This document is downloaded from DR-NTU (https://dr.ntu.edu.sg)
Nanyang Technological University, Singapore.

Toward secure blockchain-enabled Internet of Vehicles : optimizing consensus management using reputation and contract theory

Kang, Jiawen; Xiong, Zehui; Niyato, Dusit; Ye, Dongdong; Kim, Dong In; Zhao, Jun

2019

Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Toward secure blockchain-enabled Internet of Vehicles : optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3), 2906-2920. doi:10.1109/TVT.2019.2894944

https://hdl.handle.net/10356/143616

https://doi.org/10.1109/TVT.2019.2894944

© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, in any current or future media, including reprinting/republishing this material for adverstising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:https://doi.org/10.1109/TVT.2019.2894944

Downloaded on 04 Feb 2023 14:23:24 SGT

Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory

Jiawen Kang, Zehui Xiong, Dusit Niyato, *Fellow, IEEE*, Dongdong Ye, Dong In Kim, *Senior Member, IEEE*, Jun Zhao, *Member, IEEE*

arXiv:1809.08387v1 [cs.CR] 22 Sep 2018

***Abstract*—In the Internet of Vehicles (IoV), data sharing among vehicles is critical to improve driving safety and enhance vehicular services. To ensure security and traceability of data sharing, existing studies utilize consensus schemes as hard security solutions to establish blockchain-enabled IoV (BIoV). However, as miners are selected from miner candidates by stake-based voting, defending against voting collusion between the candidates and compromised high-stake vehicles becomes challenging. To address the challenge, in this paper, we propose a two-stage soft security enhancement solution: (i) miner selection and (ii) block verification. In the first stage, we design a reputation-based voting scheme to ensure secure miner selection. This scheme evaluates candidates' reputation using both historical interactions and recommended opinions from other vehicles. The candidates with high reputation are selected to be active miners and standby miners. In the second stage, to prevent internal collusion among active miners, a newly generated block is further verified and audited by standby miners. To incentivize the participation of the standby miners in block verification, we adopt the contract theory to model the interactions between active miners and standby miners, where block verification security and delay are taken into consideration. Numerical results based on a real-world dataset confirm the security and efficiency of our schemes for data sharing in BIoV.**

***Index Terms*—Internet of Vehicles, blockchain, reputation management, delegated proof-of-stake, contract theory, security**

I. Introduction

A. Background and Motivations

With the rapid development of automobile industry and the Internet of Things, vehicles generate a huge amount and diverse types of data through advanced on-board devices. Vehicles collect and share data to improve driving safety and achieve better service quality [1]. However, there exist significant security and privacy challenges for data sharing in IoV. On the one hand, vehicles may not be willing to upload data to infrastructures, e.g., through road-side units, with a centralized management architecture because of the concern on a single point of failure and personal data manipulation. On the other hand, although Peer-to-Peer (P2P) data sharing among the vehicles can solve the issues of the centralized management architecture, it is facing with the problems of data access without authorization and security protection in a decentralized architecture. These challenges adversely affect the circulation of vehicle data, even forming data 'island', and thus hinder the future development of IoV [2].

Recently, integrating blockchain technology with IoV has attracted increasing attention of researchers and developers because of decentralization, anonymity, and trust characteristics of blockchain. A secure, trusted, and decentralized intelligent transport ecosystem is established by blockchain to solve vehicle data sharing problems [2], [3]. The authors in [1] proposed a decentralized trust management system for vehicle data credibility assessment using blockchain with joint Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus schemes. Vehicle manufacturers Volkswagen [4] and Ford [5] have applied for patents that enable secure inter-vehicle communication through blockchain technologies. An intelligent vehicle-trust point mechanism using proof-of-driving-based blockchain is presented to support secure communications and data sharing among vehicles [6], [7]. Li *et al.* [8] proposed a privacy-preserving incentive announcement network based on public blockchain. The Byzantine fault tolerance algorithm is adopted to incentivize vehicles to share traffic information. Nevertheless, there exists exorbitant cost to establish a blockchain in resource-limited vehicles using computation-intensive PoW or unfair stake-based PoS [9]. Existing research attempts cannot neatly address the P2P data sharing problem among vehicles in IoV.

In this paper, we utilize high-efficiency Delegated Proof-of-Stake (DPoS) consensus scheme as a hard security solution to develop a secure P2P data sharing system for IoV. Previous study has demonstrated that a DPoS scheme is particularly suitable and practical for IoV [10], which performs the consensus process on pre-selected miners with moderate cost [11]. RoadSide Units (RSUs) as edge computing infrastructures, which are widely deployed over the whole road networks and easily reachable by vehicles, can be the miners because of having sufficient computation and storage resources [1], [12], [13]. These miners play significant roles to publicly audit and store vehicle data and data sharing records in blockchain-enabled IoV (BIoV). Traditionally, miners in DPoS schemes are selected by stake-based voting. Note that the vehicles with stakes act as stakeholders in BIoV [14]. The stakeholders with more stake have higher voting power. However, this approach

Jiawen Kang, Zehui Xiong, Dusit Niyato, and Jun Zhao are with School of Computer Science and Engineering, Nanyang Technological University, Singapore. (emails: kavinkang@ntu.edu.sg, zxiong002@e.ntu.edu.sg, dniyato@ntu.edu.sg, junzhao@ntu.edu.sg).

Dongdong Ye is with School of Automation, Guangdong University of Technology, China. (email: dongdongye8@163.com).

Dong In Kim is with School of Information & Communication Engineering, Sungkyunkwan University, Korea. (email: dikim@skku.ac.kr).

suffers from the following collusion attacks in BIoV:

- **Miner Voting Collusion:** Malicious RSUs collude with compromised high-stake stakeholders to be voted as miners. These malicious miners may falsely modify or discard transaction data during its mining process. Although the malicious miners can be voted out of the BIoV by the majority of well-behaved stakeholders in the next voting round, the stakeholders may not participate in all the voting rounds. Thus, some malicious miners cannot be removed in a timely fashion, which enables the malicious miners to launch attacks to damage the system continuously [15], [16].
- **Block Verification Collusion:** Malicious miners may internally collude with other miners to generate false results in the block verification stage, even to launch double-spending attack, which is also challenging [9], [17].

Therefore, it is necessary to design an enhanced DPoS consensus scheme with secure miner selection and block verification to defend against the collusion attacks in BIoV [9].

B. Solutions and Contributions

Reputation is defined as the rating of an entity's trustworthiness by others based on its past behaviors [1], [18], [15]. Similar to existing studies, we utilize reputation as a fair metric to propose a soft security solution for enhancing DPoS schemes through two stages: (i) secure miner selection, and (ii) reliable block verification. A reputation management scheme established on blockchain technologies is proposed for the miner selection. Miner candidates with high reputation are selected to form a miner group including active miners and standby miners, e.g., 21 active miners and 150 standby miners in Enterprise Operation System (EOS) [19]. Each vehicle has its reputation opinion on an interacting miner candidate through a subjective logic model that combines recommended opinions from other vehicles and its own opinions based on historical interactions into an accurate reputation opinion [20]. All the reputation opinions of vehicles on the candidates are recorded as reliable and tamper-proof reputation records in transparent blockchain for reputation calculation.

Moreover, for secure block verification, blocks generated by active miners can be further verified and audited by standby miners to prevent internal collusion among active miners [21]. Here, the active miners take turn to act as the block manager to generate and distribute unverified blocks. To incentivize the standby miners to participate in the block verification, we utilize contract theory to model interactions among the block manager and miners to prevent collusion attacks. The block manager works as a contract designer. Meanwhile, the miners including active miners and standby miners are followers to finish block verification for obtaining a part of transaction fee according to verification contribution [21].

The main contributions of this paper are summarized as follows.

- We propose an enhanced DPoS consensus scheme with two-stage soft security solution for secure vehicle data sharing in BIoV.

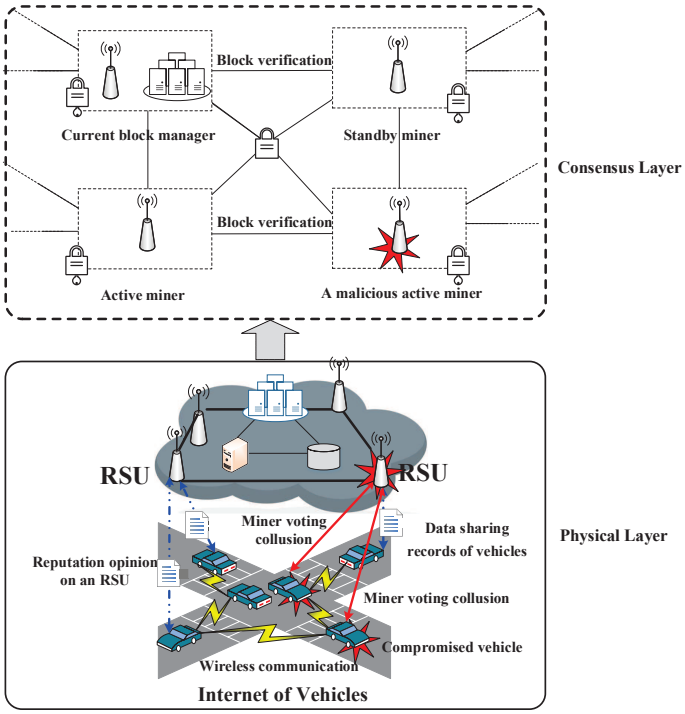

Fig. 1: The system model for blockchain-based IoV.

- In the miner selection stage, we introduce a secure and efficient reputation management scheme by using a multi-weight subjective logic model. Miner are selected by reputation-based voting for decreasing collusion between stakeholders with a lot of stake and miner candidates.
- In the block verification stage, high-reputation standby miners are incentivized to participate in block verification using contract theory for preventing internal collusion among active miners.

The rest of this paper is organized as follows. We present the system model and the enhanced DPoS consensus scheme with detailed steps for secure P2P vehicle data sharing in Section II. We illustrate the secure reputation management scheme by using the multi-weight subjective logic model in Section III. The incentive mechanism for secure block verification using contract theory is proposed in Section IV, followed by optimal contract designing in Section V. We illustrate numerical results in Section VI. Section VII concludes the paper.

II. System Model and the Enhanced DPoS Algorithm

A. System Model

As shown in Fig. 1, vehicles equipped with on-board units and advanced communication devices can access vehicular services by communicating with nearby RSUs in BIoV. The on-board units can perform simple computation, collect local data from sensing devices, and upload the data to the RSUs. Vehicles act as data collectors and share their own data with data requesters through wireless communication. Next, the vehicles upload their data sharing records as "transactions" to nearby RSUs. RSUs are deployed along roads to ensure that

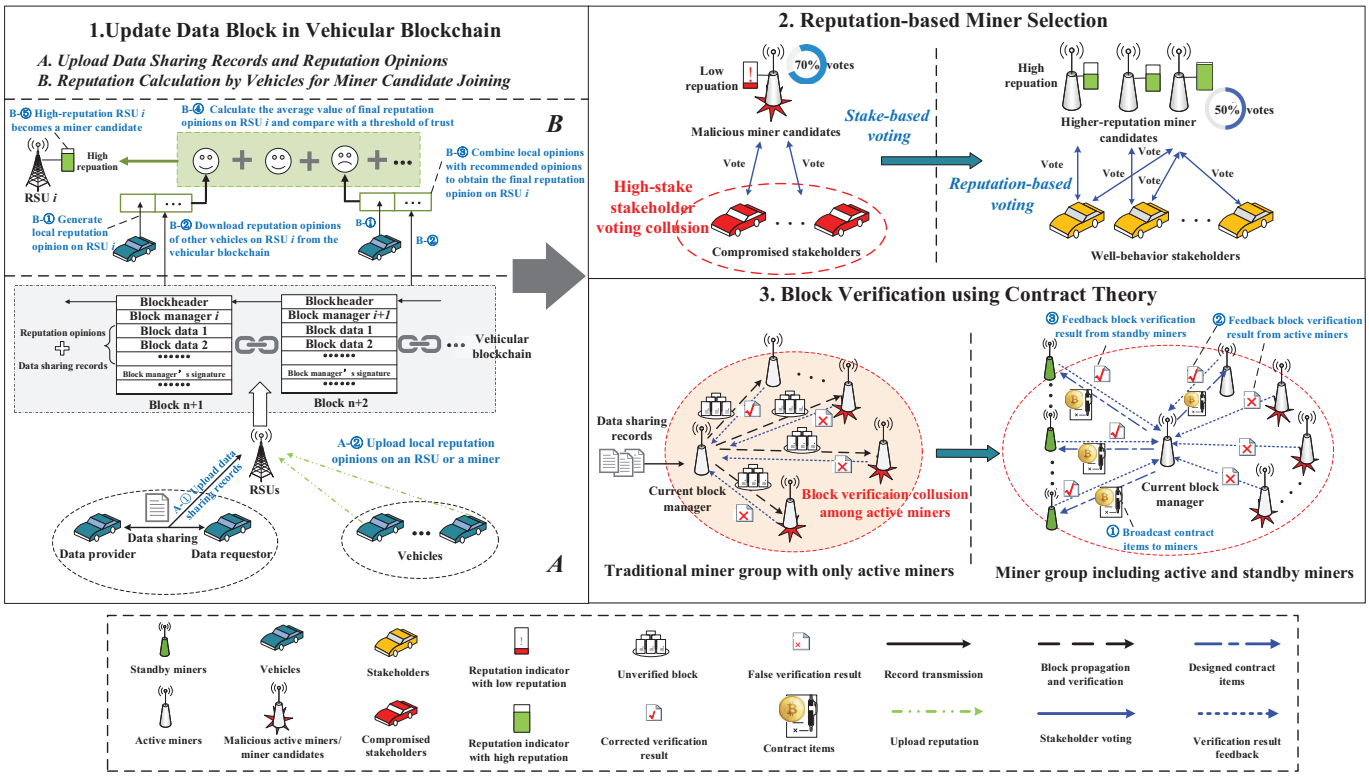

Fig. 2: The enhanced DPoS consensus scheme for blockchain-based IoV.

the vehicles are able to communicate with other vehicles and miners in a timely fashion [1], [12], [13]. Unlike traditional DPoS schemes that miners are selected by stake-based voting, RSUs with high reputation are selected as miners, whose reputation values are calculated by a multi-weight subjective logic model. More details about the model are given in Section III. The data collectors share data with each other and obtain a reward from data requesters. Next, the data collectors upload data sharing records to active miners, and the miners execute the consensus process of our enhanced DPoS consensus scheme. Finally, the vehicle's data sharing records are stored as block data and added into a blockchain, named *vehicular blockchain*, for achieving efficient proof of presence of the data sharing.

The vehicular blockchain is also a public ledger that records vehicles' reputation opinions for RSUs and miners into the block data. These reputation opinions are persistent and transparent evidence when disputes and destruction occur [22]. Vehicles assess both RSUs during vehicular services and active miners in the consensus process. The vehicles also download the existing reputation opinions about these entities in vehicular blockchain as recommended opinions. Then, vehicles generate their reputation opinions through combining their own assessments with the recommended opinions, and upload these new opinions with digital signatures to new active miners through nearby RSUs [1]. The miners perform the consensus process similar to that in data sharing. All the vehicles can obtain the latest RSUs' reputation after the reputation opinions being added into the vehicular blockchain. The system can calculate the average reputation of RSUs according to the reputation opinions in the vehicular blockchain, which is an important metric for the miner selection in the next round of the consensus process [22].

B. Adversary Model for DPoS Consensus Process

In traditional DPoS consensus schemes, miners are selected from miner candidates according to stake-based voting among stakeholders, i.e., vehicles with stake. In BIoV, as RSUs acting as miner candidates may be distributed along the road without sufficient security protection, they are semi-trusted and may be vulnerable to be directly compromised by attackers [1], [23]. Both stakeholders and miner candidates are vulnerable to arbitrary manipulation by plutocrats [16], and become compromised stakeholders and malicious miner candidates. The plutocrats, i.e., attackers, can launch voting collusion that compromises some high-stake stakeholders with greater voting power, and ask the compromised stakeholders to vote some certain miner candidates. Moreover, compromised vehicles in BIoV can generate and upload fake reputation opinions to an RSU in order to increase or decrease the reputation of the target RSU [1]. Due to the overwhelming cost, we consider that the attackers cannot compromise the majority of vehicles [22]. Only a small subset of vehicles can be compromised during a short period of time in BIoV [1], i.e., due to high mobility of vehicles.

C. The Enhanced DPoS Scheme for Blockchain-based IoV

As depicted in Fig. 2, there are mainly three parts in the enhanced DPoS consensus scheme for secure P2P vehicle

data sharing: (i) updating block data (data sharing records and reputation opinions from vehicles) and miner candidates joining, (ii) reputation-based voting for miner selection and (iii) secure block verification using contract theory. More details about steps of the proposed parts are given in the subsequent discussions.

Step 1: *System Initialization:* In vehicular blockchain, elliptic curve digital signature algorithm and asymmetric cryptography are adopted for system initialization. Every entity becomes legitimate after passing identity authentication by a global Trust Authority (TA), e.g., a government department of transportation[1]. Each legitimate entity obtains its public & private keys and the corresponding certificates for information encryption and decryption [11]. An RSU that wants to be a miner candidate first submits its identity-related information to the TA. As shown in Fig. 2, the TA verifies the validity of the RSU by calculating its average reputation according to stored reputation opinions from vehicles in the vehicular blockchain. Only if the average reputation of this RSU is higher than a threshold of trust, the RSU can become a miner candidate. The threshold can be set according to different security-level requirements [18], which is explained in Section VI-B.

Step 2: *Miner candidate joining:* Each miner candidate submits a deposit of stake to an account under public supervision after being a miner candidate. This deposit will be confiscated by the vehicular blockchain system if the candidate behaves maliciously and causes damage during the consensus process, e.g., failing to produce a block in its time slot [19], [24].

Step 3: *Reputation calculation:* As shown in Fig. 2, stakeholders can calculate all miner candidates' reputation by using a subjective logic model, which is based on historical interactions with the miner candidates and recommended opinions from other vehicles. The subjective logic model takes three weights about the historical interactions into consideration to form the local opinion on each miner candidate. The latest recommended opinions can be downloaded from the vehicular blockchain. Thus each stakeholder combines its local opinion with the recommended opinions to obtain a final reputation opinion on every miner candidate. More details about the reputation calculation are presented in Section III.

Step 4: *Miner selection:* According to the final reputation opinions calculated by Step 3, as shown in Fig. 2, each stakeholder votes for y candidates as the miners according to its ranking of the final reputation opinions for the candidates. Unlike traditional DPoS schemes, all the stakeholders have the same weight in miner voting (same voting power) even though some stakeholders owning larger stake. The top k miner candidates with the highest reputation are selected to be active miners and $(y-k)$ miner candidates can be standby miners. The active miners and standby miners form a miner group in vehicular blockchain. Here $y < k$, and k is an odd integer, such as 21 in EoS and 101 in Bitshares [19].

Step 5: *Block manager generation:* In line with traditional DPoS schemes, each of the k active miners takes turn to act as the block manager during k time slots of the consensus process. Similar to that in traditional DPoS consensus schemes, every active miner plays the role of the block manager to perform block generation, broadcasting, verification and management in its time slot.

Step 6: *Consensus process:* As shown in Fig. 2, in a time slot, the block manager first generates an unverified block, and broadcasts this block to other active miners for block verification. However, due to the limited number of active miners, malicious active miners may launch the block verification collusion attack to generate false block verification results. In the block verification stage, the more verifiers result in a more secure blockchain network [21]. Therefore, to defend this attack and further enhance security performance of the proposed DPoS consensus scheme, more verifiers are motivated and incentivized to participate in the block verification instead of only active miners finishing the verification. In other words, the miners including active miners and standby miners can act as verifiers and join the block verification process, especially the high-reputation miners, which can prevent the block verification collusion among the active miners. As such, we then design an incentive mechanism by using contract theory to encourage high-reputation miners to participate in the block verification. In the incentive mechanism, the active miner acts as the block manager and the contract designer to broadcast contract items to miners. Meanwhile, the miners choose and sign their best contract items. More details about the block verification using contract theory are described in Section IV.

In Fig. 2, for mutual supervision and verification, high-reputation miners locally audit the data block and broadcast their audit results with their signatures to each other. After receiving the audit results, each miner compares its result with those of other miners and sends a reply as a feedback to the block manager. This reply consists of the miner's audit result, comparison result, signatures, and records of received audit results. The block manager analyzes the received replies from miners. If more than two third of the miners agree on the data block, the block manager will send the records including the current audited data block and the corresponding signature to all of the miners for storage. Next, this block is stored in the vehicular blockchain. The block manager is rewarded with cryptocurrency, and the other miners participating in block verification will receive a part of the transaction fee. After k time slots, the group of miners and their categories, i.e., active or standby miners, will be updated and shuffled through new miner selection.

Step 7: *Reputation updating:* After each round of the consensus process, vehicles download and check new data block related to their data sharing records or reputation opinions in the vehicular blockchain. If the data is correct, the vehicles will update their reputation opinions for these miners and upload their opinions to new miners of the next round of consensus process. The miners perform consensus process in Step 6 to add valid reputation values into the vehicular blockchain.

Note that traditional DPoS consensus schemes mainly include the following steps: miner selection, block mining and generation, and block verification. The proposed DPoS

[1]Note that the TA is responsible for identity authorization, certificate issuance and access control of entities before running vehicular blockchain. That is, the TA does not affect the decentralization of the vehicular blockchain [22].

consensus scheme only enhances the miner selection step and block verification step for secure BIoV, while the block mining and generation steps are the same as those in traditional DPoS schemes. Therefore the enhanced steps are compatible with traditional DPoS schemes.

III. Efficient Reputation Calcualtion Using Subjective Logic Model

If a positive interaction between vehicles and RSUs/miners occurs, the vehicles will generate a positive rating for the RSUs/miners. Consequently, the vehicle's local reputation opinion on the RSUs/miners is increased. The positive interaction means that the vehicles believe that the services provided by RSUs is relevant and useful or the new data block generated by a miner is true. Note that the miner candidates with high reputation acting as miners can ensure a secure and reliable consensus process. On the contrary, some compromised vehicles may generate fake rating because of collusion with malicious RSUs or selfish purpose. More false ratings cause more negative effects on miner selection in the proposed DPoS scheme, thus resulting in unreliable and insecure BIoV. Therefore, it is necessary to design a secure and efficient reputation management scheme of RSUs, and also to defend against the collusion between RSUs and vehicles. Vehicles choose their own best miner candidates as the miners according to reputation calculation [25]. A multi-weight subjective logic model for reputation calculation is proposed in this section.

Subjective logic is utilized to formulate individual evaluation of reputation based on historical interactions and recommended opinions. It 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, negative statements and uncertainty. It also offers a wide range of logical operators to combine and relate different opinions [18]. In this paper, each vehicle (stakeholder) calculates reputation opinion taking all the recommended opinions into consideration. Due to the limited number of compromised vehicles, the false recommended opinions from the compromised vehicles have less effect on reputation calculation using subjective logic model since most vehicles are well-behaved and reliable.

A. Local Opinions for Subjective Logic

Considering a vehicle V_i and an RSU R_j, the vehicle may interact with the RSU during driving, e.g., crowdsensing or vehicle data sharing. The trustworthiness (i.e., local opinion) of V_i to R_j in the subjective logic can be formally described as a local opinion vector $\omega_{i\to j} := \{b_{i\to j}, d_{i\to j}, u_{i\to j}\}$, where $b_{i\to j}, d_{i\to j}$, and $u_{i\to j}$ represent the belief, distrust, and uncertainty, respectively. We consider that all of the vehicles have the same evaluation criteria to generate local opinions. Here, $b_{i\to j}, d_{i\to j}, u_{i\to j} \in [0,1]$ and $b_{i\to j} + d_{i\to j} + u_{i\to j} = 1$. According to the subjective logic model [20], [18], we have

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

α is the number of positive interactions and β is the number of negative interactions. The communication quality $s_{i\to j}$ of a link between vehicles i and j, i.e., the successful transmission probability of data packets, determines the uncertainty of local opinion vector $u_{i\to j}$ [18]. According to $\omega_{i\to j}$, the reputation value $T_{i\to j}$ represents the expected belief of vehicle V_i that RSU R_j is trusted and behaves normally during consensus process, which is denoted by

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

Here, $0 \le \gamma \le 1$ is the given constant indicating an effect level of the uncertainty for reputation [20].

B. Multi-weight Local Opinions for Subjective Logic

Local opinions using the subjective logic model are affected by different factors. Traditional subjective logic is evolved toward multi-weight subjective logic when considering weighting operations. Similar to [18], we consider the following weights to formulate local opinions.

- *Interaction Frequency*: It is known that the higher interaction frequency means that vehicle V_i has more prior knowledge about RSU R_j. The interaction frequency between V_i and R_j is the ratio of the number of times that V_i interacts with R_j to the average number of times that V_i interacts with other RSUs during a time window T, i.e.,
$$\mathrm{IF_{i\to j}} = \frac{N_{i\to j}}{\overline{N_i}}, \tag{3}$$
where $N_{i\to j} = (\alpha_i + \beta_i)$, and $\overline{N_i} = \frac{1}{|S|}\sum_{s\in S} N_{i\to s}$. S is the set of all of the RSUs (denoted as RSU_s) interacting with V_i during the time window. The higher interaction frequency leads to higher reputation.
- *Interaction Timeliness*: In BIoV, a vehicle is not always trusted and reliable. Both the trustfulness and reputation of V_i to R_j are changing over time. The recent interactions have higher impact on the local opinion of V_i to R_j. The time scale of recent interactions and past interactions is defined by t_{recent}, e.g., three days. The recent interactions and past interactions have different weights on the local opinions of vehicles. The parameter ζ represents the weight of recent interactions, and σ represents the weight of past interactions. $\zeta + \sigma = 1, \zeta > \sigma$.
- *Interaction Effects*: Note that positive interactions increase RSUs' reputation and negative interactions decrease the reputation of RSUs. Therefore, the negative interactions have a higher weight on the local opinions of vehicles than that of the positive interactions. Here, the weight of positive interactions is θ, and the weight of negative interactions is τ, where $\theta + \tau = 1, \theta < \tau$. The weights of interaction timeliness and interaction

effects are combined together to form a new interaction frequency as follows:

$$\begin{cases} \alpha_i = \zeta\theta\alpha_1^i + \sigma\theta\alpha_2^i, \\ \beta_i = \zeta\tau\beta_1^i + \sigma\tau\beta_2^i. \end{cases} \tag{4}$$

The positive and negative recent interactions are α_1^i and β_1^i when the current time t satisfies $t \leq t_{recent}$, respectively. When $t > t_{recent}$, the positive and negative past interactions are α_2^i and β_2^i, respectively. Therefore, the interaction frequency between two vehicles is updated as follows:

$$\mathrm{IF_{i\to j}} = \frac{N_{i\to j}}{\overline{N_i}} = \frac{\theta(\zeta\alpha_1^i + \sigma\alpha_2^i) + \tau(\zeta\beta_1^i + \sigma\beta_2^i)}{\frac{1}{|S|}\sum\limits_{s\in S} N_{i\to s}}. \tag{5}$$

Therefore, the overall weight of reputation for local opinions is $\delta_{i\to j} = \rho_i * \mathrm{IF_{i\to j}}$, where $0 \leq \rho_i \leq 1$ is predefined parameter.

C. Recommended Opinions for Subjective Logic

After being weighted, the recommended opinions are combined into a common opinion in the form of $\omega_{x\to j}^{rec} := \{b_{x\to j}^{rec}, d_{x\to j}^{rec}, u_{x\to j}^{rec}\}$. Here,

$$\begin{cases} b_{x\to j}^{rec} = \frac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X} \delta_{x\to j} b_{x\to j}, \\ d_{x\to j}^{rec} = \frac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X} \delta_{x\to j} d_{x\to j}, \\ u_{x\to j}^{rec} = \frac{1}{\sum\limits_{x\in X}\delta_{x\to j}} \sum\limits_{x\in X} \delta_{x\to j} u_{x\to j}, \end{cases} \tag{6}$$

where $x \in X$ is a set of recommenders that are other vehicles had interacted with R_j. Thus, the subjective opinions from different recommenders are combined into one single opinion, which is called the recommended opinion according to each opinion's weight [15].

D. Combining Local Opinions with Recommended Opinions

After obtaining ratings of R_j from other vehicles, a particular vehicle has a subjective opinion (i.e., local opinion) on each vehicle based on its interaction history. This local opinion should still be considered while forming the final reputation opinion to avoid cheating [15]. The final reputation opinion of V_i to R_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 follows [18]:

$$\begin{cases} b_{i\to j}^{final} = \frac{b_{i\to j} u_{x\to j}^{rec} + b_{x\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec} u_{i\to j}}, \\ d_{i\to j}^{final} = \frac{d_{i\to j} u_{x\to j}^{rec} + d_{x\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec} u_{i\to j}}, \\ u_{i\to j}^{final} = \frac{u_{x\to j}^{rec} u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec} u_{i\to j}}. \end{cases} \tag{7}$$

Similar to Eqn. (2), the final reputation opinion of V_i to R_j is

$$T_{i\to j}^{final} = b_{i\to j}^{final} + \gamma u_{i\to j}^{final}. \tag{8}$$

The final reputation opinions can be used in different steps of the proposed DPoS scheme. For Step 2 and Step 7 in Section II-C, after obtaining the final reputation opinion on an RSU, vehicles will upload and store their final reputation opinions as recommended opinions for other vehicles (stakeholders) in the vehicular blockchain. For Step 3 and Step 4 in Section II-C, stakeholders vote high-reputation miner candidates according to the reputation opinions.

IV. Incentive Mechanism for Secure Block Verification Using Contract Theory

After selecting high-reputation miner candidates as active miners by using the multi-weight subjective logic model, there still exists a potential block verification collusion attack in the vehicular blockchain. In this section, for secure block verification, we aim to design an incentive mechanism to motivate more miners (both active miners and standby miners) to participate in the block verification. Every block manager will offer a part of the transaction fee as a reward to verifiers that participate in block verification and accomplish the tasks in time. Nevertheless, to do so, there are issues for the block manager in every consensus process. Firstly, the block manager does not have prior knowledge about which miners would like to participate in verification. Secondly, it does not have an accurate reputation value of a verifier. Thirdly, it does not know the amount of resource that each verifier would contribute. The information asymmetry between the block manager and verifiers may incur too much cost for the block manager to give an incentive to the verifiers. Thus, the best strategy for the block manager is to design an incentive mechanism that can reduce the impact of information asymmetry. Moreover, the verifiers that contribute more should be rewarded more. Thus, we adopt contract theory [26] in designing the incentive mechanism.

In the kth block verification, consider a monopoly market consisting of a block manager acting as the task publisher and a set of verifiers $\mathbb{M} = \{M_1, \ldots, M_m\}$ including active miners and standby miners. Verifiers are willing to contribute different computation resources $C = \{c_1^k, \ldots, c_m^k\}$, i.e., CPU cycles per unit time to execute the block verification. I_k and O_k are the sizes of the transmitted block before verification and the verified results, respectively [26]. For simplicity, for all verifiers, the values of I_k and O_k respectively are the same in the kth block verification. For a verifier m, the occupied CPU resource of block verification task is $\mathrm{Task_m^k}$. Here, we consider that $\mathrm{Task_1^k} = \mathrm{Task_2^k} = \cdots = \mathrm{Task_m^k}$. Therefore, the block verification task is denoted as a three tuple $(\mathrm{Task_m^k}, \mathrm{I_k}, \mathrm{O_k})$. To attract more high-reputation verifiers, we define reputation as the type of a verifier. There are Q types, and the verifiers are sorted in an ascending order of reputation: $\theta_1 < \cdots < \theta_q < \cdots < \theta_Q$, $q \in \{1, \ldots, Q\}$. The larger θ_q implies a higher reputation verifier for secure block verification among miners [9], [21].

With information asymmetry, the block manager should design specific contracts to overcome its economic loss. For different types of verifiers with different reputations, the block manager offers the verifiers a contract $(R_q(L_q^{-1}), L_q^{-1})$, which includes a series of latency-reward bundles. Here, L_q is the latency of block verification for type-q verifiers and L_q^{-1} is the reciprocal of L_q. $R_q(L_q^{-1})$ is the corresponding incentive.

Note that if verifiers finish block verification faster, i.e., with smaller latency, can be rewarded more incentive [26].

A. Latency in Block Verification

As mentioned in Step 6 of Section II-C, there are four steps in the block verification process for a verifier: (i) unverified block transmission from the block manager to verifiers, (ii) local block verification, (iii) verification result broadcasting and comparison among verifiers, and (iv) verification feedback transmission from the verifiers to the manager. For a verifier m, the latency consisting of the corresponding delays of the aforementioned steps is defined as follows [26],

$$L_q(c_m^k, I_k, O_k) = \frac{I_k}{r_m^d} + \frac{\mathrm{Task_m^k}}{c_m^k} + \psi I_k \left|\mathbb{M}\right| + \frac{O_k}{r_m^u}. \quad (9)$$

r_m^u is the uplink transmission rate from the verifiers to block manager and r_m^d is the downlink transmission rate from the block manager to the verifiers. The transmission time of an unverified block from the block manager to the verifier is $\frac{I_k}{r_m^d}$. The local verification time of this block is $\frac{\mathrm{Task_m^k}}{c_m^k}$. Similar to that in [21], [27], the time of verification result broadcasting and comparison among verifiers is a function of the block size I_k, network scale (i.e., the number of verifiers $|\mathbb{M}|$) and average verification speed of each verifiers, which is denoted as $\psi I_k \left|\mathbb{M}\right|$. Here, ψ is a pre-defined parameter of verification result broadcasting and comparison, which can be obtained from statistics of previous block verification processes. The time of verification feedback is $\frac{O_k}{r_m^u}$.

r_m^u and r_m^d can be calculated based on wireless link speed, e.g., the Shannon capacity. Let locations of verifiers fix during block verification. We apply the Time-Division Medium Access (TDMA) technique, where the uplink and downlink use the same frequency channel [26]. Then, we have

$$r_m^u = r_m^d = B\log_2(1 + \frac{\varpi_m |h_m|^2}{\sum\limits_{m^- \in \mathbb{M}\setminus\{m\}} \varpi_{m^-} |h_{m^-}|^2 + N_0 B}), \quad (10)$$

where B is the transmission bandwidth and ϖ_m is the transmission power of verifier m. h_m is the channel gain of peer-to-peer link between the verifier m and the block manager or other verifiers. N_0 is the one-sided power spectral density level of white Gaussian noise, and m^- is an element in $\mathbb{M}$ excluding m.

B. Profit of the Block Manager

According to the signed contract (R_q, L_q^{-1}) between the block manager and type-q verifier, the profit of the block manager obtained from type-q verifier is denoted as

$$U_{bm}(q) = \pi[\phi_q(L_q)] - lR_q, \quad (11)$$

where l is a pre-defined weight parameter about the type-q verifier's incentive R_q. $\pi[\phi_q(L_q)]$ is the benefit of the block manager regarding a security-latency metric ϕ_q for type-q verifier. Intuitively, the block manager obtains a higher profit when the ϕ_q is bigger. Moreover, both more high-reputation verifiers and less latency can lead to bigger ϕ_q, i.e., $\frac{\partial \pi(\phi_q)}{\phi_q} > 0$, $\frac{\partial \phi_q(L_q)}{\theta_q} > 0$ and $\frac{\partial \phi_q(L_q)}{L_q} < 0$. The more verifiers participating in block verification leads to more secure block verification stage. However, this causes larger latency since the verifiers may need to communicate with verifiers through multi-hop relays [21]. Similar to that in [21], [28], we define a more general security-latency metric to balance the network scale and the block verification time for type-q verifier, which is expressed by

$$\phi_q = \begin{cases} e_1(\theta_q|\mathbb{M}|p_q)^{z_1} - e_2(\frac{L_q}{T_{\max}})^{z_2}, & \text{if } 0 < L_q < A, \\ 0, & \text{otherwise.} \end{cases} \quad (12)$$

Here $A = \frac{T_{\max} e_1 {z_2}^{-1} (\theta_q |\mathbb{M}| p_q)^{\frac{z_1}{z_2}}}{e_2 {z_2}^{-1}}$. $e_1 > 0$ and $e_2 > 0$ are pre-defined coefficients about the network scale and verification latency, respectively. p_q is the prior probability of type-q, and $\sum_{q=1}^{Q} p_q = 1$. We consider that the block manager can obtain the distribution of verifier types from observations and statistics of previous behaviours of the verifiers [26]. T_{max} denotes the maximum tolerable block verification latency to blockchain users. $z_1 \geq 1$ and $z_2 \geq 1$ are given factors indicating the effects of network scale and verification latency on block verification, respectively. The goal of the block manager is to maximize its profit through block verification as follows:

$$\max_{(R_q, L_q^{-1})} U_{bm}(q) = \sum_{q=1}^{Q} (|\mathbb{M}|p_q)(\pi[\phi_q(L_q)] - lR_q). \quad (13)$$

C. Utility of Block Verifiers

For type-q verifier, the utility function of block verification based on a signed contract is defined as

$$U_q = \theta_q \eta(R_q) - l' L_q^{-1}, \quad (14)$$

where $\eta(R_q)$ is a monotonically increasing valuation function of type-q verifier in terms of the incentive R_q. l' is the unit resource cost of block verification. Moreover, the valuation is zero when there is no incentive, i.e., $\eta(0) = 0$. The higher type-q verifier should have larger utility because of higher reputation in block verification. However, the verifier wants to maximize its utility through minimizing resource consumption in block verification. Specifically, the objective of type-q verifier is to maximize utility obtained by joining block verification, expressed by

$$\max_{(\mathrm{R_q}, \mathrm{L_q^{-1}})} U_q = \theta_q \eta(R_q) - l' L_q^{-1}, \forall q \in \{1, \ldots, Q\}. \quad (15)$$

V. Optimal Contract Designing

According to [29], to make contracts feasible, each contract item for verifiers must satisfy the following principles: (i) Individual Rationality (IR) and (ii) Incentive Compatibility (IC). IR means that each verifier will join the block verification when it receives a non-negative utility, i.e.,

$$\theta_q \eta(R_q) - l' L_q^{-1} \geq 0, \forall q \in \{1, \ldots, Q\}. \quad (16)$$

IC refers to that type-q verifier can only receive the maximum utility when choosing the contract designed for itself instead of all other contracts $(R_{q'}, L_{q'}^{-1})$, i.e.,

$$\begin{aligned} &\theta_q \eta(R_q) - l' L_q^{-1} \geq \theta_q \eta(R_{q'}) - l' L_{q'}^{-1}, \\ &\forall q, q' \in \{1, \ldots, Q\}, q \neq q'. \end{aligned} \tag{17}$$

In what follows, we consider $\pi[\phi_q(L_q)] = g_1[e_1(\theta_q|\mathbb{M}|p_q)^{z_1} - e_2(\frac{L_q}{T_{\max}})^{z_2}]$ for ease of presentation, where g_1 is unit profit gain for the block manager. Therefore, the optimization problems in (13) and (15) can be defined as follows:

$$\begin{aligned} &\max_{(\mathrm{R_q}, \mathrm{L_q^{-1}})} U_{bm} = \sum_{q=1}^{Q} |\mathbb{M}| p_q [g_1 e_1 (\theta_q |\mathbb{M}| p_q)^{z_1} - g_1 e_2 (\tfrac{L_q}{T_{\max}})^{z_2} \\ &\qquad - l R_q] \\ &\text{s.t.} \\ &\theta_q \eta(R_q) - l' L_q^{-1} \geq 0, \forall q \in \{1, \ldots, Q\}, \\ &\theta_q \eta(R_q) - l' L_q^{-1} \geq \theta_q \eta(R_{q'}) - l' L_{q'}^{-1}, \forall q, q' \in \{1, \ldots, Q\}, \\ &q \neq q', \\ &\max\{L_q\} \leq T_{\max}, \forall q \in \{1, \ldots, Q\}, \\ &\sum_{q=1}^{Q} |\mathbb{M}| p_q R_q \leq R_{\max}, \forall q \in \{1, \ldots, Q\}, \end{aligned} \tag{18}$$

where R_{max} is a given transaction fee from blockchain users.

This problem is not a convex optimization problem. However, we can find its solution by performing the following transformation.

Lemma 1 (Monotonicity). For contract (R_i, L_i^{-1}) and (R_j, L_j^{-1}), we have $R_i \geq R_j$ and $L_i^{-1} \geq L_j^{-1}$, if and only if $\theta_i \geq \theta_j$, $i \neq j$, and $i, j \in \{1, \ldots, Q\}$.

Proof: According to the IC constraints of type-i verifier and type-j verifier, we have

$$\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_j) - l' L_j^{-1}, \tag{19}$$

$$\theta_j \eta(R_j) - l' L_j^{-1} \geq \theta_j \eta(R_i) - l' L_i^{-1}. \tag{20}$$

By adding together (19) and (20), we can obtain $(\theta_i - \theta_j)[\eta(R_i) - \eta(R_j)] \geq 0$. $\eta(R_q) \geq 0$ is a monotonically increasing valuation function of R_q. When $\theta_i \geq \theta_j$, we can deduce that $\eta(R_i) - \eta(R_j) \geq 0$, i.e., $R_i \geq R_j$. When $R_i \geq R_j$, we have $\eta(R_i) - \eta(R_j) \geq 0$. Thus, we can deduce that $\theta_i \geq \theta_j$ must be satisfied [30].

Proposition 1: $R_i \geq R_j$, if and only if $L_i^{-1} \geq L_j^{-1}$.

Proof: According to the IC constraint in (19), we can obtain

$$\theta_i [\eta(R_i) - \eta(R_j)] \geq l'(L_i^{-1} - L_j^{-1}), \tag{21}$$

$$\theta_j [\eta(R_i) - \eta(R_j)] \leq l'(L_i^{-1} - L_j^{-1}). \tag{22}$$

As $L_i^{-1} \geq L_j^{-1}$, we have $\eta(R_i) \geq \eta(R_j)$ according to (21), and thus $R_i \geq R_j$. In addition, when $R_i \geq R_j$, we can obtain $L_i^{-1} \geq L_j^{-1}$ from (22). **Proposition 1** indicates that an incentive compatibility contract requires a higher payment, if verifiers have less latency in block verification. ■

Lemma 2. If the IR constraint of type-1 verifier is satisfied, the IR constraints of other types will hold.

Proof: According to the IC constraints, $\forall i \in \{2, \ldots, Q\}$, we have

$$\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_1) - l' L_1^{-1}. \tag{23}$$

Given that $\theta_1 < \cdots < \theta_i < \cdots < \theta_Q$, we also have

$$\theta_i \eta(R_1) - l' L_1^{-1} \geq \theta_1 \eta(R_1) - l' L_1^{-1}. \tag{24}$$

According to (23) and (24), we have

$$\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_1 \eta(R_1) - l' L_1^{-1} \geq 0. \tag{25}$$

The (25) indicates that with the IC condition, when the IR constraint of type-1 verifier is satisfied, the other IR constraints will also hold. Therefore, the other IR constraints can be bound into the IR condition of type-1 verifier [30]. ■

Lemma 3. By utilizing the monotonicity in **Lemma 1**, the IC condition can be transformed into the Local Downward Incentive Compatibility (LDIC), which is given as follows:

$$\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_{i-1}) - l' L_{i-1}^{-1}, \forall i \in \{2, \ldots, Q\}. \tag{26}$$

Proof: The IC constraints between type-i and type-j, $j \in \{1, \ldots, i-1\}$ are defined as Downward Incentive Compatibility (DIC), given by $\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_j) - l' L_j^{-1}$.

The IC constraints between type-i and type-j, $j \in \{i+1, \ldots, Q\}$ are defined as Upward Incentive Compatibility (UIC), given by $\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_j) - l' L_j^{-1}$.

We first prove that DIC can be reduced as two adjacent types in DIC, called LDIC. Consider three continuous types of verifiers, i.e., $\theta_{i-1} < \theta_i < \theta_{i+1}$, $i \in \{2, \ldots, Q-1\}$, we have

$$\theta_{i+1} \eta(R_{i+1}) - l' L_{i+1}^{-1} \geq \theta_{i+1} \eta(R_i) - l' L_i^{-1}, \tag{27}$$

$$\theta_i \eta(R_i) - l' L_i^{-1} \geq \theta_i \eta(R_{i-1}) - l' L_{i-1}^{-1}. \tag{28}$$

According to the monotonicity, i.e., if $\theta_i \geq \theta_j$, then $R_i \geq R_j$, $i \neq j$, and $i, j \in \{1, \ldots, Q\}$, we have

$$(\theta_{i+1} - \theta_i)[\eta(R_i) - \eta(R_{i-1})] \geq 0, \tag{29}$$

$$\theta_{i+1}[\eta(R_i) - \eta(R_{i-1})] \geq \theta_i [\eta(R_i) - \eta(R_{i-1})]. \tag{30}$$

Combine (28) and (30), we have $\theta_{i+1}[\eta(R_i) - \eta(R_{i-1})] \geq \theta_i[\eta(R_i) - \eta(R_{i-1})] \geq l' L_i^{-1} - l' L_{i-1}^{-1}$. Thus, we have

$$\theta_{i+1} \eta(R_i) - l' L_i^{-1} \geq \theta_{i+1} \eta(R_{i-1}) - l' L_{i-1}^{-1}. \tag{31}$$

Combine (27) and (31), we have

$$\theta_{i+1} \eta(R_{i+1}) - l' L_{i+1}^{-1} \geq \theta_{i+1} \eta(R_{i-1}) - l' L_{i-1}^{-1}. \tag{32}$$

We can extend (32) to prove that the DIC can be held until type-1:

$$\begin{aligned} &\theta_{i+1} \eta(R_{i+1}) - l' L_{i+1}^{-1} \geq \theta_{i+1} \eta(R_{i-1}) - l' L_{i-1}^{-1} \geq \\ &\cdots \geq \theta_1 \eta(R_1) - l' L_1^{-1}, \forall\ i. \end{aligned} \tag{33}$$

Hence, note that with the LDIC and the monotonicity, the DIC holds. Similarly, with the monotonicity and the Local Upward Incentive Compatibility (LUIC), the UIC can be proved to hold [29], [30].

According to **Lemmas 1**, **2**, and **3**, the optimization problem can be reformulated as follows:

$$\begin{aligned}
&\max_{(\mathrm{R_q},\mathrm{L_q^{-1}})} U_{bm} = \sum_{q=1}^{Q} |\mathbb{M}|p_q[g_1 e_1(\theta_q|\mathbb{M}|p_q)^{z_1} - g_1 e_2(\tfrac{L_q}{T_{\max}})^{z_2} \\
&\qquad - lR_q] \\
&\text{s.t.} \\
&\theta_1\eta(R_1) - l'L_1^{-1} = 0, \\
&\theta_q\eta(R_q) - l'L_q^{-1} = \theta_q\eta(R_{q-1}) - l'L_{q-1}^{-1}, \forall q \in \{2,\ldots,Q\}, \\
&\max\{L_q\} \le T_{\max}, \forall q \in \{1,\ldots,Q\}, \\
&\sum_{q=1}^{Q} |\mathbb{M}|p_q R_q \le R_{\max}, \forall q \in \{1,\ldots,Q\}.
\end{aligned} \tag{34}$$

Furthermore, to simplify the analysis without loss of generality, we define the concave function $\eta(R_q) = R_q$. The optimization problem in (34) is solved sequentially. Firstly, we solve the relaxed problem in (34) without monotonicity to obtain a solution. Secondly, we verify that whether the solution satisfies the condition of the monotonicity. We use the method of iterating the IC and IR constraints to obtain R_q which can be expressed as follows:

$$R_q = \frac{l'L_1^{-1}}{\theta_1} + \sum\nolimits_{k=2}^{q} \Delta_k, \tag{35}$$

where $\Delta_k = \frac{l'L_k^{-1}}{\theta_k} - \frac{l'L_{k-1}^{-1}}{\theta_k}$ and $\Delta_1 = 0$. By substituting R_q into $\sum_{q=1}^{Q} |\mathbb{M}|p_q R_q$, we have

$$\sum_{q=1}^{Q} |\mathbb{M}|p_q l R_q = |\mathbb{M}| \sum_{q=1}^{Q} l f_q L_q^{-1}, \tag{36}$$

where

$$f_q = \begin{cases} \frac{l'p_q}{\theta_q} + \left(\frac{l'}{\theta_q} - \frac{l'}{\theta_{q+1}}\right) \sum_{i=q+1}^{Q} p_i, & if\ q < Q, \\ \frac{l'p_Q}{\theta_Q}, & if\ q = Q. \end{cases} \tag{37}$$

We substitute the expression in (36) into the problem in (34) and remove all $R_q, \forall q \in \{1,\ldots,Q\}$ from the problem in (34). The problem in (34) is rewritten as follows:

$$\begin{aligned}
&\max_{(\mathrm{R_q},\mathrm{L_q^{-1}})} U_{bm} = \sum_{q=1}^{Q} |\mathbb{M}|p_q[g_1 e_1(\theta_q|\mathbb{M}|p_q)^{z_1} - g_1 e_2(\tfrac{1}{L_q^{-1}T_{\max}})^{z_2}] \\
&\qquad - |\mathbb{M}|l \sum_{q=1}^{Q} f_q L_q^{-1}, \\
&\text{s.t.} \quad L_q^{-1} \ge \tfrac{1}{T_{\max}}, \forall q \in \{1,\ldots,Q\}, \\
&\qquad |\mathbb{M}| \sum_{q=1}^{Q} f_q L_q^{-1} \le R_{\max}, \forall q \in \{1,\ldots,Q\}.
\end{aligned} \tag{38}$$

By differentiating U_{bm} with respect to L_q^{-1}, we have $\frac{\partial U_{bm}}{\partial L_q^{-1}} = \frac{|\mathbb{M}|g_1 e_2 z_2 p_q}{T_{\max}^{z_2}}(L_q^{-1})^{-(z_2+1)} - |\mathbb{M}|lf_q$, and $\frac{\partial^2 U_{bm}}{\partial (L_q^{-1})^2} = -\frac{|\mathbb{M}|g_1 e_2 z_2 p_q (z_2+1)}{T_{\max}^{z_2}}(L_q^{-1})^{-(z_2+2)} < 0$. Thus, the function U_{bm} is concave. The problem defined in (38) is a convex optimization problem because the summation of concave functions (U_{bm}) is still a concave function, and the constrains are affine. We can obtain the optimal latency requirement $L_q^{-1^*}$ and the corresponding incentive R_q^* by using convex optimization tools. Moreover, if the types of verifiers follow uniformly distributed, the monotonicity can be automatically met [29], [30]. If not, we can use infeasible sub-sequence replacing algorithm to satisfy the final optimal latency requirement [31].

Note that the proposed incentive mechanism based on contract theory can encourage efficiently high-reputation miners to join the block verification for further improving the security of the vehicular blockchain.

TABLE I: Parameter Setting in the Simulation

Parameter	Setting
Interaction frequency between vehicles and RSUs	[50, 200] times/week
Coverage range of RSUs	[300, 500] m
Speed of vehicles	[50, 150] km/h
Weight parameters	$\theta = 0.4$, $\tau = 0.6$, $\zeta = 0.6$, $\sigma = 0.4$, $\rho = 1$
Time scale of recent and past events t_{recent}	three days
Rate of compromised vehicles	[10%, 90%]
Successful transmission probability of data packets	[0.6, 1]
Vehicle to RSU bandwidth	20 MHz
Noise spectrum density	-174 dBm/Hz
Transmission power	[10, 23] dBm
Receiver power	14 dBm
Computation resource	[10^3, 10^6] CPU cycles/unit time
Input/output block data size	[50, 500] KB
Pre-defined parameters	$g_1 = 1.2$, $e_1 = 15$, $e_2 = 10$, $z_1 = 2$, $z_2 = 1$, $l = 5$, $l' = 1$, $T_{max} = 300$ s, $R_{max} = 1000$, $\psi = 0.5$

VI. Numerical Results

In this section, we first evaluate the performance of the proposed Multi-Weight Subjective Logic (MWSL) scheme based on a real-world dataset of San Francisco Yellow Cab [32]. Next, we evaluate and compare the performance of the proposed incentive mechanism based on contract theory. The mobility traces of 536 taxis driving during a month are recorded in this dataset. We observe 200 taxis running in an urban area, whose latitude and longitude are from 37.7 to 37.81 and from -122.52 to -122.38, respectively. Fig. 3 shows trace points of the 200 taxis during a month. The average time gap between two trace records is 43.34 seconds. There are 400 RSUs (miner candidates) deployed uniformly in the observation area. The update period of RSUs' reputation is 1 minute. These miner candidates are initially classified into 10 types according to their reputation values, wherein the probability for an candidate belonging to a certain type is 0.1. Major parameters used in the simulation are given in Table I, most of which are adopted from [18], [26], [30].

A. Performance of the proposed reputation scheme

In the proposed MWSL scheme, vehicles calculate reputation value of miner candidates according to local opinions and recommended opinions from other vehicles. We compare our MWSL scheme with a Traditional Subjective Logic (TSL) scheme which is a typical model using a linear function to calculate reputation [18]. More specifically,

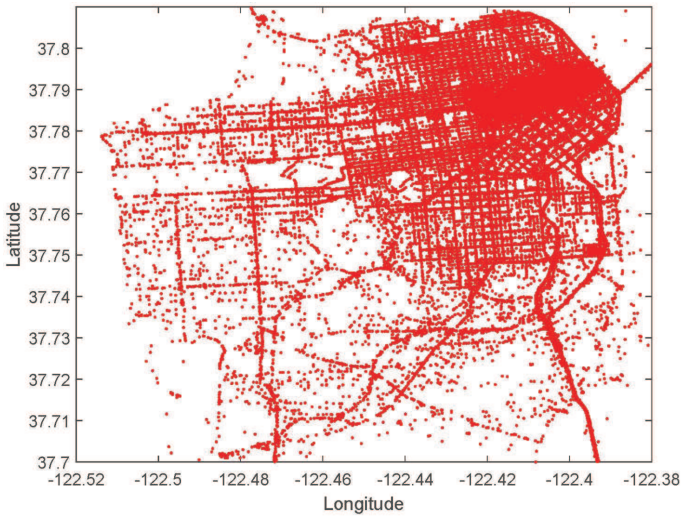

Fig. 3: Spatial distribution of vehicle trace points.

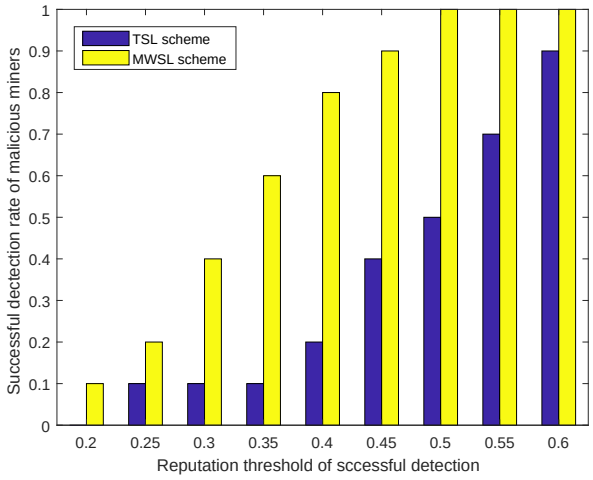

Fig. 5: Detection rate of malicious miners under different threshold values of trusted miners

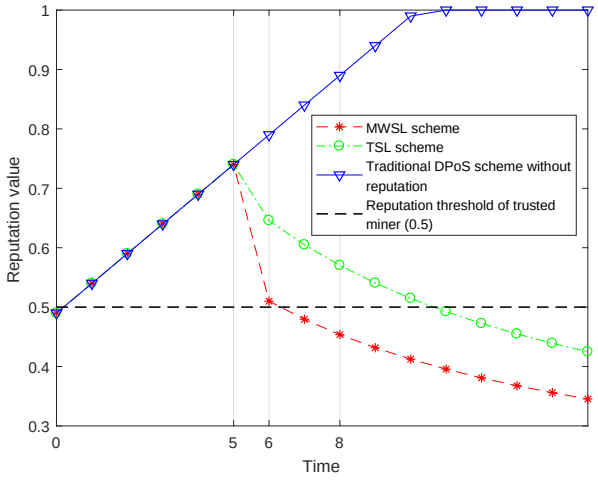

Fig. 4: The reputation values of a malicious miner.

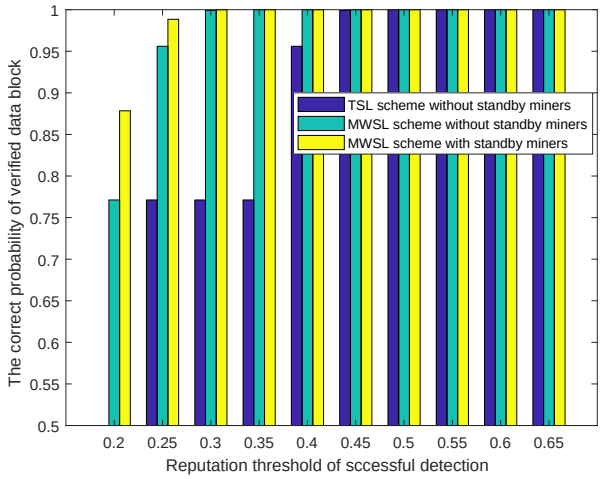

Fig. 6: Probability of corrected data blocks under different threshold values of trusted miners

$T^l_{i\to j} = (1-\kappa)T_{ave} + \kappa T_{las}$, where $T_{ave} = b^{ave}_{x\to j} + 0.5u^{ave}_{x\to j}$ and $T_{las} = b^{las}_{i\to j} + 0.5u^{las}_{i\to j}$. Here κ is the weight and is set to be 0.5. $b^{ave}_{i\to j}$ and $u^{ave}_{i\to j}$ are average values of other vehicles' $b_{i\to j}$ and $u_{i\to j}$, respectively. $b^{las}_{i\to j}$ and $u^{las}_{i\to j}$ are the latest $b_{i\to j}$ and $u_{i\to j}$ in the local opinion of vehicle i for RSU j. We consider a malicious miner candidate will firstly pretend to behave well to obtain positive reputation values from vehicles in the former 5 minutes. Then, this candidate colludes with 10 compromised vehicles and begins to misbehave to 50 well-behaved vehicles randomly. These misbehaving vehicles will generate negative reputation opinions for the candidate, while the colluded vehicles still generate positive reputation opinions for the candidate and vote it as a miner in the voting stage.

Fig. 4 shows reputation variation of a malicious miner candidate from the perspective of a well-behaved vehicles under three cases: (i) traditional DPoS scheme without reputation, (ii) TSL scheme, and (iii) MWSL scheme. In the traditional DPoS scheme without reputation, the reputation value of the compromised candidate evaluated by the vehicle is linear increasing because the well-behaved vehicle cannot detect the candidate's misbehaviors for other well-behaved vehicles. However, in the cases of TSL and our MWSL schemes, the reputation values of the candidate sharply decrease because of recommended opinions from other vehicles. The reputation value decreasing below reputation threshold of trusted miner in the MWSL scheme is faster than that of TSL because of the weights of interaction frequency, timeliness, and interaction effects on both recommended opinions and local opinions. This can avoid being misleading by compromised vehicles' recommended reputation opinions. As a result, our MWSL scheme achieves more accurate reputation calculation, and this therefore leads to more secure miner voting.

We observe the detection rate of 10 malicious miner candidates using the TSL and MWSL schemes during 60 minutes. Figure 5 shows that the MWSL scheme has much higher successful detection rate of malicious miners than that in the

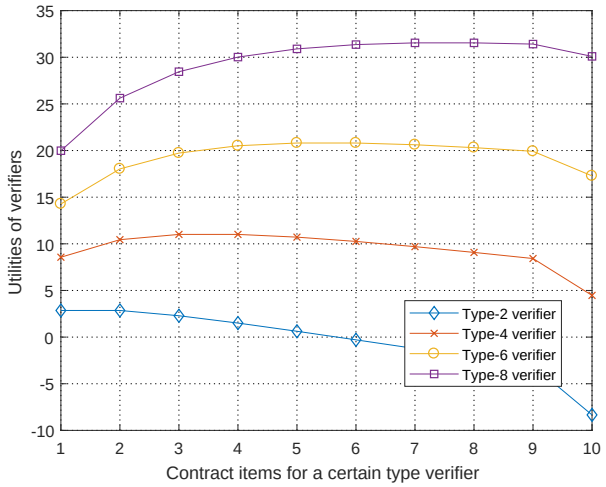

Fig. 7: Utilities of verifiers under different contract items.

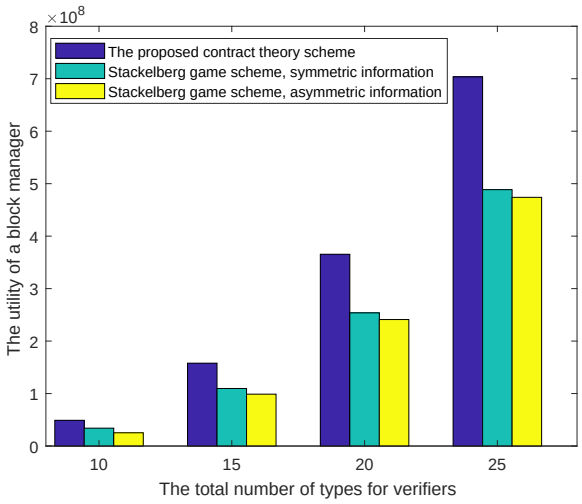

Fig. 8: The utility of a block manager under different total number of verifier types.

TSL scheme. We define a metric as the reputation threshold of successful detection, in which only the reputation of malicious miners below the threshold can be detected successfully. When the reputation threshold of successful detection is 0.5, the detection rate of the MWSL scheme is 100%, which is 100% higher than that of the TSL scheme. Due to higher detection rate in the MWSL scheme, potential security threats can be removed more effectively, which leads to a securer BIoV.

From Fig. 5, we can observe that successful detection probability is not good enough when the reputation threshold of successful detection is very low, e.g., 0.2. In the cases with a very low threshold, the active miners generated by reputation voting may launch the verification collusion attack, that more than 1/3 active miners collude to generate false verification result for a data block [33], [17]. To defend this intractable attack, standby miners should participate in block verification to improve the correct probability of verified block. The correct probability of verified block means that the data block is correctly verified without the effects of the verification collusion attack. Figure 6 shows the correct probability of data block after verification with respect to different reputation thresholds of successful detection. When the reputation threshold of successful detection is 0.2, the correct probability in our MWSL scheme with standby miners is 13% higher than that of MWSL scheme without standby miners, while the TSL scheme without standby miners cannot defend against this collusion attack. This indicates that the proposed MWSL can ensure a secure block verification, even when attackers launch internal active miner collusion.

B. Performance of the incentive mechanism based on contract theory scheme

A block manager acting as the contract publisher announces the designed contract items to other active miners and standby miners. These miners choose a contract item (R_q, L_q^{-1}) to sign, and work as verifiers to finish the block verification task according to latency requirements in the signed contract. Finally, the verifiers obtain the corresponding incentives from the contract publisher. Figure 7 shows the utilities of verifiers with type 2, type 4, type 6 and type 8. We can see that each type of verifiers obtains the maximum utility while selecting the contract item exactly designed for its type, which explains the IC constraint. All types of verifiers choose the contract items corresponding to their types with non-negative utilities, which validates the IR constraint [26].

We compare the profit of a block manager obtained from the proposed contract model, and Stackelberg game model from [30]. Figure 8 shows that the profit of a block manager increases with the total number of verifier types. The more verifier types bring both more verifiers and contract item choices for high-type (high-reputation) verifiers, leading to the more secure block verification. The utility of the proposed contract model has better performance than that of the Stackelberg game model. The reason is that in the monopoly market, the proposed contract model provides limited contract items to extract more benefits from the verifiers. However, in the Stackelberg game model, rational verifiers can optimize their individual utilities thus leading to less profit of the block manager. Moreover, the Stackelberg game model with symmetric information has better performance than that of Stackelberg game model with asymmetric information. The reason is that the game leader (the block manager) in the Stackelberg game with symmetric information can optimize its profit because of knowing the actions of followers (verifiers), i.e., the symmetric information, and set the utilities of the follows as zero [30].

VII. Conclusion

In this paper, we have introduced blockchain-based Internet of vehicles for secure P2P vehicle data sharing by using a hard security solution, i.e., the enhanced Delegated Proof-of-Stake consensus scheme. This DPoS consensus scheme has been improved by a two-stage soft security enhancement solution. The first stage is to select miners by reputation-based voting. A multi-weight subjective logic scheme has been

utilized to calculate securely and accurately the reputation of miner candidates. The second stage is to incentivize standby miners to participate in block verification using contract theory, which can further prevent internal collusion of active miners. Numerical results have indicated that our multi-weight subjective logic scheme has great advantages over traditional reputation schemes in improving detection rate of malicious miner candidates. Likewise, the proposed contract-based block verification scheme can further decrease active miners collusion and optimize the utilities of both the block manager and verifiers to further improve the security of vehicle data sharing. In the future work, we can further improve the accuracy of the miner candidates' reputation calculation through taking more weights into consideration.

REFERENCES

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

[2] 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.

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

[4] BLOCKCHAIN NEWS (2018). [Online] Available: https://www.ccn.com/volkswagen-seeks-patent-for-inter-vehicular-blockchain-communications -system/.

[5] Ford to Use Cryptocurrency for Inter-Vehicle Communication System (2018). [Online] Available: https://news.bitcoin.com/ford-cryptocurrency-inter-vehicle-communication-system/.

[6] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," *CoRR*, vol. abs/1707.07442, 2017.

[7] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," *CoRR*, vol. abs/1708.09721, 2017.

[8] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2018.

[9] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

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

[11] 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.

[12] R. A. Michelin, A. Dorri, R. C. Lunardi, M. Steger, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," *arXiv preprint arXiv:1807.01980*, 2018.

[13] N. Lasla, M. Younis, W. Znaidi, and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative its," in *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on*, pp. 1–5, IEEE, 2018.

[14] Delegated Proof-of-Stake Consensus (2018). [Online] Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[15] 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.

[16] On-Chain Vote Buying and the Rise of Dark DAOs. [Online] Available: http://hackingdistributed.com/2018/07/02/on-chain-vote-buying/.

[17] Permissioned Blockchains (2018). [Online] Available: https://monax.io/learn/permissioned_blockchains/.

[18] X. Huang, R. Yu, J. Kang, Z. Xia, and Y. Zhang, "Software defined networking for energy harvesting internet of things," *IEEE Internet of Things Journal*, vol. 5, pp. 1389–1399, June 2018.

[19] EOS Block Producer Voting Guide. [Online] Available: https://medium.com/coinmonks/eos-block-producer-voting-guide-fba3a5a6efe0.

[20] N. Oren, T. J. Norman, and A. Preece, "Subjective logic and arguing with evidence," *Artificial Intelligence*, 2007.

[21] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Communications Letters*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8432083/.

[22] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[23] 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.

[24] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, May 2018.

[25] 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.

[26] M. Zeng, Z. K. Li, Yong, M. Waqas, and D. Jin, "Incentive mechanism design for computation offloading in heterogeneous fog computing: a contract-based approach," in *IEEE International Conference on Communications*, 2018.

[27] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, 2018.

[28] X. Chen, "Decentralized computation offloading game for mobile cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 974–983, 2015.

[29] P. Bolton and M. Dewatripont, *Contract theory*. MIT press, 2005.

[30] Z. Hou, H. Chen, Y. Li, and B. Vucetic, "Incentive mechanism design for wireless energy harvesting-based internet of things," *IEEE Internet of Things Journal*, vol. 5, pp. 2620–2632, Aug 2018.

[31] L. Gao, X. Wang, Y. Xu, and Q. Zhang, "Spectrum trading in cognitive radio networks: A contract-theoretic modeling approach," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 843–855, 2011.

[32] 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.

[33] R. Chitchyan and J. Murkin, "Review of blockchain technology and its expectations: Case of the energy sector," *arXiv preprint arXiv:1803.03567*, 2018.