NT}(x_i, y_m, k)}{1 + \mathrm{NT}(x_i, y_m, k) \times \mathrm{RV}(x_i, y_m, k, r)}. \tag{6}$$

If the device numbers $y_m$and y_n are not given here, this value represents the harmonic trustrank of a domain manager $H(x_i)$, which is used to represent the comprehensive trust evaluation of $H(x_i)$.

The architecture of the trust management model is shown in Figure 2.

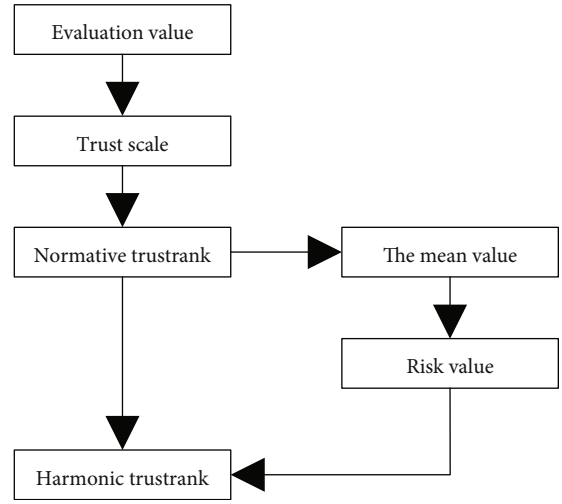


Figure 2: Trust management model.

3. Trust Management Method of Distributed Internet of Things

3.1. Blockchain Structure. In order to achieve trust integrity in data sharing and avoid the existence of irresponsible participants to make a large number of malicious evaluations of other collaborators, a new data structure of the blockchain is designed in this paper, adding the identity of the domain managers, evaluators, evaluatees, and the corresponding evaluation information for providing traceability of the trust evaluation information of the domain managers.

A blockchain can be represented as $\{B_t \mid t \in N^*\}$. $\mathrm{Head}(B_t) \subseteq B_t$ represents the block head, and $B_t - \mathrm{Head}(B_t) = \mathrm{NT}\{\cdot\}$ represents the block body. The trust data in $\mathrm{NT}\{\cdot\}$ is stored in the block body as a Merkle tree, and the root of the Merkle tree is stored in the block head. The block head stores the evaluation information between the domain managers of IoT and the connection information between the blocks. The block body stores the evaluation information between the IoT devices. Taking the evaluation of domain managers $H(x_i)$ and $H(x_j)$ as an example, we define the block structure of the trust data blockchain as follows: $B_t = \{\mathrm{Hash}(B_{t-1}), H(x_i), \mathrm{H}(x_j), \mathrm{TC}(x_j, k-1), \delta(x_j, x_i, k-1), k, \mathrm{MR}, \mathrm{HT}(x_j, k, r), r, \mathrm{NT}\{.\}\}$, where $\sigma_{H(x_j)}(\mathrm{Trl}) = \mathrm{Sig}_{H(x_j)}(\mathrm{Hash}(\mathrm{Trl}))$, $\sigma_{H(x_i)}(\mathrm{Hash}) = \mathrm{Sig}_{H(x_i)}(\mathrm{Hash}(\mathrm{Hash}(B_{t-1}), H(x_i), k, \mathrm{MR}, \mathrm{Trl}, \mathrm{PK}(x_i)))$.

$\mathrm{Hash}(B_{t-1})$ represents the hash value of the previous block B_{t-1}, a block appearing before B_t on the blockchain, $H(x_i)$ represents the identity of the block producer, and $H(x_j)$ represents the identity of the domain manager being evaluated. $\delta(x_j, x_i, k-1)$ is the evaluation value of $H(x_i)$ and $H(x_j)$, which is the $k-1$th evaluation value received by $H(x_j)$. k is the next evaluation's serial number. MR is the Merkle tree root, which is the hash result of the information in the block; Trl is the transaction details of this transaction between $H(x_i)$ and $H(x_j)$. $\sigma_{H(x_j)}(\mathrm{Trl})$ represents $H(x_j)$'s signature on the transaction details Trl. $\mathrm{PK}(x_i)$ is the public key of $H(x_i)$. $\sigma_{H(x_i)}(\mathrm{Hash})$ represents $H(x_i)$'s signature on the transaction information of this block. $\mathrm{MT}(x_j, k, r)$ represents the average value of the latest r normative trust of $H(x_j)$, and $\mathrm{RV}(x_j, k, r)$ represents the trust risk value of $H(x_j)$. $\mathrm{HT}(x_j, k, r)$ represents the harmonious trustrank of $H(x_j)$, and r represents the number of the normative trust included in risk assessment. $\mathrm{NT}\{\cdot\}$ represents the collection of normative trust $NT(x_j, y_n, k)$ of all the other IoT devices $D(x_j, y_n)$ that have been recently evaluated by IoT device $D(x_i, y_m)$. These normative trustranks constitute different records in the IoT domains to which the devices belong, and the domain manager's ID of each IoT domain is marked in the block header.

Assume that there are four sets of device specification trustrank records in the block body, namely, $\mathrm{NT}\{\cdot\} = \{\mathrm{NT}_1, \mathrm{NT}_2, \mathrm{NT}_3, \mathrm{NT}_4\}$, and the structure of the block body is shown in Figure 3.

3.2. Bookkeeping Rights Selection and Block Release. The function of bookkeeping rights selection is to determine which node is used to wrap the trust data, create a block, and then publish it to the blockchain.

3.2.1. Scenario 1. It is a long time for the domain managers $H(x_i)$ and $H(x_j)$ not to cooperate. During this time, it is impossible to share the evaluation results given by the IoT

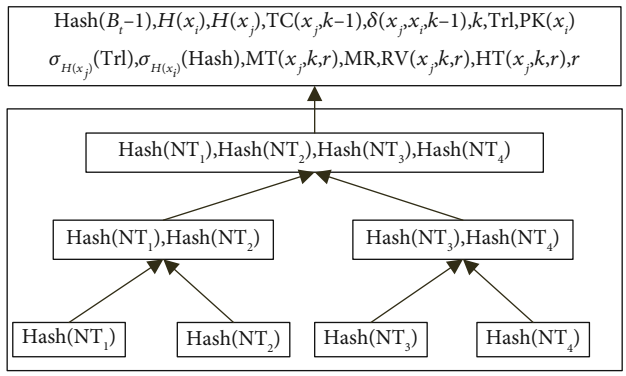


Figure 3: Block structure.

device $D(x_i, y_m)(m = 1, 2, \cdots, n)$ in $H(x_i)$ to the blockchain, and other devices cannot get the latest trust evaluation.

At the moment, firstly, the domain manager $H(x_i)$ detects the utilization rate of the local storage pool. When the utilization rate of the local storage pool reaches a critical value, it performs screening for malicious evaluation of the devices in the IoT domain. If it is determined that there are malicious evaluations of the IoT devices in this domain, these malicious evaluations will be deleted. Then, the normative trustrank of the appraiser is determined by querying the blockchain. The domain manager iterates and updates other valid evaluations of the IoT devices in the domain based on the normative trustrank, generates new blocks, and then publishes them to the blockchain. Meanwhile, the block head uses the fixed format defined in the previous section.

For this purpose, we modify the storage structure of the domain manager so that $H(x_i)$ maintains two fixed-size storage spaces, which are denoted as storage pool Pool1(x_i) and storage pool Pool2(x_i), respectively. Pool1(x_i) is used to receive all the evaluation values $\delta(x_j, y_n, x_i, y_m, l)$ presented by the subordinate equipment $D(x_i, y_m)(m = 1, 2, \cdots, n)$ and sum the evaluation values given by each evaluation device. According to whether or not the sum of the evaluation values exceeds a critical threshold, we can decide whether or not the device has performed a malicious evaluation behavior. If it exists, all the evaluations of the malicious devices will be deleted, thereby blocking all the malicious evaluation data. The evaluation values without any malicious evaluations are assigned to Pool2(x_i).$H(x_i)$ uses the evaluation value $\delta(x_j, y_n, x_i, y_m, l)$ in Pool2(x_i) to obtain the latest trust scale value TC$(x_j, y_n, k')$of $H(x_j)$ using Equation (2) and then uses Equation (3) to calculate the latest normative trust of $H(x_j)$, among which $k' = k + 1$. The detailed operation is as follows.

When the utilization of the storage space of Pool1(x_i) reaches a critical value a, that is, when $a \le ((\text{Occupied}(\text{Pool}1(x_i)))/(\text{Max}(\text{Pool}1(x_i)))) \le 1$ is satisfied, $H(x_i)$ will sum up all the evaluation values $\delta(x_j, y_n, x_i, y_m, l)(n \in N^*)$ of device $D(x_i, y_m)$ in Pool1(x_i) and the sum value is denoted as $S(x_i, y_m)$.

Then, $H(x_i)$ will verify the validity of $S(x_i, y_m)$. If $-\alpha \le S(x_i, y_m) \le \alpha$ is not satisfied, $H(x_i)$ considers this evaluation as malicious and deletes all the evaluations presented by the IoT device $D(x_i, y_m)$.

In the above discussion, Occupied(Pool1(x_i)) represents the storage capacity usage of pool Pool1(x_i), and Max (Pool 1(x_i)) represents the storage capacity of the pool. a and α are two critical value parameters which represent the storage capacity of the pool Pool1(x_i) and the repeating evaluation times of the evaluators, respectively. Based on the results of our multiple simulations, the performance of the model is well performed while $a = 0.6$ and $\alpha = 6$.

Then, $H(x_i)$ passes the remaining evaluations of Pool1(x_i) to Pool2(x_i). $H(x_i)$ queries on the blockchain $\{B_t \mid t \in N^*\}$ to obtain the latest normative trust NT(x_j, y_n, k) of $D(x_j, y_n)$. According to the deformation of Equation (3), the current trust scale value TC$(x_j, y_n, k) = f^{-1}(\text{NT}(x_j, y_n, k))$ of $D(x_j, y_n)$ can be obtained. If it fails to query the latest normative trust TC(x_j, y_n, k) of $D(x_j, y_n)$ on blockchain $\{B_t \mid t \in N^*\}$, $H(x_i)$ will calculate the trust scale value TC(x_j, y_n, k) of $D(x_j, y_n)$ using Equation (2). Then, using the condition $\text{TC}(x_j, y_n, k') = \text{TC}(x_j, y_n, k) + \sum_{l=1}^{t(x_i)} \delta(x_j, y_n, x_i, y_m, l)$, $H(x_i)$ can calculate the latest trust scale value TC(x_j, y_n, k') of $D(x_j, y_n)$. Finally, $H(x_i)$ calculates the latest normative trust NT(x_j, y_n, k') of $D(x_j, y_n)$ using Equation (3).

In this way, $H(x_i)$ calculates the normative trust NT(x_j, y_n, k') of all the IoT devices $D(x_j, y_n)$ that have been evaluated by other IoT devices in their domain and constructs the block body NT$\{\cdot\}$. All the normative trust NT(x_j, y_n, k') is organized in the form of a Merkle tree where the block head of the MR is added to the new block. $H(x_i)$ will form a new block with the newly generated block head and body NT$\{\cdot\}$ and then publish it to the blockchain.

Since there is no cooperation between $H(x_i)$ and $H(x_j)$ and the latest evaluation value is not obtained, the domain manager related to the cooperation in the block head is set to a specific value ρ (without losing generality, $\rho = 0$). These fields include trust scale value TC$(x_j, k-1)$, evaluation value $\delta(x_j, x_i, k-1)$, serial number k, transaction details Trl, signature $\sigma_{(H(x_j))}$(Trl) of $H(x_j)$on transaction information, mean value of trust MT$(x_j, k\text{-}1, r+1)$, risk value RV$(x_j, k\text{-}1, r+1)$, harmonic trustrank HT$(x_j, k-1, r+1)$, and $r + 1$.

At the same time, domain manager $H(x_j)$ of the domain of all the evaluated devices is stored in Head(B_t), which is convenient for the search of the trust data, and then, the new block $\{\text{Head}(B_t), \text{NT}\{\cdot\}\}$ is released to the blockchain, so as to ensure the timely update of the trust evaluation. The evaluation process is shown in Figure 4.

3.2.2. Scenario 2. When domain managers $H(x_i)$ and $H(x_j)$ cooperate, $H(x_i)$ evaluates the trust of $H(x_j)$ and its subordinate devices after the cooperation. $H(x_i)$ calculates the latest trust data of $H(x_j)$ and each IoT device evaluation result in domain x_j from domain x_i, generates the block head and body of the new block, and then publishes it to the blockchain.

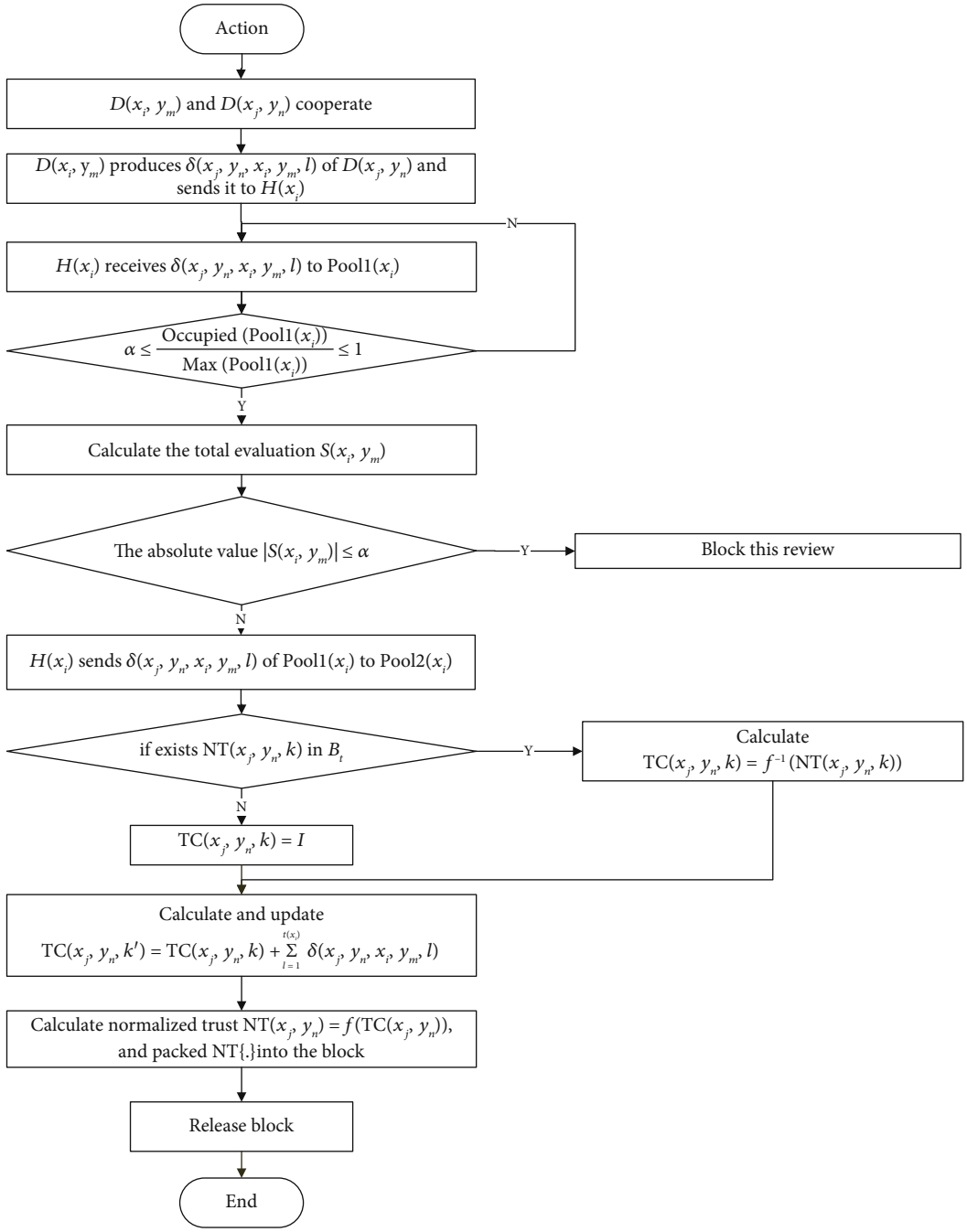
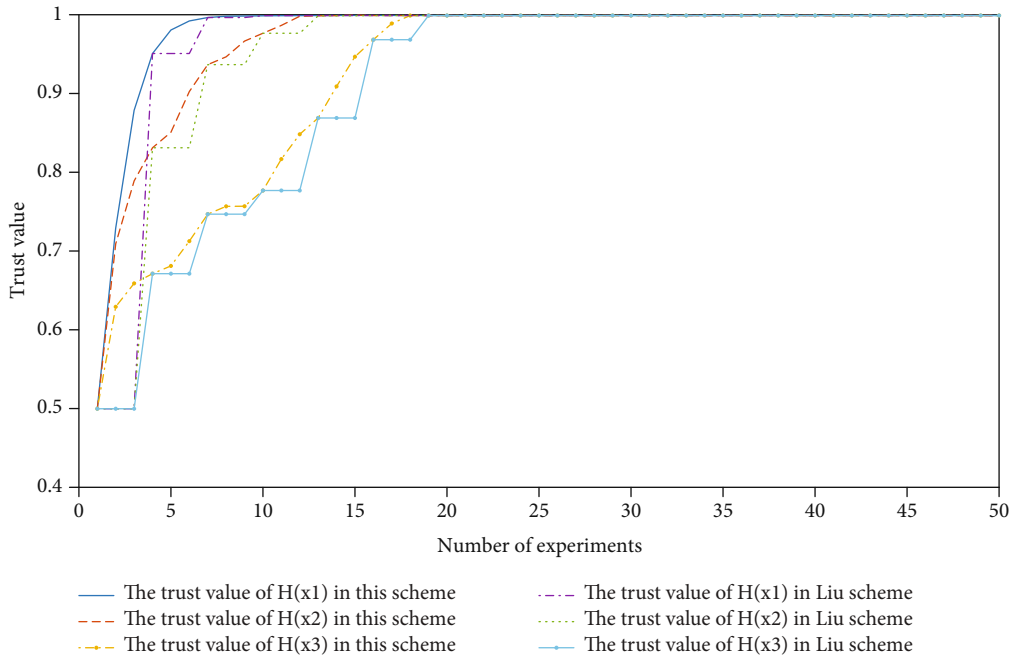


Figure 4: Evaluation flow between IoT devices.

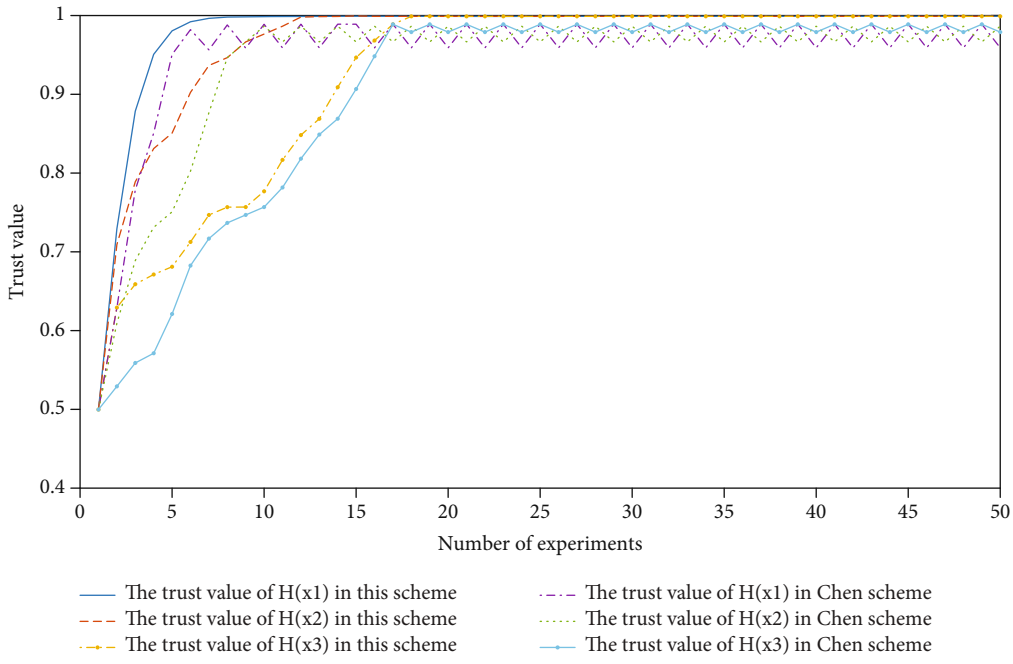
It is assumed that the evaluation value of $H(x_j)$from $H(x_i)$ is $\delta(x_j, x_i, k-1)$ at this time. $H(x_i)$ obtains $H(x_j)$'s current trust scale value TC$(x_j, k-2)$, serial number $k-1$, mean value of trust MT$(x_j, k-2, r)$, risk value RV$(x_j, k-2, r)$, harmonic trustrank HT$(x_j, k-2, r)$, and the number of the included risks r by querying the blockchain. $H(x_i)$ uses Equations (2) and (3) to calculate the latest trustrank TC$(x_j, k-1)$ and the latest normative trust NT$(x_j, k-1)$ of $H(x_j)$.

Then, $H(x_i)$ use Equations (4)–(6) to calculate the mean value of trust MT$(x_j, k-1, r+1)$, risk value RV$(x_j, k-1, r+1)$, and harmonic trustrank HT$(x_j, k-1, r+1)$ of $H(x_j)$. Finally, the fields related to this process are encapsulated in the block head Head(B_t) to form a new block. These fields include $H(x_j)$, TC$(x_j, k-1)$, $\delta(x_j, x_i, k-1)$, k, Trl, $\sigma_{(H(x_j))}$(Trl), RV$(x_j, k-1, r+1)$, HT$(x_j, k-1, r+1)$, and $r+1$.

At the moment, due to the frequent cooperation between domain manager $H(x_i)$ and the other domain managers, the time interval between the two trust data submissions is relatively short. During this period, the number of the evaluation of subordinate IoT device $D(x_i, y_m)(m = 1, 2, \cdots, n)$ stored in storage pool Pool1(x_i) of $H(x_i)$ is relatively small, so it is impossible to judge whether or not these malicious evaluations exist.

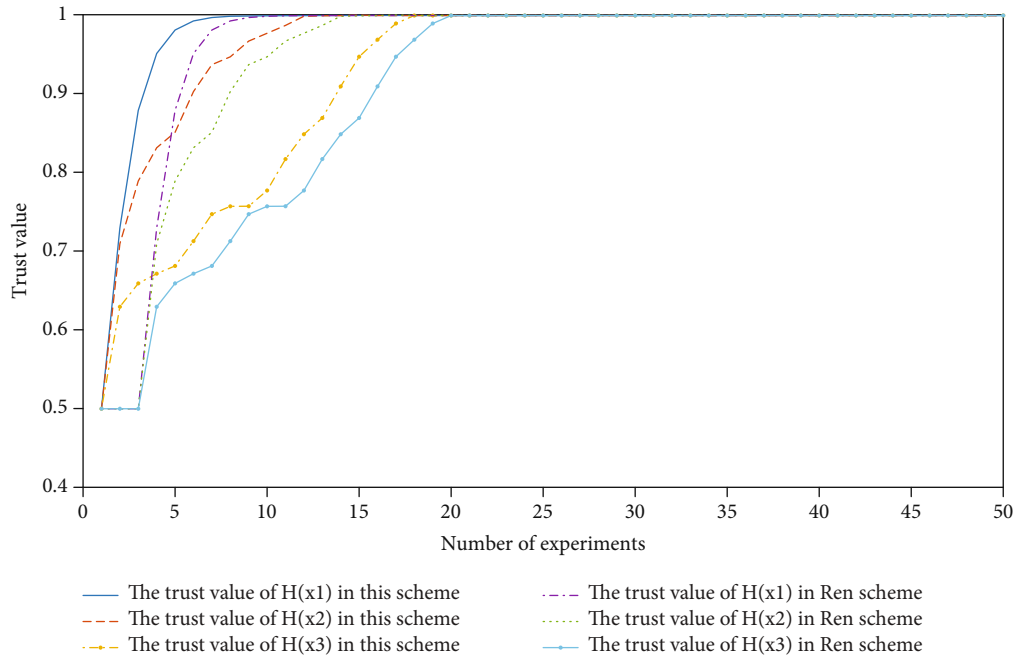


(a)



(b)

Figure 5: Continued.



(c)

Figure 5: Trends of the trustrank of the domain manager. (a) Trend of trustranks of our scheme and Liu's scheme. (b) Trend of trustranks of our scheme and Chen's scheme. (c) Trend of trustranks of our scheme and Ren's scheme.

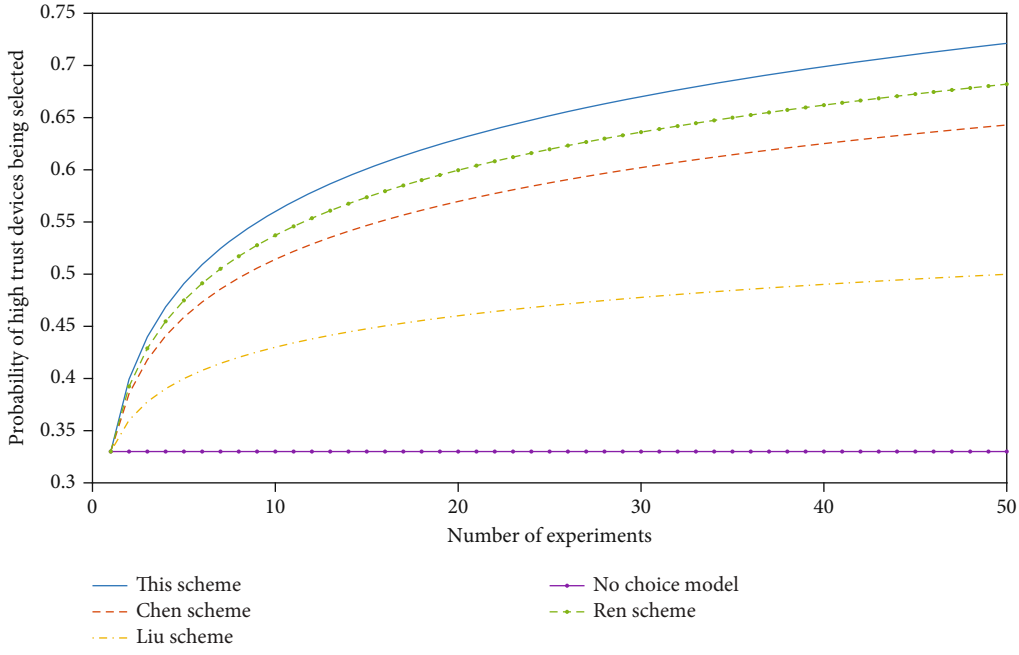


Figure 6: Comparison of the probability of a high-trust device being selected.

In this way, $H(x_i)$ sends all the evaluations stored in Pool1(x_i) to Pool2(x_i). In the subsequent work, $H(x_i)$ will iteratively calculate the evaluation data in Pool2(x_i) to obtain the trust data of the target IoT device and publish it to the blockchain. That is, $H(x_i)$ queries the current normative trustrank NT(x_j, y_n, k) of $D(x_j, y_n)(n \in N^*)$ in the blockchain and calculates the latest normative trust NT(x_j, y_n, k') of $D(x_j, y_n)$ according to Equations (2) and (3), where $k' = k + 1$. Then, $H(x_i)$ generates the block body NT$\{\cdot\}$ from the collection of NT(x_j, y_n, k') and forms a new block together with the block header Head(B_t) formed by the domain manager's trust data and then publish it to the blockchain.

The algorithm for the evaluation between the IoT devices is as follows.

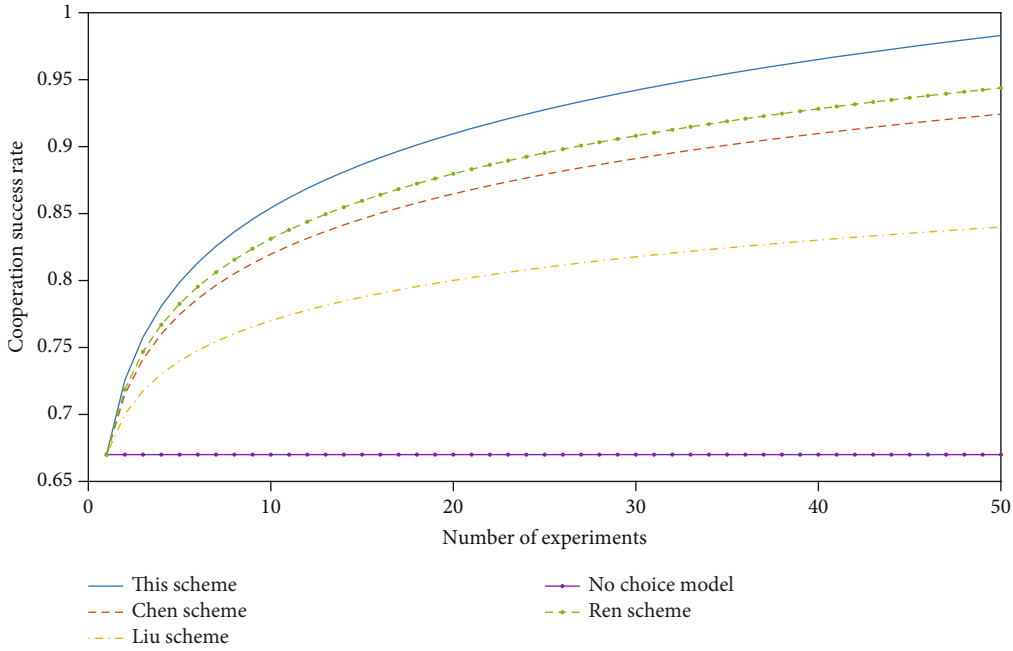


Figure 7: Comparison of cooperation success rates between devices.

Input: evaluation value $\delta(x_j, y_n, x_i, y_m, l)$ $(n \in N^*)$ given by subordinate device $D(x_i, y_m)$ of domain manager $H(x_i)$.

Output: new block B_t.

(1) *Evaluation Collection*. The storage $\text{Pool1}(x_i)$ of the domain manager continuously collects the evaluation value $\delta(x_j, y_n, x_i, y_m, l)$ given by the subordinate equipment and judges whether or not the storage space utilization rate satisfies the inequality $a \le (\text{Occupied}(\text{Pool1}(x_i))/\text{Max}(\text{Pool1}(x_i))) \le 1$ $(a = 0.6)$. If it is satisfied, $H(x_i)$ will sum up all the evaluation values $\delta(x_j, y_n, x_i, y_m, l)$ in $\text{Pool1}(x_i)$ according to the evaluation equipment $D(x_i, y_m)$ to obtain $S(x_i, y_m)$. We then judge whether or not $|S(x_i, y_m)| \le \alpha$ is satisfied. If it is, $H(x_i)$ passes the evaluation value in $\text{Pool1}(x_i)$ to $\text{Pool2}(x_i)$. Otherwise, we delete the evaluation.

(2) *Trust Data Query*. $H(x_i)$ queries on blockchain $\{B_t \mid t \in N^*\}$ to produce the latest normative trust $\text{NT}(x_j, y_n, k)$ of $D(x_j, y_n)$.

(3) *Trust Data Update*. If the query is successful, the current trust scale value $\text{TC}(x_j, y_n, k) = f^{-1}(\text{NT}(x_j, y_n, k))$ of $D(x_j, y_n)$ can be obtained according to the deformation of Equation (6) and then updated according to $\text{TC}(x_j, y_n, k') = \text{TC}(x_j, y_n, k) + \sum_{l=1}^{t(x_i)} \delta(x_j, y_n, x_i, y_m, l)$. If the query fails, $H(x_i)$ calculates the trust scale value $\text{TC}(x_j, y_n, k)$ of $D(x_j, y_n)$ according to Equation (2) and calculates $\text{NT}(x_j, y_n, k)$.

(4) *Block Publish*. The calculated $\text{NT}(x_j, y_n, k)$ constitutes the block body $\text{NT}\{\cdot\}$ of the new block, and $\text{NT}(x_j, y_n, k')$ is organized as a Merkle tree in the block header of the new block. $H(x_i)$ forms a new block together with the block body $\text{NT}\{\cdot\}$ and publishes it to the blockchain.

Table 1: Performance comparison table.

Scheme	Probability of high-trust devices being selected	Cooperation success rate
No choice model	0.33	0.67
Liu's	0.50	0.84
Chen's	0.64	0.92
Ren's	0.68	0.94
Our scheme	0.72	0.97

4. Performance Evaluation

In order to test the effectiveness of the proposed scheme, simulation experiments are carried out to analyze the update rate of trustranks, the probability of the high trustrank equipment being selected, and the success rate of the cooperation.

The experiment simulates three scenarios of the IoT domains and the corresponding IoT devices. The domain manager set is $H = \{H(x_1), H(x_2), H(x_3)\}$, including one malicious device and two benign devices. We used MATLAB to generate evaluation data for 50 device-to-device evaluations, simulating the trend of the trust data in the IoT trust model, the probability of high-trustrank devices being selected, and the success rate of cooperation between IoT devices. All the data are obtained by averaging the results of

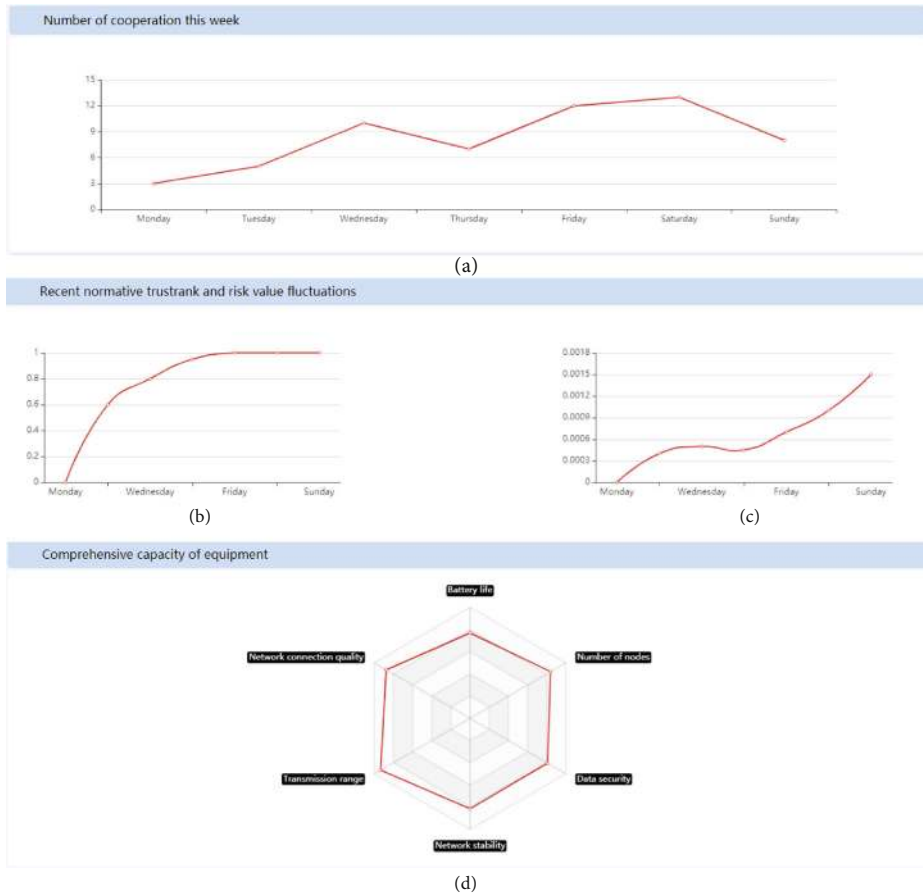


Figure 8: Detailed information of devices. (a) The numbers of cooperation with other devices in the last week. (b) The current trust value. (c) The cooperation stability in the last week. (d) The comprehensive performance analysis.

10 iterations. The experimental results are shown in Figures 5–7.

It can be seen from Figure 5(a) that the trustrank of Liu's scheme [6] is updated every fixed period of time, and the trustrank is not updated in a timely manner. However, the scheme proposed in this paper will immediately update the trustrank after each evaluation by the domain manager, which can reflect the trust status of the IoT devices and the domain managers in a timely manner, and provide more accurate services for the selection of the IoT devices. As can be seen from Figure 5(b), with the increase of the trustrank, in Chen's scheme [19], the trustrank will fluctuate when it converges, and the faster the convergence, the greater the fluctuation of the trustrank, which is not conductive to providing precise services for the selection of IoT devices. However, in this scheme that we proposed, with the increase of the trustrank, when the trustrank converges, the trustrank remains stable and no fluctuation occurs, which is more conducive to providing accurate services for equipment selection. It can be seen from Figure 5(c) that the update of trust in Ren's scheme [11] is slower than the evaluation scheme by almost two evaluation times, so the update speed of trust in this scheme is more timely.

It can be seen from Figure 5 and Table 1 that the selected probability of a high-trust device always remains unchanged at 0.33 in the no-trust model. With the increase of the number of the experiments (the number of the evaluations), compared with Liu's, Chen's, and Ren's schemes, the probability of high-trust devices being selected is steadily increased. However, this scheme has a faster rise rate, and the probability of being selected for high-trust IoT devices is also higher, which can provide a strong guarantee for the subsequent success rate of the cooperation.

It can be seen from Figure 6 and Table 1 that in the trustless model, the cooperation success rate remains unchanged at 0.67 since the IoT device is a randomly selected partner. With the increase of the number of the experiments (the number of the evaluations), the success rate of the cooperation between the devices in this scheme is steadily increasing compared with Liu's, Chen's, and Ren's schemes. However, our scheme has a faster rise rate and a higher cooperation success rate. It can effectively improve the success rate and reliability of the cooperation between the IoT devices.

5. Prototype System

To test the validity of the trust scheme, we implement the system prototype as follows.

5.1. IoT Device Details. The detailed information of the IoT device mainly includes four factors: the numbers of cooperation with other devices in the last week, the cooperation

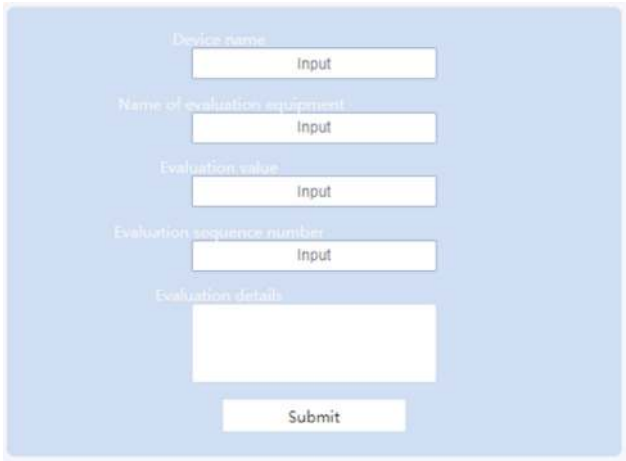


Figure 9: Evaluation operation of IoT devices.

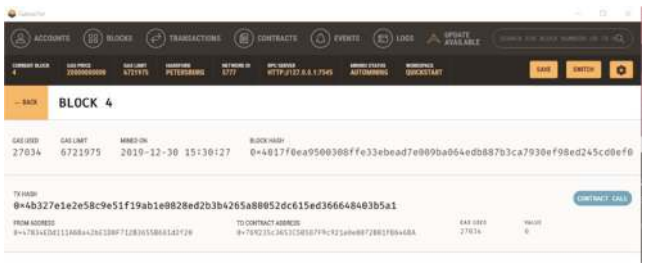


Figure 10: Block detailed information map.

stability in the last week, the current trust value, and the comprehensive performance analysis. Comprehensive consideration of risks can determine the trustworthiness of the device and the expected trust value that can be achieved in cooperation, which can help users select the most trusted devices for cooperation. The gradually changing curves of the detailed information of the IoT device are shown as in Figure 8, showing the four parameters' changing trends.

5.2. Evaluation of IoT Devices. After the users complete the cooperation, they can evaluate the cooperation according to the performance of the other party device. By filling in the information of the evaluated device, the evaluating device, and the evaluation value, the evaluation process is completed by the evaluation submission operation. The evaluation submission model is shown in Figure 9.

The trust management model in the distributed Internet of Things proposed in Section 2 calculates and updates the trust value of the evaluated device, completes the release of blocks by calling smart contracts, and realizes the sharing and synchronization of trust data.

5.3. Trust Data Block Generation. As shown in Figure 10, detailed information such as the block's hash value, block generation address, and contract address is generated. Click CONTRACT CALL to enter the transaction detail information; as shown in Figure 11, we can see the transaction data hash value.

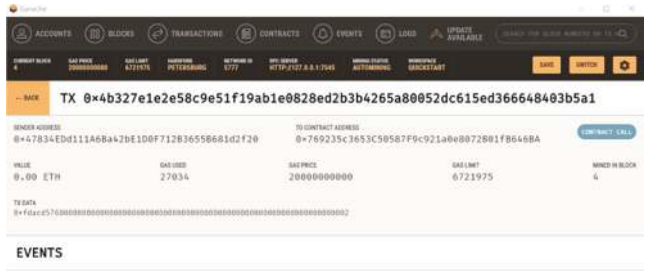


Figure 11: Details of the transactions in the block.

6. Conclusion

Aiming at the problem that the current trust mechanism relies on a trusted third party or additional trust assumptions, which leads to the vulnerability of trust data to malicious attacks, in this paper, we quantify trust into normative trust and risk measure, which can construct a comprehensive review of normative trust, and we propose a trust mechanism for distributed IoT, which modifies the storage structure of the domain manager and realizes the identification and shielding of malicious evaluations between IoT devices, solves the secure storage and sharing of trust data, and can select the device that performs well and stable. Then, it performs well in improving the success rate and reliability of cooperation on IoT devices. However, the mechanism in this paper also increases the storage space requirements of the domain manager, and how to work out this problem is the focus of the future work.

Data Availability

There is no data included in this paper.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was partly funded by the European Union Horizon 2020 DOMINOES Project (Grant Number 771066).

References

[1] W. Zhong, X. Yin, X. Zhang et al., "Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment," *Computer Communications*, vol. 157, pp. 116–123, 2020.

[2] X. Yu, H. Wang, X. Zheng, and Y. Wang, "Effective algorithms for vertical mining probabilistic frequent patterns in uncertain mobile environments," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 23, no. 3/4, pp. 137–151, 2016.

[3] X. Zheng and H. Liu, "A scalable coevolutionary multi-objective particle swarm optimizer," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 3, no. 5, pp. 590–600, 2010.

[4] L. Wang, X. Zhang, R. Wang, C. Yan, H. Kou, and L. Qi, "Diversified service recommendation with high accuracy and efficiency," *Knowledge-Based Systems*, vol. 204, p. 106196, 2020.

[5] A. Zhou, S. Wang, S. Wan, and L. Qi, "LMM: latency-aware micro-service mashup in mobile edge computing environment," *Neural Computing and Applications*, vol. 32, no. 19, pp. 15411–15425, 2020.

[6] X. Yu, W. Feng, H. Wang, Q. Chu, and Q. Chen, "An attention mechanism and multi-granularity-based Bi-LSTM model for Chinese Q&A system," *Soft Computing*, vol. 24, no. 8, pp. 5831–5845, 2020.

[7] S. Wan, R. Gu, T. Umer, K. Salah, and X. Xu, "Toward offloading Internet of vehicles applications in 5G networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2020.

[8] C. Chen, Y. Zhang, M. Khosravi, Q. Pei, and S. Wan, "An intelligent platooning algorithm for sustainable transportation systems in smart cities," *IEEE Sensors Journal*, p. 1, 2020.

[9] L. Li, T. T. Goh, and D. Jin, "How textual quality of online reviews affect classification performance: a case of deep learning sentiment analysis," *Neural Computing and Applications*, vol. 32, no. 9, pp. 4387–4415, 2020.

[10] S. Wan, X. Xu, T. Wang, and Z. Gu, "An intelligent video analysis method for abnormal event detection in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2020.

[11] Y. Cao, H. Song, O. Kaiwartya et al., "Mobile edge computing for big-data-enabled electric vehicle charging," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 150–156, 2018.

[12] J. Wang, "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207–1228, 2011.

[13] L. Qi, C. Hu, X. Zhang et al., "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[14] Y. Wang, G. Yang, T. Li, F. Li, Y. Tian, and X. Yu, "Belief and fairness: a secure two-party protocol toward the view of entropy for IoT devices," *Journal of Network and Computer Applications*, vol. 161, p. 102641, 2020.

[15] F. Li, C. Cui, D. Wang et al., "Privacy-aware secure anonymous communication protocol in CPSS cloud computing," *IEEE Access*, vol. 8, pp. 62660–62669, 2020.

[16] Z. Lv, H. Song, P. Basanta-Val, A. Steed, and M. Jo, "Next-generation big data analytics: state of the art, challenges, and future research topics," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1891–1899, 2017.

[17] Y. Wu, H. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in Industry 4.0," *IEEE Internet of Things Journal*, 2020.

[18] Y. Liu, Y. Gong, and Y. Feng, "Trust system based on node behavior detection in Internet of Things," *Journal of Communications*, vol. 35, no. 5, pp. 8–15, 2014.

[19] X. Li, *Design and Analysis of Revisable Reputation Evaluation System Based on Blockchain [Doctoral Dissertation]*, Xi'an: Xidian University, 2018.

[20] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internet of Things," *China Communications*, vol. 11, no. 2, pp. 148–156, 2014.

[21] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: a context-aware and multi-service approach," *Computers & Security*, vol. 39, pp. 351–365, 2013.

[22] X. Liu, X. Yu, H. Zhu, G. Yang, Y. Wang, and X. Yu, "A game-theoretic approach of mixing different qualities of coins," *International Journal of Intelligent Systems*, vol. 35, no. 12, pp. 1899–1911, 2020.

[23] Y. Wang, A. Bracciali, G. Yang, T. Li, and X. Yu, "Adversarial behaviours in mixing coins under incomplete information," *Applied Soft Computing*, vol. 96, p. 106605, 2020.

[24] W. M. LIU, L. H. YIN, B. X. FANG, and H. L. ZHANG, "A hierarchical trust model for the Internet of Things," *Chinese Journal of Computers*, vol. 35, no. 5, pp. 846–855, 2012.

[25] H. Benkerrou, S. Heddad, and M. Omar, "Credit and honesty-based trust assessment for hierarchical collaborative IoT systems," *IEEE*, pp. 295–299, 2016.

[26] X. Chi, C. Yan, H. Wang, W. Rafique, and L. Qi, "Amplified locality-sensitive hashing-based recommender systems with privacy protection," *Concurrency and Computation: Practice and Experience*, 2020.

[27] Y. Ren, X. Li, and H. Liu, "Blockchain-based trust management framework for distributed Internet of Things," *Journal of Computer Research and Development*, vol. 7, pp. 108–124, 2018.

[28] X. Shen, Q. Pen, and X. Liu, "Survey of block chain," *Journal of Network and Information Security*, vol. 11, pp. 11–20, 2016.

[29] D. Li and J. Wei, "Theory, application fields and challenge of the blockchain technology," *Telecommunications Science*, vol. 12, pp. 10–14, 2016.

[30] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui, and M. Zhao, "Randomness invalidates criminal smart contracts," *Information Sciences*, vol. 477, pp. 291–301, 2019.

[31] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: a survey," *Wireless Networks*, vol. 26, no. 8, pp. 5579–5593, 2020.

[32] L. Zhang, Y. Wang, F. Li, Y. Hu, and M. H. Au, "A game-theoretic method based on Q-learning to invalidate criminal smart contracts," *Information Sciences*, vol. 498, pp. 144–153, 2019.

[33] Y. Wang, G. Yang, A. Bracciali et al., "Incentive compatible and anti-compounding of wealth in proof-of-stake," *Information Sciences*, vol. 530, pp. 85–94, 2020.

[34] G. Yang, Y. Wang, Z. Wang, Y. Tian, X. Yu, and S. Li, "IPBSM: an optimal bribery selfish mining in the presence of intelligent and pure attackers," *International Journal of Intelligent Systems*, vol. 35, no. 11, pp. 1735–1748, 2020.

[35] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2019.

[36] Y. Wang, M. Zhao, Y. Hu, Y. Gao, and X. Cui, "Secure computation protocols under asymmetric scenarios in enterprise information system," *Enterprise Information Systems on*, pp. 1–21, 2019.

[37] C. Cui, F. Li, T. Li, J. Yu, R. Ge, and H. Liu, "Research on direct anonymous attestation mechanism in enterprise information management," *Enterprise Information Systems*, pp. 1–17, 2019.

[38] Q. Shao, C. Jin, and Z. Zhang, "Blockchain: architecture and research progress," *Chinese Journal of Computers*, vol. 41, pp. 3–22, 2018.