Secure and Efficient Blockchain-Based Knowledge Sharing for Intelligent Connected Vehicles

Haoye Chai, *Graduate Student Member, IEEE*, Supeng Leng, *Member, IEEE*, Fan Wu, and Jianhua He

Abstract—The emergence of Intelligent Connected Vehicles (ICVs) shows great potential for future intelligent traffic systems, enhancing both traffic safety and road efficiency. However, the ICVs relying on data driven perception and driving models face many challenges, such as the lack of comprehensive knowledge to deal with complicated driving context. In this paper, we investigate cooperative knowledge sharing for ICVs. We propose a secure and efficient blockchain based knowledge sharing framework, wherein a distributed learning based scheme is utilized to enhance the efficiency of knowledge sharing and a directed acyclic graph (DAG) system is designed to guarantee the security of shared learning models. To cater for the time-intense demand of highly dynamic vehicular networks, a lightweight DAG is designed to reduce the operation latency in terms of fast consensus and authentication. Moreover, to further enhance model accuracy as well as minimizing bandwidth consumption, an adaptive asynchronous distributed learning (ADL) based scheme is proposed for model uploading and downloading. Experiment results show that the DAG based framework is lightweight and secure, which reduces both chosen and confirmation delay as well as resisting malicious attacks. In addition, the proposed adaptive ADL scheme enhances driving safety related performance compared to several existing algorithms.

Index Terms— Knowledge sharing, DAG blockchain, intelligent connected vehicles, distributed learning.

I. INTRODUCTION

WITH the development of communications and artificial intelligence, Intelligent Connected Vehicles (ICVs) is receiving increasing interest as a promising technology for tackling the challenges faced by intelligent transportation systems [1], [2]. Served by ubiquitous Vehicle to Everything (V2X) technologies, ICVs is capable of sharing sensing data and driving information with other vehicles and traffic infrastructures to improve traffic safety and efficiency. Equipped with intelligent on-board modules, ICVs support intelligent vehicular applications and various levels of driving automation. Several advanced driving use cases (including

Advanced Driving Assistance System (ADAS), extended sensors and cooperative driving) have been specified in the fifth generation (5G) standards. However, the perception and driving models behind the ICVs are mainly data driven (e.g., trained by huge sensing and driving data). They are lack of knowledge to deal with unseen and complex driving scenarios. To address these problems, we are motivated to extend the sharing of raw sensing data to the sharing of knowledge for ICVs.

Knowledge sharing is defined as the activities of transferring or disseminating knowledge among a group of people or organizations [3]. Semantic webs and knowledge graphs have been widely used for knowledge sharing in many applications, such as Question and Answer (Q&A) systems and webpage searching systems. With the aid of emerging Distributed Learning (DL) technology, knowledge sharing for ICVs can provide great benefits to enhance road safety and driving experiences. ICVs can train their own sensing or driving data by the on-board computing devices, and obtain corresponding parameters (*e.g.* models/policies) as refined knowledge. Various levels of knowledge (such as traffic statistics, traffic control, driving rules, sensing and driving models, and crowd sourced maps) can be shared among the ICVs and the roadside infrastructures. In this case, DL based knowledge sharing enhances the perception and comprehension of the driving environment, and support driving decision making [4].

Despite the great potentials held by knowledge sharing of ICVs, several critical issues remains to be addressed. On the one hand, in the DL based knowledge sharing process, attackers could manipulate the shared knowledge or spread misleading knowledge. While central entities such as roadside units (RSUs) could be employed to manage knowledge sharing, they are subjected to various attacks such as single point of failure. On the other hand, existing DL based knowledge sharing shows weakness in sharing efficiency. There is a lack of efficient management and cooperation of the distributed knowledge that is shared by ICVs. For example, conventional federated learning enforce workers to train and share their models in a synchronous manner, resulting in a long delay due to the intermittent links among ICVs [5].

To address the above problems, we resort to emerging DAG blockchain and asynchronous distributed learning (ADL) technologies, aiming to achieve secure and efficient knowledge sharing in highly dynamic vehicular networks. Compared to existing blockchains such as Bitcoin and Ethereum, utilizing mining process with Proof-of-work and Proof-of-Stake that incur huge computation and communication loads, there is no concept of blocks in DAG, and the fundamental unit of DAG is called site that includes a micro-transaction. The new site

can be directly appended on the DAG without block mining, thus realizing the lightweight and resource-saving. From the perspective of ADL, the updating schemes of ADL support ICVs to upload their models in an asynchronous way. ICVs can obtain the on-the-fly updated model without waiting for others, that is suitable for highly dynamic vehicular networks.

However, large-scale and time-intensive ICV networks still hinder the application of existing DAG and ADL based schemes. For DAG, conventional system such as *IOTA* utilizes Markov chain Monte Carlo (MCMC) algorithm as tip selection algorithm (TSA) to reach consensus, wherein ICV needs to trace and verify previous W sites (W is called particle deep and its value is large [6]) that increase the latency of consensus. For ADL, each ICV is required to broadcast its local trained models to ADL servers. Under the large scale circumstance, it will significantly increase communication load and degrade the efficiency of knowledge sharing of ICVs. Consequently, supporting secure and efficient knowledge sharing with both DAG and ADL is a challenging problem.

To fill this gap, in this article, we propose a lightweight DAG and adaptive ADL based knowledge sharing framework, wherein ICVs collect data and train corresponding models as knowledge to be shared. RSUs continuously aggregate and update the distributed models to obtain an on-the-fly and comprehensive model that provides guidance for subsequent ICVs, such as the suggestion of driving speed. The lightweight DAG is designed to ensure the security and tamper-proof of the shared ADL models. Moreover, an adaptive ADL algorithm is proposed to further reduce bandwidth consumption during the model-sharing process in the highly dynamic ICV networks. The contributions of the paper can be summarized as follows:

- We propose a secure and efficient knowledge sharing framework for ICVs, wherein both local and cross-regional knowledge sharing are integrated. ADL is adopted to train raw data as refined knowledge to enhance sharing efficiency and DAG blockchain can guarantee the security and tamper-proof of the shared ADL models that is important for ICV safety and driving applications.
- To cater for the time-critical demand of highly dynamic ICV networks, a lightweight DAG is designed with a reversed two-hop TSA and a fast identity authentication scheme. The proposed TSA achieve fast confirmation rate and consensus by taking account of driving style of ICVs. Based on the proposed algorithm, we propose fast identity verification scheme for cross-region ICVs without introducing additional storage costs, in which two special sites are designed to accelerate the authentication process. The feasibility of the proposed lightweight DAG system is proved with mathematic analysis.
- In order to minimize bandwidth consumption as well as improving model accuracy, we further propose an adaptive asynchronous distributed learning scheme for the uploading and aggregating processes of shared knowledge. The convergence of the proposed ADL is proved, and the optimal model weight and ICV driving style are analyzed based on the optimal convergence point.

The remainder of this paper is organized as follows. We present related works of knowledge sharing, blockchain and distributed learning in Section II. The overview of the proposed DAG based knowledge sharing framework is presented in Section III. In Section IV, the lightweight DAG system is elaborated, together with the feasibility and security analysis. The design and convergence analysis of the ADL algorithm is presented in Section V. In Section VI, experiment and simulation results for the blockchain knowledge sharing and ADL algorithm are presented and discussed. Finally, the paper is concluded in Section VII.

II. Related Work

Knowledge sharing among intelligent connected vehicles has been studied recently. By utilizing the information of vehicular trajectories, a clustering scheme was proposed based on the semi-Markov process [7]. Rula *et.al* proposed a data fusion algorithm to realize vehicular context awareness [8]. A joint rate control and resource allocation scheme was developed with the information of channel states and delay constraints [9]. During the information sharing process, it is crucial to guarantee the security and reliability, which has not been addressed in these works. Tampered or malicious knowledge can cause severe safety issues and degrade system performance. In this case, the emerging blockchain technology shows strong resistance to malicious attacks, and it has attracted increasing attention.

In literature [10], a user-centric blockchain (UCB) framework was proposed to preserve the reliability of edge data, in which a lightweight consensus mechanism was developed. To maintain the traceability of data, Lin *et al*. presented a consortium blockchain [11]. For ICVs, a service-oriented public blockchain was proposed for ride-sharing that aims to guarantee trust and fair payment during the sharing process [12]. Cui *et al*. proposed a blockchain-enabled payment paradigm in which the data is encrypted and outsourced decryption is payable [13]. However, most existing works utilized "$block''$" data structures to store data in blockchains, which introduces additional packing expenditure and mining consumption. Moreover, the "$chain''$" structure leads to a time-consuming consensus process and a slow data recording, which is not suitable for large-scale ICV networks. Therefore, the existing blockchain frameworks are not readily applicable to the ICV network.

To further enhance the efficiency of knowledge sharing, DL has been studied for vehicular networks. A DL framework was developed to maintain the communication efficiency of IoV, and packet loss probability and throughput were analyzed under the framework [14]. Zhang *et al*. proposed a two time scales DL algorithm to implement mode selection and resource allocation for vehicular networks [15]. Although the above studies have made great efforts on knowledge sharing, they are either insecure or inefficient for dynamic ICV networks.

III. Design of the Knowledge Sharing Framework

The knowledge sharing framework is shown in Fig. 1. By utilizing DL based schemes, ICVs continuously collect data and extract knowledge from environment that is set as DL model in this article. The whole ICV network is divided into multiple traffic regions. In each region, there is a

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

CHAI *et al.*: SECURE AND EFFICIENT BLOCKCHAIN-BASED KNOWLEDGE SHARING FOR INTELLIGENT CONNECTED VEHICLES 3
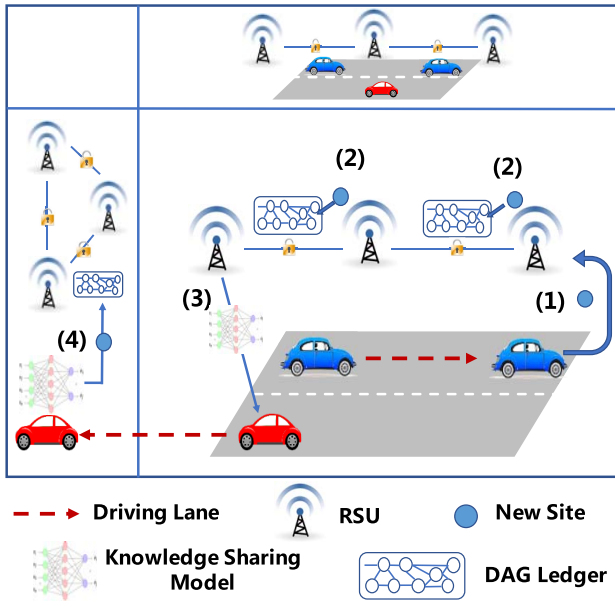

Fig. 1. Illustration of the Knowledge Sharing Framework.

consortium-based DAG blockchain, where RSUs act as DAG nodes to cache the DAG ledger. The basic workflow of the knowledge sharing process can be described by the following four steps.

(1). Knowledge Extracting and Site Generation: ICVs extract valuable knowledge from the original raw data by utilizing DL based scheme, and the knowledge is set as DL models Φ_v. Then, ICV encapsulates Φ_v together with the signature of the vehicle Sig that is generated by its private key, and the hash value H into a site. The typical format of a site S_v is

$$S_v = \{H, \Phi_v, m, c_v, \mathbf{w}, Sig_v\}, \tag{1}$$

where $\mathbf{w}$ is the vector of its own weight and cumulative weight of one site. m is driving style indicator of ICVs that is utilized to develop a lightweight DAG blockchain and adaptive ADL scheme. The specific design will be elaborated in Section. IV and V. c_v is a simple proof-of-work to prevent the Sybil Attack.

(2). Knowledge Verifying and Appending: The encapsulated site is then broadcast to surrounding RSUs that cache the DAG ledger. The issuing ICV will choose and verify two existing tips on the DAG ledger according to the tip selection algorithm. To verify the correctness of the on-chain knowledge, ICVs will download the two chosen models and test the models with its own testset. The absolute error (denoted by e) is leveraged to quantify the performance of the models [16], which can be denoted by the gap between the real output and the predict output, that is

$$e = \frac{1}{n}\sum_{i=1}^{N}|y_{i|c_v} - f(x_{i|c_v})|, \tag{2}$$

where $f(x_{i|c_v})$ is the predict output of the target model over the testset c_v and $y_{i|c_v}$ is the actual output. If the testing performance gap is smaller than a certain value, *i.e.* $e \leq \epsilon$, the verification process is deemed as valid, so that the ICV can append the new site on the DAG ledger.

(3). Local Knowledge Sharing: Within each traffic region, a consortium based DAG architecture is adopted. RSUs act as blockchain nodes to cache and synchronize local DAG ledger. At the same time, the RSUs can aggregate DL models that are cached in the DAG ledger, and act as the ADL servers to update the knowledge to obtain a comprehensive model. ICVs can check the aggregated model that is stored at their surrounding RSUs, and exploit it to make decisions.

(4). Cross-Region Knowledge Sharing: For an ICV driving across the regions, the RSUs will decide whether to deliver the cross-region knowledge to the vehicle for cross-regional sharing. The impact scope of the knowledge will be used for the delivery decision. The idea is that the knowledge with a small impact range does not need to be transmitted to nearby regions. It is noted that the RSUs will transmit to cross-regional ICVs not the total ledger, but the cross-region knowledge that is encapsulated as sites.

There are two characteristics of the proposed framework: (a) for local sharing, the RSUs have two identities at the same time: the DAG ledger maintainers and the ADL servers. The RSUs can load the knowledge cached in the ledger, and implement corresponding updating schemes according to different applications, which strengthen the cooperation between the independent, distributed knowledge in DAG ledger. Compared with conventional ADL updating schemes, the comprehensive knowledge obtained by RSU is updated with the tamper-proof distributed knowledge that is cached in the ledger, which is essentially reliable and traceable. This can prevent the single point of failure and malicious ADL servers, since other RSUs or ICVs can check the tamper-proof ledger to verify the comprehensive knowledge. (b) for cross-region sharing, existing blockchain based systems utilize global consensus mechanism to realize cross-region sharing that will introduce heavy communication cost. The proposed framework enables cross-regional ICVs to carry the knowledge, and issue the knowledge as a new site in other regions. Since there is no block packing and mining process in the DAG based framework, the new site with cross-region knowledge can be directly appended to the ledgers of other regions that realizes fast sharing of cross-region knowledge.

IV. LIGHTWEIGHT DAG FOR KNOWLEDGE SHARING

While DAG blockchain shows potentials for micro-transaction based ICV networks, it is not directly applicable to the efficiency-demanding ICV networks. Recalling the *Knowledge Verifying* step in Section. III, the issuing ICV will verify two existing tips on the DAG ledger by its own testset. The "random verification" manner used in the traditional DAG blockchain will degrade the verification rate of new sites and hinder the issue of new site, thus degrading the efficiency of knowledge sharing. Besides, traditional DAG utilizes MCMC algorithm as TSA, in which the vehicles is required to trace and verify multiple previous W sites that will increase operation latency.

To address the challenges above, we are motivated to develop a lightweight DAG system for ICVs. Specifically, we design a lightweight tip selection algorithm to enhance the
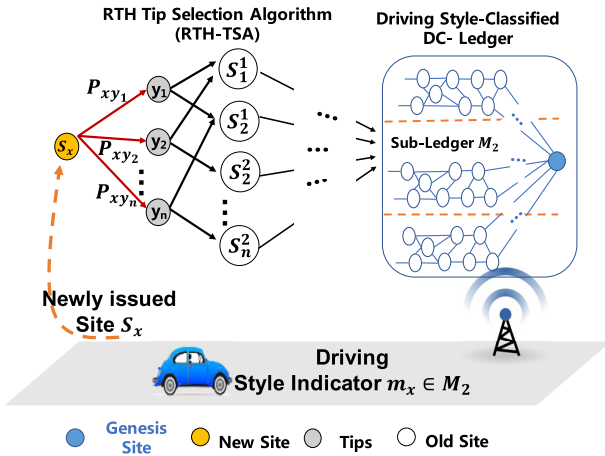
Fig. 2. Illustration of RTH-TSA Algorithm and DC-Ledger.

knowledge sharing efficiency, and a lightweight identity verification scheme to facilitate cross-regional knowledge sharing.

A. Lightweight Tip Selection Algorithm

In order to realize the lightweight of DAG, we define a parameter that is related to ICVs, namely **driving style indicator**, which is denoted as m. The driving style can characterize the features of ICVs during their driving period, and it can be the single property such as velocity, controlling parameters and routes, etc., as well as the combination of several control-related factors, such as $m = f(a, b, c)$, where a, b, c are the vehicular throttle, steering and braking, and $f()$ is the function of the parameters above. Since the models are trained with datasets that are collected by ICVs during their driving periods, the trained model is also related to the driving style of ICVs. Based on the observation, the conventional TSA of DAG can be accelerated by utilizing m.

Reversed Tow Hop TSA (RTH-TSA): The proposed RTH-TSA is illustrated in Fig. 2. Specifically, the tip selection probability of traditional DAG depends on a biased random walk that can be expressed as $P_{xy} = \frac{exp\{-\kappa(CW_x - CW_y)\}}{\sum_\kappa exp\{-\kappa(CW_x - CW_y)\}}$, where CW is the cumulative weight of the tips. However, in the knowledge sharing of vehicular context, the selection and verification of tips are related with model accuracy, as indicated in Eq. (2). It is inaccurate to verify tips by only referring to cumulative weight. Consequently, we combine the driving style m of ICVs into the selection probability, which can be expressed as

$$P_{xy_1} = \frac{exp\{-\alpha(CW_{s_1^1} + CW_{s_2^1}) - \beta(m_x - m_y)^2\}}{\sum_{z \in \mathbb{T}} exp\{-\alpha(CW_{s_1^z} + CW_{s_2^z}) - \beta(m_x - m_z)^2\}}, \quad (3)$$

where $\mathbb{T}$ represents the set of current tips of the DAG ledger and α, β are both positive weight parameters. $CW_{s_1^1}$ and $CW_{s_2^1}$ are cumulative weights of two sites that are approved by tip y_1. m_x and m_y are the corresponding driving style of tip x and y. Besides, we reverse the tracing order of site to develop fast tip selection. As indicated by $CW_{s_1^1}$ and $CW_{s_2^1}$ in (3), when a new site chooses tips to append, it does not have to trace from particle deep like traditional MCMC algorithm. Conversely, it directly chooses two existing tips from its side to connect.

The proposed RTH-TSA achieves lightweight of DAG from two aspects: **1). fast selection speed; 2). high confirmation rate.** For the first feature, traditional DAG utilizes MCMC based algorithm to select tips, in which the verifier (*i.e.* the ICVs in our article) is required to trace and verify previous W particle deep. While the proposed RTH-TSA only needs to trace a two-site deep, *i.e.* y_1 and s in Fig. 2, which will greatly reduce the selection speed of tip selection.

For the second feature, the confirmation rate is accelerated with the help of **driving style-classified ledger (DC-Ledger)**. Since the tip selection algorithm defines how a new site connects to the DAG ledger, *i.e.*, how the site is verified by others. The TSA will determine the ledger structure and how the sites are appended on the DAG. In this case, the proposed RTH-TSA enforces the new sites to verify and append behind those tips with similar driving styles. The total DAG ledger will eventually evolve to multiple sub-ledger, each of which records the sites with similar driving styles. In the DAG system, a site is deemed as confirm when its cumulative weight reaches a certain threshold. At a certain moment, the driving style of ICVs within a single traffic region are often similar. For example, there are few fast vehicles on a congested street, and most vehicles have similar driving speeds. Accordingly, the sites published by these ICVs will also be appended to the same sub-ledger based on the DC-Ledger. Therefore, compared with other sub-ledgers, the sites in this sub-ledger will also be chosen and verified by a large number of new sites, and the corresponding cumulative weight will grow rapidly, thus realizing quick confirmation.

B. Fast Identity Authentication Scheme

In the proposed framework, we utilize moving ICVs to exchange the knowledge among different traffic regions, rather than using global consensus. To ensure trust and reliability of the shared knowledge, cross-regional knowledge needs to be carried by authenticated ICVs. Therefore, it is crucial to design an identity verification scheme for those cross-regional ICVs. Existing schemes utilize identity tokens for the verification process [17], which will introduce extra storage consumption and communication cost for knowledge sharing. Therefore, we design an efficient identity verification scheme for cross-regional ICVs that does not use identity tokens.

Specifically, we design two special sites during the authentication process: one is cross-regional site S_r^c, and the other is *IdentityStone* S_{is}. As illustrated in Fig. 3, considering a cross-regional scenario that ICV y leaves region A to B. If RSUs of A decide to share the knowledge with B, they send to y the cross-regional site S_r^c. Meanwhile, RSUs of region B will issue a *IdentityStone* S_{is}, which is signed with its private key Sig_r. The formats of the two special sites are expressed as

$$S_r^c = \{H, \Phi, m, \mathbf{w} = 0, Sig_r\} \quad (4)$$

$$S_{is} = \{H, m, \mathbf{w} = 0, Sig_r\} \quad (5)$$

The reason for setting $\mathbf{w} = 0$ is to avoid affecting the current weight of the DAG ledger, which is inspired by the Project *Tangle* [6]. When a vehicle y issues the first site in the new region B, it must approve the two specific sites S_{is} and S_r^c.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

CHAI et al.: SECURE AND EFFICIENT BLOCKCHAIN-BASED KNOWLEDGE SHARING FOR INTELLIGENT CONNECTED VEHICLES
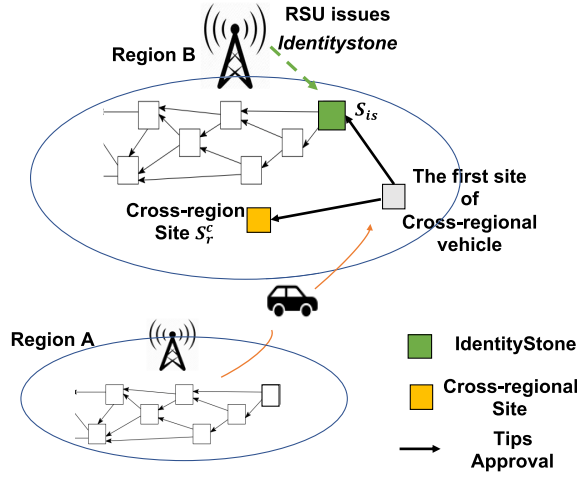
5

Fig. 3.   Fast Authentication for Cross-regional Vehicles.

After that, y is deemed to have completed identity verification. Noting that the cumulative weight of both sites is 0, the newly coming sites of other ICVs in region B will first verify the site of the cross-regional vehicle y according to Eq. (3), which completes the fast authentication of vehicle y.

C. Feasibility and Security Analysis

To ensure the feasibility and effectiveness of the proposed DAG system, it must remain convergent and fast consensus. In this subsection, the feasibility of the proposed lightweight DAG will be analyzed.

1) The Ledger Convergence: The ledger convergence indicates that the total number of tips of the DC ledger cannot escape to infinity. Assume that the ICVs issue new sites independently with the distribution I_n. Let us denote T_n as the number of tips in the proposed DAG at the n-th approval round. In this case, the total number of tips in the network can be expressed as $T_n = T_{n-1} + I_n - A_n$, where A_n is the number of approved tips by I_n. Assume that the range of m is divided into K discrete intervals $\mathbb{M} = \{M_1, \ldots, M_k, \ldots M_K\}$, and the mobility distribution of vehicles is $m(t)$ with respect to time t. For one specific sub-ledger k that locates on the mobility interval $M_k \in \mathbb{M}$, the expectation of $T_n^{M_k}$ is

$$E[T_n^{M_k}] = E[T_{n-1}^{M_k}] + E[I_n^{M_k}] - E[A_n^{M_k}]. \tag{6}$$

In order to obtain the value of $E[T_n^{M_k}]$, the distribution of $I_n^{M_k}$ and $A_n^{M_k}$ should be specified. The incoming tips can follow the poisson, uniform and gamma distributions, *etc.* Here we only select one ordinary poisson distribution with a incoming rate λ and prove the convergence. More distribution examples will be investigated in the simulation part. Hence, Eq. (5) can be expressed as $E[T_n^{M_k}] = E[T_{n-1}^{M_k}] + \lambda h P\{m(t) \in M_k\} - E[A_n^{M_k}]$, where h is the average time of each approval.

For an arbitrary incoming site x, the probability $P_{xy}^{M_k}(s)$ that site x) approves the tip y with mobility k at time s is shown in Eq. (3). For simplicity, the cumulative weight CW can be omitted since various sites have similar weights from a long-term perspective. Hence, $P^{M_k}(s) \approx \frac{exp\{-\beta[M_k - m(s)]^2\}}{\sum_{l:M_l \in \mathbb{M}} exp\{-\beta[M_l - m(s)]^2\}}$.

According to Theorem 5.2 in [18], tip approval occurs at a certain time uniformly distributed in $(0, h)$. Therefore, the probability that one site will approve those tips with driving style indicator M_k is computed by

$$P^{M_k} = \frac{1}{h} \int_0^h P^{M_k}(s)ds, \tag{7}$$

and is independent of the other tip approval events. Hence, the conditional probability is a multinomial distribution with parameters $P^{M_1}, P^{M_2} \ldots, P^{M_K}$, and the joint probability can be expressed as

$$
\begin{aligned}
&P\{A_n^{M_1}(h) \\
&= n_1, A_n^{M_2}(h) = n_2 \ldots, A_n^{M_K}(h) = n_K\} \\
&= \frac{(\sum_{k=1}^K n_k)!}{n_1!n_2!\ldots n_K!}(P^{M_1})^{n_1}(P^{M_2})^{n_2} \cdots (P^{M_K})^{n_K} e^{-\lambda h} \frac{(\lambda h)^{\sum n_k}}{(\sum n_k)!} \\
&= \prod_{k=1}^K e^{-\lambda h P^{M_k}} \frac{(\lambda h P^{M_k})^{n_k}}{n_k!}.
\end{aligned}
\tag{8}
$$

From the above analysis, it can be obtained that the variable $A_n^{M_k}(h)$ follows a Poisson distribution with parameter $\lambda h P^{M_k}$. Therefore, the expectation of T_n can be obtained

$$
\begin{aligned}
E[T_n] &= \sum_{k=1}^K E[T_n^{M_k}] = E[T_{n-1}] + \sum_{k=1}^K (E[I_n^{M_k}] \\
&\quad - \lambda \int_0^h \frac{exp\{-\beta[M_k - m(t)]^2\}}{\sum_{l:M_l \in \mathbb{M}} exp\{-\beta[M_l - m(t)]^2\}} dt) \\
&= E[T_{n-1}] + \lambda h \cdot 1 - \lambda \int_0^h 1 dt = E[T_{n-1}].
\end{aligned}
\tag{9}
$$

Consequently, during each approval round, the total number of tips of all sub-ledgers is the same as that of the previous round. Although the number of tips of each sub-ledger in each round may be different, the total number of their tips remains constant, which proves the convergence of the ledger.

2) Confirmation Delay: The confirmation delay is defined as the time it takes for the CW of one sites to reach a certain threshold. In this subsection, we will analyze the confirmation delay of sites within one specific sub-ledger of DC-ledger.

Let s_{ta} denote the target site that is located in DC sub-ledger with driving style M_k, and $W_k(t)$ be the CW of s_{ta} at time t. Assume that the number of tips remains constant within the time interval $(t, t + \delta)$ when the δ is small enough. The probability of one newly site approving at least one of the target sites can be calculated by $P_\delta = 1 - [1 - \frac{1}{\delta} \int_t^{t+\delta} P^{M_k}(s)ds]^2$.

Similar to the Birth and Death Process in [6], the increment of CW at time t can be expressed as $W'_k(t) = \lambda \frac{\int_t^{t+\delta} P^{M_k}(s)ds}{\delta} \cdot [2 - \frac{\int_t^{t+\delta} P^{M_k}(s)ds}{\delta}] = 2\lambda P^{M_k}(t) - \lambda[P^{M_k}(t)]^2$, where $P^{M_k}(t)$ depicted in the last subsection can be further simplified as $P^{M_k}(t) = \frac{2\lambda}{\sum_l e^{-\beta(M_l - M_k)[M_l + M_k - 2m_t]}}$. Let $f_t^l = \beta(M_k - M_l) * (M_l + M_k - 2m_t)$, then the growth speed of CW yields

$$W'(t) = \frac{2\lambda}{\sum_{l_0} e^{f_t^{l_0}}} - \frac{\lambda}{\sum_{l_2} \sum_{l_1} e^{f_t^{l_1} + f_t^{l_2}}}. \tag{10}$$

Therefore, given the confirmation threshold W_0, the confirmation delay can be calculated by

$$T_c = \frac{W_0}{\int_{s=0}^{t} W'(s)ds}. \tag{11}$$

It can be deduced that the cumulative weight is related to driving interval M_k and instantaneous driving style m_t. Based on Eq. (10), the confirmation delay of target site s_{ta} is proved to yield the following corollary.

Corollary 1: Given the driving style m_t of new site, the target site s_{ta} with M_k has the fastest confirmation delay if $m_t \in M_k$.

proof: To prove the corollary, we first evaluate the monotonicity of the growth speed of CW in Eq. (9). By calculating the second derivation, it yields

$$W''(t) = 2\lambda - 2\lambda P^{M_k}(t) \geq 0, \tag{12}$$

where the above inequality holds due to the $P^{M_k}(t) \leq 1$. Hence, the growth speed of CW is monotonically increasing with $P^{M_k}(t)$. Let W_0 denote the confirmation threshold, then the final confirmation delay can be expressed as $\frac{W_0}{W(t)}$. Given a deterministic time period $(0, t)$ and driving style input m_t, the confirmation delay is only related to the driving style of target site s_{ta}, *i.e.* M_k, as indicated in Eq. (10). in this case, we only need to prove $P^{M_k}(t)$ reaches the maximal value when $M_k = m_t$. Equivalently, it is only to prove that the $\sum_{l_0} e^{f_t^{l_0}}$ reaches its minimal value with $M_k = m_t$. Let $\mathcal{R} = \sum_{l_0} e^{f_t^{l_0}}$, by calculating the first order derivation of $\mathcal{R}$, it follows

$$\mathcal{R}' = \sum_{l_0} \beta[(M_l + M_k - 2m_t) + (M_k - M_l)]e^{f_t^{l_0}}$$

$$= \sum_{l_0} 2\beta(M_k - m_t)e^{f_t^{l_0}}. \tag{13}$$

Consequently, $\mathcal{R}$ reaches the minimal value when $R' = 0$, *i.e.*, $M_k = m_t$. ∎

Following *Corollary 1*, the CW increasing speed of target site within different driving style intervals M_k is related to the distribution of new site driving style m_t. Given the distribution of m_t in a certain time interval $(0, t)$, it can be inferred that the closer the interval M_k is to m_t, the faster the CW increment will be. Within the same time period, the driving styles of ICVs within the same traffic region are often similar to each other's. In this case, the new sites issued by these ICVs will firstly append to the relative concentrated intervals M_k in DC-ledger according to the RTH-TSA, then being quickly verified by subsequent sites. Moreover, based on the Corollary 1, it can be proved that the proposed lightweight DAG has a faster CW increment rate compared to conventional DAG, that is,

Corollary 2: Compared with conventional DAG, the proposed lightweight has a faster site confirmation rate.

Proof: According to the definition of confirmation delay in Eq. (10), the final delay is related to the growth speed of CW, *i.e.*, $W'(t)$. From the monotonicity proof in (11), $W'(t)$ is monotonically increasing with $P^{M_k}(t)$. In the conventional DAG that leverages random walk based TSA, each tip has approximately equal probability being selected, therefore,

given the total number of driving style intervals as $|\mathbb{M}| = K$, the tips being selected by upcoming new sites can be expressed as $P_{con}^{M_k}(t) = \frac{1}{K}$. In the proposed lightweight RTH-TSA, the probability equals $P^{M_k}(t) = \frac{1}{\sum_{l_0}^{K} e^{f_t^{l_0}}}$. Based on the *Corollary 1*, the confirmation delay of target site s_{ta} will reach the minimal point when $M_k = m_t$. Hence, the probability yields

$$P^{M_k}(t) = \frac{1}{\sum_{l_0}^{K} e^{f_t^{l_0}}} = \frac{1}{\sum_{l_0=1}^{K} e^{-\beta(M_t - M_l)^2}}$$

$$\geq \frac{1}{\sum_{l_0=1}^{K} 1} = \frac{1}{K} = P_{con}^{M_k}(t). \tag{14}$$

Hence, the CW increment rate of target site is higher than that of conventional DAG, which proves the corollary. ∎

3) Security Analysis: As the proposed lightweight DAG shows great time-efficiency than conventional DAG, it is essential to discuss the security performance.

Malicious Attackers: The attacks can be categorized into two types: intra-region attack and inter-region attack. For intra-region attack, attackers tend to issue malicious site to surrounding ICVs. While the verifying process in Eq. (2) makes sure the correctness of the site. After the site verification, new sites will choose not to append behind the malicious site, and the malicious site eventually becomes an orphan. For inter-region attack, attackers modify the cross-region knowledge of step. (4) in Section. III, trying to launch an "immediate" attack by its new identity in the new region. While the attack can be eliminated by the fast identity authentication scheme. Since the weight of both S_r^c and S_{is} are equal to 0, according to the RTH-TSA, other ICVs will firstly verify the cross-region site, and quickly discover the modified site.

Lazy Workers: The lazy workers refer to those ICVs directly append their sites behind those "old" sites rather than tips, which reduces the throughput of DAG network. According to Eq. (3), if the lazy sites are appended to the existing old sites, the probability of the lazy sites being appended will be largely reduced and they will eventually become the "orphan" sites.

Confirmation Issues: Although we have proved that the target site s_{ta} with $M_k = m_t$ has a faster confirmation rate than conventional DAG, those sites with deviated driving styles shows weakness in confirmation delay. While in vehicular networks, the driving style of most ICVs on the same traffic region at the same time period is similar. This condition ensures that most of the issued sites will be quickly confirmed. For those very few "deviated" sites, we can utilize RSUs to periodically issue confirmation sites, similar to S_r^c and S_{is} in Eq. (4), to assist sites to be quickly confirmed.

V. ADAPTIVE ASYNCHRONOUS DISTRIBUTED LEARNING

Although the proposed lightweight DAG provides lightweight and security for ICV network, there could still be accuracy and communication related issues: (a). As DL models cached in the DAG ledger are trained independently by individual ICVs, they could be far away from the optimal one obtained by joint training; (b). For large-scale vehicular

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

CHAI *et al.*: SECURE AND EFFICIENT BLOCKCHAIN-BASED KNOWLEDGE SHARING FOR INTELLIGENT CONNECTED VEHICLES 7

networks, ICVs continuously broadcasting local models significantly increase the communication load.

To tackle the above issues, we exploit an adaptive ADL to enhance the knowledge sharing system, aiming to enhance model accuracy and reduce bandwidth consumption.

A. Adaptive Asynchronous Distributed Learning Scheme

Considering the disparity of ICV training ability, one core idea of the proposed adaptive ADL is that there is no need to enforce all ICVs to upload their local models. Some local models with lower learning performance may even degrade accuracy of final model. Following this viewpoint, the specific workflow of the adaptive ADL scheme is described as follows.

1) Initialization: The RSUs cache a global model (GM) in advance with model version $V_G = 1$, and the initial GM can be obtained by offline learning methods. Each RSU caches an identical and periodically updated test dataset.
2) GM Broadcasting: The RSUs periodically broadcast the reference gap e_G of current GM that is evaluated by RSUs' test dataset as Eq. (2), current version V_G, together with its signature Sig_r to surrounding ICVs.
3) Judging the Reliability of GM: Upon receiving information from RSUs, ICVs check the received versions and signatures of GM, which can prevent the single point failure of RSUs. The ICVs will choose the version sent by most RSUs as the credible GM version.
4) Adaptive Site Issuing: After verify the reliability of the GM, the ICV will compare the test gap e_v of its own local model with reference gap e_G. If $e_v \leq e_G$, the ICV believes that its local model outperform the current GM, and it will encapsulate its model and driving styles indicator m into new site S, as indicated in Section III. (1). Else, the ICV will not issue a new site and will download the current GM from RSUs as its model.
5) Asynchronous Updating GM: By receiving a new model from ICV, the RSUs will first utilize testset to evaluate the received model. If the test gap $e_r \leq \epsilon$ (e_r is the test gap of the received local model tested by RSUs), the model is deemed as valid and can be appended to the DAG ledger. Then, the RSUs update the current version $V = V + 1$, and update the GM by a *driving style based asynchronous updating algorithm*, which will be discussed in the next subsection. Else, the RSUs will send a fail signal to ICV, and back to step (2).

With the adaptive scheme, those local models with low accuracy will not be appended on the DAG ledger, which will enhance the quality of global model GM. Furthermore, with less uploaded models the communication loads between ICVs and RSUs can be significantly reduced.

B. Driving Style Based Asynchronous Updating Algorithm

In this subsection, the updating algorithm in Step (5) will be presented. Driving style is the reflection of interaction between ICVs and external environment, which contains the knowledge of context and driving feature. For example, on the same road segment, ICVs with different driving velocities will have diverse safe braking distance. Hence, it is inappropriate

---

Algorithm 1 Driving Style Based Asynchronous Updating Algorithm

---

Initialization: N ICVs with driving style indicators $\{m_1, \ldots, m_N\}$, Global Training Time T
for $n = 1 : N$
Local Model Training:
$\theta_n^l \leftarrow \Phi$
$B_n \leftarrow$ Local training batch of vehicle n
for each local epoch in L
for batch b $\in B_n$
training model $\theta_n^l \leftarrow \theta_n^l - \gamma \bigtriangledown F^l(\theta_n^l|b)$
return Local model θ_n^l, Local Completion time t_n
Model Aggregation:
$f_{t_n} \leftarrow e^{1 - \frac{t_n}{T}}$
$\alpha_{t_n} = e^{-\widetilde{m_{t_n}}}$
$\Phi(t) = (1 - \alpha_{t_n} f_{t_n})\Phi(t^-) + \alpha_{t_n} f_{t_n} \theta_t^l$
Output Global model GM $\Phi(T)$

---

to aggregate local models regardless of their driving styles. Therefore, we propose a driving style based asynchronous updating scheme, which combines both driving styles of ICVs and the freshness of local models.

Considering a DL process that N ICVs succeed in issuing sites within T time, each ICV utilizes stochastic gradient descent (SGD) algorithm to implement local training $\theta^l(t) = \theta^l(t-1) - \gamma \bigtriangledown F^l(t)$, where θ^l represents local model and F^l is the local optimization function. Then, the global model GM Φ at time t can be expressed as

$$\Phi(t) = (1 - \alpha_t f_t)\Phi(t^-) + \alpha_t f_t \theta_t^l \qquad (15)$$

where t^- is defines as the time index of last asynchronous updating, and f_t is the function of computing the freshness of local models that is utilized to describe the decay of old weights over time. The freshness is computed as

$$f_t = e^{\frac{t}{T} - 1}, \qquad (16)$$

and α_t in Eq.(14) represents the driving-related weight, which is defined as

$$\alpha_t = 1 - \widetilde{m_t} \qquad (17)$$

where term $\widetilde{m_t}$ is the relative driving style indicator of ICV at time t, that is described as $\widetilde{m_t} = |m_t - \overline{M_t}|$, and $\overline{M_t}$ is the average driving style indicator.

The proposed updating algorithm is concluded by **Algorithm 1**. The computational complexity is mainly determined by the process from Line 2 to Line 13. According to [19], the time complexity of sampling and updating from Line 7 to Line 9 is $O(log N_{tree})$, where N_{tree} is the number of nodes in the sum-tree used to compute the priority probability. As the time complexity of model aggregation scheme in Line 11 to Line 13 is $O(1)$, the total time complexity is $O(N log N_{tree})$. It can be found that the proposed updating algorithm differs from the traditional DL process. The global model is updated with an adjustable weight $\alpha_t f_t$, which is related to the freshness of local model and driving style indicator of ICVs.

C. Analysis of Optimal Model Weight and ICV Driving Style

Since we adopt a driving style based updating algorithm, it is essential to discuss the impact of the weight on training

accuracy. The convergence bound of DL is utilized that characterizes the gap between the optimal performance and actual training performance [20], [21]. The specific proof of convergence of the updating algorithm is similar with the work of [21]. For the sake of limited space, we will directly give the convergence bound.

Convergence Bound: Under two assumptions: for all **v** and **w**: *L-smooth*: $f(\mathbf{v}) - f(\mathbf{v}) \leq (\mathbf{v} - \mathbf{w})^T \triangledown f(\mathbf{w}) + \frac{L}{2} \|\mathbf{v} - \mathbf{w}\|_2^2$, μ-*strong convex*: $f(\mathbf{v}) - f(\mathbf{v}) \geq (\mathbf{v} - \mathbf{w})^T \triangledown f(\mathbf{w}) + \frac{\mu}{2} \|\mathbf{v} - \mathbf{w}\|_2^2$, the proposed ADL within T global epoch converges to a critical point:

$$\mathcal{P} = \min_{t=0}^{T-1} \mathbb{E}\|\triangledown F(\theta_t)\|^2 \leq \mathcal{O}\left(\frac{1}{\overline{\alpha}\gamma\epsilon T H_{min}} + \frac{\gamma H_{max}^3 + \overline{\alpha} K H_{max} + \overline{\alpha}^2 \gamma K^2 H_{max}^2 + \gamma K^2 H_{max}^2}{\epsilon H_{min}}\right), \quad (18)$$

where $\overline{\alpha}$ is the expectation of driving style indicator based weight within period $(0, T)$, *i.e.* $\overline{\alpha} = \frac{1}{N_T}\sum_{t=1}^{N_T}\alpha_t$, where N_T is the total number of ICVs in T time. γ is the learning rate, $\epsilon > 0$ is a small constant. H_{min} and H_{min} are the local minimum and maximum iteration rounds, respectively. K is the maximal interval between two updating of ICV models, *i.e.* $t - t^- \leq K$.

Now we can utilize $\mathcal{P}$ to determine the optimal weight $\overline{\alpha}^*$. We approximately simplify the convergence bound as $\mathcal{P} \approx \frac{1}{\overline{\alpha}\gamma\epsilon T H_{min}} + \frac{\gamma H_{max}^3 + \overline{\alpha} K H_{max} + \overline{\alpha}^2 \gamma K^2 H_{max}^2 + \gamma K^2 H_{max}^2}{\epsilon H_{min}}$. Therefore, the bound can be expressed as a function of weight $\overline{\alpha}$. Letting x denote $\overline{\alpha}$, the bound can be transformed as

$$\mathcal{P}(x) = \frac{1}{Ax} + Bx + Cx^2 + D \quad (19)$$

where $A = \frac{1}{\gamma\epsilon T H_{min}}$, $B = \frac{K\delta}{\epsilon}$, $C = \frac{\gamma K^2 \delta H_{max}}{\epsilon}$, $D = \frac{\gamma \delta H_{max}^2 + \gamma \delta K^2 H_{max}}{\epsilon}$, $\delta = \frac{H_{max}}{H_{min}}$. By obtaining the first derivation of $\mathcal{P}(x)$, it yields $\mathcal{P}'(x) = -\frac{1}{Ax^2} + 2CX + B$. Since $A > 0$, by letting $\mathcal{P}'(x) = 0$, we can obtain a cubic equation

$$2ACx^3 + ABx^2 - 1 = 0. \quad (20)$$

Hence, the extreme values of function $\mathcal{P}$ can be obtained by solving Eq. (20). In order to solve the cubic equation and obtain a feasible solution, Cardano's formula [22] is utilized and Corollary 1 is proposed.

Corollary 3: The convergence bound $\mathcal{P}$ reaches its minimal value at point

$$\overline{\alpha}^* = \sqrt[3]{\frac{\epsilon^2 T}{2\delta^2 K^2}} \quad (21)$$

if $\gamma^3 = \frac{1}{27 T K \epsilon^2 \delta H_{min}^3}$.

Proof: For an arbitrary cubic equation $aX^3 + bX^2 + cX = d = 0$, we define three auxiliary variables

$$A_0 = b^3 - 3ac; \quad B_0 = bc - 9ad; \quad C_0 = c^2 - 3bd. \quad (22)$$

By substituting the equation above into Eq.(20), a discriminants can be obtained that

$$\triangle = B_0^2 - 4A_0C_0 = 12A^2\left(\frac{27\gamma^2 T^4 \delta^2 H_{max}^2}{\epsilon^2} - \frac{T^2\delta^3}{\gamma\epsilon^4 H_{min}}\right) \quad (23)$$

According to [22], there are one real root and two equal real roots if $\triangle = 0$. By letting $\triangle = 0$, it can be obtained that $\gamma^3 = \frac{1}{27\epsilon^2\delta H_{min}^3 T K}$, and an auxiliary parameter is defined as $\mathcal{K} = \frac{B_0}{A_0} = \frac{18AC}{A^2 B^2} = \frac{\frac{18\gamma T^2 \delta H_{max}}{\epsilon}}{\frac{T\delta^2}{\gamma\epsilon^3 H_{min}}} = 18\gamma^2\epsilon^2 H_{min}^2 T$. Then, the three real roots of Eq.(19) can be represented as

$$X_1 = \mathcal{K} - \frac{AB}{AC} = -\frac{\frac{\mathcal{K}\delta}{\epsilon}}{\frac{2\gamma \mathcal{K}^2 \delta H_{max}}{\epsilon}} = \mathcal{K} - \frac{1}{2\gamma T H_{max}}$$

$$= \mathcal{K} - \frac{27}{2}\epsilon^2\gamma^2 H_{min}^2 T = \frac{9}{2}\gamma^2\epsilon^2 H_{min}^2 T = \sqrt[3]{\frac{\epsilon^2 T}{2\delta^2 K^2}}$$

$$X_2 = X_3 = \frac{-\mathcal{K}}{2} = -9\gamma^2\epsilon^2 H_{min}^2 T. \quad (24)$$

Obviously $X_2 = X_3 < 0$, since $\overline{\alpha}$ is the expectation value of $\alpha_t > 0$, thus $\overline{\alpha} = X_1$. By substituting X_1 into the second derivation of $\mathcal{P}(x)$, and $\mathcal{P}''(X_1) > 0$. Consequently, the convergence bound $\mathcal{P}$ reach its minimal point at X_1. ∎

Based on Corollary 3, we have two remarks with respect to model weight $\overline{\alpha}$ and driving style indicator m.

Remark 1: Compare with precious GM, the new uploaded local model should have a higher weight. Corollary 3 gives the optimal weight $\overline{\alpha}^*$ that is associate with learning time T. With the increase of T, the value of $\overline{\alpha}^*$ will also increase, hence, considering a long-term training process, the weight of new updated model $\overline{\alpha}$ is greater than the previous model $(1 - \overline{\alpha})$.

Remark 2: On the basis of reducing communication cost as well as not affecting the accuracy of final model, those ICVs with indicator m_t far away from the average $\overline{M}$ should choose not to upload their local model. As indicated in *Remark 1*, the optimal $\overline{\alpha}^*$ will increase with learning time T. Since $\overline{\alpha}$ can be expressed as $\overline{\alpha} = \frac{1}{N_T}\sum_{t=1}^{N_T}\alpha_t = \frac{1}{N_T}\sum_{t=1}^{N_T}(1 - |m_t - \overline{M_t}|)$, we can decrease the number of those ICVs with m_t that are far away from the average $\overline{M_t}$, so that the value of $\overline{\alpha}$ will not decrease. The remark can be explained by the fact that the local models trained by those ICVs with a deviated driving style cannot reflect the accurate global context, and we can reduce the use of models from those ICVs to reduce the uploading communications while maintaining the global training quality.

VI. SIMULATION RESULTS

In this section, we evaluate the proposed DAG based knowledge sharing framework and adaptive ADL scheme by simulation experiments.

A. Simulation Setup

To investigate the proposed knowledge sharing framework, it is essential to firstly specify the driving style indicator m of ICVs. In this article, we will base our investigation on the open source autonomous driving environment, Airsim, which was developed by Microsoft AI & Research team [23]. In the Airsim environment, driving style is characterized with three parameters: vehicular throttle a, wheel steering b and braking c. According to the Airsim project, we formulate m as $m = \frac{a(1-c)+b^2}{2}$, the driving style indicator can reflect the following facts: whether throttle $a = 0$ or braking $c = 1$, the ICVs will
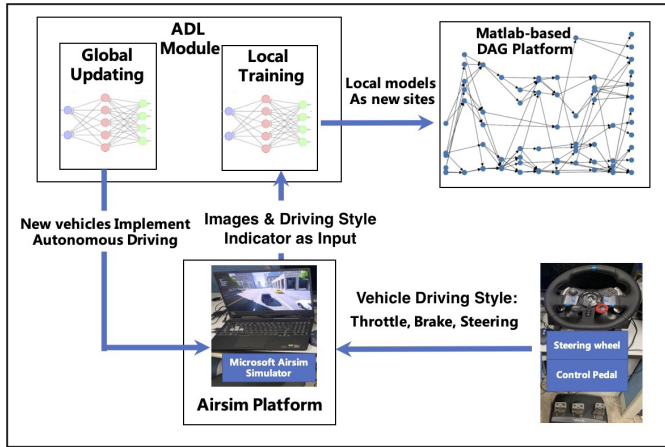
Fig. 4.   Testing Environment.

(a) Driving-style Classified Ledger

(b) Ledger Convergency

(c) Chosen Delay

(d) Authentication Delay

Fig. 5.   Performance of the Lightweight DAG.

TABLE I

SIMULATION PARAMETERS

Parameters	Value
Number of Vehicles	35
Dataset size of distributed learning	3000
Driving Style Indicator m	$m_1 \in [0.25, 0.3]$, $m_2 \in [0.3, 0.35]$, $m_3 \in [0.35, 0.45]$
Driving Throttle, Braking a, c	[0, 1]
Driving Steering b	[-1, 1]
Local model & GM network models	CNN
Own weight of each site ω	1
Sites Generation Distribution	Uniform (Uni) in (400, 500) Poisson distribution (Poi) with λ=700 Gamma distribution (Gam) with $\alpha = 200, \beta = 1$

remain stationary, and either a large a or a sharply steering of b will give a large value of driving style indicator m. It should be noted that the definition of driving style indicator is not unique, and we only adopt the equation above to demonstrate the effectiveness of the proposed schemes.

We evaluate the lightweight DAG system in Matlab, wherein new sites are generated following three distributions: uniform distribution (Uni) within (400, 500), poisson distribution (Poi) with $\lambda = 700$ and gamma distribution (Gam) with $\alpha = 200, \beta = 1$. The new site selects two tips according to Eq. (4). We further control ICVs by Logitech G29 Driving Force Steering Wheel and Pedal to simulate real driving style of ICVs. Three types of driving styles are adopted: m_1-type for ICVs has throttle $a = 0.5$, steering $b \in [-0.3, 0.3]$, braking $c = 0$, and the corresponding driving style indicator $m_1 \in [0.25, 0.3]$; m_2-type has $a = 0.6$, $b \in [-0.2, 0.2]$, $c = 0$, and $m_2 \in [0.3, 0.35]$; m_3-type has $a = 0.7$, $b \in [-0.4, 0.4]$, $c = 0$, and $m_3 \in [0.35, 0.45]$.

Then the ADL is investigated with an autonomous driving scenario based on Airsim. We adopt the city scenario of Airsim, in which 35 vehicles are utilized for evaluation of ADL. The vehicles are controlled by Logitech G29 to drive around the city and collect their surrounding images to build a dataset. The convolutional neural network (CNN) model is adopted as our local model. The driving style indicator m and the collected images are chosen as the input of the CNN model, and the output is the steering value of vehicles. Three existing algorithms are chosen as the comparison groups: the standard federated learning (FedAve) [24] that aggregates the local models from all vehicles synchronously and ignores the driving style, an autonomous driving algorithm (cook-AD) proposed by Project Road Runner at Microsoft Garage [25] that only exploit the local view of vehicles without referring to other vehicles, and the centralized CNN that trains on the whole centralized dataset. The simulation environment is illustrated in Fig. 4 and the main parameters used in the simulations are summarized in Table I.

B. Numerical Results and Discussion

The proposed lightweight DAG system is evaluated first in terms of five following aspects: features of ledger, chosen delay, authentication delay and confirmation delay. As shown
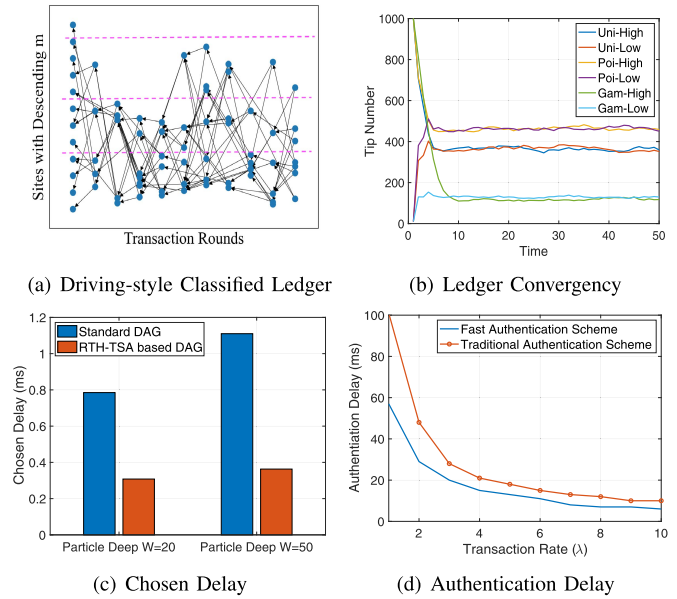
in Fig. 5 (a), y-coordinate of the point in the figure represents the value of the driving style indicator m. The driving style indicator value of the bottom point is close to 0, and the indicator value of the top point is close to 1. We set the value of the driving style indicators of genesis sites (*i.e.* points in the leftmost column) in a descending order, then we input incoming sites with different value of m in each transaction round, which choose tips according to Eq. (3). With transaction rounds, the total DAG ledger is logically divided into multiple sub-ledgers, which verifies the design of DC-ledger, as indicated in Section. IV. A. Then, the convergence results of the proposed DC-Ledger are shown in Fig. 5 (b). Three tip-arrival distributions are considered, as indicated in Section. VI. A. Two initial number of sites are set, *i.e.* high genesis sites=1000 and low genesis sites=10. It can be found that no matter what the genesis number is, the final tip number will become stable, which shows the convergence of DAG.

Then, both chosen delay and authentication delay are investigated in Fig. 5 (c) and (d). The chosen delay is defined as the time it takes for new sites to choose tips. The authentication delay is defined as the time consumption for a new cross-region site to be fully trusted by the new region. It can be figured that the proposed RTH-RST achieves fast chosen delay towards standard DAG. Since the proposed algorithm only needs to verify two old sites, rather than
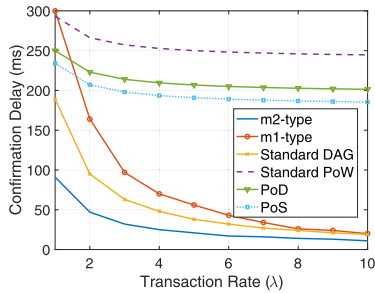
This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

10

IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS

Fig. 6.   Confirmation Delay of Sites.

Fig. 8.   Tset Gap of ADL.
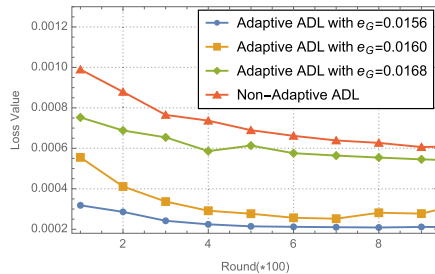

Fig. 7.   Loss Value of Final GM.

Fig. 9.   Bandwidth Consumption of ADL.

tracing back particle deep W, thus it realizes time-efficient. Moreover, the proposed lightweight DAG also support fast authentication of cross-region sites. It can be explained by the proposed authentication scheme utilizes the *identityStone* with cumulative weight $w = 0$, as indicated in Section. IV. B. Sites in new region will firstly choose the cross-region site according to Eq. (3), thus completing fast authentication.

In fig. 6, the confirmation delay is elaborated investigated. We adopt four existing blockchains with different consensus algorithms as the comparison groups: Standard DAG with MCMC algorithm, Standard PoW, Proof-of-Driving (PoD) with a simplified PoW difficulty [26] and Proof-of-Storage (PoS) [27] that is essentially a Delegated Proof-of-Stake algorithm [28]. The driving style indicators of incoming sites are set as the uniform distribution between (0.3, 0.35). It can be figured that the chain-based systems (Standard PoW, PoD and PoS) have high confirmation delay than the DAG systems. This is due to that the chain-based system is required to collect enough transactions to issue one block, while the DAG system supports node to directly issue the site, thus reducing the confirmation delay. Moreover, with the transaction rate, the DAG systems obtain ever increasing advantages on confirmation delay towards chain-based systems, which proves the superiority of DAG in micro-transaction scenario. More importantly, compared with standard DAG, the proposed lightweight DAG with m2-type shows even shorter delay, which verifies *Corollary 2* in Section IV. Although sites with m1-type have longer delay than standard DAG, we can leverage RSUs to periodical issue auxiliary site to shorten confirmation delay, similar to the design of *IdentityStone*.

Next, the proposed ADL is evaluated in terms of loss function, test gap and bandwidth consumption. We choose three different reference gaps $e_G = 0.0156, 0.0160$ and 0.0168. As can be seen in Fig. 7, all the three adaptive ADL schemes outperform the non-adaptive ADL ones. This is due to that the reference gap e_G filters some ICVs with poor local models.
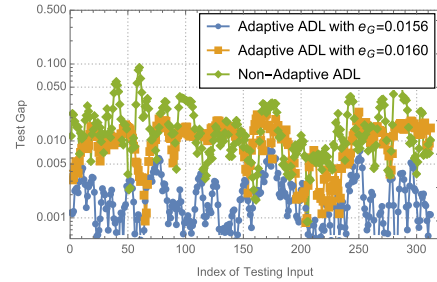
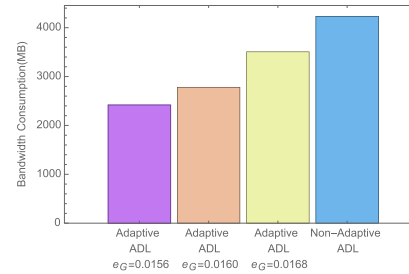Only those ICVs with a local test gap $e_v > e_G$ are allowed to upload their local models to the RSUs, which will improve the quality of global model. Besides, with the decrease of f e_G, the global loss value will be further reduced: a lower e_G means that the RSUs have a better GM. Thus, in order to upload local models, the ICVs should also train a better CNN model, which will promote the entire network to evolve in a better direction. It is also noted that when the reference gap e_G is updated to a sufficiently small value, there may be no more ICVs to upload their local models. In this case, the global model can be deemed as converged and optimal.

Test gap is defined as the gap between real output and model output calculated by test dataset. As shown in Fig.8, compared to non-adaptive scheme that enforces all ICVs to upload their models, the adaptive based schemes have a smaller gap. As the output of our CNN model is the steering value of ICVs, which is one of the crucial parameters for driving control, by utilizing the adaptive based ADL, the RSUs can obtain a more accurate global model to implement autonomous driving.

The results of communication cost measured by the bandwidth consumption are presented in Fig. 9, where the bandwidth consumption refers to the volume of uploading models. The CNN model is 120.9 MB with two convolution layers, two pooling layers, one linear layer, one flatten layer and three ramp layer. Since the adaptive ADL scheme utilizes the reference gap e_G to control the number of updated models, the consumed bandwidth will be reduced. As shown in Fig. 9, the adaptive ADL with $e_G=0.0156$ can achieve a more than 30 % reduction towards the non-adaptive scheme. By reducing the communication cost, the final leaning quality of the GM does not degrade, which proves that the proposed scheme is suitable for the large-scale ICV networks.

Then, we investigate the impact of freshness on the model learning loss. The results are presented in Fig. 10 (a). The performance of the CNN model trained in a centralized approach is adopted here as the optimal training result. It can be seen

(a) Impact of Freshness   (b) Impact of Driving Style Indicator   (c) Driving Violation Rate of different Sharing Schemes
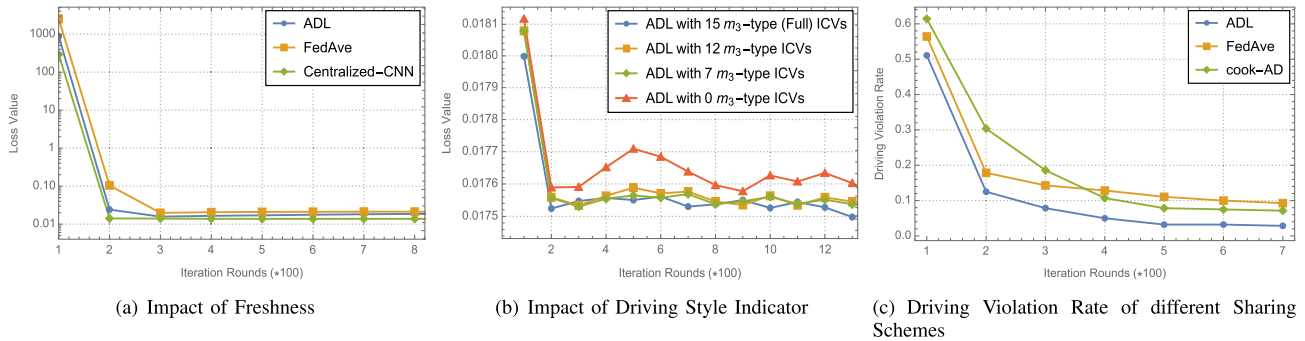
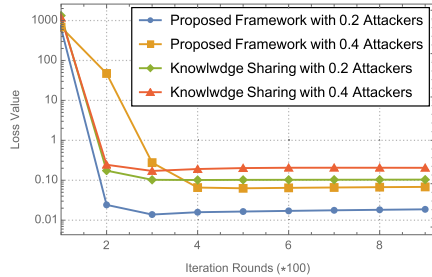Fig. 10. Performance of the Adaptive ADL.

Fig. 11. The Security Performance under Attackers.

that the proposed ADL has a loss very close to the optimal one, while that of FedAve is much deviated. According to the definition of freshness in Eq. (15), the weight of subsequent models is higher than the earlier ones. Therefore, from the perspective of global model training process, increasing the weight of new local model will enhance the final training accuracy, which is consistent with *Remark 1*.

The results on the impact of driving style indicator on the model quality are shown in Fig. 10 (b). The specific numbers of the ICVs with these three types are set as $N_{m_1} = N_{m_2} = 10$, $N_{m_3} = 15$, and the m_3-type vehicles can be regarded as those ICVs with indicators far away from the average $\overline{M}$. The loss values of both 12 ICVs with m_3-type and 7 ICVs with m_3-type are very close to that of full participants scenario. By reduce the number of those "deviated" ICVs, we can reduce the communication cost of model updating, meanwhile ensuring the learning quality of global model, which verifies the claim in *Remark 2*. Moreover, if we keep decrease the number of ICVs to the 0 m_3-type scenario in the figure, the learning loss will increase. This can be explained that although the deviated ICVs have little impact on the global model, their models do contain some information that other ICVs don't have. In order to obtain an accurate model, the final comprehensive model should aggregate some models from those deviated ICVs.

The violation rate results are presented in Fig. 10 (c). Here the violation rate is defined as the percentage of bad behaviours of new vehicles autonomous driving with the trained CNN models in Airsim, such as retrograde motion or driving to pedestrian lanes. With the iteration process, the proposed ADL algorithm achieves a 20% reduction in violation rate over the cook-AD and FedAve algorithms, which demonstrates the effectiveness of the proposed algorithm. It can also be found that both the proposed ADL and the FedAve algorithms converge faster than the cook-AD. It can be explained by that

utilizing the updating schemes, the DL-based algorithms can collect local models from multiple ICVs. The DL algorithm accelerates the cognition of global context. Although the cook-AD algorithm utilizes a preprocessing method of flipping images that enlarges the training set, it will increase the complexity of training data and reduce the convergent speed.

At last, the security of the proposed knowledge sharing framework is investigated in Fig. 11. Two scenarios with different proportions of attackers are considered with 0.2 and 0.4 attackers, respectively. The attackers share malicious models with biased driving style indicators, attempting to affect the final learned model. It can be found from the figure that the proposed framework achieves a lower loss value than that of the original knowledge sharing system. The proposed one reduces the loss function value by an average of 30%, which is mainly due to the use of DAG blockchain. The proposed knowledge framework utilizes the verification process $e \leq \epsilon$ to judge if the knowledge is legal, which can prevent the malicious data of attackers from being appended to the ledger.

VII. CONCLUSION

In this paper, we propose a knowledge sharing framework to provide security and efficiency under dynamic and mobile ICV networks. In order to enhance sharing efficiency, ADL is adopt to transfer raw data sharing to knowledge sharing. A lightweight DAG is designed to ensure the security of shared knowledge and to tackle the time-efficient issues in traditional DAG systems. A RTH-TSA is proposed for tip selection in DAG to achieve lightweight consensus and fast cross-region identity authentication. Furthermore, we propose an adaptive ADL scheme to enhance quality of shared knowledge as well as reducing communication cost during the learning process. Experiment results demonstrate the efficiency and stability of the proposed knowledge sharing framework. The proposed framework reduces a 30% loss value against malicious attacks. In addition, the proposed adaptive ADL algorithm is effective and efficient, with more than 20% reduction in terms of driving violation rate compared with existing algorithms.

REFERENCES

[1] S. R. Pokhrel and J. Choi, "Low-delay scheduling for internet of vehicles: Load-balanced multipath communication with FEC," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8489–8501, Dec. 2019, doi: 10.1109/TCOMM.2019.2941926.

[2] G. Qiao, S. Leng, S. Maharjan, Y. Zhang, and N. Ansari, "Deep reinforcement learning for cooperative content caching in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 247–257, Jan. 2020, doi: 10.1109/JIOT.2019.2945640.

[3] J.-N. Lee, "The impact of knowledge sharing, organizational capability and partnership quality on IS outsourcing success," *Inf. Manage.*, vol. 38, no. 5, pp. 323–335, Apr. 2001, doi: 10.1016/S0378-7206(00)00074-4.

[4] K. Xiong, S. Leng, J. Hu, X. Chen, and K. Yang, "Smart network slicing for vehicular fog-RANs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3075–3085, Apr. 2019, doi: 10.1109/TVT.2019.2900234.

[5] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," pp. 1–38, Oct. 2016, *arXiv:1610.02527*.

[6] S. Popov. (2018). *The Tangle*. [Online]. Available: https://www.iota.org/foundation/research-papers

[7] L. A. Maglaras and D. Katsaros, "Social clustering of vehicles based on semi-Markov processes," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 318–332, Jan. 2016, doi: 10.1109/TVT.2015.2394367.

[8] M. Ruta, F. Scioscia, F. Gramegna, S. Ieva, E. Di Sciascio, and R. P. De Vera, "A knowledge fusion approach for context aware-ness in vehicular networks," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2407–2419, Aug. 2018, doi: 10.1109/JIOT.2018.2815009.

[9] X. Chen, S. Leng, J. He, and L. Zhou, "Deep-learning-based intelligent intervehicle distance control for 6G-enabled cooperative autonomous driving," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15180–15190, Oct. 2021, doi: 10.1109/JIOT.2020.3048050.

[10] G. Li, M. Dong, L. T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among IoT services: A blockchain-based approach," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 4, no. 5, pp. 653–665, Oct. 2020, doi: 10.1109/TETCI.2019.2952587.

[11] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Trans. Ind. Informat.* vol. 15, no. 12, pp. 6367–6378, Dec. 2019, doi: 10.1109/TII.2019.2917307.

[12] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr. 2021, doi: 10.1109/TNSE.2019.2959230.

[13] H. Cui, Z. Wan, X. Wei, S. Nepal, and X. Yi, "Pay as you decrypt: Decryption outsourcing for functional encryption using blockchain," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3227–3238, 2020, doi: 10.1109/TIFS.2020.2973864.

[14] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

[15] X. Zhang, M. Peng, S. Yan, and Y. Sun, "Deep-reinforcement-learning-based mode selection and resource allocation for cellular V2X communications," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6380–6391, Jul. 2020, doi: 10.1109/JIOT.2019.2962715.

[16] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020, doi: 10.1109/TII.2019.2942190.

[17] Y. Liao, M. Wang, L. Duan, and F. Chen, "Cross-regional driver–vehicle interaction design: An interview study on driving risk perceptions, decisions, and ADAS function preferences," *IET Intell. Transp. Syst.*, vol. 12, no. 8, pp. 801–808, Oct. 2018, doi: 10.1049/iet-its.2017.0241.

[18] S. M. Ross, *Introduction to Probability Models*. New York, NY, USA: Academic, 2014.

[19] Z. Xu *et al.*, "Experience-driven networking: A deep reinforcement learning based approach," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Honolulu, HI, USA, Apr. 2018, pp. 1871–1879, doi: 10.1109/INFOCOM.2018.8485853.

[20] A. Elgabli, J. Park, A. S. Bedi, M. Bennis, and V. Aggarwal, "GADMM: Fast and communication efficient framework for distributed machine learning," *J. Mach. Learn. Res.*, vol. 21, no. 76, pp. 1–39, 2020.

[21] C. Xie, S. Koyejo, and I. Gupta, "Asynchronous federated optimization," 2019, *arXiv:1903.03934*.

[22] G. Cardano, *Artis Magnae Sive De Regvlis Algebraicis*, vol. 1545. Cambridge, MA, USA: MIT Press, 1968.

[23] Microsoft AI & Research. (2017). *Airsim*. [Online]. Available: https://github.com/microsoft/AirSim

[24] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, Fort Lauderdale, FL, USA, vol. 54, Apr. 2017, pp. 1273–1282.

[25] Microsoft. (2018). *Autonomous Driving Cookbook*. [Online]. Available: https://github.com/microsoft/AutonomousDrivingCookbook

[26] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.

[27] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, "Attribute-based secure announcement sharing among vehicles using blockchain," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10873–10883, Jul. 2021, doi: 10.1109/JIOT.2021.3050802.

[28] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 16, 2021, doi: 10.1109/TITS.2021.3086976.

Haoye Chai (Graduate Student Member, IEEE) received the B.Sc. degree in information and communication engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2016, where he is currently pursuing the Ph.D. degree. His research interests include mobile edge computing, Internet of Vehicles, and blockchain in wireless networks.

Supeng Leng (Member, IEEE) received the Ph.D. degree from Nanyang Technological University (NTU), Singapore. He has been working as a Research Fellow with the Network Technology Research Center, NTU. He is currently a Full Professor and the Vice Dean with the School of Information and Communication Engineering, University of Electronic Science and Technology of China (UESTC). He is also the Leader with the Research Group of Ubiquitous Wireless Networks. His research interests include resource, spectrum, energy, routing, and networking in the Internet of Things, Internet of Vehicles, broadband wireless access networks, and the next generation mobile networks. He has published over 200 research papers in recent years. He serves as the organizing committee chair and a TPC member for many international conferences, as well as a reviewer for over ten international research journals.

Fan Wu received the Ph.D. degree from the University of Electronic Science and Technology of China, China, in 2015. He is currently an Associate Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China. His research interests include edge intelligence, vehicular networks, and optimization techniques in resource allocation of wireless networks.

Jianhua He received the Ph.D. degree from Nanyang Technological University, Singapore, in 2002. He is currently a Reader with the University of Essex, U.K. His main research interests include wireless communications and networks, connected vehicles, autonomous driving, the Internet of Things, mobile edge computing, data analytics, AI and machine learning. He has published more than 150 research papers in international journals and conferences in these research areas. He is the Workshop Chair of MobiArch'20 and ICAV'21, a Steering Committee Member of MobiArch'21, and a member of editorial board for several international journals. He is the Coordinator of EU Horizon2020 projects COSAFE and VESAFE on cooperative connected autonomous vehicles.