Hindawi
Security and Communication Networks
Volume 2021, Article ID 5580089, 16 pages
https://doi.org/10.1155/2021/5580089

Research Article

Towards a Smart Privacy-Preserving Incentive Mechanism for Vehicular Crowd Sensing

Lingling Wang, Zhongda Cao, Peng Zhou, and Xueqin Zhao

School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao, China

Correspondence should be addressed to Lingling Wang; wanglingling@qust.edu.cn

Received 3 March 2021; Accepted 30 April 2021; Published 17 May 2021

Academic Editor: Anjia Yang

Vehicular crowd sensing is a promising approach to address the problem of traffic data collection by leveraging the power of vehicles. In various applications of vehicular crowd sensing, there exist two burning issues. First, privacy can be easily compromised when a vehicle is performing a crowd sensing task. Second, vehicles have no incentive to submit high-quality data due to the lack of fairness, which means that everyone gets the same paid, regardless of the quality of the submitted data. To address these issues, we propose a smart privacy-preserving incentive mechanism (SPPIM) for vehicular crowd sensing. Specifically, we first propose a new SPPIM model for the scenario of vehicular crowd sensing via smart contract on the blockchain. Then, we design a privacy-preserving incentive mechanism based on budget-limited reverse auction. Anonymous authentication based on zero-knowledge proof is utilized to ensure the privacy preservation of vehicles. To ensure fairness, the reward payments of winning vehicles are determined by not only the bids of vehicles but also their reputation and the data quality. Then, any rewarded vehicle can get the fair payment; on the contrary, malicious vehicles or task initiators will be punished. Finally, SPPIM is implemented by using smart contracts written via Solidity on a local Ethereum blockchain network. Both security analysis and experimental results show that the proposed SPPIM achieves privacy preservation and fair incentives at acceptable execution costs.

1. Introduction

As the population of cities starts to grow, the number of cars begins to increase, which has caused congestion problems on the roadways and the parking lots [1]. It is not only an inconvenience for commuters but can also cause billions of dollars in lost time and wasted fuel. Smart transportation is a solution to make real-time control decisions for traffic efficiency and security, where large amounts of traffic information are needed [2]. Nowadays, vehicles have more powerful sensoring, storing, and computing capabilities, and they are capable of collecting and sharing data. As for data acquisition, the ubiquity of crowd sensing has enabled the emergence of vehicular crowd sensing (VCS), which leverages the power of vehicles to collect massive traffic data [3]. As shown in Figure 1, when there is an emergent traffic event (e.g., rear-end accident or traffic jam) on the roadway, the vehicles around the location of the event can submit the real-time traffic data to the nearby road side units (RSUs), i.e., vehicles perform the crowd sensing task distributed by the transportation administration (TA) via RSUs. However, due to the resource consumption, fairness, and privacy leakage problems, vehicles may be reluctant to participate in crowd sensing tasks without an effective and fair incentive mechanism and privacy protection solutions.

Some privacy-preserving incentive mechanisms (PPIMs) have been proposed for protecting vehicles' privacy in VCS. However, these schemes either rely on a central platform [4] or lack of considering the fairness of the incentive mechanism [5], leading to collusion attack [6], potential privacy disclosure, or inadequate incentive. As the most popular distributed technology, blockchain has enabled incentive mechanism in VCS for secured authentication and collusion attack resistance. To be specific, smart contracts running on the blockchain take the place of the centralized platform to run the incentive mechanisms, which handles all interactions and overcomes the challenges of centralized execution, e.g., collusions between TA and RSUs, RSUs and

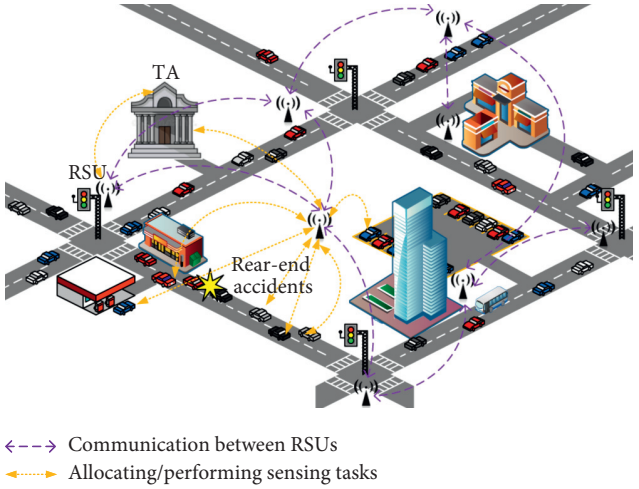

Figure 1: A vehicular crowd sensing scenario of an emergent traffic condition.

vehicles. Although a few blockchain-based PPIMs [4, 5, 7] have been proposed, they either need a trusted third party to assist the privacy protection [4, 7] or lack the fairness of the payments [5].

To address the privacy issue, a common method is to take advantage of the anonymous mechanism, i.e., each vehicle has multiple pseudonyms or anonymous credentials which can be anonymously authenticated to protect the vehicle's privacy. However, there exists limitation to perform complex operations on a blockchain, e.g., in Ethereum, and the gas requirements of an operation cannot exceed the block gas limit. Hence, it is challengeable to design "light" operations of anonymous authentication on the blockchain to fulfill the privacy protection of the vehicles in VCS.

To address the fairness issue, most auction-based incentive mechanisms [4, 8–10] encourage vehicles to take part in crowd sensing tasks, where they submit bids to the central platform to compete for a task. The platform selects winning users to perform tasks and get paid. Nevertheless, it is unfair to determine the winners and the payment only depending on the bids and without considering the reputation of the vehicles and the submitted data quality. Hence, it cannot motivate people to submit high-quality sensory data.

In this paper, to address these challenges, we propose a smart privacy-preserving incentive mechanism (SPPIM) to stimulate the vehicles to submit high-quality sensory data and get fair payment with privacy protection. We focus on the vehicles' privacy protection without a trusted platform and aim to design a fair incentive mechanism which results in a rational payment according to the past and present performance of the vehicle. Specifically, the main contributions of this paper are as follows:

(i) We design a smart privacy-preserving incentive mechanism model and give an effective SPPIM based on budget-limited reverse auction via smart contract, which can ensure fairness of the payments for vehicles and data quality assurance for the task initiator.

(ii) SPPIM preserves the vehicles' privacy by using anonymous credentials without any trusted party. Meanwhile, bids preservation is achieved by using Pedersen commitment [11] from the vehicles to the task initiator. Anyone who obtains a committed bid, except the task initiator, is unable to get information about the bid's value.

(iii) We make a theoretical security and privacy analysis of the proposed SPPIM and evaluate the performance of the incentive mechanism by computing the utility of the vehicle and the task initiator. Furthermore, we implement the proposed SPPIM on the Ethereum testnet to verify its feasibility and provide a comprehensive analysis of the performance.

2. Problem Statement

In this section, we formalize the system model of vehicular crowd sensing, the smart PPIM model, and the threat model and also identify our design goals.

2.1. System Model. The system model mainly consists of the following four entities: block chain network, fog servers, task initiator, and vehicles as shown in Figure 2.

(i) Blockchain network has a decentralized and public ledger, which is shared with the legitimate miners and vehicles, and serves for SPPIM in vehicular crowd sensing. Smart contracts are designed to define and execute contracts, consisting of functions and data. Without a trusted platform, SPPIM is executed in a verifiable manner via smart contracts. New blocks, with all transactions of the incentive mechanism for vehicular crowd sensing task, will be audited and finally added to the block chain.

(ii) Fog servers are honest but are curious and connect with vehicles via wireless links. We assume that fog servers, acting as miners, have powerful computing and storage capabilities, and they act as the consensus nodes to maintain the blockchain network. Each fog server stores the whole ledger, which enables the validation of the blocks and transactions. Fog servers are also in charge of verifying the registration of the task initiator and vehicles and take control of the data quality.

(iii) Task initiator publishes the sensing task and pays the reward to winning vehicles via smart contracts. The task initiator communicates with the fog servers via the smart contracts, which are deployed on the fog servers. In our scenario, transportation administration (TA) takes the role of the task initiator.

(iv) Vehicles assume that there are N vehicles, denoted by $V = (V_1, V_2, \ldots, V_N)$, competing for a sensing task, and each vehicle V_j will submit a bid b_j, the current reputation R_j, and the sensory data D_j. Then, vehicles can get some rewards according to their reputation and the submitted data quality.

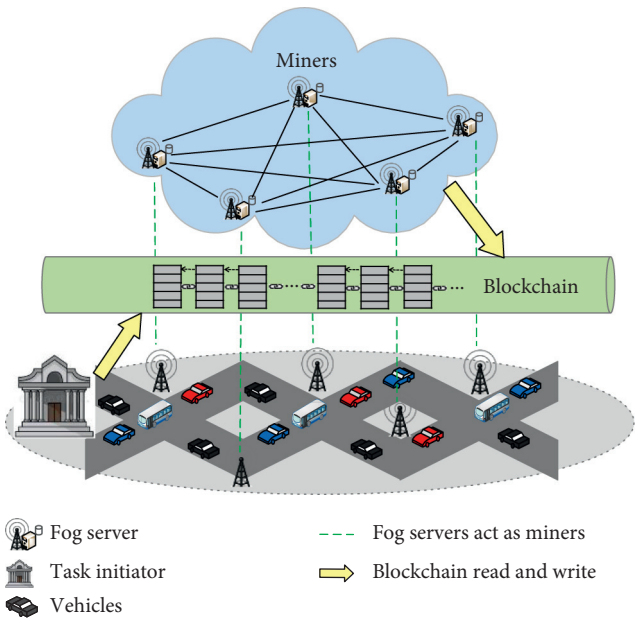

Figure 2: A system model of vehicular crowd sensing.

2.2. SPPIM Model. A decentralized PPIM system can be obtained by our SPPIM model as shown in Figure 3. We leverage the smart contract to replace the centralized platform. Our SPPIM model, based on budget-limited reverse auction [9], consists of a task initiator TA and N vehicles, i.e., $V = (V_1, V_2, \ldots, V_N)$. The task initiator wants to gather some data, such as emergent traffic conditions, and then publish a crowd sensing task. Vehicles are willing to collect this type of data and bid for the task. In this model, the task initiator acts as a buyer and vehicles act as sellers. All vehicles and the task initiator enter the auction process for reward payments and sensory data acquisition. The workflow of the proposed SPPIM model is as follows.

(i) TA deploys a sensing task via smart contract on the block chain.

(ii) Vehicles prove their legitimate identities to fog servers anonymously.

(iii) Legitimate vehicles provide their bids to fog servers, which run the deployed smart contracts to determine the winner set B_w of the auction.

(iv) Winning vehicles submit the required data, and fog servers calculate the reward payment P. Vehicles whose data quality meets the requirements get paid according to the data quality.

(v) TA gets the collected information from the fog server.

(vi) Fog servers verify all the transactions and build new blocks periodically.

We present the key notations used in this article in Table 1.

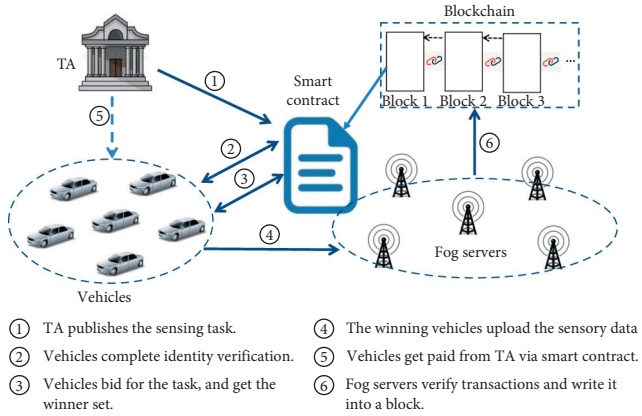

Figure 3: The smart PPIM model of vehicular crowd sensing.

2.3. Threat Model. We assume that fog servers follow the protocols but are also curious about vehicles' privacy. Task initiators and vehicles are not trusted because they can launch attacks out of self-interests.

(i) Fog servers can launch passive attacks, and they are interested in the identity of task initiators and vehicles from the submitted messages and transactions. And they may be compromised or colluded with some vehicles or task initiator leading to privacy disclosure.

(ii) A task initiator may publish a sensing task without a reward guarantee and prematurely abort a task, and it may also try to obtain the private information of vehicles by accessing the block chain.

(iii) Vehicles are also curious about other vehicles' identities and bids. A dishonest vehicle may forget its reputation and try to get private information of other vehicles. A misbehaved vehicle may steal sensory data or collude with other vehicles to get extra rewards.

(iv) External adversary can eavesdrop the transmitting messages to violate vehicles' privacy. And it may impersonate a legitimate vehicle to perform a crowd sensing task and even trick a task initiator into paying for a reward.

2.4. Design Goal. Our goal is to design a privacy-preserving incentive mechanism with enhanced fairness for vehicular crowd sensing. Specifically, the proposed SPPIM will achieve the following requirements:

(i) *User Authentication*. No adversary can impersonate a legitimated vehicle. Any participant, including the task initiator and the vehicles, should be authenticated in an anonymous way.

(ii) *Identity Privacy*. The task initiator and the vehicles' privacy can be protected. Anyone including the fog

Table 1: Key notations.

Notation	Definition
λ	The security parameter
q	A large prime whose length is λ
Z_q	An additive group of order q
G, G_T	Two cyclic groups of the same prime order q
g, g_1	Generators of G
μ	A daily verification key
$e(.,.)$	A nondegradable bilinear mapping
$H(.)$	A collision-resistant hash function
Ω	A bloom filter for fast authentication factors
$(s, Y_F = g^s)$	The fog's private key and public key
X, Y, Z	$X = g^x, Y = g^y, Z = g^z$ for $x, y, z \in Z_q$
Cred	An anonymous credential of a vehicle
V	Legitimate vehicles consist of $V_1, V_2, \ldots, V_n$
$B_{\max}$	TA's budget
$\langle b_i, R_i, \mathrm{loc}_i \rangle$	The bid, reputation, and the location of vehicle V_i
C	Pederson commitment
D	The data structure of the sensory data
$\omega_i(c), \omega_i(t)$	The weight of the accuracy of the data and the submission time
q_i	The data quality of vehicle V_i
$m\prime$	The amount of vehicles who submit high-quality data
p_i	The reward for vehicle V_i in the reward payment P

server cannot identify vehicles' real identities when a task initiator publishes a task or a vehicle performs a sensing task.

(iii) *Bid Privacy*. All vehicles cannot know the bids submitted by others before committing to their own bids. This can help prevent the vehicles' collusion.

(iv) *Financial Fairness*. Vehicles get paid depending on their bids, the past, and current performance, i.e., reputation and the data quality. Meanwhile, vehicles or TA may attempt to deviate from the contract or prematurely abort, which will affect the SPPIM. The aborting parties will be financially penalized.

(v) *Collusion Attack Resistance*. If the TA or a fog server is compromised or colluded with some vehicles or task initiator, the SPPIM can still work well.

3. Preliminaries

We take advantage of the following cryptographic building blocks and technologies to construct our SPPIM.

3.1. Cryptographic Building Blocks. Bilinear Pairing [12]. Let G_1, G_2, and G_T be three cyclic groups of the same prime order q. A function e: $G_1 \times G_2 \longrightarrow G_T$ is a bilinear map if the following properties hold:

(i) Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$, for all $u \in G_1$, $v \in G_2$, and $a, b \in Z_q$

(ii) Nondegeneracy: $e(g_1, g_2) \neq 1$, where g_1 and g_2 are generators of G_1 and G_2, respectively

(iii) Computability: there exists an algorithm which can compute $e(u, v)$ efficiently for all $u \in G_1$ and $v \in G_2$

Zero-Knowledge Proof [13]. A zero-knowledge proof is a two-party (i.e., a prover and a verifier) protocol which allows a prover to convince the verifier that something is true without revealing any information. Specifically, a prover convinces a verifier of knowledge of values $(a_1, \ldots, a_n)$ that satisfy the predicate P denoted by

$$\mathrm{ZkPoK}\{(a_1, \ldots, a_n) | P(a_1, \ldots, a_n)\}, \quad (1)$$

ZkPoK can be used as an effective way to design a secure public-key cryptosystem. In this paper, we use zero-knowledge proofs to generate the anonymous credentials of vehicles and to complete the anonymous authentication.

3.2. Reverse Auction. The auction usually acts as an effective way to allocate goods or services to bidders who give the highest bidder [14]. An auction becomes a reverse auction when swapping the roles of the buyers and the sellers. The reverse auction model was first applied in a participatory perception system in Lee and Hoh [15] and has been widely used as a design model for incentive mechanisms in mobile crowd sensing [16–18]. Similarly, the reverse auction is a good solution for monetary incentives in vehicular crowd sensing, which encourages vehicles to sell their data.

In this paper, we use reverse auction with budget constraints [9] to model our incentive scenario. The vehicles act as sellers/bidders and will be selected to collect data. And the TA acts as a buyer, who purchases data provided by the vehicles with a limited budget.

3.3. Blockchain and Smart Contracts. Blockchain [19] is a distributed and public ledger which maintains an ever-growing list of digital transactions, which can be verified and audited by any users. Since blockchain provides a secure method for online transactions among anonymous

participants, it is inherently consistent with our requirements, i.e., without a trusted third party. Recently, smart contract [20] has been adopted to allow users to define and execute contracts on the block chain. A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the predefined rules are met, the instruction of the agreement is automatically enforced. The rules of transactions in our SPPIM can be enforced with smart contracts, which avoid the collusion attack [21] between the TA and the fog server, and then vehicles' equity is guaranteed.

4. The Proposed Smart Privacy-Preserving Incentive Mechanism

In this section, we first describe the overview of our SPPIM and then specify the detailed mechanism and the corresponding smart contracts.

4.1. Overview of the Proposed Incentive Mechanism. Our proposed SPPIM consists of anonymous authentication mechanism, privacy-preserving winner selection algorithm, and fairness-enhanced reward payment scheme.

(i) *Anonymous Authentication Mechanism*. The fog servers generate the system parameters and set the private key and public key. Vehicles get their anonymous credentials with the help of fog servers via the zero-knowledge proofs of knowledge. A fast authentication factor corresponding to each legitimate vehicle is stored in a bloom filter [22], which is kept on the blockchain for quick anonymous authentication. After passing the authentication, the vehicle can compete for a sensing task.

(ii) *Privacy-Preserving Winner Selection Mechanism*. When a vehicle competes for a sensing task, it first anonymously authenticates itself and bids for it. All legitimate vehicles and TA enter the reverse auction process for the sensing task. Since the location of the same abnormal traffic condition should not be very different, vehicles with excessive location deviation will be filtered. The winner selection mechanism also takes advantage of Pedersen commitment [23] to maintain bid's privacy. Vehicles first submit their commitments to the sealed bids on the smart contracts and then reveal the commitments secretly to the fog server, who runs the winner selection algorithm to determine the winner set of the task depending on the bids, reputations, and their precise locations.

(iii) *Fairness-Enhanced Reward Payment Scheme*. To enhance the fairness of payment, the payment profile should be generated according to the current and previous performance of vehicles. This can motivate the vehicles to actively take part in crowd sensing tasks and to provide high-quality data. In time-sensitive VCS scenarios, the untimely information is useless, so vehicles are required to submit their reports timely. Hence, the data quality is quantified by two factors: the data accuracy and the submission time. The payment profile is generated by the submitted bids and the quantified data quality of the vehicles. The task initiator TA pays and gets the balance, and the vehicles get rewards according to the payment profile in an anonymous way via smart contracts. Finally, fog servers verify and write the transactions into the block.

4.2. Detailed Mechanism

4.2.1. Anonymous Authentication Mechanism. The proposed anonymous authentication mechanism consists of ① system setup; ② anonymous certificate generation; and ③ anonymous authentication described as follows:

① System setup (offline):

(i) The fog server runs setup to obtain public parameters
para $= \{G, G_T, q, g, g_1, g_T, e, H, X, Y, Z, \mu, Y_F\}$.
(G, G_T) is a bilinear map group of a prime order $q > 2^\lambda$, where λ is the security parameter. $e(.,.)$ is the bilinear map satisfying e: $G \times G \longrightarrow G_T$. g and g_1 are generators of G, and $e(g, g)$ is defined as g_T. H: $Z_q \longrightarrow Z_q$ is a collision-resistant hash function. The fog server F selects $s \in Z_q$ randomly as its private key, and the public key is computed as $Y_F = g^s$. F also selects $x, y, z, \mu \in Z_q$ to compute $X = g^x$, $Y = g^y$, and $Z = g^z$. μ is a period verification key. F initializes an empty set Ω using bloom filter. Ω is reset periodically by the fog server because anonymous credential is only valid for a certain period.

(ii) Note that a vehicle cannot apply for more than one anonymous credential within one hour for the sake of security. We use a Boolean tag T to mark the state of the vehicle, and $T = 1$ represents that the vehicle has applied for an anonymous certificate at some point. T will be updated to be $T = 0$ once in a while, e.g., one hour or later.

② Anonymous certificate generation:

(i) Assume all vehicles are welcomed to compete for the sensing task. They need to subscribe for an anonymous credential when they want to perform the task. Once the vehicle requests an anonymous credential, the fog server will set the state tag $T = 1$. Then, the vehicle selects $(k, h) \in Z_q^2$ randomly, calculates $\Delta = Y^k Z^h$, and sends $(\Delta, H(k))$ to the local fog server.

(ii) The fog checks whether $H(k)$ does exist in Ω or not. If it does, the vehicle will be guided back to the above step. Otherwise, the fog server stores $H(k)$ into Ω. Here, we call $H(k)$ as the fast authentication factor. The fog server verifies the

identity of the vehicle by the zero-knowledge proof of knowledge:

$$\mathrm{ZkPoK}\{\{k,h\}\colon \Delta = Y^k Z^h\}. \quad (2)$$

(iii) The fog returns "failure" if the proof is unsuccessful. Otherwise, the fog sends (W, ν) to the vehicle, where $\nu \in Z_q$ and $W = (X\Delta)^{(1/\nu+s+\mu)}$.

(iv) The vehicle checks whether the equation $e(W, Y_F g^{\nu+\mu}) \stackrel{?}{=} e(X\Delta, g)$ holds. It returns "failure" if the equation does not hold. Otherwise, the vehicle's anonymous credential $\mathrm{cred} = (W, \nu, k, h)$ is stored.

③ Anonymous authentication:

If a vehicle competes for a sensing task, it first authenticates itself by offering $H(k)$ to the fog servers. The fog runs the fast authentication algorithm to obtain TF. If $TF = 0$, which means $H(k)$ does not exist in Ω, the vehicle will be rejected as an illegal participant. Otherwise, the vehicle proves itself to the fog server in the zero-knowledge proof of knowledge:

$$\mathrm{ZkPoK}\{(W, \nu, k, h)\colon W^{\nu+s+\mu} = XY^k Z^h\}. \quad (3)$$

If the proof is successful, the vehicle will be maintained as a legitimate candidate vehicle for bidding (Algorithm 1).

4.2.2. Privacy-Preserving Winner Selection Mechanism. The goal of the proposed winner selection mechanism is to select the winning vehicles with privacy preservation. Three factors, the submitted bid's value, the vehicle's location, and the reputation, have been combined to determine the winning vehicles. Reverse auction with TA's budget constraints is adopted to model our mechanism. All vehicles and the TA enter the auction process for crowd sensing task. Each vehicle acts as a bidder and submits a bid commitment. The winning vehicles are determined by the winner selection algorithm as shown in Algorithm 2.

(i) The vehicle chooses a random $\gamma \in Z_q$, computes the commitment of a bid $b \in Z_q$ as $C = g^b g_1^\gamma$ (see function Commit in section 4.3.), and then sends C to the local fog server.

(ii) Then, the vehicle reveals the values of b and γ (see function Decrypt and Reveal in section C) to open the commitment C. Each vehicle V_i sends the outcome ciphertext cipher_i of encrypting (b_i, γ_i) by the public key of the local fog server Y_F.

(iii) The fog servers verify the correctness of the opening commitments to ensure that only the valid commitments store on the SPPIM contract.

Note that the ciphertext of b and γ is stored on the SPPIM contract rather than being sent directly to the fog server.

Assume the fog server F receives n bids $\langle C_i, R_i, \mathrm{loc}_i\rangle$, $i = 1, \ldots, n$ from n legitimate vehicles $V = (V_1, V_2, \ldots, V_n)$, where C_i represents the commitment of the bid b_i submitted by V_i, R_i refers to its current reputation, and $\mathrm{loc}_i = (l_1^i, l_2^i)$ is the location using longitude and latitude, respectively. F first computes the central position (l_1^0, l_2^0) of n locations and calculates the Euclidean distance ρ^i of (l_1^0, l_2^0) and $(l_1^i, l_2^i)_{i=1}^n$. Then, F checks whether $\rho^i < 100$ m holds. If $\rho^i > 100$ m, the accuracy of the data is not up to the standard and then the vehicle V_i will be rejected. Otherwise, the reward payment of the vehicle V_i will be computed depending on the submitted data quality.

The winner selection algorithm, depicted in Algorithm 2, is given by taking the bid set $B = \langle C_i, R_i, \mathrm{loc}_i\rangle, i = 1, \ldots, n$, the ciphertext cipher_i, TA's budget $B_{\max}$, and the highest bid price b_0 as inputs. The output of the algorithm is the winner set B_w.

4.2.3. Fairness-Enhanced Reward Payment Scheme. We propose a fairness-enhanced reward payment scheme, where payment profile is generated depending on the data quality and the reputation of the vehicletbl2alg3.

① *Data Quality Measurement.* To measure the data quality submitted by the vehicle, the data structure of the sensory data is defined as $D = (\mathrm{task}, \mathrm{cause}, \mathrm{proof}, \mathrm{time})$. The sensory data uploaded by the winning vehicles are stored in the form as Table 2.

(i) Task is represented by the task number to distinguish different crowd sensing tasks;

(ii) Cause refers to the cause of abnormal traffic conditions. For instance, "000″ means there is an accident at the location (l_1, l_2); "001" means there is a traffic jam at the location (l_3, l_2).

(iii) Proof is the evidence the vehicle can upload to prove the cause. How to identify the evidence is out of the scope of this paper.

(iv) Time is the current time of submitting the sensory data.

Assume the fog server F receives m sensory data $\{D_1, D_2, \ldots, D_m\}$ from m winning vehicles for the same task task, where $D_i = (\mathrm{task}, c_i, \mathrm{proof}_i, t_i)$. The data quality is quantified by the submission time t_i and the data accuracy, which is determined by hamming distance $d(.,.)$ of the *causes*.

Given cause c_i computes $m-1$ hamming distance $d(c_i, c_j)$ for all $j \neq i$ to measure the similarity of the abnormal traffic conditions. A weight $\omega_i(c)$ is assigned to measure the accuracy of the data as shown in Algorithm 3. A weight $\omega_i(t)$ is assigned to measure the submission time of vehicle V_i. The earlier the upload is, the greater weight the vehicle will gain. Finally, the data quality of V_i is quantified by

$$q_i = \theta\omega_i(c) + (1-\theta)\omega_i(t), \quad (4)$$

where θ denotes the importance of the data accuracy.

② *Payment Profile Generation.* The payment profile is generated by the data quality of the vehicle. For m vehicles, the sum of the submitted bids is $\sum_{i=1}^m b_i$, which satisfies $\sum_{i=1}^m b_i \le B_{\max}$. Finally, the payment for the vehicle V_i is given as follows:

Input: $H(k)$, Ω
Output: TF = $\{1, 0\}$
(1) Check whether $H(k)$ exists in Ω;
(2) **if** $H(k) \notin \Omega$ **then**
(3) TF = $\{0\}$;
(4) **else** TF = $\{1\}$;
(5) **end if**
(6) **return** TF

Algorithm 1: Fast authentication algorithm.

Input: $B = \langle C_i, R_i, \text{loc}_i \rangle$, cipher_i, $B_{\max}$ and b_0;
Output: The winner set B_w.
(1) $B_w = \varnothing, B\ D = 0$;
(2) $R_0 = (1/n) \sum_{k=1}^{n} R_k$;
(3) **for** $(i = 1; i++; i \le n \,\&\&\, \text{BD} \le B_{\max})$**do**
(4) $\rho^i = \sqrt{(l_1^i - l_1^0)^2 + (l_2^i - l_2^0)^2}$;
(5) **if** $\rho^i < 100\text{m}$ **then**
(6) invoke Decrypt(cipher_i);
(7) invoke Reveal(C_i);
(8) obtain $\langle b_i, R_i \rangle$;
(9) **if** $(R_i \ge R_0)$ **then**
(10) $B_w = B_w \cup \{b_i | b_i \le b_0\}$;
(11) BD = BD + b_i;
(12) **end if**
(13) **end if**
(14) **end for**
(15) **return** B_w

Algorithm 2: Privacy-preserving winner selection algorithm.

Table 2: The storage format of the sensory data.

Task	Cause	Proof	Time
No. 3	000	∗.jpg	9 : 00am
No. 3	001	∗.mp4	9 : 01am
No. 3	000	∗.jpg	9 : 03am
⋮	⋮	⋮	⋮

$$p_i = q_i \sum_{i=1}^{m} b_i. \tag{5}$$

This mechanism guarantees that as long as the vehicle provides higher quality data, they will get more rewards.

4.3. Smart PPIM Contract. In this section, our SPPIM is implemented via smart contract. After the SPPIM contracts are created, vehicles can take part in the crowd sensing task. The contract accepts the submitted messages from the TA and vehicles and executes the proposed algorithms automatically. Figure 4 illustrates the process of a SPPIM contract, involving all interactions among the TA, the vehicles, and the smart contract.

(i) TA and the vehicles first register on the fog servers. After the registration, vehicles get their anonymous credentials via zero-knowledge proof. TA can launch a crowd sensing task.

(ii) A new SPPIM contract is deployed on the blockchain. TA initiates a crowd sensing task.

(iii) Vehicles access the blockchain for new tasks and authenticate themselves by providing their anonymous credentials and the zero-knowledge proofs.

(iv) After vehicles pass the authentication step, they submit their sealed bids.

(v) The smart contract verifies the validity of the sealed bids and then executes the winner selection algorithm to determine winning vehicles.

Input: Sensory data $\{D_1, D_2, \ldots, D_m\}$ from m winning vehicles, of which the reputations are $\{R_1, R_2, \ldots, R_m\}$;
Output: Payment profile $P = \{p_i\}_{i=1}^{m}$.

for $(i = 1; i++; i \le m)$ **do**
  $\text{counter}_i = 0$;
  for $(j = 1; j++; j \le m)$ **do**
    if $d(c_i, c_j) = 0$ **then**
      counter_i++;
    end if
  end for
  if $\text{counter}_i \ge \lceil (m/2) \rceil$ **then**
    $\omega_i(c) = (1/m)(1 + (R_i / \sum_{\alpha=1}^{m'} R_\alpha))$;
  else
    $\omega_i(c) = (1/m)(1 - (R_i / \sum_{\alpha=1}^{m-m'} R_\alpha))$;
  end if
  Sort the submission time t in a nondescending order and obtain $t_1 \le t_2 \le \ldots \le t_n$;
  $\omega_i(t)$ is assigned to measure t_i;
  $q_i = \theta\omega_i(c) + (1 - \theta)\omega_i(t)$;
  $p_i = q_i \sum_{i=1}^{m} b_i$;
end for return P

Algorithm 3: Fairness-enhanced reward payment algorithm.

Table 3: A breakdown of gas costs for different functions of SPPIM contract when 10 of 20 vehicles are rewarded.

Function	Gas units	Gas cost (USD)
Create(.)	3774689	28.14
Authen(.)	4068500	30.39
Reveal(.)	1555410	11.63
WinnerSel(.)	1315028	9.75
Finalize(.)	688789	4.87

(vi) The winning vehicles submit the crowd sensing data to the fog servers.

(vii) The smart contract determines the payment profile by executing the reward payment algorithm.

(viii) The smart contract returns the balance of the TA, and vehicles get their rewards according to the payment profile.

Figure 5 provides the functions of the SPPIM contract in a detailed overview.

The Init(.) function defines all the parameters about the registration. Fog server calls the Init(.) function to get the public parameters para and generate anonymous credentials together with vehicles. After Init(.), fast authentication factors of legitimate vehicles are maintained in the bloom filter Ω.

The Create(.) function is used to deploy a new SPPIM contract on the blockchain. If TA wants to start a task, it calls Create(.) function with the parameters such as t_1, t_2, t_3, t_4, t_5, t_6 which define the time intervals for the six phases: the budget of a task TA.budget, the highest bidding price b_0, the legitimate vehicles set V, the list of bids B, the list of winning vehicles B_w, and the reward payment profile P. TA is required to pay at least TA.budget to the contract in order to prevent a malicious task initiator from initializing fake tasks and then withdrawing illegally. The highest bidding price b_0 is used to prevent malicious vehicles to submit an excessive bidding price. After the contract is deployed, it can be accessed by legitimate vehicles.

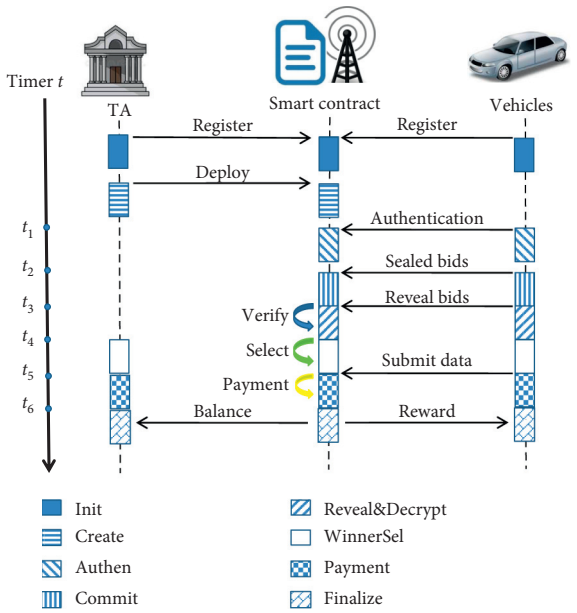

Figure 4: The process of the SPPIM contract.

The Authen(.) function authenticates all vehicles, which compete for the task, via the fast authentication algorithm

and the zero-knowledge proof. Once the vehicle passes the authentication, it can submit bid.

The Commit(.) function seals the bids to protect them from being observed by other vehicles before the bidding interval ends. Pedersen commitment scheme is used to commit a bid. Each vehicle submits a bid commitment along with the location and the reputation of the vehicle.

The Reveal(.) function is triggered by the vehicles to reveal their bids. After that the contract can execute the winner selection algorithm. The inputs of Reveal(.) function are the cipher of the bids encrypted by the public key of the fog server Y_F. To avoid repudiation attack, the ciphertext is stored on the SPPIM contract rather than being sent directly to the fog server.

The Decrypt(.) function decrypts the ciphertext of the bids submitted by the vehicles.

The WinnerSel(.) function orders the bids after all bids are revealed to determine the winning vehicles. It takes as inputs the bids, the reputation, the location of the vehicles, the TA.budget, and the highest bidding price b_0. The result of the function is the winning vehicles set B_w.

The Payment(.) function computes the reward payment of each vehicle depending on the data quality, bids, and their reputation so that the potential vehicles can get reward payment.

The Finalize(.) function returns the balance of the TA and pays incentives to vehicles after the payment profile is determined.

Init	*para* = { }, Ω = {factors}
Create	upon receiving from TA (t_1, t_2, t_3, t_4, t_5, t_6, *TA.budget*, b_0):
	Set state: = INIT, *Vehicles*: = {}
	Set *Winning vehicles* B_w: ={ }, *Payment Profile P*: ={ }
	Assert $t < t_1 < t_2 < t_3 < t_4 < t_5 < t_6$
	Assert *ledger[TA]* ≥ *TA.budget*
	Set *budget*: = *TA.budget*, *highestBid* = b_0
Authen	upon receiving from vehicle *V* (*cred, zk-proof*):
	Assert $t_1 < t < t_2$
	Set *V*→*Vehicles*
Commit	upon receiving from a vehicle *V* (*bid*):
	Assert $t_2 < t < t_3$
	Assert *V.commit* = *com (bid)*
Reveal	upon receiving from avehicle *V* (*ciphertext*):
	Assert $t_3 < t < t_4$
	Assert *V* ∈ *Vehicles*
	Set *Vehicles*[*V*].ciphertext : = *ciphertext*
Decrypt	upon receiving from a vehicle *V*(*ciphertext*):
	Assert $t_3 < t < t_4$
	Set *V.bid* = decrpy (*ciphertext*)
WinnerSel	upon receiving from vehicle *V* (*B*, *ciphertext*):
	Assert $t_4 < t < t_5$
	Algorithm 2 (*B*, *ciphertext*, *TA.budget*, b_0)→B_w
Payment	upon receiving B_w
	Assert $t_5 < t < t_6$
	Algorithm 3(B_w, Data)→*P*
Finalize	upon receiving *P*
	Assert $t > t_6$
	Set *ledger*[B_w]: = *P*

Figure 5: Functions of the SPPIM contract.

5. Privacy and Security Analysis

This section proves that our proposed SPPIM achieves user authentication, identity privacy, bid privacy, financial fairness, and collusion attack resistance.

5.1. User Authentication. In our SPPIM, all vehicles need to authenticate themselves before performing any task. We use anonymous credentials to authenticate vehicles. The unforgeability of vehicle's identity is enabled by the security of the anonymous credentials generation. An adversary can authenticate himself by forging a verified credential and then showing it to the fog server, since the anonymous credential is generated through the zero-knowledge proof, of which the security is guaranteed by the CL signature scheme [24]. So, the proposed scheme satisfies the property of user authentication as long as the credentials are not forgeable.

Furthermore, a malicious vehicle may create multiple online identities to rig the mechanism. To prevent this attack, each vehicle should and must have only one valid anonymous credential when performing one crowd sensing task. Hence, in our SPPIM, we require that a vehicle can only apply for one anonymous credential within one hour. When the vehicle requests an anonymous credential, the fog server will set the state tag T to be 1. If a vehicle requests another anonymous credential within one hour, the fog can check the recorded state tag of the vehicle to refuse its request.

5.2. Identity Privacy. We make sure the identity privacy of our SPPIM by proving the pseudonymity and unlinkability of vehicles.

First, each vehicle has different anonymous credentials $\text{cred} = (W, \nu, k, h)$ corresponding to different tasks in our SPPIM. The anonymous credential can be verified by the smart contract as the valid anonymous credential. Hence, the vehicle's pseudonymity depends on the security of the zero-knowledge proof [24], of which the security proofs are relatively straightforward.

As for the unlinkability, the fog server cannot link vehicle's identity and the vehicle's anonymous credential during vehicle registration, and the fog cannot link the vehicle's different anonymous credentials. This property also depends on the zero-knowledge proof protocols. When a vehicle is applying for an anonymous credential, the fog server does not know the values of (k, h). Meanwhile, the anonymous credential $\text{cred} = (W, \nu, k, h)$ can still be acknowledged as a valid BBS signature [25].

5.3. Bid Privacy. Our SPPIM protects the bid privacy by using Chaum–Pedersen noninteractive ZKP [23]. Vehicles send commitments rather than the actual bid. When the commitments need to be opened, each vehicle sends the ciphertext of (b, γ) using the public key of the fog server to the function Reveal(.). The ciphertext will be stored on the SPPIM contract rather than being sent directly to the fog

server. And we also require that the fog server should verify the correctness of the commitments opening once they are submitted. This requirement can prevent the malicious fog server from denying a correct opening of a commitment. Given a semihonest fog server, all committed bids maintain privacy from other vehicles. This ensures bid privacy.

5.4. Financial Fairness. On the one hand, in the phase of committing bids, once the bid interval is closed (after t_3 in Figure 4), vehicles cannot change their commitments. This property can help guarantee the financial fairness from preventing some vehicles' cheating, which violates the fairness.

On the other hand, the payment profile is determined by the data quality, which depends on the data accuracy and the submission time detailed as the expression $q_i = \theta\omega_i(c) + (1-\theta)\omega_i(t)$ in Algorithm 3. In our reward payment algorithm, the weight of the data accuracy $\omega_i(c)$ is calculated according to the accuracy of the submitted data measured by the Hamming distances and the vehicles' reputation. The weight of the submission time $\omega_i(t)$ is given according to the corresponding speed of each vehicle. Vehicles with good performance can get higher reward, and their reputation ranking can also be increased. It is fair, and it can also stimulate honest vehicles to submit high-quality data in time.

In addition, vehicles or TA may try to deviate from the SPPIM and aborts early to affect SPPIM execution. The aborting task initiator will be financially penalized by forfeiting its budget money deposited on the ledger, while aborting vehicles will be punished by lowering the reputation rating.

5.5. Collusion Attack Resistance. In our SPPIM, we consider the collusions among vehicles and between the fog server and the vehicles. In our winner selection algorithm, the highest bid price b_0 is limited to prevent the malicious vehicles' collusion to bid for an over large bid price. Suppose there are some colluded vehicles which submit very high bids with the purpose of getting high reward. Under this circumstance, the sum of their bids must be larger than the budget of the TA, which is not allowed in our budget-limited reverse auction model. So, the fixed highest bid price b_0 can successfully prevent this attack.

If a fog server is compromised or even colludes with some TA or some vehicles, the SPPIM can run fine. Since vehicles generate part of their credentials by themselves, private information $(k, h) \in Z_q^2$ is also kept secret by vehicles. Fog server cannot divulge identity information about any other vehicle to some colluded vehicles. Once the smart contract is deployed, it cannot be changed. The rules of the proposed SPPIM are executed faithfully via smart contracts, which can avoid the collusion between the fog server and the vehicles and between the fog server and the TA.

6. Performance Evaluation

We conduct extensive experiments to evaluate the performance of the proposed SPPIM with multiple vehicles and a task initiator TA, including the computational and storage costs of authentication, the utility of the vehicle and the TA, and the gas cost of each function on the SPPIM contract.

6.1. Authentication Performance. The process of generating an anonymous credential is of the smart contract. We make a simulation related to the acquisition of anonymous credentials. We use JAVA pairing-based cryptography library to implement the cryptographic algorithms in our simulation. The number of total vehicles requesting for anonymous credentials N_{vehicles} is set as $\{100, 200, 300, 400, 500\}$, and the number of authenticated vehicles N_{authen} is set as $\{10, 20, 30, 40, 50\}$. In each set of experiments with different number of vehicles, we took an average result of 100 times round.

When the vehicle requests for an anonymous credential, the execution time is around 38 ms and 45 ms at the vehicle side and the fog side. Figure 6(a) shows that, as the number of requesting vehicles increases, the time spent on each vehicle and the fog server almost maintains the same. When a vehicle competes for a task, the execution time of anonymous authentication is 18 ms and 25 ms at the vehicle side and the fog side. Figure 6(b) shows that the total time of the authentication is 213 ms, 451 ms, 659 ms, 1091 ms, and 2162 ms assuming $N_{\text{authen}} = \{10, 20, 30, 40, 50\}$ at the fog side.

Figure 7(a) indicates that our SPPIM requires at most 112 byte bandwidth per authentication. Only the fast authentication factor $H(k)$ and the credential $\text{cred} = (W, \nu, k, h)$ need to be transmitted to the smart contract deployed on the fog server. As the number of authenticated vehicles increases to 50, the bandwidth requirement is less than 6 kb, which is feasible.

As for the storage cost, the fog server needs to maintain a list of fast authentication factors of legitimate vehicles and its private key at the fog side. Since the number of the legitimate vehicles is large, we use bloom filter Ω to help diminish the storage overheads, which depends on the size of the bloom filter. The vehicle only stores the anonymous credential $\text{cred} = (W, \nu, k, h)$. Figure 7(b) shows that the storage cost is very small at both the vehicle and fog server side.

6.2. SPPIM Performance. From the reward payment algorithm in Algorithm 3, we get that the utility of vehicle V_i is p_i and the utility of TA is

$$u_{\text{TA}} = B_{\max} - \sum_{i=1}^{m} p_i. \tag{6}$$

The proposed SPPIM is effective because it brings profits to the task initiator and the honest vehicles. In our experiments, we study several factors that affect the utility of the vehicle and the TA, including the number of rewarded vehicles, the budget of the TA, and the data quality. The number of the rewarded

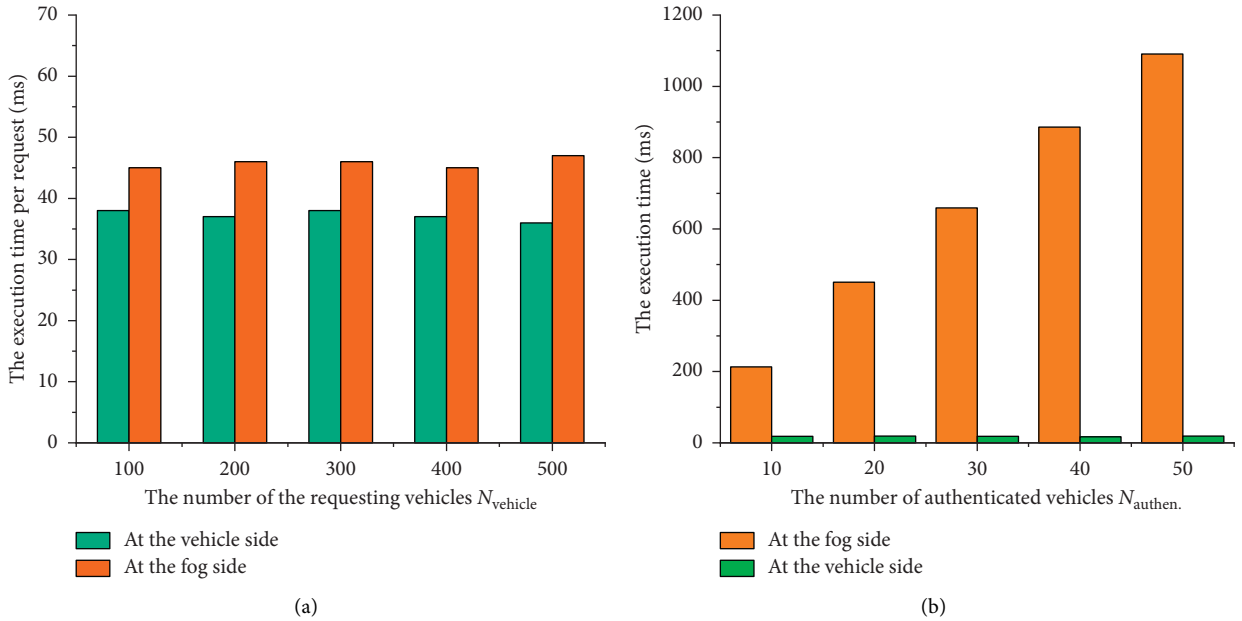

FIGURE 6: Computational costs for the vehicles and fog server: (a) computational costs of generating credential; (b) computational costs of generating authentication.

vehicles ranges from 10 to 50, and the submitted data are different in two ways: data accuracy and the submission time. As shown in Figures 8(a) and 8(b), the utility of the vehicle is nearly independent of the number of the rewarded vehicles N_{reward}, and the vehicle can get a higher utility when the budget of TA becomes bigger. Since the highest bidding price b_0 increases as the budget increases, vehicles can bid a higher price if b_0 is bigger. The utility p_i increases roughly linearly with the total bidding price of vehicles.

Figure 8(c) shows that the utility of the vehicle increases as the reputation of the vehicle increases on the premise that the data accuracy satisfies the requirement, given a fixed budget TA.budget = 200. If the submission time t_i of the vehicle is shorter (e.g., t_3 in Figure 8(c)), it can get more reward.

The utility of the TA is almost not influenced by the budget of the TA and the number of the rewarded vehicles as shown in Figure 8(d). The approximation number of the rewarded vehicles can be determined by the expression TA.budget/b_0. Once N_{reward} is fixed, the utility of the TA is determined by the payment P of the vehicles, and the average of each payment p_i is around b_0.

6.3. SPPIM Contract Cost. We implement the SPPIM contract in Solidity 0.4.18 [26] and test it on the Ethereum network. We run the experiments on a HP Pavilion Notebook with a 2.3 GHz Intel i5-6300HQ CPU and 8 GB RAM. To be specific, we create a local private Ethereum blockchain to test our SPPIM using the Geth client version 1.7.3 [27]. To realize the cryptographic algorithms on the SPPIM contract, we use Ethereum Improvement Proposals, EIP-196 [28], to fulfill elliptic curve point addition and scalar multiplication operations efficiently in the algorithm. Barreto–Naehrig E: $y^2 = x^3 + 3$ over F_q [29] is adopted in EIP-196.

Table 3 shows the consumed gas cost for different functions in SPPIM tested on the private Ethereum network where there are 20 vehicles competing for a task, and the number of the rewarded vehicles is 10. Table 3 gives the gas cost consumed by each function and the converted monetary value in US dollar. As of October 19, 2020, the ether exchange rate is 1 ether = 375.27$ [30] and the gas price is approximately 20 Gwei = 20×10^{-9} ether. We find that the financial cost of running the SPPIM contract on the Ethereum network is within reasonable bounds. The Create(.) function, to deploy SPPIM contract on the blockchain, and the Authen(.), to verify zero-knowledge proof, cost more than other functions. However, the Create(.) function executes only once to create and deploy the SPPIM contract on the Ethereum network, so it is a one-time cost and requires no more cost for its maintenance.

The cost of the Authen(.) can be seen as the price of privacy protection, which increases linearly with the number of authenticated vehicles N_{authen}, as shown in Figure 9. Note that the execution of "heavy" functions in Ethereum is impossible due to the block gas limit. In Figure 9, the gas cost is over 8m when the number of authenticated vehicles is larger than 40. When the block gas limit is 8m, the maximum value of N_{authen} should be less than 40.

Figure 10 shows the gas cost of the TA and a vehicle when the number of authenticated vehicles N_{authen} and rewarded vehicles N_{reward} varies. TA's cost increases linearly with N_{reward} as shown in Figure 10(a), while the vehicle's cost keeps constant as shown in Figure 10(b).

Figure 11 shows that the gas cost of the TA depends on the number of rewarded vehicles N_{reward}. Given a fixed N_{authen}, the gas cost of each function increases linearly with N_{reward} except for Create(.) function.

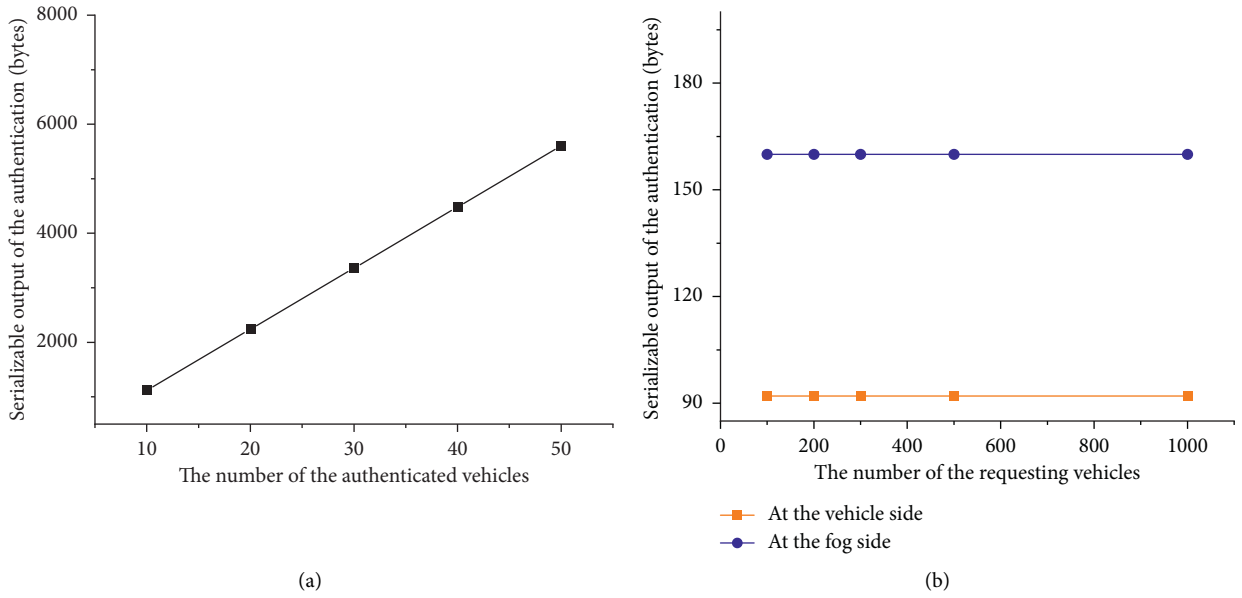

Figure 7: (a) Communication overheads between fog and vehicles; (b) storage costs at fog side and vehicle side.

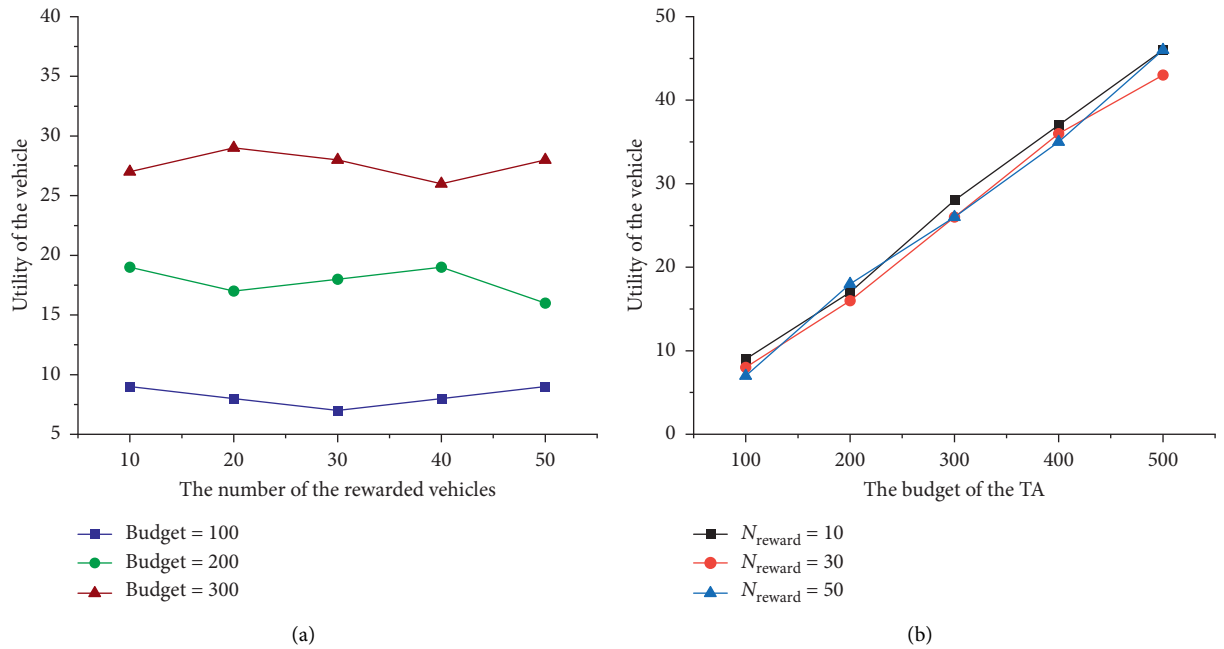

Figure 8: Continued.

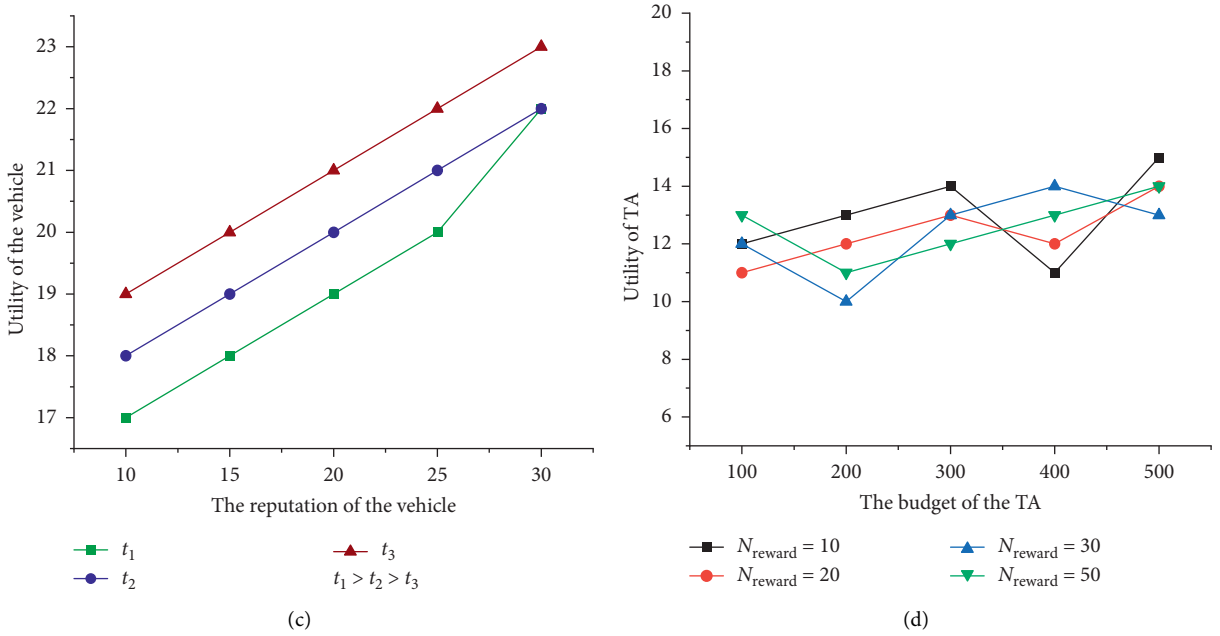

Figure 8: The utility analysis of the vehicle and the TA.

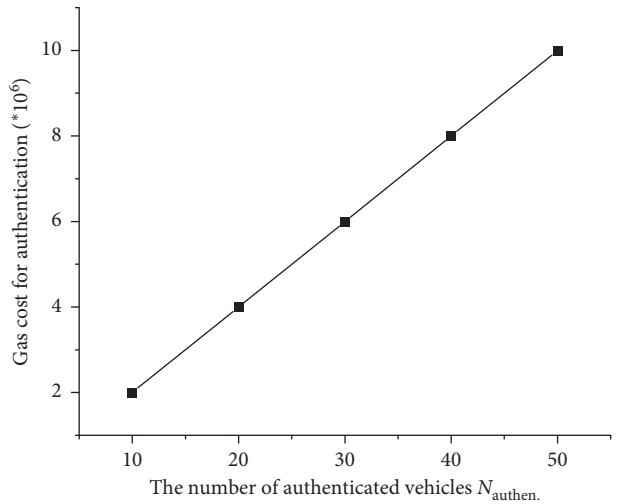

Figure 9: Gas cost for the authentication of vehicles.

7. Related Work

In this section, some related works are divided into three categories: (1) incentive mechanisms for vehicular crowd sensing; (2) blockchain-based works in vehicular network; and (3) privacy preservation for incentive mechanism in vehicular crowd sensing.

7.1. Incentive Mechanisms for Vehicular Crowd Sensing. The incentive mechanisms in vehicular crowd sensing mainly include monetary incentives and nonmonetary incentives, which stimulate vehicles via some forms of compensation, such as reputation [31], credits [32], and virtual coins [7]. Correspondingly, monetary incentive mechanism motivates vehicles to take part in tasks by financial incentives, which have stronger motivational effects and are easy to accomplish together with other incentives. Recently, Yin et al. [33] considered the scheduling problem of emergent tasks in the Internet of Vehicles and proposed a bidding mechanism to encourage vehicles to perform tasks. The winner vehicles can get some monetary reward after finishing the task. Li et al. [7] proposed an incentive announcement network, where users manage their reputation points which are earned or spent as incentives. Guo et al. [8] presented a dynamic incentive mechanism for mobile crowd

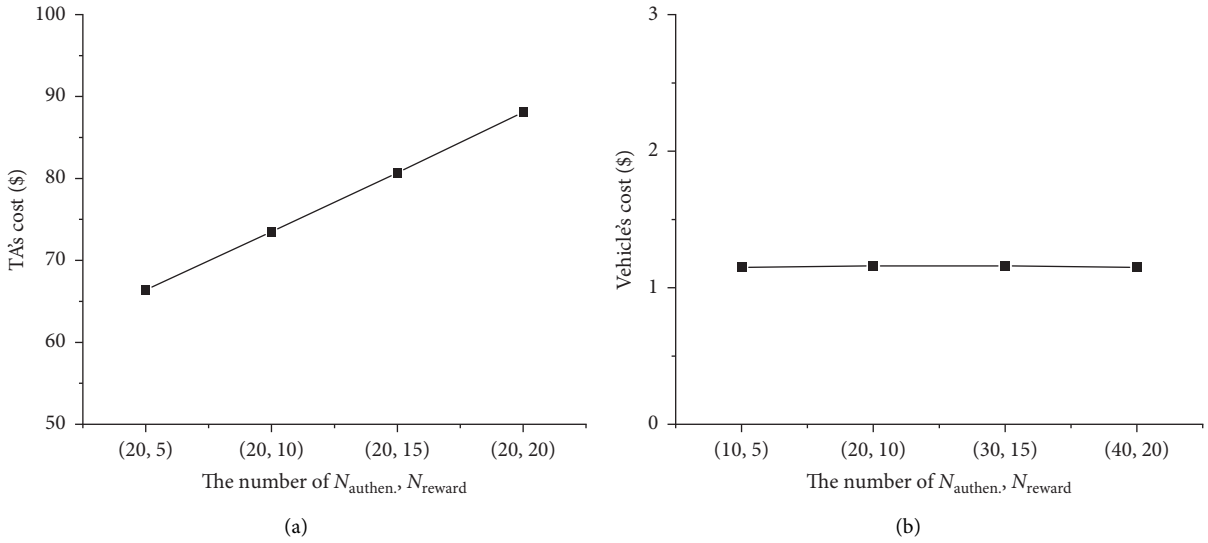

Figure 10: The average cost for the TA and a vehicle based on (N_{authen}, N_{reward}).

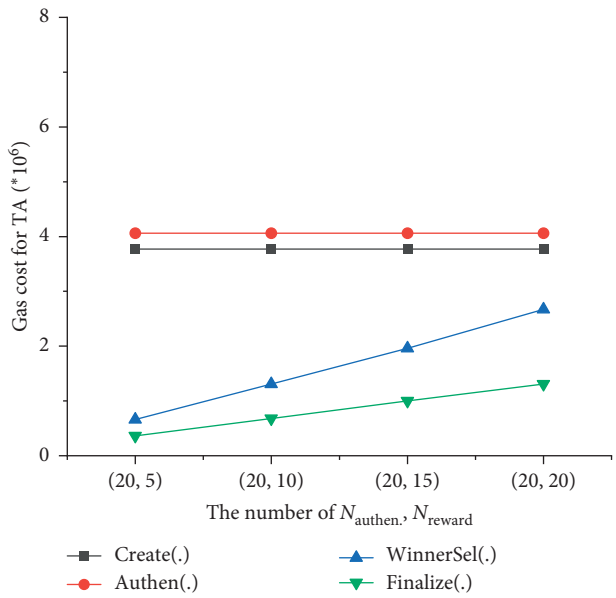

Figure 11: The gas cost for the TA based on (N_{authen}, N_{reward}).

sensing, and they pointed out that the quality of the sensing data is often neglected in the existing monetary-based incentive studies. Zhang et al. [9] presented an auction-based incentive mechanism in crowdsourcing systems, in which two allocation algorithms were given to guarantee the truthfulness and budget feasibility. In general, monetary incentives often increase user participation enthusiasm and enhance high-quality data collection habits [34]. However, most proposed monetary incentive mechanisms are centralized, which will cause privacy leakage and the single point of failure problem.

7.2. Some Works Based on Blockchain in Vehicular Network. Nowadays, there have been several works [5, 7, 35, 36] related to blockchain technology in vehicular networks. Dorri et al. [35] proposed a blockchain-based privacy-preserving communication scheme for smart vehicles. Sharma et al. [36] gave a blockchain-based transport management system in the smart city. Li et al. [7] proposed an incentive announcement network based on blockchain for smart vehicles. Li et al. [5] constructed an anonymous advertising scheme in vehicular networks. Vehicles can send transactions to the blockchain to get a predefined reward, which does not consider the data quality problem of Ad dissemination.

7.3. Privacy Preservation for Incentive Mechanism in VCS. In order to protect the privacy of vehicles, some privacy-preserving incentive mechanisms in VCS have been proposed. Lai et al. [32] took advantages of symmetric

encryption to protect personal profiles and the designated verifier signature to preserve transaction privacy in highway VANETs. Wang et al. [37] gave a node cooperation privacy protection method based on k-anonymity technology. Ten or more nodes form a k-anonymous group and submit signcrypted group data. Miners verify the legality of group data by the group blind signature algorithm that could resist against user's privacy leakage. Similarly, Wang et al. [10] utilized differential privacy technology to obfuscate bids in mobile crowd sensing. Li et al. [7] proposed a privacy-preserving incentive mechanism in VANETs. Vehicles protect their privacy by acquiring other vehicles' encrypted signatures to construct a threshold ring signature. However, there is a trusted third party who needs to generate keys and can actually trace vehicles' privacy, which is different from our SPPIM design. Lai et al. [4] utilized a blockchain-based payment system to guarantee the fairness of payments. The partially blind signature was applied to realize pseudonym management, which is designed to protect the privacy of users. However, pseudonyms are assigned by a third-party authority, which is avoided in our design. The scheme proposed by Lai et al. is simulated in MATLAB, not fulfilled on the blockchain, while our SPPIM is accomplished by the smart contract on the blockchain.

Different from existing works, we propose a hybrid solution SPPIM to address the privacy preservation and fairness problem in incentive mechanisms of VCS. Our SPPIM not only utilizes smart contracts to replace the centralized platform but also addresses the privacy-preserving problem of the vehicles and the fairness problem of the incentive mechanisms.

8. Conclusion

In this paper, we propose an effective smart privacy-preserving incentive mechanism via smart contract on the blockchain, which can ensure privacy preservation and fairness for vehicles and data quality assurance for the task initiator. Our SPPIM preserves the privacy of vehicles by utilizing zero-knowledge proof-based anonymous credentials without any trusted third party. Meanwhile, fairness-enhanced reward payments are determined by the committed bids, the reputations, and the submitted data quality of the winning vehicles. We verify the performance and the feasibility of the proposed SPPIM by implementing it on the Ethereum testnet. In the future work, we will design the optimized algorithms to enrich our current design, which can reduce the execution cost of the contract.

Data Availability

The data and VS code used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under grant 61802217 and in part by the Natural Science Foundation of Shandong Province under grant ZR2020MF061.

References

[1] L. Wang, X. Lin, E. Zima, and C. Ma, "Towards airbnb-like privacy-enhanced private parking spot sharing based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2411–2423, 2020.

[2] IoT Solutions for Smart Cities and Smart Transportation (2020), https://www.telit.com/industries-solutions/smart-cities-smart-transportation/".

[3] 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.

[4] C. Lai, M. Zhang, J. Cao et al., "SPIR: a secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 2020.

[5] M. Li, J. Weng, A. Yang et al., "Toward blockchain-based fair and anonymous Ad dissemination in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 99, pp. 11248–11259, 2019.

[6] J. Wang, M. Li, and Y. He, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, p. 1, 2018.

[7] L. Li, J. Liu, L. Cheng et al., "CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[8] B. Guo, H. Chen, Z. Yu, W. Nan, X. Xie et al., "TaskMe: toward a dynamic and quality-enhanced incentive mechanism for mobile crowd sensing," *International Journal of Human-Computer Studies*, vol. 102, pp. 14–26, 2017.

[9] Q. Zhang, Y. Wen, X. Tian et al., "Incentivize crowd labeling under budget constraint," in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2812–2820, IEEE, Hong Kong, China, May 2015.

[10] Z. Wang, J. Li, J. Hu et al., "Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform," in *Proceedings of the 2019 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2053–2061, IEEE, Paris, France, May 2019.

[11] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO '91*Springer, Berlin, Germany, 1991.

[12] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008.

[13] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[14] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *The Journal of Finance*, vol. 16, no. 1, pp. 8–37, 1961.

[15] J. Lee and B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing," in *Proceedings of the 2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 60–68, IEEE, Mannheim, Germany, April 2010.

[16] M. Xiao, K. Ma, A. Liu et al., "SRA: Secure reverse auction for task assignment in spatial crowdsourcing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 4, pp. 728–796, 2019.

[17] Y. Wei, Y. Zhu, H. Zhu et al., "Truthful online double auctions for dynamic mobile crowdsourcing," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pp. 2074–2082, Hong Kong, China, May 2015.

[18] X. Zhang, G. Xue, R. Yu et al., "Truthful incentive mechanisms for crowdsourcing," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, pp. 2830–2838, Hong Kong, China, May 2015.

[19] S. Nakamoto: Bitcoin: "A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf.

[20] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, p. 9, 1997.

[21] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: a smart contract enabled collusion-resistant e-auction," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1687–1701, 2019.

[22] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[23] T. P. P.D. Chaum, "Wallet databases with observers," in *Advances in Cryptology—CRYPTO' 92*, pp. 89–105, Springer, Berlin, Germany, 1992.

[24] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," *Advances in Cryptology—CRYPTO 2004*, Springer, Berlin, Germany, pp. 56–72, 2004.

[25] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Advances in Cryptology—CRYPTO 2004*, Springer, Berlin, Germany, pp. 41–55, 2004.

[26] Solidity 0.4.18, available: "https://solidity.readthedocs.io/en/v0.4.18/.

[27] Geth 1.7.2, https://geth.ethereum.org/downloads/.

[28] R. Christian: EIP-196: "Precompiled Contracts for Addition and Scalar Multiplication on the Elliptic Curve Alt Bn128," Ethereum Improvement Proposals, No. 196, 2017. https://eips.ethereum.org/EIPS/eip-196.

[29] P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *Proceedings of SAC 2005*, pp. 319–331, Springer, Berlin, Germany, 2006.

[30] (2020) Ethereum Price. https://ethereumprice.org/.

[31] X. Wang, J. Zhang, X. Tian et al., "Crowdsensing-based consensus incident report for road traffic acquisition," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2536–2547, 2017.

[32] C. Lai, K. Zhang, N. Cheng et al., "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559–1574, 2016.

[33] B. Yin, Y. Wu, T. Hu et al., "An efficient collaboration and incentive mechanism for Internet of vehicles (IoV) with secured information exchange based on blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1582–1593, 2019.

[34] S. Reddy, D. Estrin, M. Hansen et al., "Examining micropayments for participatory sensing data collections," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, pp. 33–36, ACM, New York, NY, USA, 2010.

[35] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: a distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[36] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: a distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, p. 84, 2017.

[37] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.