# Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems

Xiaoding Wang, Sahil Garg, *Member, IEEE*, Hui Lin, Georges Kaddoum, *Senior Member, IEEE*, Jia Hu, and Mohammad Mehedi Hassan, *Senior Member, IEEE*

***Abstract*— The fifth-generation (5G) wireless communication technology enables high-reliability and low-latency communications for the Intelligent Transportation System (ITS). However, the growingly sophisticated attacks against 5G-enabled ITS (5G-ITS) might cause serious damages to the valuable data generated by various ITS applications. Therefore, establishing a secure 5G-ITS through trust evaluation against potential threats has become a key objective. Furthermore, as a distributed shared ledger and database, Blockchain has the characteristics of non-tampering, traceability, openness and transparency, can support both trust storage and trust verification for trust evaluation. In this paper, we propose a heterogeneous Blockchain based Hierarchical Trust Evaluation strategy, named BHTE, utilizing the federated deep learning technology for 5G-ITS. Specifically, the trusts of ITS users and task distributers are evaluated using the federated deep learning and hierarchical incentive mechanisms are designed for reasonable and fair rewards and punishments. Moreover, the trusts of ITS users and task distributers are stored on heterogeneous and hierarchical blockchains for trust verification. The extensive experiment results show that: (i) the proposed BHTE can achieve reasonable and fair trust evaluations on both ITS users and task distributers; (ii) the BHTE performs excellently with high system throughput and low latency.**

***Index Terms*— Blockchain, trust evaluation, 5G, intelligent transportation systems, federated learning.**

## I. Introduction

INTELLIGENT Transportation System (ITS) [1] is a new type of transportation system that uses cutting-edge technology to transform the traditional transportation system into an informatized, intelligent, and socialized transportation system. ITS can maximize the efficiency of transportation infrastructure and improve the quality of services; at the same time, it enables society to use transportation facilities and energy efficiently [2], thereby obtaining huge social and economic benefits. It can not only solve the problem of traffic congestion, but also has a huge impact on traffic safety, traffic accident handling and rescue, passenger and cargo transportation management, and road toll systems. Starting in 2020, the global transportation system will enter a stage of rapid development, and interconnection and networking will be greatly improved compared to the past. The deployment of the fifth-generation (5G) communication technology [3] will also accelerate significantly in 2020. As of January 2020, commercial 5G networks have been deployed in 378 cities in 34 countries around the world. This will also help promote the development of intelligent transportation. Specifically, 5G networks mainly bring higher speed and more stable network connections to intelligent transportation, thus giving birth to 5G-enabled intelligent transportation systems (5G-ITS) [4]–[6].

In 5G-ITS, two major types of security threats, external threats and internal threats, severely endanger various ITS applications by injecting incorrect traffic, environment, routing and navigation data [7]. However, external threats can be prevented through effective identity authentication [8], and internal threats can be prevented through trust management [9]. Trust management plays a vital role in maintaining the efficient operation of ITS supporting 5G and ensuring the authenticity of data. As an important part of trust management, trust evaluation that quantifies trust by analyzing relevant data is widely used in social networks, digital communications, e-commerce, cloud services, and intelligent transportation systems. Because accurate trust evaluation often requires a large amount of data, this poses a major challenge to data collection, analysis, and processing.

In fact, machine learning technology has been proven to be efficient in data processing, making it suitable for accurate and efficient trust evaluation [10]. However, the learning process that requires access to data containing sensitive user information may lead to serious privacy violations. Federated learning [11], as a novel learning framework, does not require direct access to real data sets, which provides the possibility

Manuscript received 13 June 2021; revised 12 October 2021; accepted 2 November 2021. Date of publication 1 December 2021; date of current version 8 February 2023. This work was supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP-2021/18. The Associate Editor for this article was S. Mumtaz. *(Corresponding authors: Hui Lin; Jia Hu.)*

Xiaoding Wang and Hui Lin are with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China, and also with the Engineering Research Center of Cyber Security and Education Informatization, Fujian Province University, Fuzhou, Fujian 350117, China (e-mail: wangdin1982@fjnu.edu.cn; linhui@fjnu.edu.cn).

Sahil Garg and Georges Kaddoum are with the École de technologie supérieure (ETS), Montreal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org; georges.kaddoum@etsmtl.ca).

Jia Hu is with the Department of Computer Science, University of Exeter, Exeter EX4 4PY, U.K. (e-mail: j.hu@exeter.ac.uk).

Mohammad Mehedi Hassan is with the Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mmhassan@ksu.edu.sa).

Digital Object Identifier 10.1109/TITS.2021.3129417

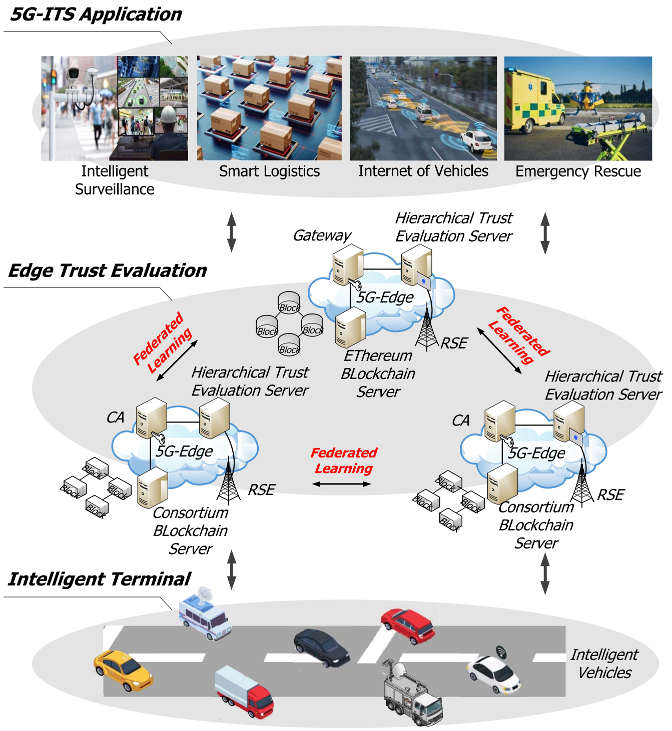


Fig. 1. Heterogeneous Blockchain and Federated Learning based Trust Evaluation Architecture for 5G-enabled ITS.

of privacy-protected machine learning. In addition, as a distributed shared ledger and database, the blockchain [12] has the characteristics of decentralization, non-tampering, traceability, openness and transparency, and supports trust storage and trust verification for trust evaluation. However, in real scenarios, heterogeneous blockchains are often deployed in heterogeneous networks [13]. The heterogeneity of blockchains poses a great challenge to trust storage and trust verification.

According to above analysis, a trust evaluation architecture (see Fig. 1) for 5G-enabled ITS is presented based on both heterogeneous blockchain and edge computing empowered federated learning. The architecture can be divided into three layers: the 5G-ITS application layer, the edge trust evaluation layer, and the intelligent terminal layer. In this architecture, the edge trust evaluation layer is consist of (I) edge servers that are responsible for trust evaluation based on data provided by intelligent vehicles at the intelligent terminal layer through roadside equipment (RSE) and (II) heterogeneous blockchain servers that account for trust verification and storage, and they can support various 5G-ITS applications, i.e., intelligent surveillance, smart logistics, internet of vehicles and emergency rescue. Based on this architecture, a heterogeneous Blockchain based Hierarchical Trust Evaluation strategy, named BHTE, is proposed utilizing federated deep learning for 5G-ITS. The main contribution of this paper is summarized as follows:

1) To achieve hierarchical trust evaluations and meanwhile preserve users' privacy for 5G-ITS, the federated deep learning is applied to evaluate the trusts of ITS users and task distributers. In addition, hierarchical incentive mechanisms are developed to accomplish reasonable and fair rewards and punishments so as to ensure the efficiency and accuracy of trust evaluation.
2) To realize trust verification, heterogeneous and hierarchical blockchains are employed to store the trusts of ITS users and task distributers. Specifically, as a hierarchical task distribution, ITS task distributers receive tasks from the ITS task provider and then distribute tasks to ITS users. Then, the trusts of ITS users and task distributers are evaluated and stored on heterogeneous and hierarchical blockchains.
3) The extensive experiment results show that: (i) the proposed BHTE can achieve reasonable and fair trust evaluation on both users and task distributers in 5G-ITS; (ii) the BHTE performs excellently in high system throughput and low latency.

The rest of this paper is organized as follows. Section II presents the related work. Section III introduces the system model and the attack model. Section IV gives the implementation details of the BHTE. Section V presents the performance evaluation. Section VI concludes this paper.

## II. Related Work

The trust evaluation for 5G-enabled intelligent transportation systems has drawn a great attention with plenty of excellent works proposed.

In [14], a conditional privacy-preserving and blockchain-based trust management scheme is proposed. In this scheme, vehicles can send messages anonymously in the untrusted environment. In addition, this scheme supports trust management using the blockchain-based technology to ensure the credibility of messages and vehicles' trusts are stored in the blockchain. In [15], an efficient trust-based intrusion detection framework is developed for autonomous vehicular networks. In this framework, the trust of each autonomous driving vehicle is evaluated first using the relevant information obtained from roadside units. Based on the trust evaluation, an intrusion detection system is proposed. Then, a machine learning based incentive mechanism is designed for stimulating reporting warnings. In [16], all GPS data, on-Board unit and safety messages are considered to evaluate the overall trustworthiness of a self-driving vehicle utilizing all certainlogic, beta distribution function and dempster-shafer theory In [17], a probabilistic graph model is used to evaluate the credibility of sensor nodes based on collected data and communication behavior, and to schedule nodes to reduce the moving distance. In [18], Wang *et al.* first transformed the credit evaluation problem into an optimization problem and proposed a heuristic mobile strategy. This strategy uses the largest neighbor distance ratio to schedule vehicles, thereby improving the efficiency of trust evaluation. In [19], a trust system that allows vehicles to make more reliable and safe decisions is proposed. The system evaluates the trust level of the vehicle and surrounding vehicles based on the current situation. In [20], a decentralized trust management scheme using blockchain is proposed. This solution uses blockchain sharding to increase transaction throughput, reduce the load on the main blockchain, update and maintain consistent and reliable trust values, and encourage peer to perform well. In [21], a VANET architecture based on software-defined trust is proposed, and the deep Q-learning method is used to obtain the best communication link strategy. The joint optimization problem of the trust degree and the reverse delivery rate of each vehicle is modeled by the Markov decision process, and finally solved by the machine learning method. In [22], a trust management model based on blockchain is proposed to realize location privacy protection. This scheme ensures the privacy and security of the vehicle by constructing an anonymous hidden area, and uses a trust management algorithm to constrain and regulate the behavior of the vehicle, and finally uses the blockchain to realize the data security of the vehicle.

Although these works contribute to the trust evaluation for 5G-ITS, there remain two problems: (i) how to achieve accurate and fair trust evaluation with the consideration of privacy preservation; (ii) how to verify users' trust through heterogeneous blockchains. In this paper, a heterogeneous Blockchain based Hierarchical Trust Evaluation strategy (BHTE) is proposed utilizing the federated deep learning technology for 5G-ITS to solve these problems.

## III. System Model

To achieve reasonable and fair trust evaluation for 5G-ITS, three entities, namely ITS task releasers, users and gateways, are considered. Fig. 2 gives the system model of the proposed BHTE.

As shown in Fig. 2, there are two types of ITS task releasers, i.e., the ITS Task Provider (ITS-TP) and the ITS Task Distributer (ITS-TD). The ITS-TP releases tasks (i.e., reporting traffic incident, environment, route, navigation through crowdsensing) to regional task-blockchains. Each ITS-TD divides the tasks released by the ITS-TP into different levels of tasks according to users' trusts. Specifically, a task distributor will provide three levels of A, B, and C tasks, i.e., the level A tasks require the highest user trust, while the level C tasks require the lowest user trust. Accordingly, the ITS-TD publishes the three levels of tasks on three regional task chains. Then, ITS-users of a certain region accept the tasks only if they can meet the trust requirements, i.e., the trust of each ITS-user should be higher than that of the task such that the ITS-TD might sign the smart contract with the ITS-user. Based on task completion, ITS-users of a specific region are either rewarded or punished by the regional ITS-TD, and then their trusts will be evaluated and stored on the corresponding regional trust-blockchain. Next, each ITS-TD uploads the task completion and trusts of ITS-users to the corresponding ITS-TP. As a result, ITS-TDs will be rewarded or punished by the ITS-TP, and the trusts of ITS-TDs and ITS-users are stored on the global trust-blockchain. Furthermore, given the privacy concern and the difficulty in model training for some ITS-TDs, a federated deep learning algorithm is developed to construct the unified trust evaluation model. Considering the regional difference, heterogeneous blockchains of different regions might have different structures (i.e., the number of sub-chains, the existence of CA, etc.). That suggests the data exchange between heterogeneous blockchains requires data transformation through gateways.

In this system model, two type of attacks, namely the task sabotage attack and the privacy leakage attack, should be considered.

1) *Task Sabotage Attack*: Such attack is launched by malicious ITS-users who aim to sabotage the tasks, i.e., deliberately leaving the task uncompleted. To prevent such attack, the trust requirement is introduced to the task acceptance such that only ITS-users of higher trusts can apply for tasks.
2) *Privacy Leakage Attack*: Since each ITS-TD is assumed to be semi-trusted, sharing data about ITS-users with other ITS-TDs during the local trust evaluation might expose users' privacy. Therefore, the federated deep learning mechanism eliminates the need to directly access the data of ITS-users to prevent privacy leakage. On the other hand, ITS-TP could also suffer from privacy leakage attack due to malicious ITS-users might learn sensitive task information. In literature [23], [26], we have already proposed a task and ITS-user partition mechanism against such attack, in which the budget of the task releaser is assumed to be limited. However, only dynamic budget adjustments can reward or punish ITS-users fairly. This is achieved through the hierarchical incentives of the hierarchical task allocation mechanism designed in this paper.

## IV. The Implementation of the Proposed BHTE

The proposed strategy BHTE consists of three modules, namely the hierarchical task distribution module, the hierarchical trust evaluation module, and the trust storage and verification module. All three modules collaborate to provide the heterogeneous blockchain based hierarchical trust evaluation for 5G-ITS.

### A. Hierarchical Task Distribution

In this paper, we consider the hierarchical task distribution scenario. According to the system model, there are two types of task blockchains, i.e., the global task-blockchains and the regional task-blockchains. Note that global blockchains might be heterogeneous to regional blockchains, while the blockchains are homogeneous within each region. This provides the opportunity of hierarchical task distribution. To be specific, the ITS-TP releases a number of tasks on each global task-blockchain for the corresponding ITS-TD of a specific region, in which the ITS-TD plays the role of a task receiver. Then, the ITS-TD distributes the tasks received from the ITS-TP on the corresponding regional task-blockchains for ITS-users, where ITS-users serve as task receivers. In fact, based on such hierarchical task distribution, we are able to design a reasonable and fair incentive mechanism to reward/punish task receivers hierarchically such that the budget for each ITS-TD can be adjusted dynamically for better trust evaluation.

### B. Hierarchical Trust Evaluation

Based on the hierarchical task distribution, we give the corresponding trust evaluation. Specifically, each ITS-TD of a

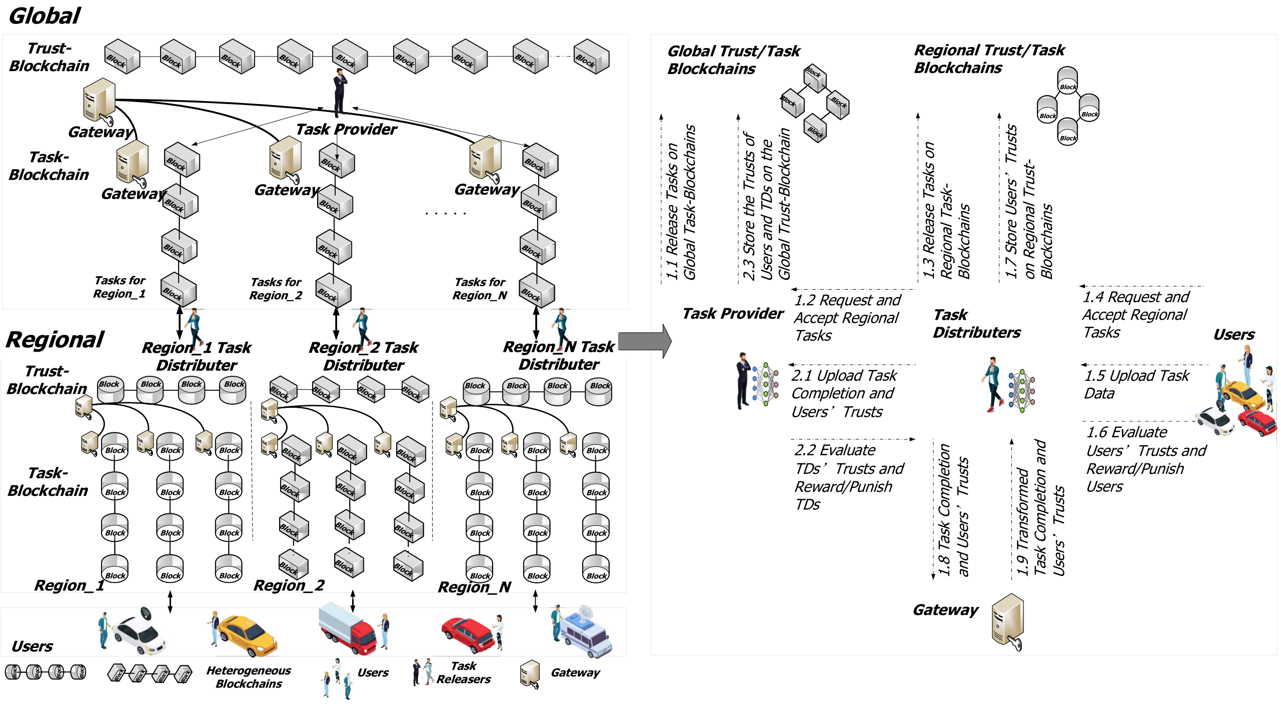

Global
Trust-Blockchain
Block
Gateway
Task Provider
Task-Blockchain
Gateway
Gateway
Gateway
. . . . .
Tasks for Region_1
Tasks for Region_2
Tasks for Region_N
Regional
Region_1 Task Distributer
Region_2 Task Distributer
Region_N Task Distributer
Trust-Blockchain
Task-Blockchain
Region_1
Region_2
Region_N
Users
Heterogeneous Blockchains
Users
Task Releasers
Gateway
Global Trust/Task Blockchains
Regional Trust/Task Blockchains
1.1 Release Tasks on Global Task-Blockchains
2.3 Store the Trusts of Users and TDs on the Global Trust-Blockchain
1.3 Release Tasks on Regional Task-Blockchains
1.7 Store Users' Trusts on Regional Trust-Blockchains
Task Provider
1.2 Request and Accept Regional Tasks
Task Distributers
1.4 Request and Accept Regional Tasks
Users
2.1 Upload Task Completion and Users' Trusts
1.5 Upload Task Data
2.2 Evaluate TDs' Trusts and Reward/Punish TDs
1.6 Evaluate Users' Trusts and Reward/Punish Users
1.8 Task Completion and Users' Trusts
1.9 Transformed Task Completion and Users' Trusts
Gateway

Fig. 2. The system model of the proposed BHTE.

specific region evaluates the trusts of ITS-users within. Then, the ITS-TP evaluates the trusts of all ITS-TDs. Note that the ITS-TP applies the deep reinforcement learning algorithm for trust evaluation on ITS-TDs due to the assumption that the ITS-TP is fully-trusted. In addition, all ITS-TDs perform trust evaluation on ITS-users utilizing the federated deep learning algorithm for privacy preservation because ITS-TDs are assumed to be semi-trusted.

*1) Trust Evaluation on ITS-Users Utilizing Federated Deep Learning:* To evaluate the trust of the $i$th specific ITS-user $u_i$, the task completion $\mathcal{C}_{u_i}$ of the ITS-user is considered. In this paper, the completion rate $\mathcal{CR}_{u_i,t_j}$ on each task $t_j$ that $u_i$ accepts is used to calculate the task completion $\mathcal{C}_{u_i}$, i.e., $\mathcal{C}_{u_i} = \alpha \cdot \mathcal{CR}_{u_i,t_j}$. Suppose the tasks $t_j$ is released with a trust bonus $\mathcal{TB}_{t_j}$, based on the task completion $\mathcal{C}_{u_i}$, the $i$th ITS-user's trust $\mathcal{T}_{u_i}$ can be updated by measuring the task completion as

$$\begin{cases} \mathcal{T}_{u_i} \rightarrow \mathcal{T}_{u_i} + \mathcal{TB}_{t_j}, & if\ \mathcal{C}_{u_i} \geq 0.5 \\ \mathcal{T}_{u_i} \rightarrow \mathcal{T}_{u_i} - \mathcal{TB}_{t_j}, & otherwise, \end{cases} \tag{1}$$

Note that the sum of each task trust bonus $\mathcal{TB}_{t_j}$ equals to the budget of task trust bonus $\mathcal{TB}^{Budget}$ set by the corresponding ITS-TD. Although Eq. (1) can quantify the update of each ITS-user's trust, a well-designed reward/punishment mechanism is required to encourage honest ITS-users and punish malicious ones for better task completion of ITS-users. Note that each ITS-user will get the trust bonus if the task is actually completed, i.e., the completion rate $\mathcal{C}_u$ is above the threshold 0.5. However, many ITS-users might not be able to complete the tasks, therefore it is reasonable and fair to share the corresponding trust bonuses by the ITS-users who actually complete the tasks. Therefore, we introduce the *softmax* function to calculate the distinguishable "share" for each task-completed ITS-user. For example, if there are $\mathcal{M}$ ITS-users complete the tasks including $u_i$ and up to $\mathcal{K}$ tasks failed to be completed, then the ITS-user $u_i$ can receive an extra trust bonus $\mathcal{TB}^{Extra}_{u_i}$, i.e.,

$$\mathcal{TB}^{Extra}_{u_i} = \sum_{k=1}^{\mathcal{K}} \mathcal{TB}_{t_k} \cdot [e^{\mathcal{C}_{u_i} - 0.5} / \sum_{j=1}^{\mathcal{M}} e^{\mathcal{C}_{u_j} - 0.5}], \tag{2}$$

Then, we update $\mathcal{T}_{u_i}$ by

$$\mathcal{T}_{u_i} \rightarrow \mathcal{T}_{u_i} + \mathcal{TB}_{t_j} + \mathcal{TB}^{Extra}_{u_i}. \tag{3}$$

According to the latest trust, the ITS-user can apply for the tasks with the corresponding trust requirement.

Note that the parameter $\alpha$ determines the trust of ITS-user. Thereby, each ITS-TD should discover the optimal parameters for reasonably and fairly evaluating ITS-users' trusts and encouraging ITS-users to perform well in task completion. In fact, the Deep Reinforcement Learning (DRL) algorithm, i.e., Deep Deterministic Policy Gradient (DDPG), can be used by the ITS-TD to find the optimal parameters by building the regional trust evaluation model. However, considering the difficulties in model training for some ITS-TDs and the privacy preservation for ITS-users, we develop a federated deep learning algorithm that integrates the federated learning framework and the deep reinforcement learning algorithm DDPG. In general, $\mathcal{L}$ ITS-TDs train their own regional trust evaluation models and sent them to the fusion server. Then, the fusion server gives each regional model a specific weight. As a result, the universal model is built as the weighted average of all regional models without access to the real data-set of each region that contain sensitive information about ITS-users.

Thus, ITS-users' privacy is preserved, considering that all ITS-TDs are assumed to be semi-trusted.

Specifically, for the $j$th ITS-TD, the algorithm DDPG requires 4 neural networks [24], namely an actor network $\pi$, a critic network $Q$ and their target networks $\pi'$ and $Q'$. The actor network make a choice about which action $a$ should be taken for the state $s$, while the critic network assesses this choice. In the trust evaluation, we consider the state $s$ consists of the participation of all ITS-users, i.e., $s = (\mathcal{P}_{u_1}, \mathcal{P}_{u_2}, \ldots, \mathcal{P}_{u_N})$ with $\mathcal{P}_{u_i} = 0$ and $\mathcal{P}_{u_i} = 1$ indicating the $i$th ITS-user does and does not take any task respectively. Then, let the parameter $\alpha$ comprise the action $a$, i.e., $a = \alpha$. Based on the current state $s$, the action $a$ is chosen and the reward $r$ is calculated. In fact, the ITS-user's reaction on the trust evaluation, which can be observed from the task completion, is somehow related to the reward. Therefore, the reward is given by

$$r = \frac{1}{\mathcal{N}_j} \sum_{i=1}^{\mathcal{N}_j} \tilde{\mathcal{C}}_{u_i}, \tag{4}$$

where $\mathcal{N}_j$ denotes the number of ITS-users who work for the $j$th ITS-TD, $\zeta_j$ represents the importance factor of the $j$th task $t_j$ that the $i$th ITS-user $u_i$ accepts (i.e., a task of a higher trust requirement is of more importance), $\mathcal{O}$ denotes the number of tasks that the ITS-user $u_i$ accepts during the interval of decision-making on action $a$, and $\tilde{\mathcal{C}}_{u_i} = \frac{1}{\mathcal{O}} \sum_{j=1}^{\mathcal{O}} \mathcal{CR}_{u_i,t_j} \cdot \zeta_j$.

In the training process of DDPG, we sample $N$ experience to update the critic network with the loss function

$$\mathcal{L}(\vartheta^Q) = \frac{1}{N} \sum_{i=1}^{N} [Q(s_i, a_i | \vartheta^Q) - \mathcal{Y}_i]^2, \tag{5}$$

where

$$\mathcal{Y}_i = r_i + \gamma\, (Q(s_{i+1}, \pi(s_{i+1} | \vartheta^{\pi'}) | \vartheta^{Q'})). \tag{6}$$

Accordingly, we update $\pi$ utilizing policy gradient as

$$\nabla_{\vartheta^\pi} J = \frac{1}{N} \sum_{i=1}^{N} [\nabla_a Q(s, a | \vartheta^Q) | s = s_i, a = \pi(s_i | \vartheta^\pi) \\ \nabla_{\vartheta^\pi} \pi(s | \vartheta^\pi) | s = s_i]. \tag{7}$$

When $\pi$ and $Q$ are updated, the parameters of target networks $\vartheta^{Q'}$ and $\vartheta^{\pi'}$ are updated with a learning rate $\kappa$. Once the learning process converges, the DDPG based regional trust evaluation model is built.

As in the previous analysis, the universal trust evaluation model is obtained by weighted average of $L$ regional models through the fusion center, and reasonable weights are the key to ensuring the performance of the universal model. Therefore, within the federated learning framework, we use the deep reinforcement learning algorithm DDPG to calculate a set of optimal weights for the aggregation of various regional models. Specifically, in order to ensure the universal applicability of the universal model, we introduce a feedback mechanism. That is, we try to make the trust evaluation for ITS-users in various regions based on the universal model close to that based on the regional model. Since the trust evaluation depends on the task completion of ITS-users, we use the ratio of the task completion based on the universal model to the task completion based on the regional model as the status $s$, i.e., $s = (\frac{\mathcal{C}_1^U}{\mathcal{C}_1^R}, \frac{\mathcal{C}_2^U}{\mathcal{C}_2^R}, \cdots, \frac{\mathcal{C}_\mathcal{L}^U}{\mathcal{C}_\mathcal{L}^R})$, where $\mathcal{C}_i^U$ denotes the overall task completion of ITS-users on the $i$th region based on the universal model, while $\mathcal{C}_i^R$ denotes the overall task completion of ITS-users on the $i$th region based on the regional model. For the regional model aggregation, the set of weights consists of the action $a$, i.e., $a = (w_1, w_2, \ldots, w_\mathcal{L})$. Then, the feedback mechanism needs to be combined with reward $r$ design, i.e.,

$$r = \frac{1}{\mathcal{L}} \sum_{i=1}^{\mathcal{L}} \mathcal{C}_i^U / \mathcal{C}_i^R, \tag{8}$$

The update of all neural networks of the DDPG are referring to that given in the previous section. When the DDPG based federated learning converges, the optimal set of weights is discovered and then the universal model is built.

*2) Trust Evaluation on Task Distributers Utilizing Deep Reinforcement Learning:* Once an ITS-user claims to complete the task, the task completion will be sent to the corresponding ITS-TD first and then to the ITS-TP later. And these data will be used by the ITS-TP to evaluate the trust of the ITS-TD. Similar to ITS-user trust evaluation, the task completion $\mathcal{C}_{TD_i}$ of the $i$th ITS-TD is calculated by $\mathcal{C}_{TD_i} = \frac{1}{N_i} \sum_j \eta \cdot \mathcal{C}_{u_j}$, where $N_i$ represents the number of ITS-users who works for the $i$th ITS-TD. Consider each set of tasks are released at a time with a trust bonus for ITS-TD, denoted by $\mathcal{TB}_{TD}$, and a trust bonus for ITS-users, denoted by $\mathcal{TB}_u$, the $i$th ITS-TD's trust $\mathcal{T}_{TD_i}$ and the budget of task trust bonus $\mathcal{TB}^{Budget}$ given to ITS-users who works for the $i$th ITS-TD can be updated based on the task completion $\mathcal{C}_{TD_i}$ as

$$\begin{cases} \mathcal{T}_{TD_i} \rightarrow \mathcal{T}_{TD_i} + \mathcal{TB}_{TD}, & if\ \mathcal{C}_{TD_i} \geq 0.5 \\ \mathcal{T}_{TD_i} \rightarrow \mathcal{T}_{TD_i} - \mathcal{TB}_{TD}, & otherwise, \end{cases} \tag{9}$$

$$\begin{cases} \mathcal{TB}^{Budget} \rightarrow \mathcal{TB}^{Budget} + \mathcal{TB}_u, & if\ \mathcal{C}_{TD_i} \geq 0.5 \\ \mathcal{TB}^{Budget} \rightarrow \mathcal{TB}^{Budget} - \mathcal{TB}_u, & otherwise. \end{cases} \tag{10}$$

To achieve fair and reasonable trust evaluation on ITS-TDs, the optimal parameter $\eta$ should be obtained. Similar to the trust evaluation on ITS-users, the trust evaluation on ITS-TDs are realized utilizing the DRL algorithm DDPG as well. Let the participation $\mathcal{P}_{TD_i}$ of each ITS-TD comprise the state $s$, i.e., $s = (\mathcal{P}_{TD_1}, \mathcal{P}_{TD_2}, \ldots, \mathcal{P}_{TD_L})$. This is because an ITS-TD of a low trust might not be able to receive any task from the ITS-TP, which is similar to the task distribution on ITS-users. Accordingly, the parameter $\eta$ consists of the action $a$, i.e., $a = \eta$. The action $a$ is chosen based on the current state $s$, and then the reward $r$ is calculated by $r = \frac{1}{\mathcal{L}} \sum_{i=1}^{\mathcal{L}} \mathcal{C}_{TD_i}$. And the update of all neural networks is referring to that given in the previous section. Note that the trust evaluation on ITS-TDs is determined by that on ITS-users and vice versa. That suggests we train both models by fixing one model and training the other until all of them are converged. In fact, the Wolpertinger architecture [25] can be applied to the DDPG algorithm to greatly reduce its complexity. However, by doing so, the trust evaluation accuracy will drop due to the parameters, i.e., $\alpha$ and $\eta$, will be searched in the discrete action space rather than the continuous action space.

### C. Trust Storage and Verification

Recall that the task distribution is implemented based on trusts, i.e., the ITS-TP needs to know whether the ITS-TDs are trustworthy and each TD should be aware of the trustworthiness of ITS-users. Thereby, the trusts of both ITS-users and ITS-TDs are stored on blockchains. Considering the heterogeneity of different blockchains, the data format of ITS-users' trusts stored on regional trust-blockchains and that of ITS-TDs stored on the global trust-blockchain might be different, thereby gateways are required to perform the cross-blockchain data transformation.

To be specific, when each ITS-TD wants to upload the ITS-users' trusts to the ITS-TP, the target data format request is made to the specific gateway of the corresponding global task-blockchain. According to the target data format, the gateway of each regional trust-blockchain will perform the data transformation, i.e., the gateway will assign an orderer node to transform the data in Hyperledger, and then transformed ITS-users' trusts are uploaded to the ITS-TP. Next, the ITS-TP calculates the trusts of ITS-TDs. Eventually, the trusts of both ITS-users and ITS-TDs are stored on the global trust-blockchain for trust verification.

## V. Performance Evaluation

### A. Experiment Setup

The simulation is implemented to evaluate the performance of the proposed strategy BHTE in the similar experimental environment as literature [26]. We deploy BHTE on the Hyperledger Fabric platform, the network environment of which is built on a server equipped with an Intel Core i5 processor, 8G running memory, a CPU frequency of 3.2GHZ, and an Ubuntu system. The environment configuration of the Hyperledger Fabric employed is set as follows. There are 4 orderer nodes, 5 peer nodes, and 1 CLI, where the orderer nodes are used to sort transactions, the peer nodes are used to verify transactions, and the CLI is used to call the client. For each region, three task chains are constructed, in which each task chain contains 3 peer nodes, and 2 of total 5 peer nodes are shared by three task chains. In addition, we set there are 3 regions, two of which are capable of training their own trust evaluation models. In order to simulate the heterogeneity of blockchains, we use different configurations (i.e., the configurations that differ slightly from the above one) for blockchains in different regions. The results of the simulation experiment are obtained by averaging the results of each region. Table I gives the parameters of this experiment. The dataset used in this experiment is the Foursquare dataset [27]. This data set contains 2,153,471 users, 1,143,092 places, 1,021,970 check-ins, 27,098,490 social relationships, and 2,809,581 ratings assigned by users to places. All of these are extracted from the Foursquare application through a public API, and all user information is anonymous, and the user's geographic location is also anonymous. These data are contained in five files: "users.dat", "containers.dat", "checkins.dat", "socialgraph.dat" and "rating.dat". To be specific, the user data is composed of a group of users, so each user has a unique ID and geospatial location representing the location of the user's hometown; the event data is composed of a group of places, so that each place has a unique ID and Geospatial location; the check-in data marks the user's check-in at the place, each check-in has a unique ID, user ID and place ID; the socialgraph data contains the social connections between users, and each social relationship is composed of two users ID composition; the rating data contains an implicit rating, used to quantify how much users like a particular place. We divide the dataset to generate a set of tasks (i.e., check-in tasks) of three levels A, B and C, in which level A tasks have the highest trust requirements while level C tasks have the lowest trust requirements. We set the number of ITS-users to be 1000, in which there are 200, 600 and 200 ITS-users can apply for level A, B and C tasks, respectively. We set the trust values of all users are the same such that they can only apply for level C tasks. In addition, the trust bonus of each task is set. A task will be applied for by a ITS-user only if the ITS-user's trust is higher than the task's trust requirement. Once two ITS-users compete for a task, the ITS-user of a higher trust will be assigned to the task by the ITS-TD, if there are still a number of users required in this task.

TABLE I
EXPERIMENT SETUP

| *Parameter* | *Description* | *Range* |
|---|---|---|
| $Num\_Users$ | number of ITS-users | [200,1000] |
| $Num\_Tasks$ | number of tasks | [500,3500] |
| $Block\_Size$ | size of block | [2,10] mb |
| $Tran\_Size$ | size of transactions | [100,500] B |
| $Send\_Rate$ | send rate | [1000,5000] tps |
| $\gamma$ | discounter factor | 0.9 |
| $\kappa$ | learning rate | 0.1 |

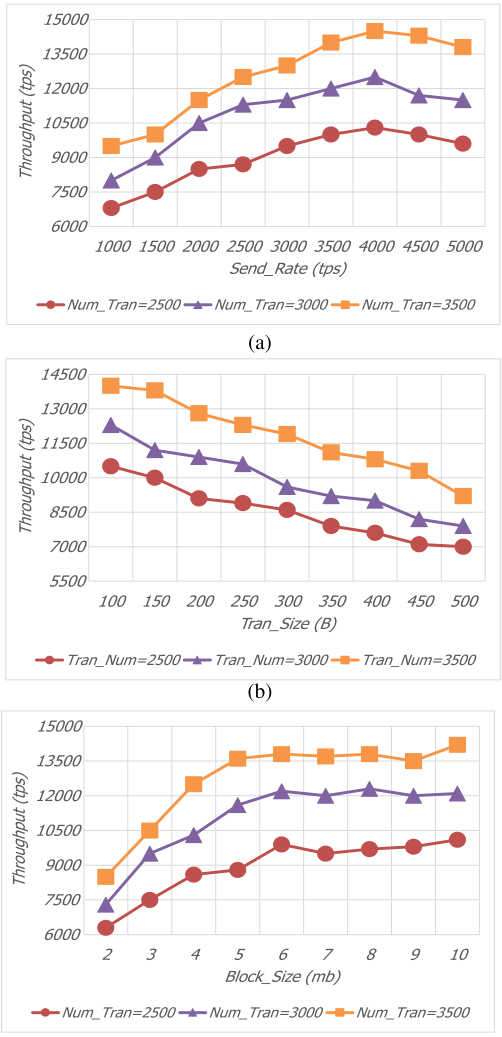
### B. Performance Metrics

We first validate the performance of the BHTE in terms of system throughput and latency considering the send rate $Send\_Rate$, the transaction size $Tran\_Size$, and the block size $Block\_Size$. Then, we compare the performance of the BHTE with baseline approaches BPDC [23] and DB-SCS [26] in terms of participation rate and completion rate, considering the number of ITS-users $Num\_Users$ and the number of tasks $Num\_Tasks$.

- *System Throughput*: A higher transaction processing speed contribute to a better system throughput.
- *Transaction Latency*: A better transaction processing capacity results in a lower latency.
- *Completion Rate*: The percentage of tasks the ITS-user actually completed.
- *Participation Rate*: The percentage of ITS-users who accept the tasks.
- *Algorithm Convergence*: The convergence of the algorithm determines its application. For example, the 5G-ITS applications demand highly efficient and fast convergent algorithms.

### C. Experiment Results

*1) System Throughput:* As shown in Fig. 3(a), it is obviously that for each transaction number the throughput



(a)

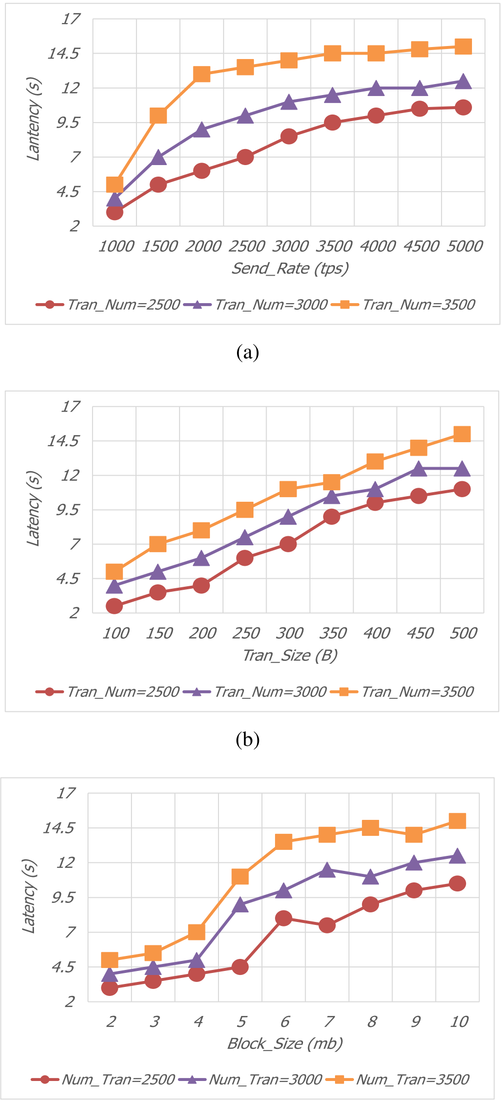
(b)

(c)

Fig. 3. The system throughput of the proposed BHTE with the variation of (a) $Send\_Rate$, (b) $Tran\_Size$, and (c) $Block\_Size$.

increases gradually as the $Send\_Rate$. In addition, the maximum throughput for 3500 transactions reaches 14500tps, compared with 13000tps of 3000 transactions and 10000 tps of 2500 transactions, when the $Send\_Rate$ for each $Num\_Tran$ is up to 4000tps. Furthermore, a higher transaction number $Num\_Tran$ always results in a higher throughput at any $Send\_Rate$. This is because, as more ITS-users decide to accept the tasks released on the heterogeneous and hierarchical blockchains, more transactions will be generated such that a higher throughput is obtained. That indicates the proposed BHTE can encourage ITS-users to accept and complete tasks by efficiently evaluating their trusts.

As shown in Fig. 3(b), we find that the throughput of each $Tran\_Num$ decreases as the $Tran\_Size$ increases. The possible reason is that the $Tran\_Size$ becomes larger, resulting in a decrease in the number of transactions that can exist in a block. Although the throughput decreases as the $Tran\_Size$ increases, the throughput reaches 9000tps, 8000tps, and 7000tps for $Tran\_Num = 3500$, $Tran\_Num = 3000$, and $Tran\_Num = 2500$, respectively.



(a)

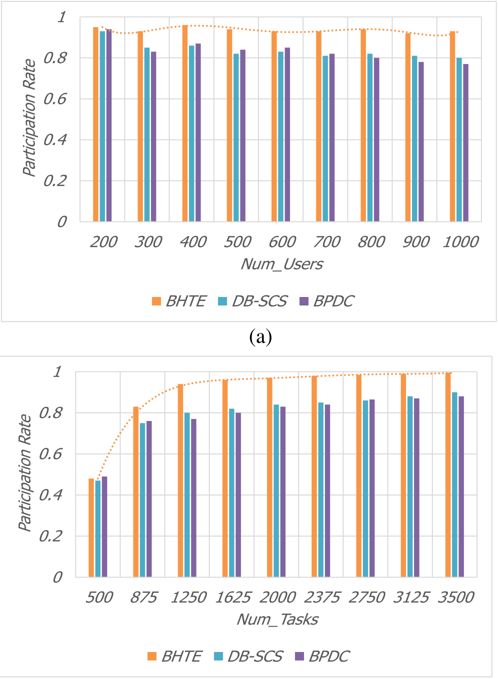
(b)

(c)

Fig. 4. The latency of the proposed BHTE with the variation of (a) $Send\_Rate$, (b) $Tran\_Size$, and (c) $Block\_Size$.

In Fig. 3(c), it is clear that with the growth of the $Block\_Size$, the throughput increases for each $Num\_Tran$. In addition, when there are 3500 transactions, the maximum throughput is up to 14000tps, compared with 12000tps for 3000 transactions and 10500tps for 2500 transactions, with the $Block\_Size$ equals to 10mb, respectively. Similar to the $Send\_Rate$, more transactions contribute to higher throughput for each $Block\_Size$.

*2) Latency:* Observed from Fig. 4(a), we find that the latency increases with the $Send\_Rate$ and eventually levels off for each $Tran\_Num$. When the send rate reaches 5000tps, the highest latency is nearly 15s for 3500 transactions compared with 12s for 3000 transactions and 10.5s for 2500 transactions. That suggests a higher latency is result from a higher transaction number. Since the proposed BHTE is highly efficient in trust evaluation, the average latencies for transaction number 3500, 3000 and 2500 are 12.7s, 9.9s and 7.8s, respectively.



(a)

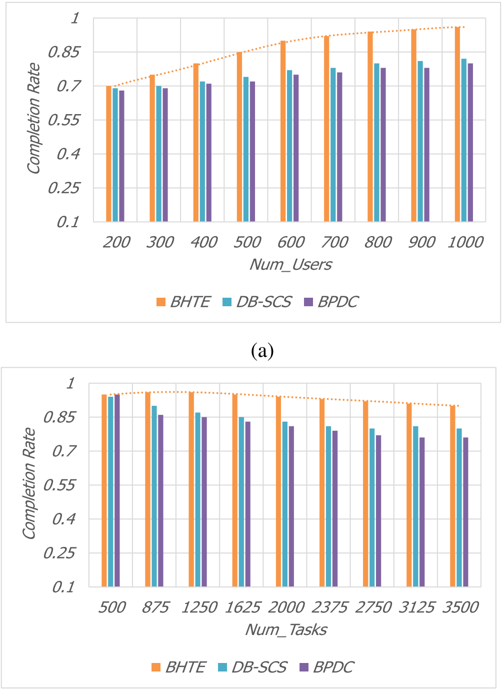
(b)

Fig. 5. The participation rate comparison between the proposed BHTE and baselines with the variation of (a) $Num\_Users$ and (b) $Num\_Tasks$.

In Fig. 4(b), it is clear that the latency rises as the $Tran\_Size$ for each $Tran\_Num$. In addition, the highest latencies for all transaction numbers are reached at $Tran\_Size = 500B$. Although a higher $Tran\_Size$ will contribute to a higher latency, the average latencies are still less than 10s.

As shown in Fig. 4(c), the latency rises as the $Block\_Size$ grows for each $Tran\_Num$ as we expected. In addition, the highest latencies for transaction number 3500, 3000 and 2500 obtained at the block size of 10mb equal to 15s, 12.5s, and 11s, respectively. Although a higher transaction number results in a higher latency, the average latencies are about 11s, 8.8s and 6.7s only for 3500 transactions, 3000 transactions and 2500 transactions, respectively.

*3) Participation Rate:* As shown in Fig. 5(a), although the participation rate experiences the fluctuation with the $Num\_Users$ increase, the BHTE has the highest average participation rate 94% compared with 83% of DB-SCS and 82% of BPDC. As shown in Fig. 5(b), with the growth of the $Num\_Tasks$, the participation rate for all approaches increases. In addition, the highest participation rate of BHTE almost 98%, while that of either DB-SCS or BPDC is less than 90%. It is evident that the BHTE performs better than all baseline approaches. The reason for that is as follows. Continuingly completing the tasks results in tremendous trust improvement on ITS-users that allows them to apply for tasks of higher trust requirements. Note that the BHTE can provide the reasonable and fair trust evaluation, for which more ITS-users will be encouraged to accept tasks. Further, with a high task participation rate, ITS-users tend to put forward task applications of a higher trust requirement. Compared with baselines, BHTE can provide accurate trust evaluation and dynamical rewards/punishments. That explains the fact that the participation rate of either MTES or MTEP is almost 10% lower than that of BHTE.



(a)

(b)

Fig. 6. The completion rate comparison between the BHTE and baselines with the variation of (a) $Num\_Users$ and (b) $Num\_Tasks$.

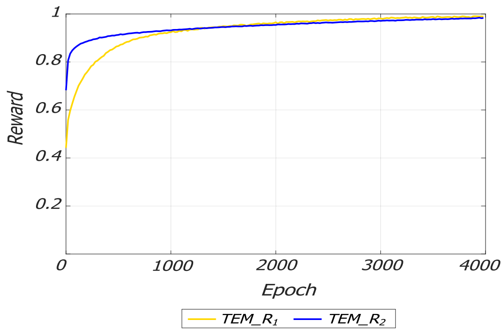


Fig. 7. The convergence of the proposed BHTE.

*4) Completion Rate:* As shown in Fig. 6(a), it is clear that the task completion rate grows as the $Num\_Users$ increases for each approach. The highest completion rate of the proposed BHTE is about 95%, which are 13% higher than that of DB-SCS and 15% higher than that of BPDC. The reason for that is as follows. Since the number of tasks exceeds the number of users at beginning, users can apply for tasks and improve their trusts by completing tasks. On this basis, users can apply for tasks with a higher trust requirement, thus the completion rate rises. Compared with the baseline approaches, the proposed BHTE can dynamically adjust trust rewards and punishments, so that those who are able to complete tasks can apply for higher-level tasks with less competitions. The baseline approaches don't have such mechanism, and a large number of users with similar trusts will compete for tasks, so the task completion rate is lower than that of the BHTE.

As shown in Fig. 6(b), the completion rate decreases as the $Num\_Tasks$ increases. However, the BHTE manages to acquire nearly 94% completion rate on average, compared with 85% of DB-SCS and 82% of BPDC. The reason for that is as follows. Since the $Num\_Tasks$ is less than the $Num\_Users$ at first, users apply for tasks through competition. This means that only users with high trusts can apply for tasks successfully, and the majority of tasks can be completed because users with high trusts have the capability to complete the tasks. As the $Num\_Tasks$ increases, most users can apply for tasks. However, some users with low trusts may not be able to complete the task, so the task completion rate drops. With the further increase in the $Num\_Tasks$, only users who can complete the task are likely to apply for the task. This is because the trusts of users who cannot complete the task has fallen below the threshold for being able to apply for the task, so the task completion rate has stabilized. Compared with the baseline approaches, the proposed BHTE can effectively reward and punish users for completing tasks, so the completion rate is higher than that of baselines.

*5) Algorithm Convergence:* Fig. 7 shows the convergence of the proposed BHTE, where $TEM\_R_i$ represents the trust evaluation model of BHTE on the $i$th region. As shown in Fig. 7, both $TEM\_R_1$ and $TEM\_R_2$ converge around 2000 epoches, and the reward at convergence are both close to 0.9. This indicates that both $TEM\_R_1$ and $TEM\_R_2$ can perform trust evaluation on users reasonably, thus motivating users to complete tasks. The result shown in Fig. 7 suggests that the BHTE proposed in this paper can be applied to trust evaluation in various 5G-ITS applications.

## VI. Conclusion

To defend the security threats against 5G-ITS, in this paper, we propose a heterogeneous Blockchain based Hierarchical Trust Evaluation strategy (BHTE) utilizing federated deep learning for 5G-ITS. Specifically, the trusts of ITS users and ITS task distributers are evaluated using the federated deep learning technology, and hierarchical incentive mechanisms are developed to realize reasonable and fair rewards and punishments such that the efficiency and accuracy of trust evaluation are further improved. Moreover, the trusts of ITS users and ITS task distributers are stored on heterogeneous and hierarchical blockchains for trust verification. The extensive experiment results show that the proposed BHTE performs excellently in high system throughput and low latency for various 5G-ITS applications.

## References

[1] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, “A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles,” *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 7, 2021, doi: 10.1109/TITS.2021.3084396.

[2] S. Mumtaz, H. Lundqvist, K. M. S. Huq, J. Rodriguez, and A. Radwan, “Smart direct-LTE communication: An energy saving perspective,” *Ad Hoc Netw.*, vol. 13, pp. 296–311, Feb. 2014.

[3] M. S. Omar *et al.*, “Multiobjective optimization in 5G hybrid networks,” *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1588–1597, Jun. 2018.

[4] A. H. Sodhro *et al.*, “Towards 5G-enabled self adaptive green and reliable communication in intelligent transportation system,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5223–5231, Aug. 2021, doi: 10.1109/TITS.2020.3019227.

[5] T. do Vale Saraiva, C. A. V. Campos, R. D. R. Fontes, C. E. Rothenberg, S. Sorour, and S. Valaee, “An application-driven framework for intelligent transportation systems using 5G network slicing,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5247–5260, Aug. 2021, doi: 10.1109/TITS.2021.3086064.

[6] K. Yu, L. Lin, M. Alazab, L. Tan, and B. Gu, “Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled intelligent transportation system,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4337–4347, Jul. 2021.

[7] C. Lai, R. Lu, D. Zheng, and X. Shen, “Security and privacy challenges in 5G-enabled vehicular networks,” *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[8] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, “Delegating authentication to edge: A decentralized authentication architecture for vehicular networks,” *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 24, 2020, doi: 10.1109/TITS.2020.3024000.

[9] X. Chen, J. Ding, and Z. Lu, “A decentralized trust management system for intelligent transportation environments,” *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 13, 2020, doi: 10.1109/TITS.2020.3013279.

[10] G. Karmakar, A. Chowdhury, R. Das, J. Kamruzzaman, and S. Islam, “Assessing trust level of a driverless car using deep learning,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4457–4466, Jul. 2021, doi: 10.1109/TITS.2021.3059261.

[11] Z. Yu, J. Hu, G. Min, Z. Zhao, W. Miao, and M. S. Hossain, “Mobility-aware proactive edge caching for connected vehicles using federated learning,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5341–5351, Aug. 2021, doi: 10.1109/TITS.2020.3017474.

[12] P. K. Sharma and J. H. Park, “Blockchain-based secure mist computing network architecture for intelligent transportation systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5168–5177, Aug. 2021, doi: 10.1109/TITS.2020.3040989.

[13] M. Ali, S. Qaisar, M. Naeem, and S. Mumtaz, “Energy efficient resource allocation in D2D-assisted heterogeneous networks with relays,” *IEEE Access*, vol. 4, pp. 4902–4911, 2016.

[14] X. Liu, H. Huang, F. Xiao, and Z. Ma, “A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[15] R. Xing, Z. Su, N. Zhang, Y. Peng, H. Pu, and J. Luo, “Trust-evaluation-based intrusion detection and reinforcement learning in autonomous driving,” *IEEE Netw.*, vol. 33, no. 5, pp. 54–60, Sep. 2019.

[16] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and S. Islam, “Trustworthiness of self-driving vehicles for intelligent transportation systems in industry applications,” *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 961–970, Feb. 2021.

[17] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, “MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2054–2062, Mar. 2020.

[18] T. Wang, H. Luo, X. Zeng, Z. Yu, A. Liu, and A. K. Sangaiah, “Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1797–1806, Mar. 2021.

[19] T. Rosenstatter and C. Englund, “Modelling the level of trust in a cooperative automated vehicle control system,” *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 4, pp. 1237–1247, Apr. 2018.

[20] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, “Blockchain-based adaptive trust management in internet of vehicles using smart contract,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2020.

[21] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, “Software-defined vehicular networks with trust management: A deep reinforcement learning approach,” *IEEE Trans. Intell. Transp. Syst.*, early access, Oct. 1, 2020, doi: 10.1109/TITS.2020.3025684.

[22] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, “Blockchain-based trust management model for location privacy preserving in VANET,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021.

[23] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, “A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications,” *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7204–7212, Oct. 2021, doi: 10.1109/TII.2020.3035006.

[24] M. Z. Khan, S. Harous, S. U. Hassan, M. U. G. Khan, R. Iqbal, and S. Mumtaz, "Deep unified model for face recognition based on convolution neural network and edge computing," *IEEE Access*, vol. 7, pp. 72622–72633, 2019.

[25] G. Dulac-Arnold *et al.*, "Deep reinforcement learning in large discrete action spaces," 2015, *arXiv:1512.07679*.

[26] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3755–3764, Jun. 2021.

[27] M. Sarwat, J. J. Levandoski, A. Eldawy, and M. F. Mokbel, "LARS*: An efficient and scalable location-aware recommender system," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 6, pp. 1384–1399, Jun. 2014.

**Xiaoding Wang** received the Ph.D. degree from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2016. He is currently an Associate Professor with the College of Computer and Cyber Security, Fujian Normal University. His main research interests include network optimization and fault tolerance.

**Sahil Garg** (Member, IEEE) is currently working as a Post-Doctoral Research Fellow with the Department of Electrical Engineering, École de technologie supérieure, Université du Québec, Montreal, Canada. His research interests include machine learning, big data analytics, knowledge discovery, cloud computing, the Internet of Things, software defined networking, and vehicular *ad-hoc* networks. Some of his research findings are published in top-tier journals, such as IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, *IEEE Network*, *IEEE Communications Magazine*, *IEEE Wireless Communications Magazine*, *IEEE Consumer Electronics Magazine*, *FGCS* (Elsevier), *Information Sciences* (Elsevier), and various international conferences of repute, such as IEEE GLOBECOM, IEEE ICC, IEEE WCNC, IEEE VTC, IEEE INFOCOM Workshops, ACM MobiCom Workshops, ACM MobiHoc Workshops, etc. He was a recipient of the prestigious Visvesvaraya Ph.D. Fellowship from the Ministry of Electronics and Information Technology under the Government of India (2016–2018). For his research, he also received the IEEE ICC Best Paper Award in 2018 at Kansas City, USA. He serves as the Managing Editor for *Human-Centric Computing and Information Sciences* (Springer) and an Associate Editor for *IEEE Network* Magazine, IEEE SYSTEMS JOURNAL, *Applied Soft Computing* (Elsevier), *FGCS*, and *International Journal of Communication Systems* (Wiley). He also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications.

**Hui Lin** received the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University, China, in 2013. He is currently a Professor with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou, China, where he is also the M.E. Supervisor. He has published more than 50 papers in international journals and conferences. His research interests include mobile cloud computing systems, blockchain, and network security.

**Georges Kaddoum** (Senior Member, IEEE) received the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, Toulouse, France, in 2008. He held the ÉTS Research Chair position in physical-layer security for wireless networks. He has published over 200 journals and conference papers and two pending patents. He was a recipient of the "Research Excellence Award of the Université du Quebec, in 2018" and the "Research Excellence Award-Emerging Researcher" from ÉTS, in 2019. Additionally, he was a co-recipient of the Best Papers Awards of the IEEE PIMRC 2017 and the IEEE WiMob 2014. Moreover, he received the "Exemplary Reviewer Award" from IEEE TRANSACTIONS ON COMMUNICATIONS twice in 2015 and 2017. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and the IEEE COMMUNICATIONS LETTERS.

**Jia Hu** received the B.Eng. and M.Eng. degrees in electronic engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2004 and 2006, respectively, and the Ph.D. degree in computer science from the University of Bradford, U.K., in 2010. He is currently a Senior Lecturer in computer science at the University of Exeter. His research interests include edge-cloud computing, resource optimization, applied machine learning, and network security. He has published over 80 research papers within these areas in prestigious international journals and reputable international conferences. He has received the Best Paper Awards at IEEE SOSE'16 and IUCC14. He has served as the General Co-Chair for IEEE CIT'15 and IUCC'15, and the Program Co-Chair for IEEE ISPA'20, ScalCom'19, SmartCity'18, CYBCONF'17, EAI SmartGIFT'2016, etc. He serves on the editorial boards of *Computers and Electrical Engineering* (Elsevier). He has guest-edited many special issues on major international journals, such as IEEE INTERNET OF THINGS JOURNAL, *Computer Networks*, and *Ad Hoc Networks*.

**Mohammad Mehedi Hassan** (Senior Member, IEEE) received the Ph.D. degree in computer engineering from Kyung Hee University, South Korea, in February 2011. He is currently a Professor with the Information Systems Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. He has authored or coauthored more than 260 publications, including publications in refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include cloud computing, edge computing, the Internet of Things, body sensor networks, big data, deep learning, mobile clouds, smart computing, wireless sensor networks, 5G networks, and social networks. He has served as the Chair and a Technical Program Committee Member for numerous reputed international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC. He was a recipient of various awards, including the Best Conference Paper Award from IEEE International Conference on Sustainable Technologies for Industry 4.0 (STI) 2020, the Best Journal Paper Award from the IEEE SYSTEMS JOURNAL in 2018, the Best Paper Award from CloudComp Conference in 2014, and the Excellence in Research Award from KSU (two times in 2015 and 2016). He is one of the top 2% scientists of the world in the networking and telecommunication fields. He is one of the top computer scientists in Saudi Arabia as well. Recently, four of his publications were recognized as ESI highly cited papers.