applied sciences

MDPI

Article

Reputation-Based Blockchain for Spatial Crowdsourcing in Vehicular Networks

Wenlong Guo [1], Zheng Chang [2,3,*], Yunfei Su [1], Xijuan Guo [1], Timo Hämäläinen [3], Jian Li [4] and Yuan Li [5]

[1] The Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, The College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China
[2] The School of Computer Science, University of Electronic Science and Technology of China, Chengdu 610051, China
[3] The Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland
[4] The School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China
[5] The Department of IoT Technology Research, China Mobile Research Institute, Beijing 100053, China
* Correspondence: zheng.chang@uestc.edu.cn

Abstract: The sharing of high-quality traffic information plays a crucial role in enhancing the driving experience and safety performance for vehicular networks, especially in the development of electric vehicles (EVs). The crowdsourcing-based real-time navigation of charging piles is characterized by low delay and high accuracy. However, due to the lack of an effective incentive mechanism and the resource-consuming bottleneck of sharing real-time road conditions, methods to recruit or motivate more EVs to provide high-quality information gathering has attracted considerable interest. In this paper, we first introduce a blockchain platform, where EVs act as the blockchain nodes, and a reputation-based incentive mechanism for vehicular networks. The reputations of blockchain nodes are calculated according to their historical behavior and interactions. Further, we design and implement algorithms for updating honest-behavior-based reputation as well as for screening low-reputation miners, to optimize the profits of miners and address spatial crowdsourcing tasks for sharing information on road conditions. The experimental results show that the proposed reputation-based incentive method can improve the reputation and profits of vehicle users and ensure data timeliness and reliability.

Keywords: blockchain; reputation; crowdsourcing; incentive mechanism; vehicular networks

Citation: Guo, W.; Chang, Z.; Su, Y.; Guo, X.; Hämäläinen, T.; Li, J.; Li, Y. Reputation-Based Blockchain for Spatial Crowdsourcing in Vehicular Networks. *Appl. Sci.* **2022**, *12*, 11049. https://doi.org/10.3390/app122111049

Academic Editor: Juan-Carlos Cano

Received: 1 October 2022
Accepted: 25 October 2022
Published: 31 October 2022

1. Introduction

1.1. Background

The demands for low-carbon and sustainable green energy have prompted large-scale applications of vehicular networks and accelerated the development of electric vehicles (EVs). By 2030, the number of EVs is expected to exceed 140 million [1]. EVs are integrated with many embedded devices, the use of which requires huge parallel data processing and communication capabilities. Researchers and stakeholders have proposed a crowdsourcing-aided EVs serving scheme, i.e., vehicle users involved in large-scale perception [2,3]. As increasingly multifunctional services need to make full use of the dynamic information of EVs, the crowdsourcing framework can help achieve coordination and unity between the application layer, network layer, and collection layer. The crowdsourcing system is utilized to encourage EV users to join the execution of complex tasks [4]. One of the key factors regarding the EV routing problem with recharging stations is the collection of credible road/traffic conditions [5], which also presents a major goal of crowdsourcing tasks [6]. Traditional crowdsourcing platforms usually employ a centralized cloud server to manage tasks. They are often vulnerable to a single point of failure and inadequate operational transparency. Thus, if the server is attacked, the entire crowdsourcing platform collapses.

Meanwhile, traditional crowdsourcing platforms are notorious for being untrustworthy and unfair. The distributed blockchain can also be a decentralized crowdsourcing platform. The crowdsourcing task centers on solving a task request submitted by the user, by submitting it to the blockchain and publishing it in the form of a Proof of work (PoW) problem.

Blockchain facilitates the transfer and exchange of information and data in the absence of a third-party [7]. In vehicular networks, the distributed ledger mainly monitors the legitimacy of transactions by recording the index of transactions jointly by the geographical distributed vehicles; the consensus mechanism mainly achieves the consensus, to complete the validity verification; the encryption algorithm is utilized to encrypt and decrypt keys and signatures, which renders it unbreakable. The essence, solutions and required computational resources of crowdsourcing tasks and blockchain PoW puzzles are equivalent. Different from traditional crowdsourcing platforms, since there is no third-party participation in the blockchain-crowdsourcing system, the security and efficiency are determined by computational capability or the degree of participation of vehicle nodes. As mentioned, crowdsourcing tasks are divided according to attributes, and according to attribute task assignment miners can choose sub-tasks that are suited to their abilities. The execution of the task is different from that in the traditional methodology. It is processed and executed in the blockchain network in the form of a blockchain transaction. Therefore, we can see that when the PoW problem is solved, the crowdsourcing task is completed. Taking the EV charging task as an example, customers will receive solutions by sending their task requirements (such as charging piles, road condition information, usage of the piles, traffic congestion, etc.) to the blockchain. When miners generate unresolved blocks, verification nodes are required to verify. In short, EV charging tasks are solved efficiently and safely through the blockchain.

Based on distributed ledger technology, blockchain adoption can ensure that transactions cannot be tampered or forged, an especially important consideration behind its successful application in digital economics. Blockchain provides a feasible solution for distributed edge computing deployment scenarios, e.g., Vehicular Networks [8], Drone Networks [9], Non-Fungible Tokens (NFTs) [10]. Blockchain technology can realize the distributed deployment of application services without intermediaries, so that individuals who lack trust can interact in a safe and credible manner. The security and high efficiency of blockchain technology mainly depends on the participation of a large scale of nodes, that is, more miners involved in blockchain will provide better system performance concerning security and efficiency. However, there are still some limitations that need to be solved urgently: (1) The blockchain nodes lack motivation to become involved in the blockchain, especially weak-computational ability nodes; (2) Although the blockchain nodes are mostly low-power devices, redundant computational resources are still present; (3) The blockchain ensures that damage to system security can occur only when the computational capability reaches more than 51%; however, it cannot supervise and guarantee the honest behavior of nodes. Hence, the current research focus aims at the design of a credible blockchain incentive mechanism based on a reputation framework, so that the vehicle-crowdsourcing platform can achieve credible and reasonable resource allocation.

To improve mining efficiency and incentive, we propose the utilization of cooperative pool mining to solve the proof of work puzzle, and finally achieve consensus. A mining pool refers to a resource pool where miners share their computational capabilities on the crowdsourcing blockchain framework. Miners who meet the mining pool protocols/contracts can become involved in mining by contributing computational resources, and the pool can join in computing as a cluster of miners through mining pool protocols. Vehicle miners can choose to participate in mining pools (or sidechains) according to their computational capability to obtain benefits. The benefit is the utility of pool miners, including direct and indirect rewards. The mining pool incentive distributes rewards based on the contribution of computational resources, which can directly motivate miners to participate in honest mining, referred to as direct utility; reputation is an evaluation indicator for miners' honest behavior and performance, which is generated by historical behaviors and interactions.

The combination of incentive and reputation encourages the honest participation of vehicle miners to achieve high efficiency and credible crowdsourcing task deployment.

1.2. Related Work

Recently, there has been a popular trend in blockchain structure formulation in edge-based applications, e.g., Vehicular Networks [11], Drone Networks [12] and NFTs [13]. By abstracting the terminal as a virtual node, vehicles and drones serve as edge nodes and participate in blockchain computing as miners to achieve edge computing resource coordination and system performance optimization.

In the current literature, the use of distributed crowdsourcing schemes for task solving has received significant interest. To guarantee privacy, Li et al. [14] established a blockchain-based decentralized framework for crowdsourcing system, by allowing users to store encrypted solutions in the distributed storage, and implemented a software prototype on the Ethereum public test network with a real-world dataset. To mitigate the biased evaluation of malicious requesters, Wu et al. [15] proposed a privacy-aware verification protocol leveraging the threshold Paillier cryptosystem, which dives into the concrete crowdsourcing modules and key functionalities against curious and even malicious participants, and subsequently a confident-aware TD algorithm to estimate the task truths was formulated. To address some of the existing limitations in the crowdsourcing system, Lin et al. [16] leveraged blockchain technology to study the security and privacy requirements of blockchain-based crowdsourcing systems, and proposed a concrete solution with a prototype implementation. Through inserting known result subtasks into crowdsourced computing tasks, Yang et al. [17] suggested a novel consensus mechanism (Proof of Capturing-Work) and developed the blockchain to conveniently manage trust for crowdsourcing networks. Tan et al. [18] proposed to divide the crowdsourcing service process into nine stages, and a novel Proof of Capturing-Work (PoCW) to achieve consensus, which can be managed by smart contracts during the execution of each step, to conveniently manage trust for crowdsourcing networks.

Further, some researchers have adopted the blockchain-based reputation approach to address the incentive problem of crowdsourcing participants. To handle issues concerning efficiency and safety, Kang et al. [19] introduced reputation as a metric to measure reliability and trustworthiness of the nodes, and then designed a reputation-based worker selection scheme for reliable federated learning via the use of a multi-weight subjective logic model. Moreover, they proposed an effective incentive mechanism combining reputation with contract theory to motivate high-reputation mobile devices with high-quality data to participate in model learning, in order to achieve secure reputation management for miners with non-repudiation and tamper-resistant properties. To support communication between peers, Asheralieva and Niyato [20] formulated a novel self-organized shard formation algorithm to maximize both its payoff and the coalition reputation, via the implementation of a new reputationed-based voting scheme, establishing a novel self-organized shard formation algorithm that converges to the reputation-based stable shard structure. To encourage honest behavior in IoT, a credit-based incentive approach is proposed for consensus protocol to provide a new module of reputation, so that each cooperative or non-cooperative behavior can be rewarded or punished, respectively. Miners can then share a global view of reputation [21], so as to encourage nodes to join in network collaboration. Similarly, Rehman et al. [22] proposed a novel fine-grained FL concept to decentralize the shared ML models on the edge servers, and then suggested the core requirements of fine-grained federated learning systems and the concept of the blockchain-based fine-grained reputation-aware approach in edge computing to maintain trustworthy collaborative training. Gruhler et al. [23] investigated the design, implementation, and evaluation of a reputation scheme for the Blockchain Signaling System (BloSS). The blockchain reputation scheme and the smart contract-enabled process automated reputation management were also published to diminish malicious behavior, automatically discouraging users from malicious behavior by providing necessary incentives for cooperation among

service providers and consumers. Tang et al. [24] proposed a reputation-based mechanism for the PoW mechanism computation in the blockchain, in which miners are incentivized to conduct honest mining, where the reputation depends on historical evaluation, and also suggested a new reputation-based mechanism to encourage honest mining. To prevent internal collusion among active miners, Kang et al. [25] designed a reputation-based voting scheme to ensure secure miner selection evaluation of candidates' reputation via interactions and recommended opinions, and adopted the contract theory to model the interactions between active miners and standby miners, where block verification security and delay are taken into consideration to ensure secure miner selection.

In addition, some researchers improve blockchains by applying reputation mechanisms across many scenarios. In vehicular networks, a combination of the incentive and reputation mechanisms, especially the distributed execution of crowdsourcing tasks in the vehicular networks, can motivate the vehicles and users to join in the mining process, which in turn promotes system security performance and efficiency.

1.3. Motivation and Contribution

Motivated by the aforementioned observations, especially in [24,25], we establish a reputation-based blockchain for spatial crowdsourcing in vehicular networks. Generated from historical behaviors and interactions, the combined reputation evaluation and incentive mechanism encourages vehicle miners to participate honestly in pool mining. Specifically, the main contribution of this paper are:

- A blockchain-based crowdsourcing framework is proposed for vehicular networks. Without the presence of a third-party, the crowdsourcing framework is completed based on the supervision and operation of smart contracts, which can ensure user privacy and data security.
- An incentive scheme based on blockchain reputation is designed. Estimated from the historical behaviors and interactions, honest behavior is incentivized. In addition, comprehensive reputation and local reputation will encourage more vehicle miners to provide high-quality information for real-time crowdsourcing tasks.
- An honesty behavior reputation update algorithm is proposed to determine the general necessary conditions for pool miners and iteratively obtain the benefits. Subsequently, the proportion of high-reputation miners can be increased by the proposed low-reputation miner screening algorithm, which can improve the integrity level.
- Extensive simulations are conducted to verify and analyze the proposed reputation mechanism. The results show that the incentive method proposed in this paper can improve the efficiency and data reliability of the considered spatial crowdsourcing problem in Vehicular Networks.

1.4. Structure

The remainder of the paper is organized as follows. The system model is introduced in Section 2. In Section 3, we formulate the reputation-based blockchain scheme. Section 4 proposes spatial reputation to address the problems in gathering road conditions. In Section 5, a simulation is conducted with detailed discussions provided. Finally, Section 6 provides concluding remarks.

2. System Model

2.1. System Architecture

As shown in Figure 1, we consider a reputation-based crowdsourcing platform for vehicular networks. The red EVs in Figure 1 are requested to obtain real-time road conditions, and then broadcast the task to the blockchain-based crowdsourcing platform. The crowdsourcing platform employs blockchain to conduct crowdsourcing transactions and update reputation scoring. In this context, all vehicles (white vehicles represent candidate miners and blue vehicles depict miners in service) are considered as potential miners for participating in the mining process of the crowdsourcing task.

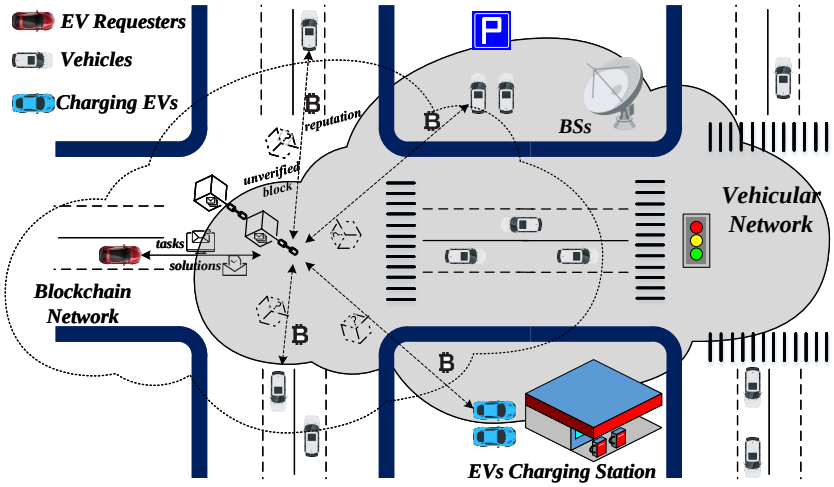

Figure 1. System model for performing spatial crowdsourcing tasks via blockchain-based interaction approach in vehicular network.

The edge network deconstructs large-scale services originally handled by the cloud into smaller and easier-to-manage parts, and distributes them to the edge nodes for processing. This process reduces latency, improves efficiency, and enhances security and privacy protection. For vehicular networks, vehicles, base stations, and edge servers will serve as edge nodes for computing, processing, and storage, which can reduce latency and improve the real-time performance of high-bandwidth applications [26]. The edge-based vehicular networks move a portion of the computational capability of the core network to the edge. The computing tasks can be selected according to real environmental conditions and constraints to perform calculations locally in the vehicle or offload to the nearest edge nodes for computing. In vehicular networks, the vehicle acting as the miner node uses its hardware capabilities to perform specific tasks, such as mining. Meanwhile, the BSs and edge servers can be utilized as trusted nodes to realize offline storage/interaction/processing. Complex and sensitive transactions can also be offloaded to high-level entities with rich computational resources. Vehicle users with weak computational capabilities are primarily utilized for securing their interaction connectivity and basic processing. Weak-capability nodes act as miners to perform normal sensing and actuation tasks, and essential blockchain functions (e.g., verification, mining, and transactions). In addition, complex PoW puzzles and corresponding benefits will also prompt vehicle users to increase their computational capability in order to obtain benefits.

The blockchain-based crowdsourcing task execution approach mainly centers on the distribution and execution of vehicle/customer tasks. Specifically, crowdsourcing task solutions are mainly divided in to distribution, execution, and recovery. For crowdsourcing distribution, we deploy execution of the transaction within the block, using the blockchain network for broadcasting. When vehicle miners receive information about crowdsourcing tasks, they will join in the computing after weighing private information (i.e., hardware capability) acting as miners. This details the mining process. Once vehicles/miners finish and publish the unverified block to the blockchain, the verification nodes/vehicles (which also contain the miners) will verify the results, representing the verification of crowdsourcing users. The first miner/vehicle to succeed is rewarded, representing recovery of the crowdsourcing task. That is, crowdsourcing within the vehicular networks is executed as a process of generating new blocks.

To fully utilize the vehicles' redundant hardware resources, the established crowdsourcing tasks are mainly aimed at lightweight applications (e.g., collaboration, feedback, collection, etc.), which is enough to support most lightweight blockchain applications. Even for computationally intensive crowdsourcing tasks, different approaches [27,28] can be adopted: offload to a higher layer network; or encourage customers to increase their

budgets, incentivizing vehicles to enhance their computational capability. To improve readability, Table 1 list the key notations.

Table 1. Summary of the key notations.

Notations	Meanings
$\mathcal{M}$	the set of all miners
$\mathcal{L}$	the set of all pools
i	the i-th pool
j	the j-th miner
$-j$	the miners except miner j
$R_j(n)$	the local reputation of miner j in the n-th round
$R_j^O(n)$	the local objective reputation of miner j
$R_j^S(n)$	the local subjective reputation of miner j
$\widehat{R}_j$	the comprehensive reputation of miner j
$\mathcal{B}_{Cs}$	the crowdsourcing side-chain
$\mathcal{B}_{-Cs}$	the remaining chains except $\mathcal{B}_{Cs}$
$N_j^{\mathcal{B}_{Cs}\to\mathcal{B}_{-Cs}}(n)$	the interactions in the crowdsourcing chain
$X^{\mathcal{B}}(n)$	the minimum number of interactions
R_j^{I}	the estimations of reputation obtained
$R_{-j}^{\mathrm{I}}(n)$	the normalized reputation evaluation of miner j
$E_f^{(i)}$	the fixed reward
$E_p^{(i)}$	the performance reward
$E_\varepsilon^{(i)}$	the participant reward
$\lvert\mathcal{L}^{(i)}\rvert$	the number of miners in the pool
$\lvert\mathcal{H}^{(i)}\rvert$	the number of honest miners in the pool
$u_j(n)$	the utility function of miner j in the n-th round
$h^{(i)}$	the entry threshold of pool i
f_j	the reputation fluctuation of miner j
T_j	the survival times
Q_j	the probability of being dishonest for miner j
$\widehat{u}_j(n)$	the accumulated estimated reward of miner j
d	the distance attribute of individual subtasks
v	the volume of budget segments
$\mathcal{L}^{(i)}$	the set of miners in pool i
D^{tar}	the distance threshold set by the requesters
κ	the number of continuous credibility
$R_{B^{Fixed}}^{(i)}$	the value of unit reputation for each segment
$f_{Screen}^{(i)}(n)$	the screening threshold of pool i
$E\left(R_j^{(i)}(n)\right)$	the expected reputation of pool i

2.2. Blockchain

A block consists of a block head and a block body. The block head plays an important role in blockchain networks by ensuring immutability [29]. Only by changing the block head, can an attacker tamper with the blockchain ledgers from the genesis blockchain, rendering their chance of success nearly impossible. The block body is responsible for recording transactions and information during the generation process, e.g., storage and processing. The details are as follows.

(1) The block head is mainly composed of the data version, block hash, merkle root, timestamp, etc. The data version records the attributes and types of accessed data. The block hash consists of both the previous and current block, thus the immutability arises precisely because the hash of the currently created block is determined by the hash of the previous block, and will act as the index of the next block hash. The Merkle root is the binary hash tree created from all transactions in the block, and each data record is hashed into Merkle tree. (2) The block body is mainly composed of data size, block interval, action

counter, block lock timer, data, etc. The block size indirectly defines the maximum number of transactions transferred within a block, mainly determined by the amount of data in the generated block. The block interval defines the waiting time for data to be written into the blockchain ledger, which is measured by the complexity of crowdsourcing tasks. The block lock timer records the last block of transactions. Further, the data part is mainly responsible for all data operations, i.e., interactions, packaging, and chaining, etc.

Blockchain technology utilizes a chain structure to verify and store data, a consensus mechanism (PoW) to generate and update blocks, cryptography algorithms to ensure the security of transmission and access, and smart contracts to program and manipulate transactions. The essence of a blockchain network is to maintain an ever-growing and immutable ledger. The blockchain can be regarded as a structured list maintained and verified based on a consensus mechanism. From a functional point of view, the processing of data in the blockchain can be divided into two parts: data-chain and node-chain. The data-chain refers to the processing and storage of block data in a chain structure; while node-chain details the information sharing by multiple nodes through interaction. In general, data are stored off-chain (data-chain), while transactions are performed on-chain (node-chain). The transactions could be collected and packaged into new blocks according to the chain structure. Driven by a consensus mechanism, the transaction records are saved in the nodes until consensus is reached [30,31]. In blockchain, the block hash is the key point of generating secure blocks. The so-called hash calculates the block to obtain an eigenvalue with a length of 256 bits. That is, as long as the block or transaction content remains unchanged, a unique 256-bit binary hash value will be obtained. The block hash calculates the hash value by hashing the block head, and then obtains the unique block. The blocks are connected in series through the hash calculations, thus forming a chain-type distributed ledger.

2.3. Smart Contract

Based on smart contracts [32], the formulated reputation-based blockchain motivates more miners to join pool mining driven by profits (i.e., reputation and incentive). The evaluation of comprehensive/local reputation can enhance the security of vehicle nodes selected as miners or validators [33]. Therefore, spatial crowdsourcing blockchain-based reputation mechanism can incentivize the participation of EV users as miners to assist in computing tasks.

The proposed distributed reputation mechanism is mainly based on the supervision and implementation of smart contracts. Specifically, it mainly executes the publishing process and recycle of crowdsourcing tasks. The design principle of the smart contract [14] includes the following connotations: User Registration Contracts (URC), User Description Contracts (UDC), Task Relationship Contracts (TRC) and Main-Side Contracts (MSC). The definitions are given as follows:

- URC. Once a miner or customer/requester joins the crowdsourcing platform, their individual information is first registered in URC. Note that when the requestor initiates service requests, the publishing of crowdsourcing tasks will be charged based on complexity (e.g., time delay, throughput, etc., see Section 4.2). In addition, miners in different blockchains are able to have multiple virtual addresses and corresponding public–private key pairs.
- UDC. The historical behaviors and interactions, individual configuration, and corresponding task information are stored by UDC. We propose to construct multiple indicators of reputation to evaluate blockchain players. Accordingly, reputation could be evaluated and updated in real-time within mining step-by-step, so as to reflect the reputation scoring. Once requesters submit the crowdsourcing information list, the creation of a corresponding pointer can help find the crowdsourcing information that they submitted through TRC.
- TRC. TRC mainly depicts the interaction between requesters and miners, including task publishing, miners' actions, incentive/reputation evaluations. In accordance

with the requesters, miners are first evaluated based on their reputation. To optimize mining strategy, qualified high-reputation miners will be allocated computational tasks according to the presented the low-reputation miner screening algorithm for mining pools under the limited budget (see in Section 4.3).

- MSC. Side chains are derived from the main chain which is a process driven by MSC. Being compatible with the smart contract from the main chain, the side chain is derived for functional scenarios, and the MSC is utilized to perform the conversion of cross-chain information (i.e., revenue and reputation). The assets of all chains are updated synchronously in real-time. Based on multiple virtual identities generated by URC, miners can allocate computing resources on multiple chains.

For clarity, we formulate logic flow diagrams to show the operation steps of the designed system in Figure 2. As illustrated, EV customers first submit the requirements of crowdsourcing tasks and establish them to the blockchain network. The blockchain network then broadcasts to all users according to UDC and URC, and deploys to the main- or side-chains for processing based on their task attributes. According to whether the tasks are deployed to multiple chains, the local reputation and comprehensive reputation of the participating miners are calculated. Consider the scenario where rational miners join in the cooperative mining, then according to the honesty behavior reputation update algorithm (Algorithm 1), if the current mining pool access and inventory conditions are not met, then they cannot join. The distance factor and the comprehensive reputation value included in the crowdsourcing task are utilized to calculate the spatial reputation. The miners in the pool are then screened according to the low-reputation miner screening algorithm for mining pools (Algorithm 2), and the lower reputation miners are excluded. Finally, after the published calculation results are verified, the miners who complete the mining gain reputation and incentive increments.

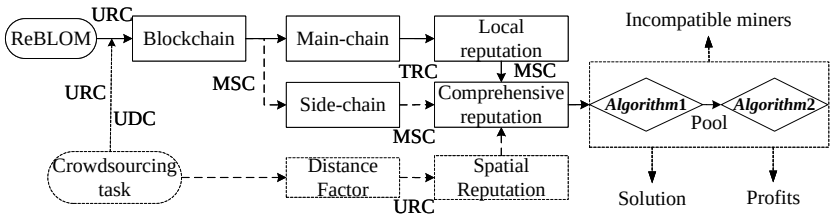

Figure 2. The logic flow diagram.

Algorithm 1 Honesty behavior reputation update algorithm

Input: The historical record, reputation entry threshold $h^{(i)}$ and the reputation fluctuation f_j.
Output: Reputation, historical record, rewards and optimal behaviors.
Initialize T_j, $B_j(a,n)$, $\overline{R}_j$
Repeat
while $n_e \in N$
for $\overline{R}_j - \frac{f_j}{\sqrt{n}t_{a/2(n-1)}} \geq h^{(i)}, \sigma_j^2 \leq \frac{h_j^2 X_a^2(n-1)}{n-1}$ and $f_j \in B_j(a,n)$.
Miner j can join the pool i to solve PoW puzzles.
Calculates f_j and $h^{(i)}$ to obtain T_j.
if $C_j = H$
$T_j \leftarrow T_j + 1$
Calculate u_j^H according to (15).
else
$T_j \leftarrow T_j - 1$
Calculate u_j^D according to (15).
do until $T_j > 0$
Calculate $\widehat{u}_j(n)$ according to (16).
Update the reputation R_j.
loop
end if
end for
end while
end

Algorithm 2 A low-reputation miner screening algorithm for mining pools

Input: $h^{(i)}$, f_j, $E\left(R_j^{(i)}(n)\right)$.
Output: $f_{Screen}^{(i)}(n)$, $|\mathcal{L}^{(i)}|$, $\sum_{i \in M_\tau^{(i)}} R_j^{(i)}(n)$.
Initialize D^{tar}, $\zeta_{\min}^c$, $R_{B_\tau}^{(i)}$.
Repeat
while $n_s \in N$
  for $\overline{R}_j - \frac{f_j}{\sqrt{n} t_{a/2(n-1)}} \geq h^{(i)}, \sigma_j^2 \leq \frac{h_j^2 X_a^2 (n-1)}{n-1}$ and $f_j \in B(a, n)$.
    Miner j can join the pool i to solve PoW puzzles.
    Randomly adjust the screening threshold $f_{Screen}^{(i)}(n+1)$.
    Screen the pool miners of high-reputation.
    if $E\left(R_j^{(i)}(n)\right) \geq f_{Screen}^{(i)}(n+1)$
      Miner could be admitted joining in $(n+1)$-th mining
      $|\mathcal{L}^{(i)}| \leftarrow |\mathcal{L}^{(i)}| + 1$
    else
      Miner j would be expelled from the first screening.
    end if
    Calculate $\sum_{i \in \mathcal{L}^{(i)}} R_j^{(i)}(n)$ and compare to $E\left(R_j^{(i)}(n)\right)$.
    do until $\sum_{i \in \mathcal{L}^{(i)}} R_j^{(i)}(n) < E\left(R_j^{(i)}(n)\right)$.
      Subtract ε from $f_{Screen}^{(i)}(n+1)$ by the ε-greedy policy.
      Update $\sum_{i \in \mathcal{L}^{(i)}} R_j^{(i)}(n)$.
    loop
  end for
end while
end

2.4. Analysis

The blockchain mainly reflected in the unique hash structure makes successful tampering or forgery impossible. In this work, the application of blockchain is mainly reflected as follows: Blockchain nodes differ according to their infrastructure and expected benefits. Most nodes participate in mining to obtain incentive and reputation from block generations. All nodes are responsible for verifying the validity of newly generated blocks. Some trusted nodes are responsible for off-chain storage of data and ledgers to obtain other rewards. It can be observed that the choice to join the blockchain depends on the resource redundancy invested in mining. In addition, rational users can quickly switch between different clusters (mainly based on the distance properties). Although some vehicles may have poor storage or computational capability, most nodes are only responsible for storing the latest transaction records of the current cluster, while trusted nodes are in charge of all ledgers. The flexibility of nodes demonstrates that their architecture mainly exists in the form of small clusters, and the task attributes are mainly related to the property. This also encourages miners to choose how to join the blockchain and how to obtain profits based on the capabilities of their infrastructure.

In the considered blockchain-based system, miners have the right to synchronously choose to become involved in computing on any chain (main- or side-chain) for profit. The profit mainly refers to the utility income of miners joining in the blockchain, including incentive and reputation. The incentive is mainly the direct utility benefits of fixed reward, performance reward and participate reward, obtained by participation in mining (or a dividend reward obtained by joining in mining pools). Reputation mainly comes from behavioral income in the blockchain network, also known as indirect utility income, and mainly includes local subjective reputation, local objective reputation and cross-chain reputation, etc. In this work, incentive and reputation are positively correlated.

3. Reputation-Based Honest Blockchain Pool Mining

Once the customers publish the computational tasks, blockchain miners are incentivized to participate in generating new blocks. Therefore, we propose a reputation-based honest blockchain pool mining mechanism (ReBLOM) in this section.

3.1. Reputation Mechanism

Reputation is defined as a comprehensive judgment on the behaviors of miners, which relates directly to the benefits/profits offered to miners. For crowdsourcing tasks in one chain, reputation mainly comes from local subjective and objective evaluation. Similarly, for complex task execution systems, in addition to local reputation, the evaluation integration of all main- and side-chains is also included.

There are $m(m \in \mathcal{M})$ miners joining in $l(l \in \mathcal{L})$ mining pools. $\mathcal{M}$ is the set of all miners, while $\mathcal{L}$ represents the set of all pools. In blockchain, the PoW consensus mechanism rewards the first node to successfully publish the solution. The miners can then receive a reward based on the proportion of their volunteered computational resources. In the process of $n(n \in N)$ times of pool mining rounds, rational miners take profit-driven actions to maximize their utility. To encourage honest actions, we suggest a reputation-based method by exploring historical behaviors and interactions. The interaction refers to the process of sending and receiving information, mainly including information plaintext, communication channel, receiver, transmission, etc. With regard to the blockchain network, it mainly refers to the process of obtaining blockchain broadcasts, publishing calculation results, accepting verification results, profit acquisition, etc.

Honest behavior means that rational miners conduct mining independently according to protocols such as smart contracts and mining pool management rules. When the optimal participation decision/strategy is obtained through continuous strategy iteration optimization, it will not seek to actively change its behavior strategy in fear of compromising its own benefits. Dishonest behavior mainly refers to selfish malicious miners adopting malicious measures/attacking (e.g., block withholding attack, selfish mining, eclipse attack and stubborn mining) to destroy mining pools, in order to fraudulently obtain benefits beyond their contributions.For the honesty attribute, the behavior strategy/decision of miners is denoted as j is $C_j = \{H, D\}(j \in \mathcal{M})$, where H and D represent the honest and dishonest behaviors, respectively. That is, while $C_j = H$, the action of miner j would be judged and recorded as honest, and the reputation and survive times will be increased; otherwise, they will be updated accordingly. Let $\mathcal{H}$ and $\mathcal{D}$ be the sets of honest and dishonest miners, respectively.

Next, the definition of reputation is given. Note that comprehensive reputation is mainly applicable to cross-chain mining, while local reputation mainly refers to the reputation obtained by pool mining on the current chain.

3.2. Local Reputation

After n-th times pool mining, the local reputation $R_j(n) \in [0, 1]$ of miner j can form a set of local reputation, which is $\mathrm{R}_j = \left[R_j(1), R_j(2), \cdots, R_j(n)\right]^T$. The reputation stems mainly from an evaluation of the historical behaviors and interactions. Consider that the local reputation evaluation consists of two parts: objective reputation $R_j^O(n)$ (see in Section 4.2) obtained via successful pool mining and subjective reputation $R_j^S(n)$ comes from the subjective reputation evaluation among all miners, which is collected from the interaction during the calculation/verification process when the blockchain crowdsourcing task is executed [25].

Accordingly, historical interaction records in recent n times are utilized to develop individual evaluation of subjective reputation $R_j^S(n)$, which is a process of information fusion based on subjective beliefs. Note that for a rational miner j, positive and honest evaluations can increase the positive effects. Since miners can also post crowdsourcing tasks as customers, such subjective reputation evaluation is of considerable significance as reference.

There exist various forms of interactions among miners, such as information exchange and data sharing. Assuming that the subjective reputation evaluation of miner j to the other members is $W_{j\to -j} = \{b_{j\to -j}, d_{j\to -j}, \gamma_{j\to -j}\}$, where $b_{j\to -j}, d_{j\to -j}, \gamma_{j\to -j} \in [0,1]$ are honest, dishonest and stochastic coefficients, respectively. Since $b_{j\to -j}+d_{j\to -j}+\gamma_{j\to -j}=1$, then we have

$$\begin{cases} b_{j\to -j} = \gamma_{j\to -j}\frac{\theta_j}{\theta_j+\vartheta_j} \\ d_{j\to -j} = \gamma_{j\to -j}\frac{\vartheta_j}{\theta_j+\vartheta_j} \\ \gamma_{j\to -j} = s_{j\to -j} \end{cases} \tag{1}$$

where θ_j and ϑ_j are the positive/honest and negative/dishonest evaluations, respectively. Then, $s_{j\to -j} = s(\alpha_j, n)$ is the uncertainty, which is positively correlated with the computational capability proportion α_j.

Subjective logic introduces the notion of uncertainty, the belief that individual miners may be in super- or partially overlapping states, to study the effect of parameters on the model. According to the subjective logic model [34], the stronger computational capability would lead to higher reputation, then the miners are less affected by subjective reputation evaluation, so the malicious evaluation of selfish miners will have less negative impacts on them. Furthermore, $j \to -j$ is the objective evaluation of j from all nodes except miner j. α_j is the computational capability proportion upon the whole blockchain. Moreover, $\alpha_j = \frac{s_j}{\sum\limits_{j\in\mathcal{M}} s_{-j}}$ is mainly determined by the CPU capability and hardware basics, where s_j is the computational resource of miner j.

We denote the computational resource proportion of miner j as α_j and $\alpha^{(i)}$ depicts the computational capability proportion of pool i among the whole blockchain network. To simplify computation, we usually utilize local reputation to characterize reputation for most tasks. This is mainly because local reputation is more informative for simple tasks, and comprehensive reputation can be easily calculated from local reputation. Furthermore, the miner j means the miner labeled j in the blockchain network, and pool (i) is the (i)-th pool, where the superscript (i) and subscript j represents the pool i and the miner j. Therefore, the subjective reputation is defined as follows

$$R_j^S(n) = \sum_{j\in\mathcal{M}} \left(b_{j\to -j} + \lambda_j \gamma_{j\to -j}\right) \tag{2}$$

where $\lambda_j \in [0,1]$ denotes the influence of computational capability of miner j.

Let the weights of objective reputation and the subjective reputation be ω_j^O and ω_j^S, respectively, the total local reputation of miner j is

$$R_j(n) = \omega_j^O R_j^O(n) + \omega_j^S R_j^S(n) \tag{3}$$

As depicted, the total reputation of miner j reflects the miner's historical behavior and computational capability.

3.3. Comprehensive Reputation

Reputation evaluation should be bound to the individual reputation/property, so it can circulate and trade in the blockchain. For the identification of cross-chain reputation, comprehensive reputation $\widehat{R}_j$ can be obtained according to the reputation conversion method based on historical interaction (cache-chain, offload-chain, etc.). We can define it as

$$\widehat{R}_j = \phi R_j + (1-\phi) R_j^{\mathrm{I}} \tag{4}$$

where R_j^{I} is the estimation of reputation obtained through multiple main- or side-chain recommendations.

In addition, the mutual evaluation between different chains can also have an impact on the overall comprehensive reputation. This is mainly to improve efficiency and make full use of the capabilities of weaker nodes, we define that the complex crowdsourcing tasks can be divided according to their properties and help to perform their own duties. As stated in the text, the side-chains are derived from the trusted node of the main chain, according to different task attributes. The main purpose is to enable miners to mine on multiple chains and update digital assets (revenue and reputation) synchronously. We also add some definitions.

Consider side-chains $\mathcal{B} = \{\mathcal{B}_{Cs}, \mathcal{B}_{Ca}, \mathcal{B}_{Down}, \ldots\}^T$ are derived from the main-chain, where $\mathcal{B}_{Cs}, \mathcal{B}_{Ca}, \mathcal{B}_{Down}$ are the crowdsourcing blockchain, caching blockchain, and offloading blockchain, respectively. $\mathcal{B}_{-Cs}$ is the collection of all chains except $\mathcal{B}_{Cs}$. Until the $(n+1)$-th mining round, the number of interactions in the crowdsourcing blockchain $\mathcal{B}_{Cs}$ with the remaining chains is $N_j^{\mathcal{B}_{Cs} \to \mathcal{B}_{-Cs}}(n)$ (the computing resources contributed by miners in different chains are independent), and the minimum number of interactions is $X^{\mathcal{B}}(n)$. Once $N_j^{\mathcal{B}_{Cs} \to \mathcal{B}_{-Cs}}(n) \geq X^{\mathcal{B}}(n)$, we have $\phi = 1$; otherwise, miner j has not gained any reputation increment, and the comprehensive reputation is calculated according to R_j^{I}.

$$R_j^{\mathrm{I}}(n) = \frac{1}{m} \sum_{j=1}^{m} R_{-j}^{\mathrm{I}}(n) \tag{5}$$

where $R_{-j}^{\mathrm{I}}(n)$ is the normalized reputation evaluation of all miners.

Then, the comprehensive reputation of miner j is

$$\widehat{R}_j(n) = \phi R_j(n) + (1-\phi) \frac{1}{m} \sum_{j=1}^{m} R_{-j}^{\mathrm{I}}(n) \tag{6}$$

3.4. Utility Function

Since the incentive problem of the blockchain $\mathcal{B}_{Cs}$ is the main priniciple of investigation, we focus on the distribution of profit and reputation in the pool. The reputation-based Shapley Value method [35] is utilized to realize the distribution of incentives, which satisfies the following conditions:

- The reward is unrelated to the order of joining in the group. Honest pool miners contribute computational resources for mining and obtain reward based on their contributed proportion.
- The miners can only obtain rewards based on contributions. There are only two roles in the mining pool, pool managers and miners. Pool managers collect management fees based on the participation, and miners receive only dividends.
- The benefits of multiple tasks do not conflict with each other. Miners can choose to contribute part of computational resources to join multiple chains. The incentive and reputation between tasks can be individually accumulated, where the proof of cross-chain assets needs to be based on side-chain protocols.
- The strategy set of pool miners consists of honest or dishonest actions, but only honesty can be rewarded.

Assume a weight value function

$$v_j^{(i)}(\alpha_j, \Delta R_j(n)) = \sum_{s \in \mathcal{H}} \omega\left(|\mathcal{H}^{(i)}|\right) \frac{\Delta R_j(n)}{R_j(n)} \tag{7}$$

where $\omega\left(|\mathcal{H}^{(i)}|\right) = \frac{(|\mathcal{M}^{(i)}| - |\mathcal{H}^{(i)}| - 1)! |\mathcal{H}^{(i)}|!}{|\mathcal{M}^{(i)}|!}$ and $\Delta R_j(n) = R_j(n+1) - R_j(n)$, $|\mathcal{M}^{(i)}|$ and $|\mathcal{H}^{(i)}|$ denote the volume of pool miners and honest miners in pool i, respectively.

Then the expected utility function (i.e., incentive) of pool i is

$$u^{(i)} = p^{(i)} E_1^{(i)} + E_\varepsilon^{(i)} - c^{(i)} \tag{8}$$

where $p^{(i)} = \frac{\alpha^{(i)}}{\sum_{j=1}^{\mathcal{M}} \alpha^{(i)}} e^{-\lambda t^{(i)}}$ is the probability of successfully rewarded, and delay function $\lambda t^{(i)}$ is related to the transactions of each block; $E_1^{(i)}$ is a combination of fixed reward and performance reward, i.e., $E_1^{(i)} = E_f^{(i)} + E_p^{(i)}$; the participant reward $E_\varepsilon^{(i)}$ depends on the degree of participation in the computing process while the new block is generated. In addition, $c^{(i)}$ is used to compensate for the cost of pool managers.

The incentive consists of fixed reward, performance reward and participant reward [36]. Among them, the fixed reward $E_f^{(i)} = E_f^{\max}\left(\frac{1}{2}\right)^{\frac{t_c}{T}}$ mainly comes from the reward generated by the block, which is related to the time slot when the miner joins the blockchain, where $E_f^{\max}$ is the constant reward from genesis block, the "half-life" is T and t_c is the time point when miners start mining; the performance reward $E_p^{(i)} = r\pi_b$ is mainly related to the number of transactions contained in the generated block, where r is an evaluation factor and π_b is the size of block; and the participant reward $E_\varepsilon^{(i)} = \varepsilon\alpha_i$ is mainly from the system compensation, which is related to the degree of computational capability involved in computing, where ε is an evaluation factor. For the blockchain network, the total reward mainly comes from the generation of new blocks and the fees from EV customers.

Then the utility function of miner j is

$$u_j(n) = u^{(i)} \sum_{\mathcal{B}} \left(v_j^{(i)}\left(\alpha_j, \Delta R_j(n)\right) - c_j \right) \tag{9}$$

where c_j is the cost of miner j.

3.5. Reputation Estimation Based on Probability Interval

When $(n+1)$-th mining round starts, the minimum criterion for joining the mining is the entry threshold $h^{(i)}(i \in \mathcal{L})$ for the pool i, and we have $\mathrm{h} = \left[h^{(1)}, h^{(2)}, \ldots, h^{(\mathcal{L})}\right]^T$. If $R_j(n) < h^{(i)}$, they are not allowed to enter pool i.

While $n \to \infty$, the reputation distribution of miner j obeys the normal distribution of $N\left(\mu_j, \frac{\sigma_j^2}{n}\right)$, where we have the expectation μ_j, variance σ_j^2 and arithmetic mean $\overline{R}_j$. Based on the confidence interval estimate, the reputation interval at the confidence level of $1-a$ could be obtained as [24]:

$$B_j(,n) = (\overline{R}_j(n) - \frac{\sigma_j}{\sqrt{n}} t_{\frac{a}{2}(n-1)}, \overline{R_j}(n) + \frac{\sigma_j}{\sqrt{n}} t_{\frac{a}{2}(n-1)}) \tag{10}$$

where $\sigma_j = \frac{1}{n-1} \sum_{n=1}^{N} \left(R_j(n) - \overline{R}_j\right)^2$.

That is, the reputation level of miner j after n-th mining is in the reputation interval $B_j(a,n)$. It can reflect the level of creditworthiness in a certain period, while the stability of the reputation is depicted by reputation fluctuation f_j. We propose a hypothesis test with confidence level of α to calculate the rejection interval, then the miner j is rejected as being dishonest within the rejection interval, i.e.,

$$\sigma_j^2 \geq \frac{f_j^2 X_a^2 (n-1)}{n-1} \tag{11}$$

3.6. Incentive Decision-Making Based on Probability Interval

Based on the above-mentioned reputation calculation process, we can limit the joining of dishonest users by setting mining pool entry conditions. Next, we explore such condition of the mining pool from the perspective of behavioral benefits (i.e., incentive and reputation).

To eliminate dishonest behaviors, we introduced the survival times $T_j(T_j \in N)$ and the probability Q_j of being dishonest. Consequently, the reputation incremental after each mining rounds also reflects the honesty evaluation of the decision-making, i.e., honest decision would produce a positive fluctuation. Then we take the reputation evaluation of miners as single variable, the problem of mining strategy could be transformed into the parameter interval estimation problem of the $0-1$ distribution. Q_j subjects to the confidence level of p as the confidence interval of $1-a$. Since the mathematical expectation and variance are $\mu_{(0,1)} = p$ and $\sigma^2_{(0,1)} = p(1-p)$, respectively, then conclusions can be obtained according to the central-limit theorem:

$$\frac{\sum_{t=1}^{N} X_t - np}{\sqrt{np(1-p)}} = \frac{n\overline{X} - np}{\sqrt{np(1-p)}}, t \in N \tag{12}$$

where p is a probability parameter of event 1.

Approximately, we have $X \sim N(0,1)$, and

$$P\left\{-z_{a/2} < \frac{n\overline{X} - np}{\sqrt{np(1-p)}} < z_{a/2}\right\} \approx 1-\alpha \tag{13}$$

Since $-z_{a/2} < \frac{n\overline{X}-np}{\sqrt{np(1-p)}} < z_{a/2}$ is equivalent to $\left(n + z^2_{a/2}\right)p^2 - (2n\overline{X} + z^2_{\alpha/2})p + n\overline{X}^2 < 0$, then we get a confidence interval (p_1, p_2) with an approximate confidence level of $1-\alpha$ for p, which is

$$p_{1,2} = \frac{1}{2\left(n + z^2_{a/2}\right)}((2n\overline{X} + z^2_{a/2}) \pm \sqrt{(2n\overline{X} + z^2_{a/2})^2 - 4\left(n + z^2_{a/2}\right)n\overline{X}^2}) \tag{14}$$

Let $p_1 \leq p_2$, then we have $1 - Q_j \in (p_1, p_2)$.

If miners maintain honesty in all iterations, they will meet the rules so as to enter pools to accumulate/slash reputation and T_j via iterations. While T_j decreases to 0, miner j is eliminated.

Next, when miners choose to engage in honest or dishonest behavior, the immediate estimation rewards would be u_j^H and u_j^D as follows.

$$\begin{cases} u_j^H = u\left(T_j, (\mu_j - h^{(i)} - \left(\frac{\sigma_j}{f_j}\right)^2)\right) \\ u_j^D = 0 \end{cases} \tag{15}$$

where $u(\cdot)$ is the utility related to the factors $(\cdot)$.

Consider the utility function of miner j is $u_j(n)$, the accumulated estimated reward would be

$$\widehat{u}_j(n) = \sum_{n=1}^{N}\left(\frac{\overline{R_j} - \mu_j}{\sigma_j^2} + Q_j u_j^H + \chi u_j(n-1)\right) \tag{16}$$

where χ is a coefficient. χ represents the comprehensive utility function of miners and the influence coefficient of the previous rounds of mining, which is mainly based on the fact that the reputation of the current round of mining behavior is affected by the previous rounds.

A reputation-based incentive method to promote honest mining is formulated in Algorithm 1 as follows. First, the miners who join the mining pool are evaluated according

to the access conditions. When the conditions are satisfied, the miners are allowed to join the mining pool for calculation, otherwise, they will be eliminated. After joining the pool, miners can solve the PoW puzzle by contributing computational resources. After successfully mining, the miners will be rewarded according to their contribution proportion. During the iteration, the current and historical behaviors of the miners can be evaluated. For honest behaviors, the miner's survival time is increased by 1, or otherwise decreased by 1. Once the survival time reaches 0, the current miner would be eliminated. At this point, the miner's revenue and reputation are updated according to (15) and (16). Until the next round starts, the judgment is made again. Obviously, the result of the algorithm is to maximize miner honesty through parameter setting, so its convergence can be guaranteed.

In next section, we will focus on a typical case where the road conditions information planned for the charging path of EVs could be packed as crowdsourcing tasks, and the spatial crowdsourcing method is used to process it by adding the distance factor.

4. ReBLOM-Based Crowdsourcing for EVs Routing Problem with Recharging Station

In this section, we focus on a typical case of EV charging, which utilizes the presented reputation-based incentive method for spatial crowdsourcing.

4.1. Spatial Crowdsourcing

Spatial reputation refers to the comprehensive evaluation of current reputation level, service ability, distance from the targets, and continuity of honesty decision-making. Obviously, higher credibility can lead to greater honest probability of solving blockchain puzzles and higher profits. Combining with the characteristics of spatial crowdsourcing, we design a spatial reputation model to motivate honesty decisions.

In this work, we consider the payment of customers with a limited budget. Note that if a rational customer has additional requirements (e.g., urgency and timeliness), they can choose to pay additional expenses to motivate more miners joining in the computing to meet its needs. We classify these expenses into the extra rewards that successfully mining pools/miners can obtain, which will produce a positive effect on the formulated incentive mechanism, which is omitted here due to space limitations.

4.2. Crowdsourcing Task for Road Conditions

As mentioned, the process of solving crowdsourcing tasks mainly includes distribution, execution and recovery. Task distribution refers to the release of road condition requests, the execution means the computing process of miners, and recovery consists of verification and reputation evaluation. Judging the decisive factors of crowdsourcing tasks can help analyze the difficulty level based on URC, and maximize the incentive effect.

Suppose the crowdsourcing task $\mathcal{T}_u = (\mathcal{T}_1, \mathcal{T}_2, \ldots)^T$ with the distance attribute d could be divided into u sub-tasks according to ingredients, the benefits and reputation bonus are divided as follows.

$$\begin{aligned} C^d_{\mathcal{T}_1} &= \omega_{1,1} V_I + \omega_{1,2} V_{II} + \omega_{1,3} V_{III} + \omega_{1,4} V_{IV} \\ C^d_{\mathcal{T}_2} &= \omega_{2,1} V_I + \omega_{2,2} V_{II} + \omega_{2,3} V_{III} + \omega_{2,4} V_{IV} \\ &\ldots \\ C^d_{\mathcal{T}_u} &= \omega_{u,1} V_I + \omega_{u,2} V_{II} + \omega_{u,3} V_{III} + \omega_{u,4} V_{IV} \end{aligned} \tag{17}$$

where the weight factors are

$$\begin{aligned} &\omega_{1,1} + \omega_{1,2} + \omega_{1,3} + \omega_{1,4} = 1 \\ &\omega_{2,1} + \omega_{2,2} + \omega_{2,3} + \omega_{2,4} = 1 \\ &\ldots \\ &\omega_{u,1} + \omega_{u,2} + \omega_{u,3} + \omega_{u,4} = 1 \end{aligned} \tag{18}$$

Then we have

$$C^d_{\mathcal{T}_u} = V_I \sum_{\eta=1}^{u} \omega_{\eta,1} + V_{II} \sum_{\eta=1}^{u} \omega_{\eta,2} + V_{III} \sum_{\eta=1}^{u} \omega_{\eta,3} + V_{IV} \sum_{\eta=1}^{u} \omega_{\eta,4} \tag{19}$$

where $V_I - V_{IV}$ are the subjective (it mainly refers to subjective road conditions, such as driving status, vehicle status, etc.), objective (the mainly objective road conditions factors), interaction (historical interaction evaluations) and stochastic factors, respectively.

In addition, $V_I - V_{IV}$ are the determining factors for the difficulty of the crowdsourcing task. Rational miners can choose their individual task preference according to the vehicle status and configuration. In this way, the system can also maximize the reward for miners to join the blockchain. To study the preference effect of multiple factors/weights, we formulate the following schemes:

- Based on the *Fuzzy Evaluation Theory* [37], the factors $V_I - V_{IV}$ (i.e., subjective, objective, interaction and objective factors) that determine the difficulty of the task can be effectively evaluated. First of all, by constructing a multi-level analysis structure model through the AHP method, the factor universe of the evaluation object can be determined; secondly, determine the comment level universe set, where a set of various total evaluation results in the evaluator creating the object to be evaluated; thirdly, establish the fuzzy relationship matrix and then determine the fuzzy weight vector of the evaluation factors, that is, assign the corresponding weights to each factor; finally, the fuzzy comprehensive evaluation model is obtained. Fuzzy evaluation deals with the fuzzy evaluation objects by precise digital means, and can make a scientific, reasonable and realistic quantitative evaluation for the data that contains the ambiguity.
- *Entropy Value Method* [38]. According to the definition of information entropy, for a special index (e.g., $V_I - V_{IV}$), we can use the entropy value to judge the degree of dispersion of an index: a smaller entropy value will lead to a greater degree of dispersion of the index, and a greater impact (i.e., weight) of the index on the comprehensive evaluation [39]. The scheme is as follows: first, the index system for evaluation needs to be determined; then, the maximum/minimum values in each index are eliminated to reduce the influence of extreme value data on the entropy; thirdly, the critical value method or Z-score method can help quantify each index, that is, converts the actual value of the index into an index evaluation value that is not affected by the dimension; finally, calculates the index entropy and weight, and obtains the index weighted calculation score. The main advantage of this method lies in the construction of a two-level evaluation system: the upper layer may need to be constructed in combination with experience, while the indicators at the bottom are more detailed and the weights are more difficult to determine.

4.3. Distance-Based ReBLOM Crowdsourcing

Spatial reputation evaluation could be solved by the mentioned reputation estimation method. The quality and the difficulty of the spatial crowdsourcing are determined by the reputation level and distance. Then the discount on reputation related to the distance is

$$\delta_j = \log_{D^{tar}} d_j^{tar} \tag{20}$$

where D^{tar} is the distance threshold set by the requesters, and d_j^{tar} is the distance between the miner j and target location. Hence, we have $\delta_j \in [0, 1]$. Accordingly, longer distances will result in a smaller discount to reputation.

Consider the continuous behavioral factor for decision-making as:

$$\zeta_j^c = \frac{\arctan(\kappa - \zeta^c_{\min}) + \arctan(\zeta^c_{\min})}{\pi/2 + \arctan(\zeta^c_{\min})} \tag{21}$$

where $\kappa(\kappa \in N)$ is the number of continuous credibility, and $\zeta^c_{\min}$ is the minimum number of credibility establishments.

When the trustworthiness of the vehicle miner is less than the minimum trust establishment times, i.e., $\kappa < \zeta^c_{\min}$, it is impossible to determine whether the trustworthy behavior continues or malicious behavior occurs. Otherwise, the miners maintain continuity, which means no malicious behavior.

Hence, a hypothetical definition of objective reputation is

$$R^O_j(n) = R\Big(\zeta^c_j, \delta_j, \overline{B}_j(\alpha_j, n), R^O_j(n-1)\Big) \tag{22}$$

According to (14), we then combine the continuity factor ζ^c_j and the comprehensive reputation records $\widehat{R}_j(n)$ for decision-making as:

$$C_j = \begin{cases} H, & p_1 \geq 0.5, c^f_j \geq 0.5; p_2 < 0.5, c^f_j \geq 0.5, \overline{R}_j > 0.5 \\ D, & else \end{cases} \tag{23}$$

In detail, if $p_1 \geq 0.5$ and $c^f_j \geq 0.5$, the decision would be honest; while $p_2 < 0.5$, $\overline{R}_j > 0.5$ and $c^f_j \geq 0.5$, the situation would also be credible honest; otherwise, decisions will be unreliable.

After successful mining, the miner will obtain the corresponding reward based on the contributed computational resources. For dishonesty, the penalty factor is determined according to the penalty function $P_j(y)$, where y is the number of lasted continuous untrustworthy services. Further, the penalty factor increases rapidly at the beginning, and then tends to remain constant. Coping with dishonest behaviors, the final benefits are

$$R^O_j(n) = \begin{cases} R^O_j(n), & C_j = H \\ P_j(y) \cdot R^O_j(n), & C_j = D \end{cases} \tag{24}$$

where

$$P_j(y) = \frac{1}{2 \times (1 + e^{-y})} \tag{25}$$

According to (6), we have the comprehensive reputation of miner j

$$\widehat{R}_j(n) = \phi\Big(\omega^O_j R^O_j(n) + \omega^S_j R^S_j(n)\Big) + (1-\phi)\frac{1}{m}\sum_{j=1}^{m} R^{\mathrm{I}}_{-j}(n) \tag{26}$$

4.4. Distance-Based Spatial Reputation for EVs Charging

Let the budget $B^{Fixed}_{\pi}(\pi = 1, 2, 3, \ldots)$ of the EV requester be limited/fixed, we divide the budget equally according to the distance into v segments. In each segment, the optimal reputation for miners of computing spatial crowdsourcing would be selected by the proposed reputation-based method, to ensure real-time feature and accuracy of the obtained spatial crowdsourcing. Similar to (19), the spatial crowdsourcing task of generating block becomes the execution of v sub-block tasks. Hence, each segment can be calculated by blockchain nodes to obtain v sub-blocks.

Taking the mining pools as individuals to solve the crowdsourcing tasks, we then transform the revenue optimization problem of the miners into pools. Obviously, a higher reputation miner within the pool would lead to a higher probability of honest mining, and thus result in a higher probability of receiving incentives. The following incentive optimization problem is proposed.

$$\begin{aligned} \mathbf{P1}: \max_{C_j=\{H,D\}} \; & u^{(i)} \\ s.t. \quad & T_j > 0 \\ & \Delta R_j(n) > 0 \\ & \kappa \geq \zeta^c_{\min} \end{aligned} \tag{27}$$

Based on (7)–(9), the incentive optimization problem can be formulated as a non-cooperation game model and solved via the convex method (as studied in our previous work in [36]). Next, we will raise the probability of honest mining by improving the occupation of high-reputation miners, to increase the probability of being rewarded.

The measurement of reputation of mining pool i is defined as in (28). It also depicts the total volume of miners joining in the pool i. That is, the value of unit reputation for each segment is

$$R^{(i)}_{B^{Fixed}_{\pi}} = \xi \frac{B^{Fixed}_{\pi}}{v \sum\limits_{i \in \mathcal{L}^{(i)}} R^{(i)}_j(n)} \tag{28}$$

where ξ is the coefficient parameters and $\sum\limits_{i \in \mathcal{L}^{(i)}} R^{(i)}_j(n)$ represents the sum of the reputation of all the miners in pool i.

Next, we suggest the screening threshold $f^{(i)}_{Screen}(n)$ of pool i illustrates the screening conditions before each mining rounds starts, where $f^{(i)}_{Screen}(n) \geq f^{(i)}$. It follows the changes of volumes of high-reputation miners and the total expected reputation of the pool.

In detail, when the n-th mining session finishes, the pool manager will randomly adjust the screening threshold $f^{(i)}_{Screen}(n+1)$ based on the mining results $u^{(i)}(n)$, the volume of high-reputation miners $|\mathcal{L}^{(i)}|$, and expected reputation $E\left(R^{(i)}_j(n)\right)$. We eventually formulate Algorithm 2 to remove the low-reputation miner from the pool, and in order to enhance the efficiency and honesty.

Based on Algorithm 1, new evaluation conditions are added to exclude low-reputation miners to retain high-reputation miners in Algorithm 2, thereby increasing the integrity level of the mining pool. After screening the candidate miners who join the mining pool, first remove the miners who do not meet the access conditions. Secondly, according to the mining pool management rules, randomly set the mining pool miner reputation screening threshold, and then sort the reputation of all candidates. Next, select miners whose reputation value is higher than the threshold, and sum up the reputation of all candidates. If it is less than the expected reputation of the mining pool, the greedy strategy is utilized to increase the value of threshold, and the evaluation is made again until the expected reputation is reached. If it exceeds the expected reputation of the pool, jump out of the loop and cull the remaining miners.

In summary, Algorithm 2 is utilized to optimize the pool screening threshold $\left(f^{(i)}_{Screen}\right)^*(n+1)$, to select a set of miners with higher reputation on the premise of meeting the expected reputation, and ultimately improving mining efficiency and ensuring integrity. Obviously, it is convergent and can exactly find the optimal $\left(f^{(i)}_{Screen}\right)^*(n+1)$ through iterations. Apart from the Quicksort algorithm, Algorithm 2 first compares $R^{(i)}_j(n) > f^{(i)}_{Screen}(n+1)$, the number of calculations is n_s, and then selects candidate miners with higher reputation. The algorithm generation complexity is $O(n_s)$ (best case), and if $\sum\limits_{i \in \mathcal{L}^{(i)}} R^{(i)}_j(n) < E\left(R^{(i)}_j(n)\right)$, thus the algorithm iterations stops. Otherwise, the iteration will continue until $\sum\limits_{i \in \mathcal{L}^{(i)}} R^{(i)}_j(n) < E\left(R^{(i)}_j(n)\right)$ are met, leading to the complexity of $O(n_s \log n_s)$ (worst case scenario, similar to the Dichotomy algorithm). Due to the limitation of space, we omit it here.

4.5. Potential Threats

In the vehicular networks, there are some widespread security threats [40] related to authentication, availability, integrity, and confidentiality. In particular, potential dangers whereby selfish malicious vehicle miners may cause damage to data communication and interaction security and the way our proposed scheme can mitigate the effects are listed here:

- "Sybil" attack: In distributed vehicle-to-vehicle communication systems, malicious attackers can claim or register different identities to disrupt normal functioning. In the vehicular environment, selfish nodes with multiple identities and malicious intent can control other vehicles/nodes at a given moment, thereby disrupting the system performance. Considering the dynamic and fast-moving nature of the vehicular networks, such attacks are easily launched by attackers, so as to cause substantial damage to the system [41]. The blockchain has the characteristics of distributed ledgering and can utilize asymmetric encryption theory to ensure the security of information interaction/communication between blockchain nodes, e.g., ECC. Secondly, URC (see in Section 2.3) can ensure the confirmation of user identity at all stages of communication, such as the corresponding key, unreproducible digital signature and unique ID, etc. Thereby users participating in blockchain cannot be forged and duplicated. Further, based on the main-side chain mechanism established by TRC and MSC, it can realize real-time synchronization of comprehensive reputation across chains and assets, where is under the premise of correct identity verification. Finally, a trusted certificate authority based on smart contracts inside the block can also verify the identity of communicating entities to prevent "Sybil" attacks.
- Denial of Service attack: In this kind of attack [7], malicious nodes can disrupt vehicle-to-vehicle communications by sending fake customer requests. That is, the attacker bombards the real server/host node with requests, so that the blockchain system perform excessive and useless calculations, rendering it unable to serve real requests. Hence, it may result in the consumption of computational resources and interruption of the normal service. As a result, EVs will not be able to obtain the required data, e.g., road conditions, and the stability of vehicular networks can even be undermined. In our scheme, when customers generate service requests, they will first submit their task requirements and publish to blockchain network. Once the validity of crowdsourcing tasks can be verified, the customer can release the tasks in the form of transactions after being paid (i.e., part of the incentive). Based on customer payment acting as a pledge, validity verification as a means, and penalty function (see in Section 4.3) as a defensive measure, it can verify customer identity and requests, thereby protecting the system from Denial of Service attack. It should be added that for miners, the historical honesty/dishonesty behaviors in each mining rounds will be recorded in the ledger, which is obviously bound to the unique ID. For the mining pool, a miner joins in by contributing computational resources, and the survival time indicator will serve as the most direct index to determine the historical honest behavior of miners.
- Man in the Middle (MITM) attack: Malicious vehicle nodes mislead real vehicles in the vehicular networks by modifying routing information. MITM [30] establishes contact with senders and receivers, respectively, from which malicious entities obtain confidential information (i.e., keys or data), and falsify information. MITM is a critical attacker as all the vehicles can be spoofed as though the information came from real nodes. The attacker accesses the vehicular system and the sent packets, modifies the real transactions, and sends them to the sink nodes. In the formulated blockchain-based reputation system, the information exchange between vehicle nodes is realized through unique paired public/private keys. The data packets transmitted by the channel are all encrypted, and excluding the corresponding key, cannot be read. Due to the characteristics of the blockchain-distributed ledger, information/data cannot be forged or tampered with unless it reaches 51% of the system's computing power. Likewise, a decentralized network structure can minimize this kind of attack.

- Malicious Trust Center attack [30]: Malicious nodes act as relay nodes and are also responsible for forwarding information/packs, but in the wrong direction. That is, malicious nodes masquerade as vehicle relay nodes that maintain a high reputation value and honest historical behavior. Similar to a black hole attack, the masquerading relay node sends a packet to a malicious node, where it is then dropped. In the traditional centralized reputation mechanism, the reputation values of vehicle miners are stored in a centralized trust center. Therefore, a malicious trust center may obtain benefits by tampering with or forging the reputation value of vehicle participants. In our proposed system, transactions are stored on the blockchain, and not on a trusted center. This ensures that the reputation value will not be tampered with by malicious nodes, and solves the potential threat brought about by malicious trust centers. Moreover, the calculation of local reputation and comprehensive reputation depends on subjective and objective reputation evaluation and cross-chain historical reputation. The information recorded in the previous block is difficult to forge or tamper with through disguise or attack.

5. Performance Evaluation

In this section, we evaluate the performance of the proposed excitation method through numerical simulation. For the proposed methods, we mainly focus on the influence of reputation thresholds and historical behaviors on the incentives of miners, e.g., the number of miners, budgets, and spatial reputation.

The structure of the performance evaluation is as follows. In Section 5.1, we considered the setting of the experimental environment and the definition of the performance specification; and then the positive effect of the incentive mechanism based on the reputation was characterized in Section 5.2; Then in Section 5.3, the performance of the spatial reputation-based crowdsourcing framework was anaylzed; finally, we compared the performance between the formulated algorithms (Algorithms 1 and 2) and the traditional Nicehash algorithm in Section 5.4.

5.1. Experiment Specification

Regarding the simulation scenarios and data, we mainly refer to the datasets of Next Generation Simulation and Mirror-Traffic, consisting of various vehicle types, road types, and road conditions. Accordingly, we then designed the simulation model suitable for this work by analyzing its data statistics and characteristics. Since it is mainly aimed at EVs crowdsourcing solutions in a finite geographical area, some of the simulation parameters are: the number of vehicles selected is $[50, 200]$, the reputation threshold is $[-1, 1]$, reputation fluctuation threshold is $[0.10, 0.30]$, and the initial reputation record of the vehicle miner is randomly selected within the given reputation range.

Furthermore, interaction parameters refer to operations (e.g., data reception and transmission), which are fed back communication parameters such as delay and throughput. Thus, the interaction parameters are quantified as system security performance and efficiency. In detail, the honest mining ratio is assessed based on the judgment of miners' historical behaviors and the reputation increment. While continuing to increase in difficulty, the act of solving crowdsourcing tasks (i.e., mining) is more efficient. It is utilized to express the probability of honest miners. In each mining round, reputation fluctuation mainly determines the upper and lower limits of the fluctuation value of reputation, which can reflect the reliability of the mining behavior within a certain mining period. Further, it can also reflect the extent of historical reputation changes. In addition, the level of spatial reputation is generated from comprehensive reputation, distance factors, etc., to express the degree of the integrity and reliability of transactions. We then define it as an indirect response to the authenticity. That is, higher reputation and reliability result in strong authenticity. Moreover, data performance can be obtained by the spatial reliability, historical data reliability and reputation.

5.2. Performance of the Reputation-Based Incentive Mechanism

We first assume that all pools are capable of reaching the optimal mining state, including honesty, fluctuations, entry thresholds, rewards, and reputation. Subsequently, focusing on the mining rounds required to reach the best state reflects the benefits offered by the proposed scheme.

(i) In Figure 3, the increase in the number of mining rounds will lead to an increase in the proportion of honest miners. This mainly results from the high reputation increasing the probability of mining and obtaining incentive, which will attract more candidate miners to become involved in the current mining pool. Thus, there will be more honest miners in the pool under the presence of the reputation threshold. Again, the horizontal axis represents the number of mining rounds required to achieve total honesty. Moreover, while the mining rounds remain unchanged, a high reputation threshold also means lower honesty. This is because the low-reputation miners can be eliminated as the reputation threshold increases. In addition, more rounds are required for the mining pool to reach the optimal state. This also confirms that the formulated algorithms can produce a positive effect on maintaining honest behavior and improving the level of reputation.

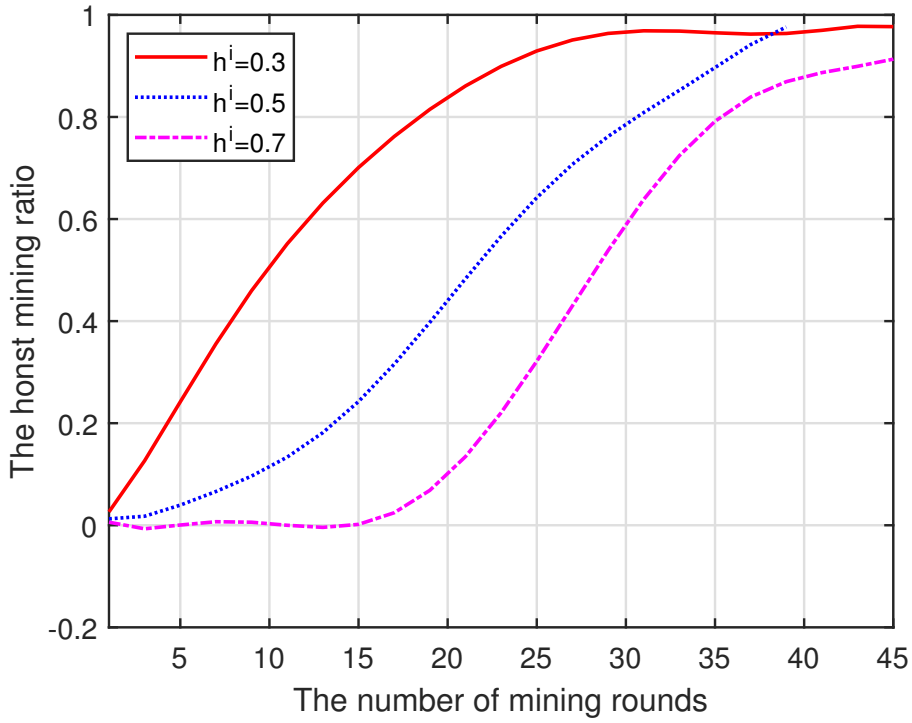

Figure 3. Mining rounds vs. Honesty.

(ii) Figure 4 shows the relationship between the number of fluctuating miners in the pool and mining rounds. As the mining rounds increase, the fluctuating miners decrease: first, it decreases faster reflecting the elimination of miners who met the fluctuation threshold; then, most miners take honest actions and the probability of being eliminated decreases. Thus, the lower reputation entry threshold will encourage more miners join the pool and decrease the number of fluctuating miners. Similar to Figure 3, the higher threshold leads to less mining rounds to arrive at the smallest fluctuation.

(iii) Figure 5 illustrates the total revenue of the pool as the number of mining rounds increases. As the number of honest miners $|\mathcal{H}^{(i)}|$ in the pool increases, the total benefit also increases. Furthermore, the faster increase is a result of the lower reputation entry threshold. In addition, if we were to fix the budget, the threshold size would directly determine the time required to reach the optimal reward, that is, smaller thresholds are able to rapidly produce a peak.

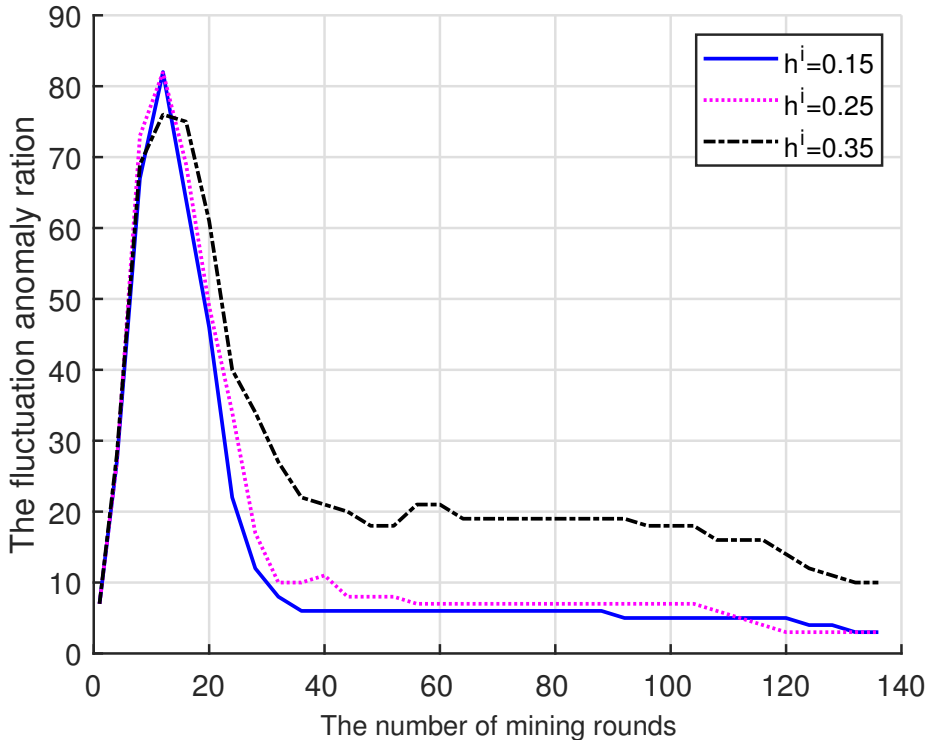

Figure 4. Mining rounds vs. Fluctuation.

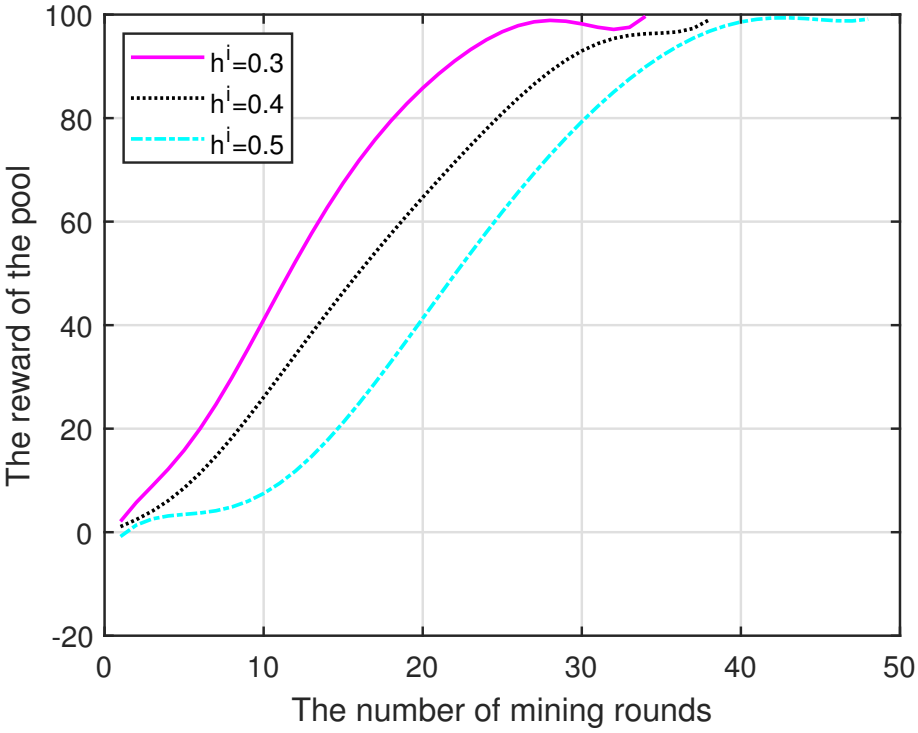

Figure 5. Mining rounds vs. Reward.

(iv) In Figure 6, it can be found that the entry threshold reputation produces a greater impact on the number of mining rounds, while the fluctuation reputation has little effect. Note that this happens while the number of mining rounds required and the proportion of honest pool miners reach the optimal level. We can also observe the changes in curve fluctuation caused by different fluctuation values.

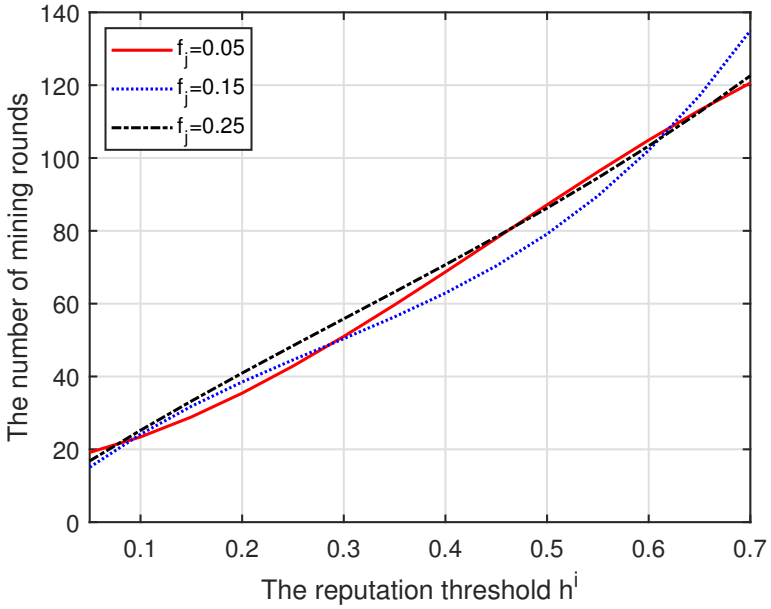

Figure 6. Reputation vs. Mining rounds.

(v) Figure 7 illustrates the relationship between the number of vehicles participating in the calculation and the overall pool reputation. As the amounts of players increases, the sum of their reputations will gradually increase. Moreover, the slope gradually decreases before it starts to slowly decrease. This is mainly due to the fact that: when an increasing number of vehicles have just joined the pool, the reputation level will increase; however, once the number of vehicles exceeds the peak, dishonest miners are eliminated as a result of the joining threshold implemented, and then a slow downward trend begins.

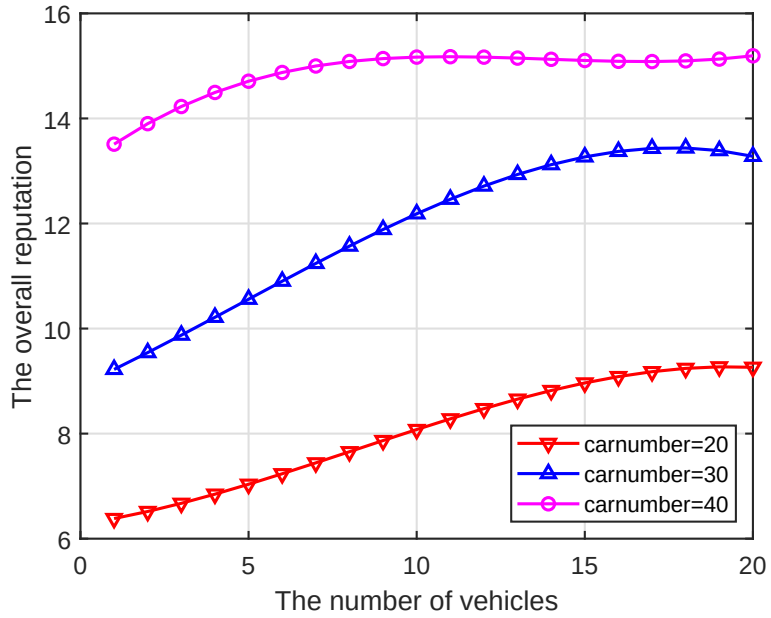

Figure 7. Vehicles vs. The overall reputation.

5.3. Performance Based on Spatial Crowdsourcing Reputation

This section details the characterization of the performance for spatial reputation, which contains nearly 50 missions.

(i) As we can see in Figure 8, the increase in the number of vehicles will directly lead to increased data collected to complete the crowdsourcing missions, thereby shortening the mission time and improving the efficiency of road-condition gathering. Due to budget

constraints, the collected data will drop from the peak and then shift back and forth. In addition, the greater increases produced a larger amount of provided data. Eventually, different budgets could bear a significant impact on the size of the collected data.

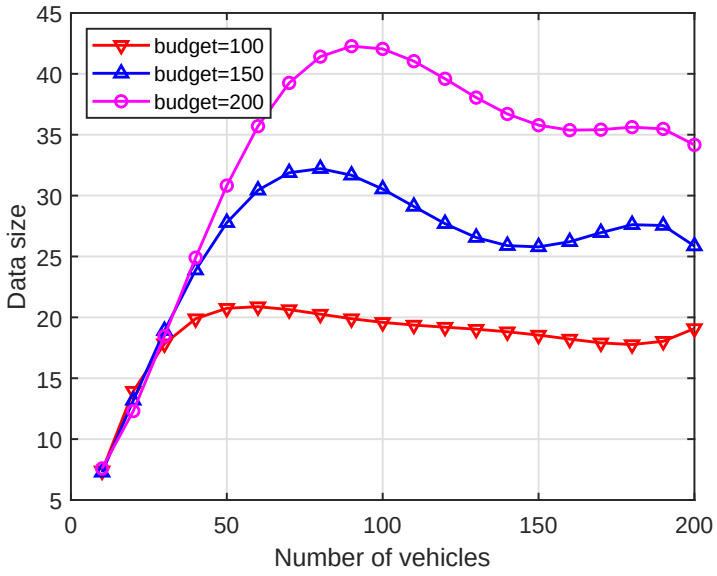

Figure 8. Vehicles vs. Data size.

(ii) As plotted in Figure 9, a high-reputation entry threshold has considerable impact on the data authenticity. The impact of the threshold on authenticity shows a trend of first decreasing and then increasing. This is mainly because a high reputation threshold leads to a lower overall reputation level, until it subsequently promotes more users with a background of honest behavior to join and enhance the reputation of the pool.

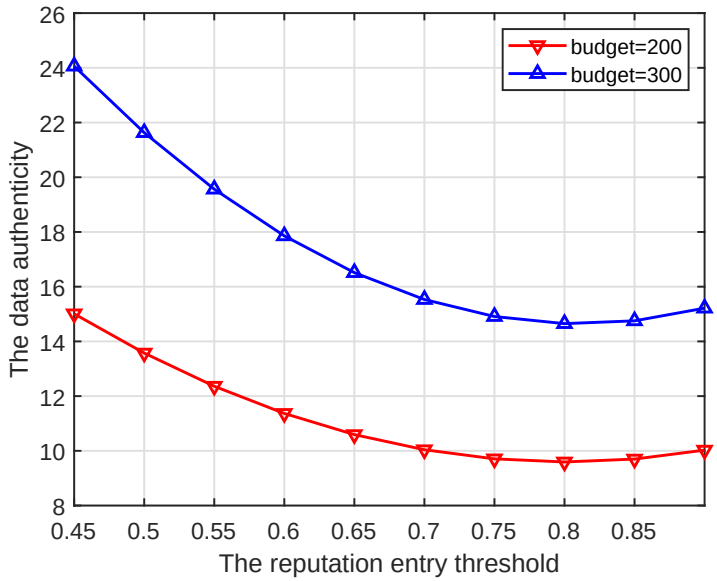

Figure 9. Entry threshold vs. Data authenticity.

(iii) We can see from Figure 10 that the increase in the number of vehicles participating in crowdsourcing tasks leads to improved data authenticity. As such, a farther distance from the target location (effective radius) would motivate more miners to become involved in the computing. This is because more blockchain users will improve the security of task in computing and verifying. This can also be analyzed from the perspective of budget, that is, a longer radius generates higher budgets, which in turn inspires more users to participate.

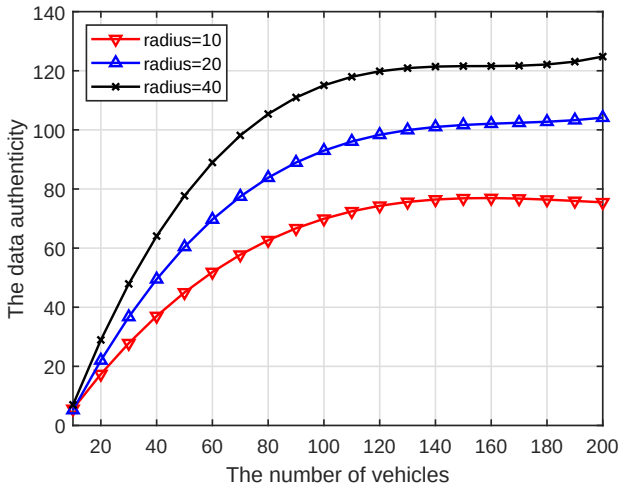

Figure 10. Vehicles vs. Data authenticity.

5.4. Algorithm Performance

Consider three pools named A, B and C, in which Algorithms 1 and 2 are deployed to the pool B and C. Among them, pool A adopts the general mining pool random algorithm (the original algorithm used in NiceHash platform [42])). Note that any miners who successfully reached the entry condition of pool A can select to join A and make the mining decisions, while miners who join pool B and C need to satisfy the conditions of Algorithms 1 and 2.

(i) As shown in Figure 11, once the iteration progresses, the effect of Algorithm 1 on the mining pool converges and fluctuates continuously. This is mainly because in each round of mining, miners who have completed mining choose to enter/exit the current pool/blockchain, based on their incentive and reputation. Obviously, the peaks and troughs of the proposed Algorithm 1 generates better effects. We can find that the averages of A and B are approximately equal to 14 and 17, respectively. The main reason for this is that under the action of Algorithm 1, miners demonstrating low-reputation and dishonest behaviors cannot meet the access conditions of B. Similarly, in Figures 12 and 13, it can be easily concluded that the probability of successful mining and the miner's income (with equal reputation and computation capability) generated by B have improved, i.e., Algorithm 1 is better than that of the general random sampling algorithm. Further, compared with the Figure 14, the mean value of C is about 20, and $C > B > A$, which means that the blockchain-based crowdsourcing system based on the spatial reputation has produced better positive effects.

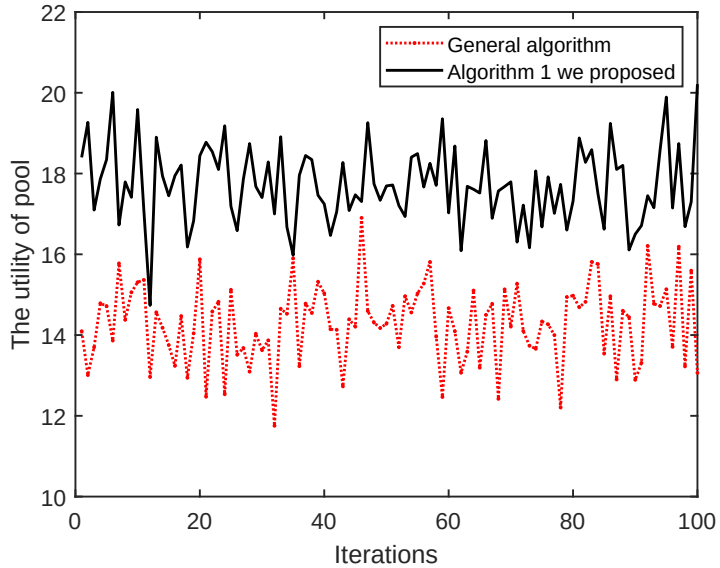

Figure 11. Iterations vs. The utility of pool.

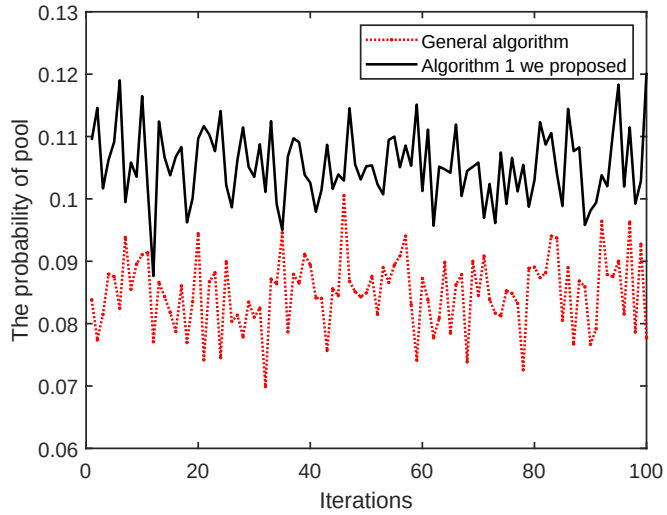

Figure 12. Iterations vs. The probability of pool.

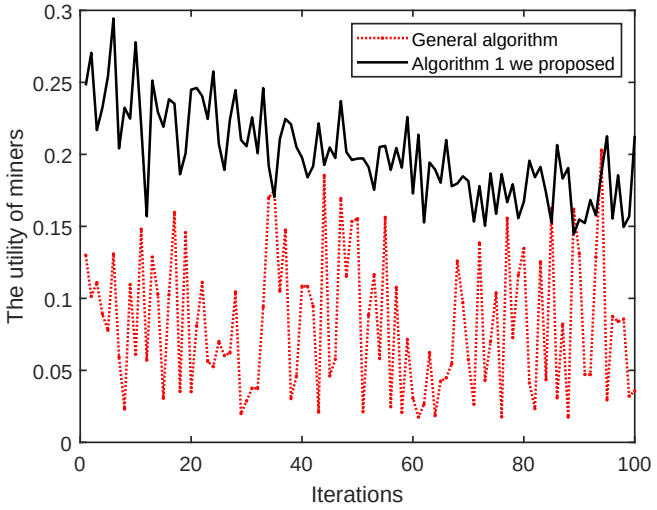

Figure 13. Iterations vs. The utility of miners.

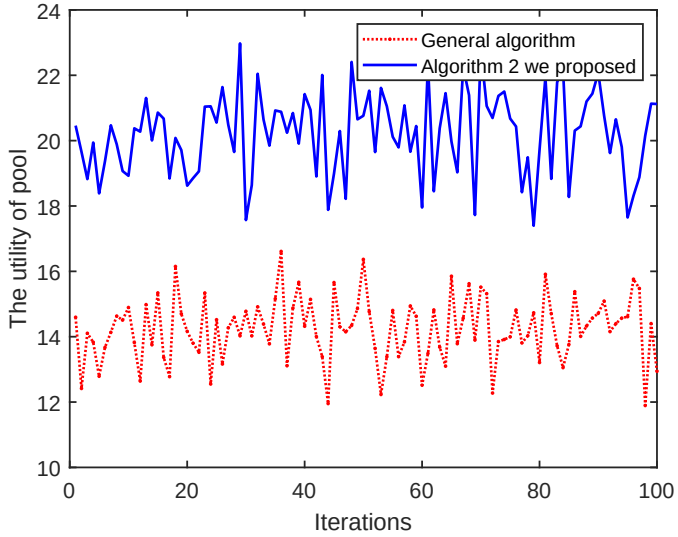

Figure 14. Iterations vs. The utility of pool.

(ii) In Figure 14, as the iterations increase, pool C can obtain significantly higher returns than A. This is mainly because Algorithm 2 mainly excludes low-reputation miners in each round, so the total reputation of the pool C is higher than A, which also leads to higher returns for the mining pool. In addition, pool C has a higher overall probability of successful mining in Figure 15. Based on the blockchain consensus mechanism, this also means that the computational capability of pool C is stronger, and it also shows the positive correlation between reputation, computational capability and profits. We then choose two miners with equal reputation and computational capability in A and C, respectively, to illustrate the profits of pool miners in Figure 16. It also shows that high-reputation miners obtain higher profits in pool C, mainly because pool A contains some low-reputation/dishonest miners, which damages the overall mining capacity and reputation of pool A. In addition, after analyzing the profits of single miner, it is found that the overall trend in C is one of decline, mainly because when we set a threshold for the iterations to screen low-reputation, the reputation of miners in C were successively evaluated. The reduced reputation value, however, is still higher than A, which also validates the assumed model.

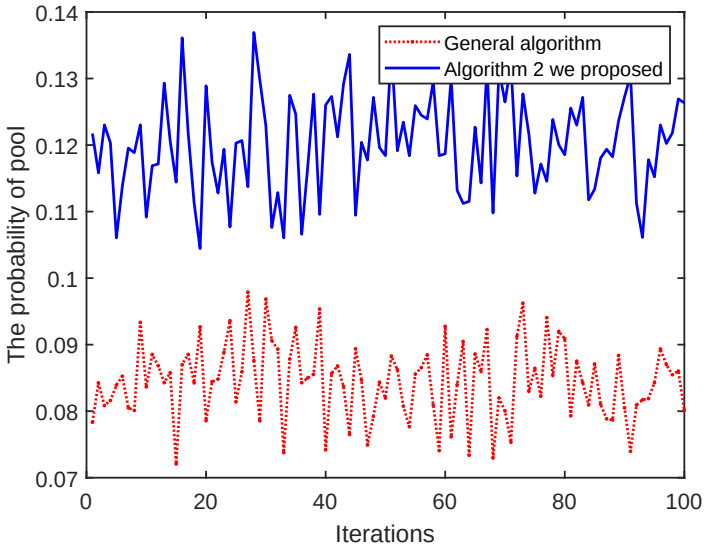

Figure 15. Iterations vs. The probability of pool.

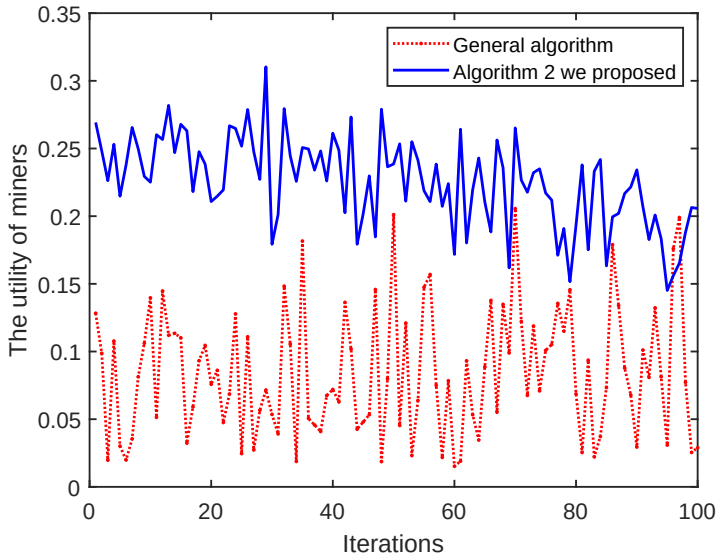

Figure 16. Iterations vs. The utility of miners

(iii) In addition, comparing B with C, C is better than B in terms of utility, probability of successfully and miner's profits. That is because Algorithm 2 has stricter conditions and thresholds when screening low-reputation miners, and thus produces better results. Further, since the security and efficiency of the blockchain structure are mainly determined by the computational capability, this also provides supporting evidence that the proposed algorithms can enhance system security and improve efficiency.

6. Conclusions

In this paper, we present a reputation-based decentralized spatial crowdsourcing framework for vehicular networks. Generated by historical behaviors and interactions, reputation can solve problems regarding truthfulness and continuity, and motivate vehicle users to provide high-quality crowdsourcing of road conditions. Next, the honesty behavior reputation update algorithm and low-reputation miner screening algorithm for the pool mining are utilized to improve the trustworthiness and efficiency. Through simulation study, the proposed method is shown to be capable of optimizing the revenue of miners and motivating high-quality crowdsourcing tasks of road conditions under a limited budget.

Although the proposed blockchain–crowdsourcing model can improve the security performance and efficiency of the system, there are still some challenges to be overcome. For example, the threat of attacks (e.g., 51% attack and withholding block attack) brought about via rapid derivation of the chains; the balance of profit and consumption of joining the crowdsourcing tasks; and the synchronization of cross-chain transactions and currencies caused by fast-driving EVs and complex crowdsourcing transactions. These also represent the crucial points currently limiting the application of blockchain in vehicular networks. In the future, we will also work on optimizing the model to address the above issues.

Author Contributions: Conceptualization, W.G. and Y.S.; methodology, W.G. and Y.S.; software, W.G. and Y.S.; validation, W.G., Z.C. and Y.S.; formal analysis, W.G., Z.C. and Y.S.; investigation, W.G., Z.C., Y.S., X.G., T.H., J.L. and Y.L.; writing—original draft preparation, W.G. and Y.S.; writing—review and editing, W.G., Z.C. and X.G.; supervision, Z.C., X.G., T.H., J.L. and Y.L.; funding acquisition, Z.C. and X.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by NSFC under Grant 62071105, Innovation Capability Improvement Plan Project of Hebei Province (22567626H), CSC funding (202108130129), the joint project of China Mobile Research Institute& X-NET (2022H002), the 131 project, the fund project of Intelligent Terminal Key Laboratory of Sichuan Province (SCITLAB-1015).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, R.; Wang, J.; Zhang, B. High Definition Map for Automated Driving: Overview and Analysis. *J. Navig.* **2020**, *73*, 324–341. [CrossRef]
2. Galvagno, A.; Previti, U.; Famoso, F.; Brusca, S. An Innovative Methodology to Take into Account Traffic Information on Wltp Cycle for Hybrid Vehicles. *Energies* **2021**, *14*, 1548. [CrossRef]
3. Okwuibe, G.C.; Li, Z.; Brenner, T.; Langniss, O. A Blockchain Based Electric Vehicle Smart Charging System with Flexibility. *IFAC-PapersOnLine* **2020**, *53*, 13557–13561. [CrossRef]
4. Zhu, S.; Cai, Z.; Hu, H.; Li, Y.; Li, W. Zkcrowd: A Hybrid Blockchain-Based Crowdsourcing Platform. *IEEE Trans. Industr Inform.* **2020**, *16*, 4196–4205. [CrossRef]
5. Das, H.S.; Rahman, M.M.; Li, S.; Tan, C.W. Electric Vehicles Standards, Charging Infrastructure, and Impact on Grid Integration: A Technological Review. *Renew. Sust. Energ. Rev.* **2020**, *120*, 109618. [CrossRef]
6. He, Y.; Zhang, C.; Wu, B.; Geng, Z.; Xiao, K.; Li, H. A Trusted Architecture for Ev Shared Charging Based on Blockchain Technology. *High-Confid. Comput.* **2021**, *1*, 100001. [CrossRef]
7. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]

8. Wang, X.; Garg, S.; Lin, H.; Kaddoum, G.; Hu, J.; Hassan, M.M. Heterogeneous Blockchain and Ai-Driven Hierarchical Trust Evaluation for 5g-Enabled Intelligent Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, 1–10. [CrossRef]
9. Babel, M.; Gramlich, V.; Körner, M.-F.; Sedlmeir, J.; Strüker, J.; Zwede, T. Enabling End-to-End Digital Carbon Emission Tracing with Shielded Nfts. *Energy Inform.* **2022**, *5*, S1. [CrossRef]
10. Alsamhi, S.H.; Shvetsov, A.V.; Kumar, S.; Hassan, J.; Alhartomi, M.A.; Shvetsova, S.V.; Sahal, R.; Hawbani, A. Computing in the Sky: A Survey on Intelligent Ubiquitous Computing for Uav-Assisted 6g Networks and Industry 4.0/5.0. *Drones* **2022**, *6*, 177. [CrossRef]
11. Gao, L.; Li, L.; Chen, Y.; Xu, C.; Xu, M. Fgfl: A Blockchain-Based Fair Incentive Governor for Federated Learning. *J. Parallel Distrib. Comput.* **2022**, *163*, 283–299. [CrossRef]
12. Alsamhi, S.H.; Shvetsov, A.V.; Shvetsova, S.V.; Hawbani, A.; Guizan, M.; Alhartomi, M.A.; Ma, O. Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. *IEEE Trans. Green Commun. Netw.* **2022**, 1. [CrossRef]
13. Chiacchio, F.; D'Urso, D.; Oliveri, L.M.; Spitaleri, A.; Spampinato, C.; Giordano, D. A Non-Fungible Token Solution for the Track and Trace of Pharmaceutical Supply Chain. *Appl. Sci.* **2022**, *12*, 4019. [CrossRef]
14. Li, M.; Weng, J.; Yang, A.; Lu, W.; Zhang, Y.; Hou, L.; Liu, J.N.; Xiang, Y.; Deng, R.H. Crowdbc: A Blockchain-Based Decentralized Framework for Crowdsourcing. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 1251–1266. 2881735. [CrossRef]
15. Wu, H.; Düdder, B.; Wang, L.; Sun, S.; Xue, G. Blockchain-Based Reliable and Privacy-Aware Crowdsourcing with Truth and Fairness Assurance. *IEEE Internet Things J.* **2022**, *9*, 3586–3598. [CrossRef]
16. Lin, C.; He, D.; Zeadally, S.; Kumar, N.; Choo, K.-K.R. Secbcs: A Secure and Privacy-Preserving Blockchain-Based Crowdsourcing System. *Sci. China Inf. Sci.* **2020**, *63*, 130102. [CrossRef]
17. Yang, H.; Wang, G.; Zhai, Z.; He, X. Towards Decentralized Trust Management Using Blockchain in Crowdsourcing Networks. In Proceedings of the 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China, 29–30 October 2020. [CrossRef]
18. Tan, L.; Xiao, H.; Shang, X.; Wang, Y.; Ding, F.; Li, W. A Blockchain-Based Trusted Service Mechanism for Crowdsourcing System. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020. [CrossRef]
19. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Zhang, J. Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory. *IEEE Internet Things J.* **2019**, *6*, 10700–10714. [CrossRef]
20. Asheralieva, A.; Niyato, D. Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in Iot Blockchains with Mobile-Edge Computing. *IEEE Internet Things J.* **2020**, *7*, 11830–11850. [CrossRef]
21. Wang, E.K.; Liang, Z.; Chen, C.-M.; Kumari, S.; Khan, M.K. Porx: A Reputation Incentive Scheme for Blockchain Consensus of Iiot. *Future Gener. Comput. Syst.* **2020**, *102*, 140–151. [CrossRef]
22. Rehman, M.H.u.; Salah, K.; Damiani, E.; Svetinovic, D. Towards Blockchain-Based Reputation-Aware Federated Learning. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020. [CrossRef]
23. Gruhler, A.; Rodrigues, B.; Stiller, B. A Reputation Scheme for a Blockchain-Based Network Cooperative Defense. In Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 8–12 April 2019.
24. Tang, C.; Wu, L.; Wen, G.; Zheng, Z. Incentivizing Honest Mining in Blockchain Networks: A Reputation Approach. *IEEE Trans. Circuits Syst. II Express Briefs.* **2020**, *67*, 117–121. [CrossRef]
25. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh.* **2019**, *68*, 2906–2920. [CrossRef]
26. Alsamhi, S.H.; Almalki, F.A.; Afghah, F.; Hawbani, A.; Shvetsov, A.V.; Lee, B.; Song, H. Drones' Edge Intelligence over Smart Environments in B5g: Blockchain and Federated Learning Synergy. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 295–312. [CrossRef]
27. Liang, X.; Yan, Z.; Kantola, R. Gaimmo: A Grade-Driven Auction-Based Incentive Mechanism with Multiple Objectives for Crowdsourcing Managed by Blockchain. *IEEE Internet Things J.* **2022**, *9*, 17488–17502. [CrossRef]
28. Alsamhi, S.H.; Almalki, F.A.; Al-Dois, H.; Shvetsov, A.V.; Ansari, M.S.; Hawbani, A.; Gupta, S.K.; Lee, B. Multi-Drone Edge Intelligence and SAR Smart Wearable Devices for Emergency Communication. *Wirel Commun. Mob. Comput.* **2021**, *2021*, 6710074. [CrossRef]
29. Liu, W.; Wu, H.; Meng, T.; Wang, R.; Wang, Y.; Xu, C.-Z. Aucswap: A Vickrey Auction Modeled Decentralized Cross-Blockchain Asset Transfer Protocol. *J. Syst. Architect.* **2021**, *117*, 102102. [CrossRef]
30. Wang, Y.; Su, Z.; Zhang, N. BSIS: Blockchain-Based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network. *IEEE Trans. Industr Inform.* **2019**, *15*, 3620–3631. [CrossRef]
31. ElSalamouny, E.; Sassone, V. An Hmm-Based Reputation Model. In Proceedings of the Advances in Security of Information and Communication Networks, Cairo, Egypt, 3–5 September 2013.
32. Malik, N.; Wei, Y.M.; Appel, G.; Luo, L. Blockchain Technology for Creative Industries: Current State and Research Opportunities. *Int. J. Res. Mark.* 2022, *in press*. [CrossRef]
33. Camilo, G.F.; Rebello, G.A.F.; Souza, L.A.C.d.; Duarte, O.C.M.B. A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020. [CrossRef]

34. Oren, N.; Norman, T.J.; Preece, A. Subjective Logic and Arguing with Evidence. *Artif. Intell.* **2007**, *171*, 838–854. [CrossRef]
35. Shen, M.; Duan, J.; Zhu, L.; Zhang, J.; Du, X.; Guizani, M. Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1229–1241. [CrossRef]
36. Guo, W.; Chang, Z.; Guo, X.; Wu, P.; Han, Z. Incentive Mechanism for Edge Computing-Based Blockchain: A Sequential Game Approach. *IEEE Trans. Industr. Inform.* **2022**, *18*, 7899–7909. [CrossRef]
37. Sharifi, M.; Manaf, A.A.; Memariani, A.; Movahednejad, H.; Dastjerdi, A.V. Consensus-Based Service Selection Using Crowd-sourcing under Fuzzy Preferences of Users. In Proceedings of the 2014 IEEE International Conference on Services Computing, Anchorage, AK, USA, 27 June–2 July 2014. [CrossRef]
38. Houda, Z.A.E.; Hafid, A.S.; Khoukhi, L. Cochain-Sc: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using Sdn and Smart Contract. *IEEE Access*. **2019**, *7*, 98893–98907. [CrossRef]
39. Xia, D.; Xu, J.; Liu, W.; Zhao, X.; Zhang, R.; Li, Y.; Su, S. Ev Charging Guidance Strategy Considering Dynamic Road Network and Personalized Driving Conditions. In Proceedings of the 2019 IEEE 3rd International Electrical and Energy Conference (CIEEC), Beijing, China, 7–9 September 2019. [CrossRef]
40. Kumar, S.; Velliangiri, S.; Karthikeyan, P.; Kumari, S.; Kumar, S.; Khan, M.K. A Survey on the Blockchain Techniques for the Internet of Vehicles Security. *Trans. Emerging Telecommun. Tech.* **2021**, e4317. [CrossRef]
41. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil Attacks and Their Defenses in the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [CrossRef]
42. Yuen, M.C.; Lau, K.M.; Ng, K.F. An Automated Solution for Improving the Efficiency of Cryptocurrency Mining. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 7–11 January 2020. [CrossRef]