This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks

Jiawen Kang, Rong Yu, *Member, IEEE*, Xumin Huang, Maoqiang Wu, Sabita Maharjan, *Member, IEEE*, Shengli Xie, *Senior Member, IEEE*, Yan Zhang, *Senior Member, IEEE*

***Abstract*—The drastically increasing volume and the growing trend on the types of data have brought in the possibility of realizing advanced applications such as enhanced driving safety, and have enriched existing vehicular services through data sharing among vehicles and data analysis. Due to limited resource of vehicles, mobile edge computing integrated with vehicular networks gives rise to Vehicular Edge COmputing and Networks (VECONs) for providing powerful computing and massive storage resources. However, vehicular edge computing servers consisted of roadside units cannot be fully trusted, which may result in serious security and privacy challenges. We exploit consortium blockchain and smart contract technologies to achieve secure data storage and sharing in vehicular edge networks. These technologies efficiently prevent data sharing without authorization. In addition, we propose a reputation based data sharing scheme to ensure high-quality data sharing among vehicles. A three-weight subjective logic model is utilized for precisely managing reputation of the vehicles. Numerical results based on a real dataset show that our schemes achieve reasonable efficiency and high-level security for data sharing in VECONs.**

***Index Terms*—Vehicular edge computing, blockchain, smart contracts, security and privacy, reputation management.**

I. Introduction

WITH rapid development of vehicular telematics and applications, vehicles generate a huge amount and several different types of data. For example, a self-driving vehicle can create 1 GB data per second from cameras, radar, GPS, etc [1]. Moreover, vehicles can cooperatively collect and share data of common interest [2], [3]. Data collected by the vehicles consists of objective and subjective information. The objective information mainly includes traffic-related data, such as road and weather conditions, and parking lot occupancy. The subjective information includes things such as rating of a hotel and quality of vehicular services [4]. Sharing of data has made it possible to realize goals such as improved driving safety, and to obtain higher service quality during travelling.

Due to resource constraints, vehicles cannot support massive data storage and large-scale data sharing. Vehicle-generated data becomes increasingly fine-grained and complex, which increases the burden on data transmission. Meanwhile, the data more locally relevant for vehicles has spatial scope and explicit lifetime of utility, such as current traffic information at an intersection, which requires low latency and location awareness for vehicular data sharing [2]. To address these challenges, mobile edge computing is a promising paradigm that can be embedded at the network edge infrastructures, e.g., Roadside Units (RSUs), to support massive data storage, computing and sharing close to the vehicles [2], [5]. Vehicular networks integrated with mobile edge computing are evolving towards Vehicular Edge COmputing and Networks (VECONs) [6].

Although VECONs pave the way for high performance networks at the edge, security and privacy issues are critical challenges for VECONs. RSUs in VECONs play an important role to temporally store and manage vehicular data. But the RSUs are semi-trusted because that they are usually distributed along the road without strong security protection, which are vulnerable to being compromised by attackers [2], [7], [8]. Vehicles therefore may not be willing to upload their data to the RSUs because of privacy concerns. Likewise, Peer to Peer (P2P) data sharing among vehicles raises the issues such as data access without authorization and the need of ensuring security in a decentralized manner. These challenges influence the sharing of vehicular data, and thus hinder the pace for development of VECONs [9].

Recently, blockchain technology has attracted growing attention and research work in the context of vehicular networks because of its characteristics of decentralization, anonymity and trust. Blockchain can facilitate establishing a secure, trusted and decentralized intelligent transport ecosystem, to address data sharing problems thus contributing in creating better usage of the transport infrastructures and resources [9], [10], [11]. The authors in [12] present an intelligent vehicle-trust point mechanism using blockchain to support secure communications among vehicles. However, due to high cost to establish a public blockchain in resource-limited vehicles, the existing methods do not work well in P2P data sharing among vehicles in VECONs.

Motivated by these developments, we exploit the consortium blockchain technology to develop a secure P2P data sharing system for vehicular data named vehicular blockchain in this

This work was supported in part by programs of NSFC under Grant nos. 61379115, 61422201, 61501127, 61370159, 61503083 and U1301255, U1501251, the Science and Technology Program of Guangdong Province under Grant nos. 2015B010129001, 2015B010106010, 2016A030313705, 2014B090907010, 2015B010131014, and is partially supported by the projects 240079/F20 funded by the Research Council of Norway.

Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu and Shengli Xie are with School of Automation, Guangdong University of Technology, China. Emails: {kjwx886@163.com, yurong@ieee.org, huangxu_min@163.com, maoqiang.wu@vip.163.com, shlxie@gdut.edu.cn}.

Sabita Mahajan is with Simula Metropolitan Center for Digital Engineering, and University of Oslo, Norway. Email: sabita@simula.no.

Yan Zhang is with Department of Informatics, University of Oslo, Norway. Email: yanzhang@ieee.org.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

paper. Consortium blockchain is a specific blockchain with multiple pre-selected nodes to establish the distributed shared database with moderate cost [13], [14]. Here, the pre-selected nodes are RSUs. Vehicular blockchain is established on RSUs to publicly audit and store shared data and records of data sharing. The authors in [8] propose a public blockchain-based trust management system, wherein vehicles validate received messages from neighboring vehicles using bayesian inference model. Unlike that in [8], we also utilize smart contracts to design vehicular data storage and sharing schemes, which are self-executing scripts residing on blockchains and allow for distributed automation of multi-step processes. These smart contract-based schemes enable data management automation with high efficiency, and defend against second-hand data sharing without authorization as well. Moreover, data quality is a core element of the development of vehicular data sharing [9]. Vehicles as data sources may provide irrelevant or incorrect information to other vehicles due to defective sensors, compromised firmware, or even selfish purpose [4], [8], [15]. Previous researches have indicated that the quality of data depends on the vehicles' reputation [16]. It is essential to design a mechanism to quantify vehicles' reputation based on the interactions among vehicles [4], [8]. Vehicles choose the best data provider according to reputation.

The main contributions of this paper are summarized as follows.

- We propose to utilize consortium blockchain to establish a secure and distributed vehicular blockchain for data management in VECONs.
- We deploy smart contracts on the vehicular blockchain to achieve secure and efficient data storage on RSUs, and data sharing among vehicles.
- We develop a reputation based data sharing scheme with three-weight subjective logic model to choose more reliable data source to improve data credibility.

The rest of this paper is organized as follows. We introduce the core system components of secure P2P data sharing system using blockchain in Section II. We illustrate secure and efficient data storage and sharing schemes running on vehicular blockchain in Section III. We propose a reputation based data sharing scheme with subjective logic model for high-quality sharing in Section IV. We provide security analysis and numerical results in Section V. Section VI concludes the paper.

II. Core System Components for Distributed Data Storage and Decentralized Data Sharing

A. Vehicular Edge Computing and Networks (VECONs)

VECONs are composed of a user layer, an edge layer, and a cloud layer as shown in Fig. 1. In the user layer, vehicles equipped with onboard units can access services by communicating with RSUs. The onboard units perform simple computations, collect local data from sensing devices, and upload data to the edge layer [2]. In the edge layer, several nearby RSUs (edge nodes) deployed along the road can be combined to form a vehicular edge cluster. Each vehicle communicates with the nearest RSU to access a local vehicular

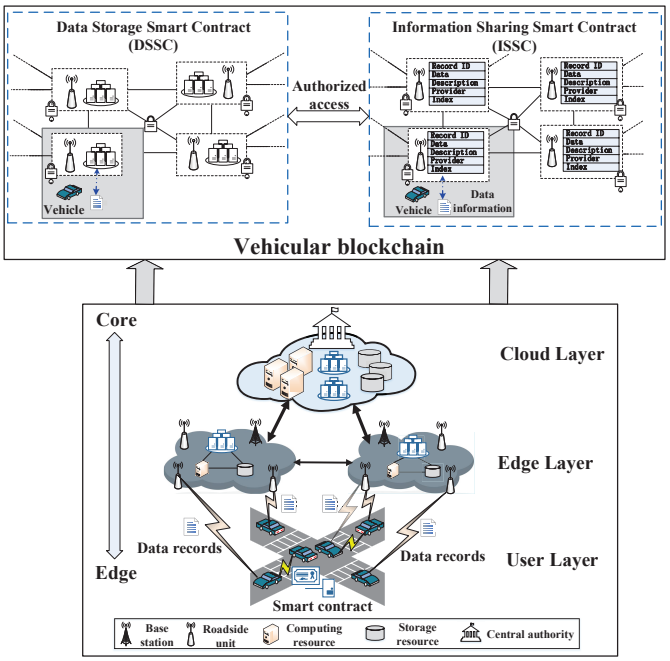

Fig. 1: Secure peer to peer data sharing system using consortium blockchains

edge cluster. Vehicular edge clusters temporarily store the data from vehicles and deliver the data to a central cloud through wired connections if necessary. The central cloud in the cloud layer manages all vehicular edge clusters. This central cloud can be a data center of the ITS, which can store massive data permanently and carry out complicated and delay-tolerant computing tasks for vehicles. While the frequently used data and time-sensitive tasks from vehicles can be stored and executed at the edge of vehicular networks, e.g., local vehicular edge clusters.

B. Vehicular Blockchain and Smart Contracts

To decrease cost of establishing a blockchain, unlike traditional public blockchains [11], [17], [18], we utilize consortium blockchain technology to form a vehicular blockchain, which performs distributed data storage and secure data sharing. A consortium blockchain is a special blockchain in which the consensus process is executed on pre-selected edge nodes, e.g., RSUs. Here, the consensus process is an important data audit stage before adding the data into vehicular blockchain. Some RSUs are chosen and authorized to carry out the consensus process in the vehicular blockchain. For distributed data storage and secure P2P sharing among vehicles, we also design a model of vehicular blockchain using smart contract technologies in VECONs. This model includes data requestors, data providers, edge nodes, a Data Storage Smart Contract (DSSC) and an Information Sharing Smart Contract (ISSC) running on the vehicular blockchain.

1) Data requestors and data providers: Vehicles play different roles in P2P vehicular data storage and sharing: data requestors and data providers. The data requestors apply for shared data from the data providers. The data providers collect

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

traffic-related information, and share their data stored in edge nodes for getting rewards based on their contributions [16]. Each vehicle chooses its own role according to data demands and driving plan.

2) Edge nodes: We consider RSUs at the edge of VECONs are the edge devices (nodes). The RSUs are upgraded to have computational capabilities and storage space for computing and storage services. A certain number of RSUs in the same area form a vehicular edge cluster. There are a local controller and a storage pool in each vehicular edge cluster as shown in Fig. 2. The local controller works as a data broker to manage data requests from local data requestors. A storage pool stores local data uploaded by vehicles. Each data requestor sends a request about data demand to the nearest RSU after finding the best local data provider by ISSC. The data providers will make decisions about data sharing authorization. The RSUs act as not only data aggregators in DSSC, but also miners in ISSC.

3) Data storage smart contract for distributed data storage: DSSC for distributed data storage mainly consists of the following components.

- Raw data: Due to limited storage resource of data providers, a variety of raw data, such as information about ice on road, traffic conditions, parking lot occupancy, and rating of a restaurant, are stored in edge nodes. These data can be used for various types of researches, e.g., data analysis. For security and privacy protection, the raw data should be anonymous, and should be encrypted and attached with digital signatures of data providers. The data providers use different pseudonyms to encrypt different raw data for decreasing the relevance of raw data generated by the same data provider [19], [20].
- Data blocks: As shown in Fig. 2, edge nodes (i.e., RSUs) working as data aggregators will periodically integrate received raw data into a data block, and broadcast the data block to other edge nodes for verification. Before a new data block is inserted into immutable vehicular blockchain, a consensus should be reached among the edge nodes through a mechanism named proof-of-storage in DSSC. A local controller generates a storage address list of raw data for each data provider. The data provider searches and reads its raw data according to the corresponding storage address list.
- Proof-of-storage about storage resource contributions: The edge node with the most contribution on storage space in every vehicular edge cluster is rewarded by vehicle coins over a period of time, which is an incentive to encourage edge nodes to provide enough storage space for local storage. Here, the vehicle coin is a specific crypto-currency for VECONs. The total amount of contributed storage is recorded by a local controller, which is the proof-of-storage for edge nodes about storage resource contributions.

4) Information sharing smart contract for decentralized data sharing: There are three components in ISSC as follows.

- Metadata: A data provider first generates an index of its raw data as a metadata before uploading to vehicular blockchain using DSSC. The metadata generally contains a pseudonym of the data provider, storage address of raw data in vehicular edge clusters, data description (e.g., type, accuracy, size, sampling frequency, collection time, and sharing permission, etc.), reputation opinions of vehicles, and digital signature for verification. A data sharing record includes entity information of data sharing, sharing range and so on. The metadata and sharing records are integrated into a block and uploaded to an edge node for verification among edge nodes. More details are provided in Section III-B and IV.
- Proof-of-work about data audit for edge nodes: Each edge node collects and verifies local metadata in its coverage. All edge nodes broadcast their local metadata to other edge nodes in the vehicular blockchain. Every edge node periodically structures newly received metadata into a local data block, and competes to find an available hash value based on parameters of the local data block. Similar to traditional proof-of-work in Bitcoin [18], this hash value should meet a preset difficulty controlled by the whole blockchain system to adjust generation speed of new data blocks. The fastest edge node adds its local data block to the vehicular blockchain using DSSC after verification by other edge nodes, and thus it gets a certain amount of vehicle coins as rewards. Edge nodes can use received vehicle coins to further upgrade their storage and computation resources.

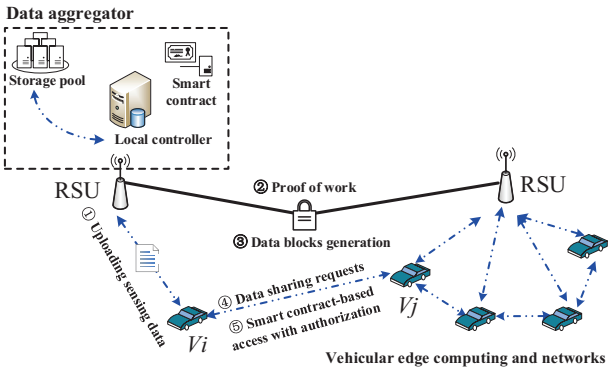

Fig. 2: Secure data storage and sharing using blockchain in vehicular edge networks

III. Secure and Efficient Data Storage and Sharing Schemes in the Vehicular Blockchain

A. An Overview of Our Proposed Schemes

In this paper, smart contracts are exploited to achieve secure, reliable, and efficient data sharing. A smart contract is a script resided on blockchains to enable automation of multi-step processes, which cannot be modified or interrupted because of the distributed nature. For this reason, the usage of smart contracts could improve the reliability, efficiency and security of the vehicular blockchain. Two smart contracts, i.e., DSSC and ISSC, are deployed on vehicular blockchain to enable secure and decentralized data sharing.

Fig. 2 shows that vehicles driving along the road generate and upload raw data and their corresponding metadata to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

TABLE I: MAIN SYMBOLS USED IN THIS PAPER

Notation	Description
v_i	The i^{th} vehicle in VECONs.
PID_i^k	The k^{th} pseudonym of v_i. Each vehicle has ν pseudonyms, $\{PID_i^k\}_{k=1}^{\nu} = \{PID_i\}$.
DAG_j	The j^{th} local data aggregator in VECONs.
$i \rightarrow j$	The entity i sends a message to the entity j.
$x\|\|y$	Element x concatenates to y.
RSU_k	The k^{th} RSU in VECONs.
$PK_i, SK_i, Cert_i$	Public and private key pair of the entity i, and the corresponding certificate.
$E_{PK_x}(m)$	Encryption of message m with public key of entry x.
$E_{SK_x}(m)$	Encryption of message m with private key of entry x.
$Sign_{SK_x}(m)$	Digital signature on message m with private key of entry x.
$timestamp$	Time record of the current event.

nearby RSUs by DSSC. The raw data will be securely stored in the vehicular blockchain using proof-of-storage. Meanwhile, for efficiently decentralized data sharing, data requestors first search data through ISSC, then find out related information of data of interest. The data requestors communicate with the data providers to apply for access authorization. After that, the data requestors pay the data providers using vehicle coins. With the help of proof-of-work about data audit, raw data and sharing records are audited and verified by RSUs, then added into vehicular blockchain. More details about the proposed schemes are given as follows.

B. Secure Data Storage Scheme using DSSC

1) Raw data storage in the vehicular blockchain:

- *Step 1: System initialization and key generation.* In the vehicular blockchain, elliptic curve digital signature algorithm and asymmetric cryptography are used for system initialization. Every vehicle becomes a legitimate vehicle after passing identity authentication by a trusted central authority, e.g., a government department of transportation. A legitimate vehicle v_i with the true identity ID_i obtains its public & private keys and the corresponding certificates (i.e., $\{PK_{PID_i^k}, SK_{PID_i^k}, Cert_{PID_i^k}\}_{k=1}^{\nu}$) for encrypting sensing data. When v_i carries out system initialization, v_i downloads the latest data information from storage pools of nearby edge nodes in the vehicular blockchain.
- *Step 2: Uploading shared data.* A vehicle v_i first sends an upload request to a local RSU of vehicular edge cluster. Here, the RSU acts as a local data aggregator (denoted as DAG_j). This request includes the current pseudonym being used (PID_i^k), and the corresponding signature $Sig_{PID_i^k}$ and certificate $Cert_{PID_i^k}$ to ensure reliability and truthfulness of the request. After receiving the request, DAG_j verifies the request and sends a response back to v_i. If v_i is allowed to upload data, v_i will send its shared data ($Data$) as a record after encryption with the public key $PK_{PID_i^k}$ of PID_i^k to DAG_j, namely,

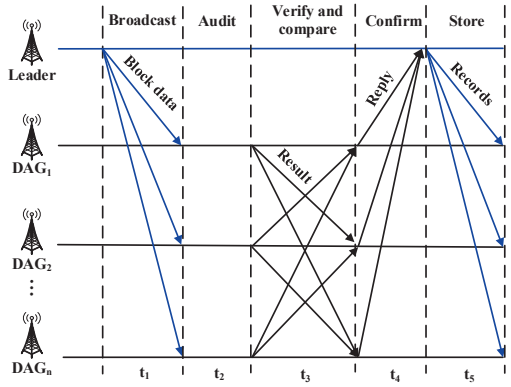

Fig. 3: The consensus process for ISSC.

$$v_i \rightarrow DAG_j : \text{Record} = E_{PK_{DAG_j}}(Data\_1||Cert_{PID_i^k} ||Sig_{PID_i^k}||timestamp),$$
$$where\ Data\_1 = E_{PK_{PID_i^k}}(Data||timestamp),$$
$$Sig_{PID_i^k} = Sign_{SK_{PID_i^k}}(Data\_1).$$

- *Step 3: Generating data blocks.* Each DAG in the same vehicular edge cluster periodically gathers uploaded $Record$s from local vehicles. A DAG j generates a new data block with a timestamp and broadcasts them to other DAGs on vehicular blockchain for audit and verification. During a period of time, the DAG with the most contribution of storage resource in a vehicular edge cluster, that is recorded by the local controller in the vehicular edge cluster, can work as the leader of block generation in this round. This leader collects all received $Record$s and generates a Merkle hash value of the $Record$s linked to the prior block in the vehicular blockchain [18]. After that, the new block is broadcasted to all DAGs, and then added into the vehicular blockchain.

2) Metadata and sharing record storage in the vehicular blockchain: Both metadata of raw data (as information index) and sharing records are stored in RSUs, and are shared among vehicles using proof-of-work for data audit. More details of metadata and sharing record storage are shown as follows.

- *Step 1: Generating information index.* Before v_i uploading its $Record$, the vehicle generates a data information index about the $Record$ as follows,

$timestamp$	$Record$ ID
Description	Data owner
Reputation opinions	Storage address
Information indexes and sharing records	

- *Step 2: Building information blocks and finding proof-of-work.* v_i sends its data information index to a nearby DAG (e.g., DAG_j). DAG_j collects all local information (e.g., indexes) during a certain period, and then encrypts and digitally signs these indexes to guarantee authenticity and accuracy. Fig. 1 shows that the index records are structured into blocks. For traceability and verification, each block contains a cryptographic hash to the prior blocks in the vehicular blockchain. Similar to that in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

Bitcoin, the DAGs try to find their own valid proof-of-work about data audit (i.e., a hash value meeting a certain level of difficulty). Each DAG calculates the hash value of its block based on a random nonce value φ, the previous block hash value, timestamp, and data blocks' merkel root and so on (denoted as $previous_{data}$) [21]. Namely, $Hash(\varphi + previous_{data}) < Difficulty$. Here, $Difficulty$ can be adjusted by the system to control the speed of finding out the specific φ. After finding a valid proof-of-work (i.e., φ), the fastest miner (DAG) broadcasts the block and the specific φ to other DAGs in the vehicular blockchain. Other DAGs audit and verify the records in the block and φ. If other DAGs agree on the block, data information in this block will be added to the vehicular blockchain by a linear, chronological order, and the fastest miner (DAG) is awarded by vehicle coins.

- *Step 3: Carrying out a consensus process.* The consensus process is carried out by authorized DAGs and a leader acted by the fastest DAG with a valid proof-of-work. Fig. 3 shows that the leader broadcasts block data $Block\_data$ with timestamp and its proof-of-work to other authorized DAGs for verification and audit. For mutual supervision and verification, these DAGs audit the block data and broadcast their audit results with their signatures to each other. After receiving the audit results, each DAG compares its result with others and sends a reply ($Reply$) back to the leader. This reply consists of the DAG's audit result my_result, comparison result $Comparison$, signatures, and records of received audit results $Rece\_results$. The leader analyzes the received replies from DAGs. If all the DAGs agree on the block data, the leader will send records including current audited block data and a corresponding signature to all authorized DAGs for storage. After that, this block is stored in the vehicular blockchain, and the leader is awarded by vehicle coins. More details about the consensus process are given in **Protocol 1**. If some DAGs don't agree on the block data, the leader will analyze the audit results, and send the block data to these DAGs once again for audit if necessary [13].

Protocol 1: Distributed Consensus Protocol for DAGs

1. The leader broadcasts block data to all DAGs in the vehicular blockchain for verification and audit.

$DAG_j \rightarrow All$: $\mathrm{Record} = (Block\_data||Block\_hash ||Cert_{BS_j}||Sig_{DAG_j}||timestamp,$

where $Block\_hash = Hash(Block\_Data||timestamp)$,
$Sig_{DAG_j} = Sign_{SK_{DAG_j}}(Block\_data||Block\_hash)$.

2. The DAGs broadcast their own audit results to each other for mutual supervision and verification, and then send their replies back to the leader.

$DAG_l \rightarrow DAG_j$: $\mathrm{Reply} = E_{PK_{DAG_j}}(Data\_2 ||Cert_{DAG_l}||Sig_{DAG_l}||timestamp),$

where $Data\_2 = (my\_result||Rece\_results||Comparison)$,
$Sig_{DAG_l} = Sign_{SK_{DAG_l}}(Data\_2)$.

3. The leader adds new block data into vehicular blockchain after verifying by DAGs, and broadcasts the block data to all DAGs for storage.

$DAG_j \rightarrow All$: $Data\_block = (Data\_3||Sig_{DAG_j}||timestamp),$

where $Data\_3 = (Block\_data||Block\_hash||\{Cert_{DAG}\}||timestamp),$
$Sig_{DAG_j} = Sign_{SK_{DAG_j}}(Data\_3).$

C. Secure and Efficient Data Sharing Scheme using ISSC

The P2P data sharing process among vehicles using ISSC consists of the following steps.

1) Step 1: Uploading data sharing requests. Data requestors first download the latest data blocks in the vehicular blockchain from DAGs, and search their data of interest by information indexes. The data requestors choose their optimal data providers according to reputation of providers. More details about the reputation calculation are given in Section IV. For example, a data requestor v_m sends a data sharing request (Req) to a data provider v_i. This request includes time, the usage of requested data, and sharing times, etc.

$$v_m \rightarrow v_i : \mathrm{Req} = E_{PK_{v_i}}(\mathrm{Request}||Cert_{v_m}||timestamp).$$

2) Step 2: Data sharing authorization. After receiving the request Req, v_i verifies the identity of v_m, and defines the data access constraints based on the request from v_m. After that, v_i sends the access constraints, pseudonyms' private keys of uploaded data, public key of the data requestor and so on to a nearby RSU, e.g., RSU_j.

$$v_i \rightarrow RSU_j : Message = E_{PK_{RSU_j}}(Constraints||SK_{PID_i^k} ||PK_{v_m}||timestamp||Cert_{v_i}).$$

The ISSC is triggered by $Message$ from v_i. RSUs first verify the certificate of v_i, and check the shared data information of v_i in the vehicular blockchain. The RSUs obtain and integrate the shared data stored in the vehicular blockchain according to the given pseudonyms' private keys of shared data. The shared data is encrypted with the public key of data requestor v_m. If v_i and v_m are at the same coverage of a local DAG, the shared data will be sent to v_m directly. Otherwise, the shared data will be sent to a DAG nearby v_m.

$$RSU_j \rightarrow RSU_{j+1} : Shared\_data = E_{PK_{RSU_{j+1}}}(Data\_2 ||timestamp||Cert_{RSU_j}),$$
$$Data\_2 = E_{PK_{v_m}}(Data||Cert_{v_i}||Cert_{RSU_j}||timestamp).$$

3) Step 3: Recording and generating data sharing events in the vehicular blockchain. After obtaining the shared data, the data requestor pays for the the provider using vehicle coins, and generates a record of the data sharing event, and adds this record as a data block into vehicular blockchain similar to the steps in Section III-B. Moreover, similar to [14], each vehicle has a wallet account to store and manage personal vehicle coins. During a payment process, for privacy protection, we use random pseudonyms as public keys of a vehicle's wallet account, named wallet addresses, to replace the true address of the wallet account for privacy protection. The mapping relationships between the wallet account and the corresponding wallet addresses are recorded in the trusted authority.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

IV. Subjective Logic for Reputation Management in VECONs

In VECONs, vehicles may provide irrelevant data (information) to each other although the vehicles have similar "genomes" [4]. The vehicles may share false information because of faulty sensors, infection from computer viruses, or even selfish purpose [8], [15]. If a positive sharing interaction occurs between two vehicles, namely, v_m believes that the data shared by v_i is relevant and useful, the relationship from v_m to v_i is strengthened and the reputation of v_i is enhanced. Besides, previous researches have also indicated that the higher reputation of nodes brings higher data quality in mobile crowd sensing [16]. Vehicles choose the best data provider according to reputation values [8]. It is essential to design a mechanism to quantify vehicles' reputation based on their interactions [4]. We therefore propose to make use of a reputation based sharing scheme with three-weight subjective logic model for high-quality data sharing in this section.

Subjective logic is utilized to formulate the individual evaluation of reputation based on occurring interactions, which is a framework for probabilistic information fusion operated on subjective beliefs about the world. The subjective logic utilizes the term opinion to denote the representation of a subjective belief, and models positive statements, negative statements and uncertainty. It also offers a wide range of logical operators to combine and relate different opinions [6].

A. Local Opinions for Subjective Logic

Considering two vehicles v_i and v_j, the trustworthiness (i.e., local opinion) of the data requestor v_j to the data provider v_i in subjective logic can be formally described as a local opinion vector $\omega_{i\to j}$, i.e., $\omega_{i\to j} := \{b_{i\to j}, d_{i\to j}, u_{i\to j}\}$, where $b_{i\to j}, d_{i\to j}, u_{i\to j}$ represent the belief, distrust, and uncertainty, respectively. $b_{i\to j}, d_{i\to j}, u_{i\to j} \in [0,1]$ and $b_{i\to j} + d_{i\to j} + u_{i\to j} = 1$. Here,

$$\begin{cases} b_{i\to j} = (1-u_{i\to j})\frac{\alpha}{\alpha+\beta}, \\ d_{i\to j} = (1-u_{i\to j})\frac{\beta}{\alpha+\beta}, \\ u_{i\to j} = 1 - s_{i\to j}, \end{cases} \tag{1}$$

where α is the number of positive events, while β is the number of negative events. The uncertainty of local opinion vector $u_{i\to j}$ depends on the quality of communication between vehicles i and j. The quality of communication $s_{i\to j}$ refers to the probability that data packets of data sharing requests are transmitted successfully during communication. According to $\omega_{i\to j}$, the reputation value $T_{i\to j}$ represents the expected belief of v_i that v_j provides true and relevant data, which can be expressed as

$$T_{i\to j} = b_{i\to j} + \gamma u_{i\to j}. \tag{2}$$

Here, γ is a given constant given by vehicles, which indicates the uncertainty effect level on reputation for vehicles. This constant can be set as 0.5 by default [6].

B. Three-weight Local Opinions for Subjective Logic

Traditional subjective logic is evolved toward multi-weight subjective logic when considering weighting operations. In VECONs, we consider different weights to formulate local opinions. Compared with traditional subjective logic models, the advantages of the three-weight subjective logic model can obtain more accurate and reliable reputation when taking the following weights into consideration.

- *Interaction Frequency*: It is known that the higher interaction frequency means that the data requestor (v_i) has more prior knowledge about the data provider (v_j) leading to more accurate and reliable reputation calculation. The interaction frequency is the ratio of interaction times between the data requestor and the data provider to average interaction number of the data requestor with other data providers during a time window T, namely, $IF_{i\to j} = \frac{N_{i\to j}}{\overline{N_i}}$, where $N_{i\to j} = (\alpha_i + \beta_i)$, and $\overline{N_i} = \frac{1}{|M|}\sum_{m\in M} N_{i\to m}$. M is the total number of vehicle m that interacts with vehicle i (i.e., the data requestor) during a time window. The higher interaction frequency brings higher reputation.
- *Event Timeliness*: In VECONs, a vehicle is not always trustable and reliable. Both the trustfulness between the data provider and requestor, i.e., the reputation of v_i to v_j are changing over time. The recent events have a larger impact on the local opinion of v_i to v_j, while the past events have less impact on this local opinion for more accurate and reliable reputation calculation. The time scale of recent events and past events is t_{recent}, e.g., a week. Moreover, the negative events have higher weight on the local opinions of vehicles than that of the positive events. Here, the weight of positive events is θ, and the weight of negative events is τ. $\theta+\tau = 1, \theta < \tau$. ζ represents the weight of recent events, σ is the weight of past events. $\zeta + \sigma = 1, \zeta > \sigma$. The weights of event-timeliness and negative/positive events are combined together to form a new interaction frequency as follows.

$$\begin{cases} \alpha_i = \zeta\theta\alpha_1^i + \sigma\theta\alpha_2^i, \\ \beta_i = \zeta\tau\beta_1^i + \sigma\tau\beta_2^i, \end{cases} \tag{3}$$

where the numbers of recent positive events and negative events are α_1^i and β_1^i when the current time t satisfies $t \le t_{recent}$, respectively. When $t > t_{recent}$, the numbers of positive and negative past events are α_2^i and β_2^i, respectively. Therefore, the interaction frequency between the data requestor and the data provider is updated as,

$$IF_{i\to j} = \frac{N_{i\to j}}{\overline{N_i}} = \frac{\theta(\zeta\alpha_1^i + \sigma\alpha_2^i) + \tau(\zeta\beta_1^i + \sigma\beta_2^i)}{\frac{1}{|M|}\sum_{m\in M} N_{i\to m}}. \tag{4}$$

- *Trajectory Similarity*: Data collected by vehicles is locally relevant for vehicles, and has spatial scope. To enable location awareness and improve data relevance, trajectory similarity is taken into consideration on reputation calculation during data sharing among vehicles. The higher trajectory similarity means the sharing data from the data provider is more relevant leading to high-quality, more accurate and reliable data sharing [20]. The trajectory coefficients of vehicles are represented by $\upsilon = \{speed, location, direction\}$. The weights of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

corresponding coefficients in υ are ψ_1, ψ_2, ψ_3, and $\psi_1 + \psi_2 + \psi_3 = 1$. The similarity degree of two trajectory segments (denoted as L_i and L_j) for vehicle i and vehicle j is $SIM(L_i, L_j)$, which is calculated as

$$SIM\left(L_i, L_j\right) = 1 - DISS(L_i, L_j). \tag{5}$$

Here $DISS(L_i, L_j)$ is the normalized dissimilarity of two trajectory segments L_i and L_j, and is defined as,

$$\begin{aligned} DISS(L_i, L_j) = \psi_1 speed(L_i, L_j) + \psi_2 location(L_i, L_j) \\ + \psi_3 direction(L_i, L_j). \end{aligned} \tag{6}$$

We consider that $DISS(L_i, L_j)$ depends on differences of speed, location, and direction for two trajectory segments. The speed difference of two trajectory segments can be expressed as,

$$speed(L_i, L_j) = \frac{|V_{ave}(L_i) - V_{ave}(L_j)|}{\max[V(L_i), V(L_j)]}, \tag{7}$$

where $V(L_i)$ and $V(L_j)$ are the speeds of vehicles i and j during their trajectory segments, respectively. $V_{ave}(L_i)$ and $V_{ave}(L_j)$ are the average speeds of these two vehicles.

We use $location(L_i, L_j)$ to describe the location difference of trajectory segments. The numbers of sample points of L_i and L_j are respectively denoted as e and k during a time window T. The sets of sample points in chronological order are $\{P_{i1}, P_{i2}, \ldots, P_{ie}\}$ and $\{P_{j1}, P_{j2}, \ldots, P_{jk}\}$. We measure the similarity of the trajectory segments by the longest common subsequence (LCS) that has been widely used in time series trajectory clustering. The LCS is utilized to match two sequences by allowing them to stretch without rearranging the sequence of the elements [22]. For trajectory segments L_i and L_j, the LCS is described as $lcs\left(L_i, L_j\right) = \{P_{ie} = P_{jk} | e = k\}$, here, $e \in \{1, 2, \ldots, E\}, k \in \{1, 2, \ldots, K\}$. Hence, the location difference of trajectory segments $location(L_i, L_j)$ is given by

$$location(L_i, L_j) = \frac{\max(e, k) - num[lcs(L_i, L_j)]}{\max(e, k)}, \tag{8}$$

where $num[lcs(L_i, L_j)]$ is the number of points in LCS for trajectory segments L_i and L_j.

The directory difference of two trajectory segments is the angle between two trajectory segments. Here, we use φ as the angle of two trajectories L_i and L_j. More specifically,

$$direction(L_i, L_j) = \begin{cases} \frac{\sin\varphi}{2}, 0 < \varphi \leq \frac{\pi}{2}, \\ \frac{1}{2} + \frac{|\sin(\varphi + \frac{\pi}{2})|}{2}, \frac{\pi}{2} < \varphi \leq \pi. \end{cases} \tag{9}$$

Therefore, the overall weight of reputation for local opinions is

$$\delta_{i \to j} = \rho_1 IF_{i \to j} + \rho_2 SIM\left(L_i, L_j\right), \tag{10}$$

where ρ_1 + ρ_2=1, and $0 < \rho_1 \leq 1$, $0 < \rho_2 \leq 1$.

C. Combining Recommended Opinions

After calculating the weights, the opinions are combined into a common opinion in the form $\omega_{x \to j}^{rec} := \{b_{x \to j}^{rec}, d_{x \to j}^{rec}, u_{x \to j}^{rec}\}$, where

$$\begin{cases} b_{x \to j}^{rec} = \frac{1}{\sum\limits_{x \in X} \delta_{x \to j}} \sum\limits_{x \in X} \delta_{x \to j} b_{x \to j}, \\ d_{x \to j}^{rec} = \frac{1}{\sum\limits_{x \in X} \delta_{x \to j}} \sum\limits_{x \in X} \delta_{x \to j} d_{x \to j}, \\ u_{x \to j}^{rec} = \frac{1}{\sum\limits_{x \in X} \delta_{x \to j}} \sum\limits_{x \in X} \delta_{x \to j} u_{x \to j}, \end{cases} \tag{11}$$

where $x \in X$ is a set of recommended vehicles that have interacted with v_j. Thus, the subjective opinions from different recommenders (neighboring vehicles) are integrated into one single opinion, which is named as the recommended opinion according to each opinion's weights [23].

D. Combining Local Opinions with Recommended Opinions

After obtaining shared data from data providers, a data requestor has a subjective opinion (i.e., local opinion) for each data provider based on interaction histories. This local opinion should still be considered while forming the final opinion to avoid cheating [23]. The final opinion of v_i to v_j is formed as $\omega_{x \to j}^{final} := \{b_{x \to j}^{final}, d_{x \to j}^{final}, u_{x \to j}^{final}\}$, where $b_{i \to j}^{final}$, $d_{i \to j}^{final}$ and $u_{i \to j}^{final}$ are respectively calculated as:

$$\begin{cases} b_{i \to j}^{final} = \frac{b_{i \to j} u_{x \to j}^{rec} + b_{x \to j}^{rec} u_{i \to j}}{u_{i \to j} + u_{x \to j}^{rec} - u_{x \to j}^{rec} u_{i \to j}}, \\ d_{i \to j}^{final} = \frac{d_{i \to j} u_{x \to j}^{rec} + d_{x \to j}^{rec} u_{i \to j}}{u_{i \to j} + u_{x \to j}^{rec} - u_{x \to j}^{rec} u_{i \to j}}, \\ u_{i \to j}^{final} = \frac{u_{x \to j} u_{i \to j}}{u_{i \to j} + u_{x \to j}^{rec} - u_{x \to j}^{rec} u_{i \to j}}. \end{cases} \tag{12}$$

Similar to Eqn. (2), the final reputation of v_i to v_j is

$$T_{i \to j}^{final} = b_{i \to j}^{final} + \gamma u_{i \to j}^{final}. \tag{13}$$

E. Choosing the Optimal Data Provider for Data Sharing

For a data requestor, it chooses an optimal data provider by comparing the final reputation values of data provider candidates. There exists a candidate with the highest reputation value for each data requestor during a period of time. The optimal data provider can be found by

$$v_j^* = \arg\max_{j \in M} (T_{i \to j}^{final}). \tag{14}$$

As shown in Fig. 4, the operations of finding the optimal data provider consist of the following steps.

- *Step 1*: A data requestor v_i first downloads the latest data blocks on the vehicular blockchain. v_i searches data provider candidates through information indexes of shared data. Next, v_i finds candidates' local opinions given by other vehicles (denoted as v_x) that had interacted with the candidates. The local opinion of v_x for a certain candidate (e.g., v_j) includes local opinion vector and the corresponding overall weight of reputation for its local opinion, i.e., $\omega_{x \to j} := \{b_{x \to j}, d_{x \to j}, u_{x \to j}\}$ and $\delta_{x \to j}$.
- *Step 2*: v_i combines these local opinions from v_x to calculate a common recommended opinion $\omega_{x \to j}^{rec} := \{b_{x \to j}^{rec}, d_{x \to j}^{rec}, u_{x \to j}^{rec}\}$. For v_i, it generates its local opinion for v_j according to its interaction history and received

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

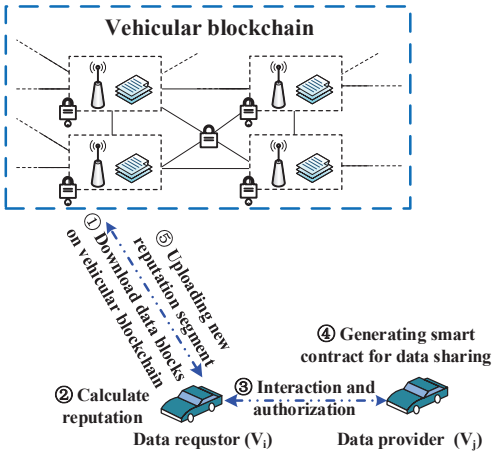

Fig. 4: The operations of finding the optimal data provider.

safety messages during driving. For driving safety, vehicles are required to periodically broadcast safety messages (consisting of current positions, speeds, directions and so on) to neighboring vehicles. These safety messages increase the awareness of vehicles about their neighbors' whereabouts and warn drivers of dangerous situations [24]. The local opinions of vehicles can be calculated based on the received safety messages during a period of time. Thus, v_i obtains the final reputation values for candidates using Eqn. (13) in a time window.

- *Step 3*: v_i compares the final reputation values of candidates and uses Eqn. (14) to find out the optimal data provider. v_i interacts with the data provider to request authorization of data sharing.
- *Step 4*: After verification, the data provider generates a smart contract for v_i. More details about secure data sharing using ISSC are given in Section III.
- *Step 5*: v_i uploads its local opinion as a new reputation opinion for its optimal data provider (e.g., v_j). Similar to the data sharing events in Section III-C, this updated local opinion will be formed as a data block of vehicular blockchain.

V. Security Analysis and Numerical Results

A. Security Analysis for Vehicular Blockchain

Unlike traditional communication security and privacy protection, our vehicular blockchain uses consortium blockchain and smart contract technologies to ensure security and privacy protection during data storage and sharing. Consortium blockchain ensures data traceability, and the automatic execution of smart contracts protects data security sharing. For data providers, the decentralized characteristic of vehicular blockchain's architecture defends against data security risks brought by centralized data storage [9]. The transparency characteristic of vehicular blockchain during data sharing avoids second-hand sharing without authentication from data providers. The anonymous operations using pseudonyms during data storage and sharing bring privacy protection for data providers and data requestors. We provide more details about the blockchain-related security performances as follows [25].

TABLE II: Parameter Setting in the Simulation

Parameter	Setting
Interaction frequency among vehicles	[50, 200] one week
Communication range between two vehicles	[300m, 500m]
Angle between two trajectory segments	$(0, \pi]$
Speed of vehicles	[50 km/h, 150 km/h]
Weight of positive events θ and negative events τ	0.6, 0.4
Weight of recent events ζ and past events σ	0.6, 0.4
Time scale of recent and past events t_{recent}	7 days
Weights of trajectory similarity ψ_1, ψ_2, ψ_3	0.3,0.4,0.3
Predefined parameters of reputation	$\rho_1 = 0.5$, $\rho_2 = 0.5$
Rate of abnormal vehicles	[10%, 90%]
Quality of communication $s_{i \to j}$	[0, 0.4]

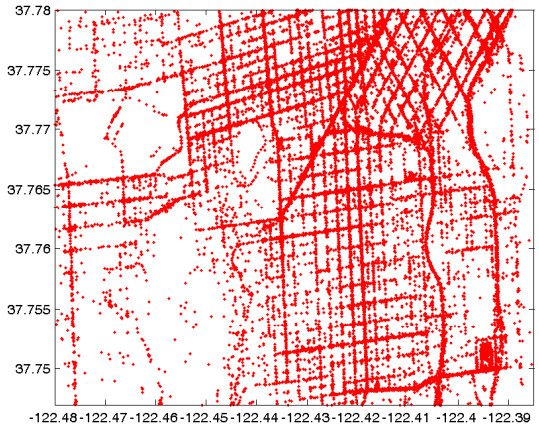

Fig. 5: Spatial distribution of vehicles' trajectories.

- Get rid of a trusted intermediary: With the help of the robust and scalable consortium blockchain, vehicles can share data with others in a P2P manner without involvement of a globally trusted intermediary [14].
- Sharing record authentication: All sharing records are publicly audited and authenticated by other entities. It is impossible to compromise all entities due to overwhelming cost. So the sharing records with errors can still be discovered and corrected before structuring into a block.
- Data unforgeability: No adversary can act as vehicles to corrupt the vehicular blockchain. It is because that the adversary cannot forge a digital signature of any vehicle, or gain control over the majority of the network's resources [25]. An adversary only controlling a few of RSUs in the vehicular blockchain cannot learn anything about the raw data, as it is encrypted with keys of vehicles.
- Secure self-execution: Data storage smart contract and information sharing smart contract, that are run on vehicular blockchain, are autonomous, self-executed and self-maintained in the form of computer codes. These smart contracts do not need mutual trust, and are completely automatic. So no human factor is needed, and no human factor can control these smart contracts once it goes into effect [9].

B. Numerical Results

We evaluate the performance of the proposed Three-Weight Subjective Logic (TWSL) scheme based on a real dataset

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2875542, IEEE Internet of Things Journal

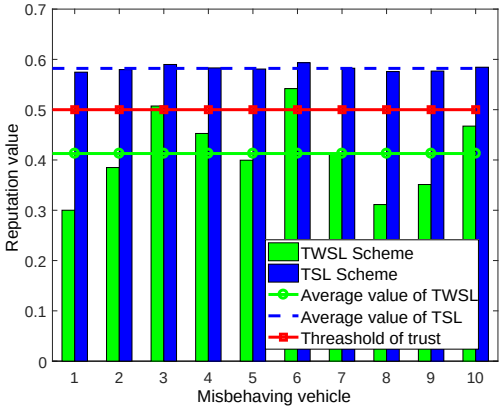

Fig. 6: The reputation comparison of 10 abnormal vehicles during 120 minutes.

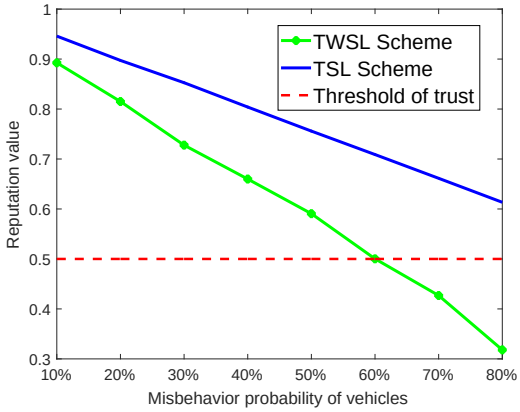

Fig. 8: Reputation changes of an abnormal vehicle under different misbehavior probability.

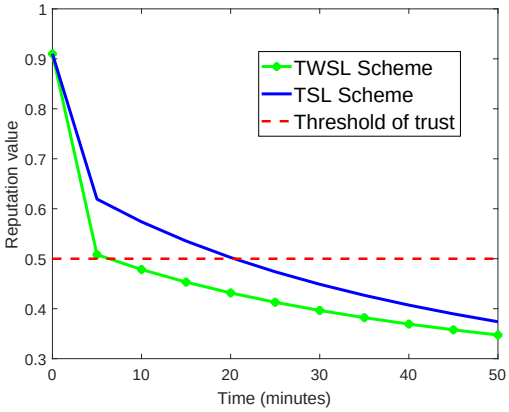

Fig. 7: Reputation changes of an abnormal vehicle over time.

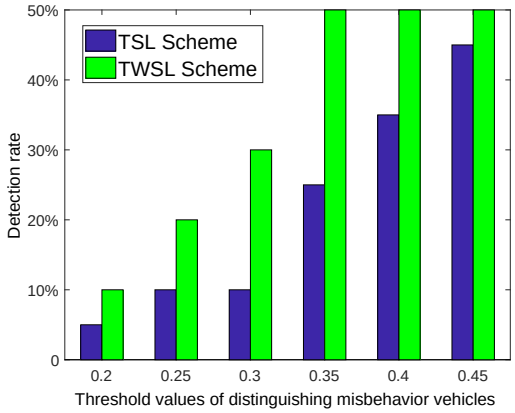

Fig. 9: Detection rates under different trust thresholds.

from San Francisco Yellow Cabs [26]. This dataset includes mobility traces of 536 urban taxis over a period of one month [27]. We take 100 taxis as examples and choose an observation area, whose latitude is from 37.747 to 37.78, and the longitude is from -122.48 to -122.385, as shown in Fig. 5. The observed area is approximately $8.34 \times 3.67\ km^2$. The average time gap between two trace records is 43.34 seconds, i.e., data collection period of vehicles [27]. We set the update period of reputation is 15 minutes, and the observation time of our simulation is 240 minutes. In an urban area, the vehicles often take familiar routes in a specified time period, such as similar trajectories from home to work in the day time [20]. So the vehicles would like to share data for obtaining rewards and promoting vehicular services. More parameters about our simulation are listed in Table I.

A vehicle sends data requests to data providers with a high reputation. The quality of communication $s_{i\to j}$ affects the uncertainty of local opinion vector $u_{i\to j}$. Vehicles calculate reputation based on their local opinions and recommended opinions from other vehicles. Our proposed TWSL scheme is used to calculate the reputation of vehicles according to the interaction events between vehicles. We compare TWSL scheme with a widely accepted Traditional Subjective Logic (TSL) model using a linear function to calculate reputation [28]. The linear function is represented as: $\Gamma_{i\to j} = \omega\Gamma^{ave}_{x\to j} + (1-\omega)\Gamma^{las}_{i\to j}$, where $\Gamma^{ave}_{x\to j} = b^{ave}_{x\to j} + 0.5 * u^{ave}_{x\to j}$ and $\Gamma^{las}_{i\to j} = b^{las}_{i\to j} + 0.5 * u^{las}_{i\to j}$. $b^{ave}_{x\to j}$ and $u^{ave}_{x\to j}$ are two average values of $b_{x\to j}$ and $u_{x\to j}$ from recommended opinions of other vehicles, respectively. $b^{las}_{i\to j}$ and $u^{las}_{i\to j}$ are the latest parameters in local opinion of vehicle i for vehicle j. ω is the weight and can be set as 0.5 [6], [28].

We set that all the abnormal vehicles initially pretend to behave normally within a short period of time (20 minutes), that provide high-quality data with high value of ϖ, e.g., $\varpi = 0.8$. Here, ϖ is the probability that an abnormal vehicle behaves normally in order to hide its malicious intent. Their initialized reputation values are represented by $w_0 = [0.64, 0.16, 0.2]$. After the camouflage time, they do some misbehaviors and ϖ becomes 0.2. To detect the misbehavior, the system updates the reputation values in every time period.

As shown in Fig. 6, we randomly choose 10 abnormal vehicles for reputation update during the observation time. The abnormal vehicles randomly interact with normal vehicles [1, 4] times during 60 minutes. All the reputation values of the abnormal vehicles are lower than the initial reputation value w_0. The reputation values calculated by TWSL scheme are lower than that of TSL scheme. It is because that all the reputation opinions are combined and weighted adequately by considering prior knowledge (interaction frequency, event timeliness, and trajectory similarity). In this way, we pay more

attention to reputation opinions with better quality and avoid being misleading from reputation opinions with lower quality. As a result, highly accurate reputation computation is achieved using TWSL scheme, thus ensuring high-quality data sharing among vehicles.

Fig. 7 shows the reputation changes of an abnormal vehicle over time. Here, the misbehavior probability of this abnormal vehicle is 70%. The abnormal vehicle first pretends to provide high-quality data to other vehicles for winning trust from a target vehicle. The initial reputation value for the target vehicle is $w_0 = [0.9, 0.05, 0.05]$. Meanwhile, the abnormal vehicle randomly interacts with other normal vehicles. Due to the misbehavior events, the reputation value of the abnormal vehicle is decreased continuously over time, as illustrated in Fig. 7. The reputation updated by TWSL scheme is much more accurate, leading to lower reputation value for the abnormal vehicle. After 10 minutes, the reputation value is descended to 0.5, which is below than that of TSL scheme. This means that the abnormal vehicle has a higher probability for being detected when the threshold of trust is 0.5 in the TWSL scheme.

For an abnormal vehicle, its reputation value is affected by different misbehavior probabilities. Fig. 8 shows the misbehavior probability impacts on reputation values. With the higher misbehavior probability, the average reputation value of the abnormal vehicles using our TWSL scheme is lower than that of TSL scheme because of the considered weights. For example, when the misbehavior probability is 60%, our TWSL scheme is 38% lower than that of TSL scheme. So our TWSL scheme is sensitive for the misbehavior, although malicious vehicles try to camouflage themselves. It is beneficial to detect and eliminate the misbehaviors timely in VECONs.

We study detection rate of abnormal vehicles using TWSL scheme and TSL scheme within 60 minutes. Fig. 9 shows the proposed TWSL scheme can distinguish much more abnormal vehicles compared to TSL scheme. Note that, with higher threshold value of trust, more abnormal vehicles will be distinguished. When the threshold value of trust is 0.35, the recognition rate of abnormal vehicles in TWSL scheme has already been more than 100%, while that of TSL scheme is only 50%. Due to higher detection rate in the proposed TWSL scheme, potential security threats can be removed more effectively, which brings a secure VECONs.

VI. Conclusion

In this paper, we have presented a secure P2P data sharing system in vehicular computing and networks. We utilized consortium blockchain and smart contract technologies to achieve secure and efficient data storage and data sharing. These technologies efficiently prevent second-hand data sharing without authorization. In addition, we have proposed a reputation based data sharing scheme with the three-weight subjective logic model considering interaction frequency, event timeliness, and trajectory similarity. This scheme can achieve accurate reputation management for high-quality data sharing among vehicles. The vehicles can choose the optimal data providers with high-quality data during sharing in VECONs. Security analysis shows that our system ensures security of data storage and data sharing. Numerical results indicate that the proposed three-weight subjective logic scheme has great advantages over the traditional reputation schemes in improving detection rate of abnormal vehicles to ensure security during data sharing.

References

[1] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[2] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146–152, 2017.

[3] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: A content-centric framework," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60–66, 2017.

[4] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.

[5] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring mobile edge computing for 5g-enabled software defined vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 55–63, 2017.

[6] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[7] D. Huang, S. Misra, M. Verma, and G. Xue, "Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[8] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, in press, 2018.

[9] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *Big Data Computing and Communications (BIGCOM), 2017 3rd International Conference on*, pp. 117–121, IEEE, 2017.

[10] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[11] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," in *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2663–2668, Nov 2016.

[12] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in *IEEE 4th World Forum on Internet of Things*, pp. 62–67, Feb 2018.

[13] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, pp. 3154–3164, Dec 2017.

[14] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3690–3700, Aug 2018.

[15] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42–47, 2015.

[16] S. Delgado-Segura, C. Tanas, and J. Herrera-Joancomartł, "Reputation and reward: Two sides of the same bitcoin.," *Sensors*, vol. 16, no. 6, pp. 1–23, 2016.

[17] Y. Zhang and J. Wen, "The iot electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, pp. 1–12, 2016.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[19] J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, and Y. Zhang, "Location privacy attacks and defenses in cloud-enabled internet of vehicles," *IEEE Wireless Communications*, vol. 23, pp. 52–59, October 2016.

[20] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "Mixgroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, 2016.

[21] I. Alqassem and D. Svetinovic, "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in *Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE*, pp. 436–443, IEEE, 2014.
[22] L. Zheng, Q. Feng, W. Liu, and X. Zhao, "Discovering trip hot routes using large scale taxi trajectory data," in *International Conference on Advanced Data Mining and Applications*, pp. 534–546, Springer, 2016.
[23] Y. Liu, K. Li, Y. Jin, Y. Zhang, and W. Qu, "A novel reputation computation model based on subjective logic for mobile ad hoc networks," *Future Generation Computer Systems*, vol. 27, no. 5, pp. 547–554, 2011.
[24] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, pp. 2627–2637, Aug 2018.
[25] G. Zyskind, O. Nathan, *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshops (SPW)*, pp. 180–184, IEEE, 2015.
[26] C Projects. (2013).[Online] Available: http://www.yellowcabsf.com/.
[27] M. A. Hoque, X. Hong, and B. Dixon, "Analysis of mobility patterns for urban taxi cabs," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, pp. 756–760, IEEE, 2012.
[28] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, pp. 1987–1997, IEEE, 2003.

Jiawen Kang received the M.S. degree from the Guangdong University of Technology, China, in 2015, and the Ph.D. degree at the same school in 2018. His research interests mainly focus on blockchain, security and privacy protection in wireless communications and networking.

Rong Yu (M'08) received his Ph.D. degree from Tsinghua University, China, in 2007. After that, he worked in the School of Electronic and Information Engineering of South China University of Technology. In 2010, he joined the Institute of Intelligent Information Processing at Guangdong University of Technology, where he is now a full professor. His research interests include wireless networking and mobile computing in featured environments such as Edge Cloud, Connected Vehicles, Smart Grid, and Internet of Things. He is the co-inventor of over 30 patents and author or co-author of over 100 international journal and conference papers. He was the member of home networking standard committee in China, where he led the standardization work of three standards.

Xumin Huang is now a Ph.D. student of networked control systems in Guangdong University of Technology, China. His research interests mainly focus on network performance analysis, simulation and enhancement in wireless communications and networking.

Maoqiang Wu is now a Ph.D. student of networked control systems in Guangdong University of Technology, China. His research interests mainly focus on blockchain, resource management in wireless communications and networking.

Sabita Maharjan (S'09-M'13) received her Ph.D. degree in networks and distributed systems from the University of Oslo, and Simula Research Laboratory, Norway, in 2013. She is currently a senior research scientist at Simula Metropolitan Center for Digital Engineering, Norway, and an associate professor (adjunct position) at the University of Oslo, Norway. Her current research interests include wireless networks, network security and resilience, smart grid communications, cyber-physical systems, machine-to-machine communications, and software defined wireless networking.

Shengli Xie (M'01-SM'02) received the M.S. degree in mathematics from Central China Normal University, Wuhan, China, in 1992, and the Ph.D. degree in control theory and applications from the South China University of Technology, Guangzhou, China, in 1997. He is currently the Director of Laboratory for Intelligent Information Processing and a Full Professor with the Faculty of Automation, Guangdong University of Technology, Guangzhou, China. He has authored two monographs and over 100 scientific papers in journals and conference proceedings. He holds a dozen of patents. His current research interests include automatic control and signal processing, and focus on blind signal processing.

Yan Zhang (SM'10) received the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is currently a Full Professor with the Department of Informatics, University of Oslo, Norway. His current research interests include next-generation wireless networks leading to 5G, green and secure cyber-physical systems, such as smart grid, healthcare, and transport. He is an IEEE Vehicular Technology Society (VTS) Distinguished Lecturer. He is also a Senior Member of the IEEE ComSoc, the IEEE CS, the IEEE PES, and the IEEE VTS. He is a fellow of the IET. He is an Associate Technical Editor of the IEEE Communications Magazine, an Editor of IEEE Network Magazine, an Editor of the IEEE Transactions on Green Communications and Networking, an Editor of the IEEE Communications Surveys and Tutorials, an Editor of IEEE Internet of Things Journal, and an Associate Editor of the IEEE Access. He serves as the Chair in a number of conferences, including the IEEE GLOBECOM 2017, the IEEE PIMRC 2016, the IEEE CloudCom 2016, the IEEE ICCC 2016, the IEEE CCNC 2016, the WCSP 2016, the IEEE SmartGridComm 2015, and the IEEE CloudCom 2015. He serves as a TPC member for numerous international conferences, including the IEEE INFOCOM, the IEEE ICC, the IEEE GLOBECOM, and the IEEE WCNC.