applied sciences

MDPI

Article

Analysis of Malicious Node Identification Algorithm of Internet of Vehicles under Blockchain Technology: A Case Study of Intelligent Technology in Automotive Engineering

Jing Chen [1,*], Tong Li [2] and Rui Zhu [3]

[1] School of Information, Yunnan University, Kunming 650500, China
[2] School of Big Data, Yunnan Agricultural University, Kunming 650201, China
[3] School of Software, Yunnan University, Kunming 650091, China
* Correspondence: cjing@mail.ynu.edu.cn

Abstract: False messages sent by malicious or selfish vehicle nodes will reduce the operation efficiency of the Internet of Vehicles, and can even endanger drivers in serious cases. Therefore, it is very important to detect malicious vehicle nodes in the network in a timely manner. At present, the existing research on detecting malicious vehicle nodes in the Internet of Vehicles has some problems, such as difficulties with identification and a low detection efficiency. Blockchain technology cannot be tampered with or deleted and has open and transparent characteristics. Therefore, as a shared distributed ledger in decentralized networking, blockchain can promote collaboration between transactions, processing and interaction equipment, and help to establish a scalable, universal, private, secure and reliable car networking system. This paper puts forward a block-network-based malicious node detection mechanism. Using blockchain technology in a car network for malicious node identification algorithm could create a security scheme that can ensure smooth communication between network vehicles. A consensus on legal vehicle identification, message integrity verification, false message identification and malicious vehicle node identification form the four parts of the security scheme. Based on the public–private key mechanism and RSA encryption algorithm, combined with the malicious node identification algorithm in the Internet of Vehicles, the authenticity of the vehicle's identity and message is determined to protect the vehicle's security and privacy. First, a blockchain-based, malicious node detection architecture is constructed for the Internet of vehicles. We propose a malicious node identification algorithm based on the blockchain consensus mechanism. Combined the above detection architecture with the consensus mechanism, a comprehensive and accurate verification of vehicle identity and message authenticity is ensured, looking at the four aspects of vehicle identification, accounting node selection, verification of transmission message integrity and identification of the authenticity of transmission messages. Subsequently, the verification results will be globally broadcast in the Internet of Vehicles to suppress malicious behavior, further ensure that reliable event messages are provided for the driver, improve the VANET operation environment, and improve the operation efficiency of the Internet of Vehicles. Comparing the proposed detection mechanism using simulation software, the simulation results show that the proposed blockchain-based trust detection mechanism can effectively improve the accuracy of vehicle node authentication and identification of false messages, and improve network transmission performance in the Internet of Vehicles environment.

Keywords: blockchain technology; intelligent technology; internet of vehicles; malicious nodes; identification algorithm

Citation: Chen, J.; Li, T.; Zhu, R. Analysis of Malicious Node Identification Algorithm of Internet of Vehicles under Blockchain Technology: A Case Study of Intelligent Technology in Automotive Engineering. *Appl. Sci.* **2022**, *12*, 8362. https://doi.org/10.3390/app12168362

Academic Editors: Pijush Samui, Aydin Azizi, Ahmed Hussein Kamel Ahmed Elshafie, Yixia Zhang and Danial Jahed Armaghani

Received: 22 May 2022
Accepted: 8 August 2022
Published: 21 August 2022

1. Introduction

Establishing an intelligent transportation system using the Internet is a wise choice. This kind of intelligent system is used in the field of transportation: using the real-time

interactions between cars, trains and boat vehicles to coordinate data on their trajectory and running state can to help alleviate the frequent road safety accidents, improve the robustness of network security, etc. As a more advanced system in the field of transportation, the intelligent transportation system has good prospects for the future development of intelligent transportation. The intelligent transportation system could combine computer science, sensors, the Internet of Things and AI technology and be applied to the delivery of goods, service management and vehicle production. This would further strengthen the relationship between vehicles, roads and users, accelerate improvements in driving safety, reduce road jams and reduce the energy losses caused by the construction of a new transportation management system. The connection of the vehicle, the driver and the road is the core role of the intelligent transportation system. At the same time, the intelligent transportation system can also provide the corresponding service management agency. According to the analysis of relevant research conclusions, the use of intelligent transportation system can provide more intelligent road information for locomotives, and can also promote the vehicles can easily obtain the state information in front of any road, and make more effective use of road infrastructure and other resources. A large number of scholars in the field have shown that, with the use of intelligent transportation system technology, traffic jams in the next 20 years will be reduced to 40%, the existing road blockage problems will be effectively solved, the traffic accident rate could be reduced by 8%, and the resulting accident deaths would be reduced by 30~70%, which is of great significance for the healthy growth in domestic transportation and stable economic development. In recent years, the safety problems with Internet of Vehicles systems have gradually become a research hotspot. The Internet of Vehicles has the characteristics of complex dynamic topology changes, rapid vehicle movement, and unreliable transmission, which means that both the internal and external network are faced with security threats, such as malicious attacks. This means that solving the network security problems has become a great challenge. In recent years, VANET has been proposed as the basis of ITS to improve traffic efficiency and ensure the safety of vehicles and drivers. As VANET is characterized by its dynamic topology, high mobility, and variability, it is vulnerable to various attacks originating from malicious nodes. Malicious nodes in the Internet of Vehicles will broadcast and forward false traffic warning messages for selfish purposes, which will lead to traffic congestion, threaten people's lives, damage the entire VANET network function and affect its performance. They also discard received messages or refuse to help other vehicle nodes to forward messages. To enable the vehicle to operate normally and communicate on the road, it is necessary to detect false information in a timely fashion. Therefore, ensuring VANET security has become a pervasive area of research, and issues related to identifying malicious nodes and creating messages remain the focus of VANET security research.

2. Application of Regional Chain Technology in the Internet of Vehicles

The deep integration of the Internet of Things, computers, mobile communication and other technologies with intelligent transportation promotes the wide application of vehicular communication and computing equipment in vehicles. This also transforms vehicles from traditional vehicles to mobile devices with computing communication abilities. This makes communication between vehicles possible, leading to the birth and rapid rise of Internet of Vehicles technology. The Internet of Vehicles is essentially a dynamic communication system for communication between vehicles and mobile public networks. The Internet obtains the data that are shared with the vehicle, and analyzes data on the vehicle and road, vehicle and the driver, the driver and the driver, and the relationship between the driver and the third-party service providers. According to the analysis, the existence of the above relationship can be used to solve the urban traffic problems, and thus help to manage the urban intelligent transportation. In recent years, the safety problem of Internet of Vehicles systems has gradually become a research hotspot. The Internet of Vehicles has the characteristics of complex dynamic topology changes, fast vehicle movement, and unreliable transmission; therefore, both the internal and external network are faced with

security threats such as malicious attacks, which mean that solving the network security problems has become a great challenge.

The network environment of the Internet of Vehicles is very complex and changeable. The authentication and trust detection methods of on-board and network (VANET) technology are not applicable to the Internet of Vehicles network environment, because this can only handle a small number of simple event requirements, and cannot effectively store, query and trace big data on vehicles. With the development of blockchain technology as a new technology solution, the problems regarding storing and querying big data on the Internet of Vehicles can be solved. The blockchain core technology consensus mechanism can ensure the security and reliability of data transmission in the network. In actual intelligent transportation applications, recording transactions' traceability through the blockchain can effectively and strongly ensure behavior traceability and responsibility backtracking, achieve fairness and justice, and promote the efficient operation of various affairs. In practice, the security risks in the Internet of Vehicles are still very large, so we need to pay closer attention to the harm caused by malicious node attacks. The rational use of blockchain technology is of great significance to the process of detecting malicious nodes in the Internet of Vehicles. The vehicle status can be globally broadcast to fundamentally suppress malicious behavior, thus ensuring that the driver is provided with reliable event messages.

Therefore, to reduce the security threat problem and network security problems, and protect the security and privacy of vehicles, it is necessary to improve the malicious node identification of the Internet of Vehicles, as well as to reasonably determine vehicle identity and the authenticity of the information. Based on this, this research chose to use a malicious node identification algorithm, focusing on the implementation of malicious node identification algorithms in the Internet of Vehicles under regional chain technology, and judge the main value of malicious node identification algorithms in the Internet of Vehicles.

3. Research Status Quo

Many domestic and foreign researchers have put forward corresponding detection and identification methods to resolve network security problems in the Internet of Vehicles.

This paper applies blockchain technology to the Internet of Vehicles to detect and identify malicious nodes, and solve the problems in the traditional Internet of Vehicles trust model. Abboud, K., Omar, H.A., et al. [1] proposed a method using RFID technology, which is implemented by verifying the vehicle's interactions with the cloud while driving on the road. According to the statistics, the vehicle will use electronic tags to send the data requiring authentication to the cloud storage, and the cloud storage will authenticate the vehicle data after receiving the information, and broadcast the information in the cloud network. Lu Zhongmei, Chen Wei, et al. [2] proposed a vehicle privacy protection method that combines the certificates issued to a vehicle by a trusted agency and pseudonyms authorized by a trusted agency to build an intelligent privacy authentication system to jointly authenticate a vehicle's identity. However, due to the frequent communication problems in the Internet of vehicles, the certification requirements cannot be met efficiently and in a timely manner. These schemes enable the vehicle to communicate on the road according to the pseudonym produced by the authority, and authenticate the identity of the vehicle through interaction with the RSU. However, these schemes are relatively dependent on the RSU, which leads to the problem of excessive RSU workload [3–5].

The application of blockchain in the Internet of Vehicles derives from the following research conclusions. VANET traditional certification and trust detection methods have many problems, which make it difficult to adapt them to the complex networking network environment. Traditional security mechanisms can only deal with a few simple events, cannot store vehicle big data, and struggle with problems regarding queries and traceability. The rise of blockchain technology means that it could be a way to solve the problems with new technology for networking security [6]. Arushi A, Kumar YS, et al. [7] propose a certified and secure data transmission algorithm to ensure that real information is communicated between nodes. The authors also introduced blockchain to some of the connected car

services to improve efficiency. However, the vehicle needs to be registered at a centralized authority, and the system still has a single-point-of-failure problem. Wagner M, Mcmillin B, et al. [8] proposed a new blockchain architecture with local, physically verified transactions. With this new architecture, they proposed a protocol that protects vehicle self-organized networks (VANET) that do not regularly communicate with the RSU or other infrastructure components. In addition, they proposed a way to overcome the real-time challenges of applying Bitcoin's blockchain to disconnection by changing the transaction validation mechanism and blockchain management process, and adding a trusted CA.

In sum, the security risks in the Internet of Vehicles are great, and the harm caused by malicious node attacks cannot be ignored. Existing methods to reduces these risks in the Internet of Vehicles have been effective in their target applications, but they also face several technical challenges, including the need to improve detection accuracy and enhance privacy protection. Some scholars have applied blockchain technology to the Internet of Vehicles to solve these security and trust problems. Blockchain technology leads to decentralization and means that information cannot be tampered with, and the existing blockchain technology is used to detect malicious nodes. However, the accuracy of security messages and the malicious node detection rate need to be further improved. Therefore, the reasonable use of blockchain technology to detect malicious nodes in networks requires further research and exploration [8].

4. Application of Blockchain Technology in the Internet of Vehicles

4.1. Blockchain Technology

Blockchain technology is essentially a distributed database that stores a large amount of data, with specific transactions on each block, and notes the time when messages occur. They are connected in chronological order to form a chain structure [9]. A block in a blockchain is simply called a list of records, while a blockchain can be regarded as a record chain composed of many blocks, forming a public ledger that records a lot of encrypted data. The ledger is publicly shared among individual users. Each transaction is recorded into a new block, in which the recorded data are unchangeable and time-linked [10]. Finally, together, these new blocks form a complete blockchain in chronological order. The blockchain provides secure shared databases, ledgers, and transaction logs without being managed by central trusts [11–13]. The consistency and synchronization of the data in a blockchain are achieved through a consensus mechanism, in which a group of participants in a distrust peer network collaborate in a fully transparent way and only accept valid transactions [14]. However, Bitcoin was originally designed without taking privacy into consideration. By viewing the ledger, any public key can be used to trace back to one's real identity [15].

4.2. Structure of the Malicious Node Identification Algorithm

The ways in which vehicles communicate with each other using VANET can be divided into the following three main categories of message transmission: beacon messages, early warning messages, and entertainment messages [16–19]. Warning messages have the highest priority level among the three messages, mainly because they may threaten the performance of the Internet of Vehicles, and even affect the personal safety of drivers and passengers. In essence, the main function of early warning messages is to send road safety warning messages to the vehicle as soon as possible when an emergency occurs, making them is very important for safe driving [20]. This study mainly focuses on the authenticity of traffic early warning messages in VANET. The warning message report table is shown in Table 1.

Table 1. Warning message report form.

Event ID	Event Type	TTL_{Event} (Lifecycle of the Warning Message)	Ran_{msg} (Transmission Range of the Alert Message)
I	Traffic congestion	$Th_{t\text{-}I}$	$Th_{d\text{-}I}$
II	Traffic accident	$Th_{t\text{-}II}$	$Th_{d\text{-}II}$
III	Road construction	$Th_{t\text{-}III}$	$Th_{d\text{-}III}$
IV	Road icing	$Th_{t\text{-}IV}$	$Thd_{\text{-}IV}$

Emergencies are divided into the following four categories: traffic jams, traffic accidents, road construction, road icing [21]. The lifetime and transmission range of the alert message for each emergency are recorded. After the analysis, different types of early warning messages were found to have different life cycles and transmission ranges for the four categories of traffic jams, traffic accidents, road construction and road icing. The scheme structure diagram expression is shown in Figure 1.

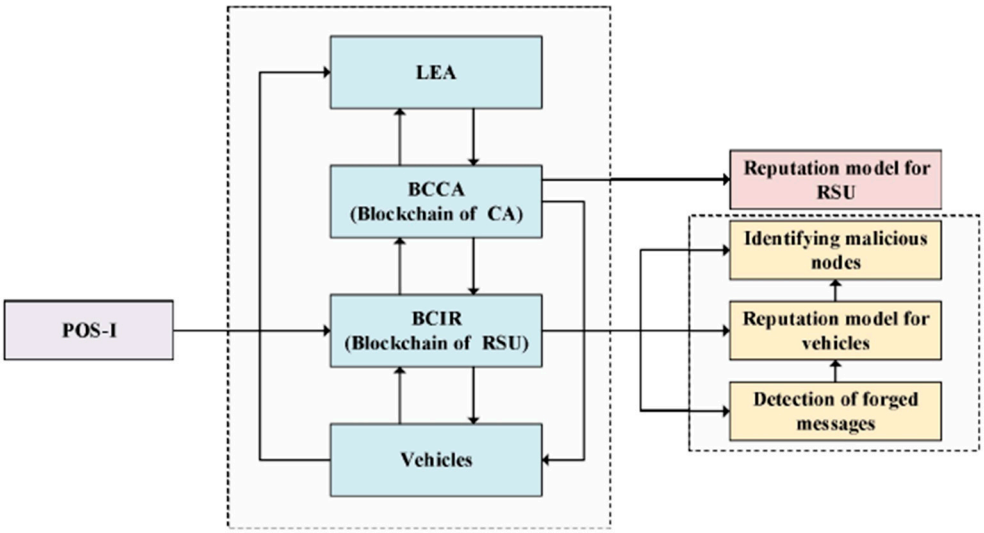

Figure 1. Schematic structure diagram.

4.3. Authentication Algorithm

There are several authentication algorithms: authentication based on shared key, authentication based on biological features, and public key encryption algorithm. Different authentication methods also have different security levels. This paper adopted the authentication method based on the shared key, which means that the server side and the user share one or one set of passwords. When the user requires authentication, the user submits a password that is jointly owned by the user and the server, either by entering the password or through a device that holds the password.

A set of vehicles in the Internet of Vehicles are set to V, obtaining:

$$V = \{V_1, V_2, V_3, \ldots V_i, V_j \ldots V_n\}$$

In the above formula, any vehicle source sending a message node is represented by V_j (source sending message node), and V_i (target receiving message node) represents the target receiving the message node. After V_j sends a message to V_i, V_i carefully verifies the integrity of the message, and then produces a series of interactive behaviors with other entities in the network [22,23]. If the alert message issued by V_j is acquired by V_i, then V sends out the collected messages. The information is sent to the nearest roadside unit (RSU) in the communication range, and the RSU must identify the information and determine whether the information is legal. After the data package sent by V_i is received by RSU, the first step in judging the message's credibility is make an accurate judgment of whether

V_i has a legal identity [24–29]. When combined with CA (authentication center in the network), the detailed authentication verification process is as follows:

Step 1. For the RSU within the vehicle communication range, vehicle V_i transmits the request, based on which the message received from vehicle V_j is recognized [30].

Step 2. After the RSU receives the request, a pseudonym containing vehicle V_i is sent with a PID_v instead. A random number (L) is reported to the nearest surrounding CA for authentication. L is randomly produced by a linear congruence generator (LCG). The LCG calculation is described as follows [30]:

$$\begin{cases} L_0 = \mathrm{d} \\ L_{\mathrm{r}+1} = (A \times L_r + Z) \mathrm{mod}(M) \end{cases}$$

In this formula, d represents the seed value, the current system time is its set initial value, the increment value is Z, multiplier is A, modulus size is M, and Z and M are prime. Generally, M will take the power square of 2.

Step 3. If the CA receives information from the RSU, the RSU will conduct a traceability search of the real situation of vehicle V_{i} using vehicle mapping, according to the pseudonym of vehicle V_i in the first step, and obtain the real vehicle identity information accordingly. An audit result (report) is produced after the search. In the audit results, if the false vehicle information is backed up in the results, then vehicle V_{i} is legal; if there is no record, then vehicle V_i is an illegal vehicle. Then, a random key, L, is encrypted using a private key (PR_{CA}) to generate a session key K_n. After the encryption of a random key L, a private key (PR_{CA}) is used to generate a session key, K_n. After using K_n for report encryption, $E_{K_n}[report]$ is obtained. After completing the above work, the RSU receives an encrypted message. By taking the result of the public key (PK_{j}) encryption under the RSU, the corresponding generating encryption function is as follows (E represents the encryption function, and the encrypted ciphertext is C):

$$E : C = E_{PB_{RSU}}[E_{PB_{RSU}}[K_n] \| E_{k_n}[report]]$$

Step 4. When the inspection results after CA encryption are transmitted to the RSU, the RSU uses the private key (PR_{RSU}) to decrypt the generated ciphertext C, corresponding to $E_{PB_{\mathrm{Rsu}}}[K_{\mathrm{n}}]$ and $E_{K_n}[report]$. Based on the above, the RSU key is used to decrypt $E_{PB_{\mathrm{Rsu}}}[K_{\mathrm{n}}]$, and the obtained session key is K_n. After the same operation, the report views the audit results of CA, to make the final judgment on whether vehicle V_i is legal. The detailed decryption function is as follows (D represents the decryption function):

$$D : [E_{PB_{RSU}}[K_n] \| E_{k_n}[report]] = D_{PB_{RSU}}[C]$$

After completing the above four steps, the RSU can make an accurate judgment regarding the legitimacy of vehicle V_i.

4.4. POS Consensus Algorithm Improvement

Compared with other traditional consensus algorithms, the main purpose of the nodes in BCIR is to fake the message verification using computer technology. Therefore, this study set up a new consensus mechanism POS1 algorithm for VANET: (1) If RSU wants to participate in the selection of bookkeeping node, it will register with CA the first time the selection of a new bookkeeping node is initiated, and will submit a part of the deposit according to the standard. This can become a candidate and enter the next step of bookkeeping selection. (2) All RSU applications are accepted by the CA, and the full energy value of the RSU will be updated. The algorithm updates are as follows:

Part 1. No matter which RSU has its own initial energy value in the blockchain network, in VANET, the RUS performs the very diverse work. For example, it actively participates in campaign billing nodes; assists CA in verifying vehicle identity information; forwards packets and assists in verifying vehicle messages; broadcasts messages; etc. Due to the differences the behavior of the participating network, the energy value of the RSU will also change. For example, in VNAET, when RSU broadcasts information, the energy will undergo a changing consumption trend. To give RSU enough encouragement, RSU

needs to receive enough energy return, and the reward should be greater more than the amount of energy consumed to continue smoothly.

Part 2. The size of the RSU registration number needed to participate in the accounting node election is the variable, where any RSU corresponds to ITS own k value (energy value). If the number is 0, then $k = 0$.

Part 3. In the new round with several bookkeeping choices, CA records any registered RSU as R_n; the corresponding k is added 1 on the original basis to obtain the energy value of $(k + 1)$.

Part 4. If the energy value before R_n registration is set to Egy_{0-l}, then the deposit corresponding to R_n registration is ΔEgy_{0-l}, corresponding to the energy value that is to be reduced. The calculation is as follows:

$$\Delta Egy_{0-l} = \frac{k}{2(k+1)} Egy_{0-l}$$

Part 5. The latest RSU energy value Egy_{n-1} obtained after successful registration and deposit is as follows:

$$Egy_{\mathrm{n}-l} = Egy_{0-l} - \Delta Egy_{0-l}$$

Part 6. As long as the RSU is registered, the above steps should be followed before updating the latest energy value.

(3) For the latest energy values of all current RSU candidates, CA needs to create energy value statistics. According to the set threshold Th_{Egy}, if the latest energy value Egy_{n-1} is lower than Th_{Egy}, then CA will eliminate the RSU that should have been Egy_{n-1} the first time, and the RSU will withdraw from the election. If the latest energy value Egy_{n-1} is greater than Th_{Egy}, then the RSU continues and accepts the next election.

(4) The equity value corresponding to the RSU that is already owned in the election lineup should be calculated at this stage. The equity essentially refers to the assets or energy owned by the node. In other words, if the RSU behavior is very active, more interest will be obtained. If the behavior of the RSU is very negative, fewer benefits will arise.

Part 1. Based on the blockchain conditions, we set the exit time of the equity proof mechanism (POS) as ΔT_{POS}. At every period of exit time, the accounting function will be stimulated accordingly. If the RSU needs to select the accounting node but the interval ΔT_{POS} time has not met the standard, then, during this process, the RSU will submit the application to the CA the first time, and the application content will immediately trigger a bookkeeping election immediately. At this time, the CA in the network will be the first to elect a new accounting node.

Part 2. As there are obvious differences between the network behaviors in which each RSU participates, the corresponding energy values also show a constantly changing trend. CA needs to record each RSU, that is, to record the energy value corresponding to the RSU in each stage from the first round to the last round. The energy value corresponding to the RSU of each round is set to Egy_{x}, and the energy value of the RSU differs at different moments. Therefore, the energy value of RSU cannot be uniformly estimated for a certain round, that is, the energy value does not have a certain value. In the current study, the energy value of the RSU in each round was considered as the energy value of the last moment corresponding to the RSU in this round.

Part 3. While participating in the election, each RSU is counted by CA from the first registration election. RSU participates in and initiates many elections in the latest election, and the number of elections is recorded as J. Following the above steps, CA will calculate the energy value corresponding to the RSU in round J. In addition, the corresponding equity value in each RSU election is recorded as $Stake_{R-l}$, and $Stake_{R-l}$'s calculation formula is as follows (in the formula, a represents the return growth rate in the POS algorithm mechanism, and the constant a generally takes a value of 0.05; Egy_{x} means the corresponding energy value for each round of RSU, which is set to Egy_{x}):

$$Stake_{R-1} = \sum_{x=1}^{J} Egy_x \times (1 + a\%)^J$$

Part 4. If round F is set as a particular number, five rounds are generally selected during the calculation process, and the energy value of the corresponding RSU is in a stable state. Then, in the process of RSU equity value calculation, we the J value corresponding to RSU is chosen as zero. The corresponding J value should not be considered until the corresponding energy value of RSU changes. This is because, if the RSU does not participate in the network transaction for a very long time, the corresponding energy value will be in a stable and constant state; in other words, the energy value does not change. The F round is set as a specific round, and the equity value and J value are considered, aiming to stimulate RSU activity, and stimulate RSU to more actively participate in the election and network behavior.

Part 5. Following the above steps, CA calculates the equity value of all candidate RSU candidates and determines that the accounting node of this round is the maximum equity value corresponding to RSU. After determining the new accounting node, CA will immediately update the energy value corresponding to the RSU. By setting the energy value of the RSU after the J election as Egy_{J}, the energy value of the RSU after the $(\mathrm{J}-1)$ election is recorded as $Egy_{\mathrm{J}-1}$; the refund proportion of the deposit is expressed by P_{r}; the reward issued by the successful RSU accounting node is recorded as $\Delta Egy_{\mathrm{reword}}$; the attenuation coefficient is $\mathrm{e}^{\frac{1}{\Delta T_{J-1-J}}}$. The correct update process is as follows:

$$Egy_{\mathrm{J}} = Egy_{\mathrm{J}-1} \cdot \mathrm{e}^{\frac{1}{\Delta T_{J-1-J}}} + \Delta Egy_{\mathrm{consume}}.P_r + \Delta Egy_{\mathrm{reword}}$$

To express the RSU revenue in the form of an increased energy value, the actual reward is calculated as follows:

$$\Delta Egy_{\mathrm{reword}} = \frac{1 - \Delta Egy_{J-1}}{2}$$

CA will also reset the J value of the accounting function RSU. After this round, the J value of the RSU is counted again. When the RSU obtains the bookkeeping function, CA will also reset ITS J value, and the J value of the RSU will start counting again after this round. The following algorithm details the incentive consensus mechanism (see Algorithm 1).

Algorithm 1 Consensus mechanism POS-I

Input: Egy_0, k, $\mathrm{Th}_{\mathrm{Egy}}$, $\Delta\mathrm{T}_{\mathrm{POS}}$, a, J, Pr;
Output: committer peer;
1: RSU sends a request to CA:
2: BCCA initializes an election for selecting committer peer;
3: **for** all RSU participating in the election do
4: R_{l} submITS $\Delta Egy_{\mathrm{consume}-1} = \frac{k}{2(k+1)} Egy_{o-l}$ as deposit;
5: Calculate $Egy_{\mathrm{e}-1} = Egy_{o-l} - \Delta Egy_{\mathrm{consume}-1}$;
6: **if** $Egy_{\mathrm{e}-1} < Th_{Egy}$ Then;
7: R_{l} cannot participate in the election;
8: **else**
9: R_{l} is regarded as a candidate;
10: **end if**
11: Calculate $\mathrm{Stake}_{\mathrm{R}-1} = \sum_{x=1}^{J} Egy_x \times (1 + \mathrm{a}\%)^J$;
12: **end for**
13: Selecting the node whose has Max_{stake} as the committer peer;
14: Calculate $\Delta Egy_{\mathrm{reword}} = \frac{1-Egy_{J-l}}{2}$
15: Calculate $Egy_J = Egy_{J-1} \times \mathrm{e}^{\frac{1}{\Delta T_{J-1-J}}} + \Delta Egy_{consume} \times \mathrm{Pr} + \Delta Egy_{reword}$,
16: Output committer peer.

5. Results Analysis of the Malicious Node Identification Algorithm of Blockchain Technology

5.1. Simulation Software Setting

The experimental simulation verifies the performance of the false message detection mechanism on the ONE simulation platform. ONE is a discrete-time engine open-source simulation platform written in the Java language. It is a simulation software that is mainly used to design and evaluate the routing mechanisms of data forwarding and message communication in the Internet of Vehicles. The ONE simulation platform contains a variety of simulation modules, which will be updated during each simulation process to realize the whole simulation function. The main functions of the ONE simulation platform include: mobile modeling of nodes, sending, receiving and processing routing messages, node communication, visual representation of results, etc. This platform has various different communication protocols to simulate the process of message transmission and generate the trajectory information during the transmission process. All ONE's components are independent of each other. ONE simulates the network simulation environment to test and optimize the security scheme performance. In the simulation experiments, a motion model based on the shortest path map was used in the ONE to simulate vehicle behavior on the road. The model initially places nodes in random locations, but selects a specific destination for all nodes in the map. Vehicle nodes are not arbitrary and include various types: emergency vehicles (police cars and ambulances), vehicles with fixed lines (buses and trams), and randomly distributed vehicles (private cars and taxis). There are two scenarios in the simulation experiments: low flow density and high flow density. Each simulation was run 20 times on average. In the experiment, the number of malicious vehicles that sent forged or forged messages in VANET ranged from 10% to 45%. When malicious vehicles exceed 45%, VANET's efficiency will dramatically decline, and it will be unable to provide any reliable services.

- Suppose an attacker cannot attack more than half the vehicles on the network.
- Authorities and the RSU are equipped with customized hardware with high computing abilities.
- Certification bodies and RSU are equipped with custom hardware, with a much higher computing power than general computers.
- As long as the public or private keys are not stolen, encryption technology can be used to provide secure communication channels between entities.

5.2. Evaluating Indicator

According to the requirements of the Internet of Vehicle malicious node identification algorithm, we selected the following indicators to verify the performance and results of the algorithm.

The first indicator is the false alarm rate (*FAR*), detecting the number of messages identified as false using the N_i representative, and detecting the number of false messages identified as true information using the N_j representative, from which *FAR* can be obtained:

$$FAR = \frac{N_i}{N_j}$$

The second indicator is the missed detection rate (*MDR*), where the number of detected true messages identified as false messages is replaced by N_{miss}, while the number of detected messages identified as true messages is N. From this, the *MDR* is obtained:

$$MDR = \frac{N_{miss}}{N}$$

Simulation experiments were carried out to verify the results of the malicious node identification algorithm of the Internet of Vehicles, and *FAR* and *MDR* were used to evaluate the results of the Internet of Vehicles' trust evaluation algorithm. The independent variable taken by the experiment is the proportion of malicious vehicle nodes in all vehicle networks,

and the results of the malicious vehicle node identification algorithm are evaluated for low-traffic-density and high-traffic-density conditions.

Whether the traffic density is low or high, the malicious node identification algorithm is less than 20%, and the *FAR* decreases as the percentage increases. At the same time, a significant trend towards decreased *MDR* also occurs with increasing percentage. Details are shown below. In the presence of a false information attack and black hole attack, the anti-attack performance of the malicious message detection algorithm is analyzed using several details: delivery rate (*Dr*), average end-to-end delay (*Ad*), and network overhead (*Or*).

First, *Dr* is calculated. The actual meaning of *Dr* is the ratio of the number of messages that are successfully sent to the target node or the designated location to the total number of messages that are generated and sent by the source vehicle nodes in the network. The calculation formula is as follows:

$$Dr = \frac{N_a}{N_t}$$

In the formula, the total number of messages generated and sent by the source vehicle node is N_t, the number of messages successfully sent to the target vehicle or designated location is N_a, and there is a proportional relationship between the communication quality between the nodes and *Dr*. In other words, the higher the *Dr*, the higher the communication quality, meaning that the overall network performance is very good. If the *Dr* is lower, then the communication quality is lower, meaning that the overall network performance is very poor.

Second, *Ad* is calculated. *Ad* is a very important indicator when evaluating the anti-attack performance of malicious message detection algorithms; by using the Ad evaluation method, how the additional overhead of security measures increases latency in the routing process can be described. The actual meaning of *Ad* is the average time taken to pass a message between two nodes

$$Ad = \frac{\sum_{n-1}^{N} T_n}{N}$$

In this formula, the total number of sent messages is recorded as N; the total time taken to send each message during N messages is $\sum_{n-1}^{N} T_n$. After analysis, an inverse relationship was found between *Ad* and the overall simulation performance; that is, if *Ad* is shorter, the corresponding performance is better, and if *Ad* is longer, the corresponding performance is worse.

Finally, *Or* is calculated. *Or* is another very important indicator when evaluating the anti-attack performance of the malicious message detection algorithm. This refers to the ratio of the total number of nodes involved showing the target node the total number of nodes involved in forwarding the message to the nodes required for transmission. The calculation formula is as follows:

$$Or = \frac{Num_{relay}}{Num_{total}}$$

In the formula, the number of nodes involved in forwarding the packet is recorded as Num_{relay}; the number of all nodes required during the transmission is recorded as Num_{total}. After analysis, an inverse relationship was found between *Or* and performance. That is, the smaller *Or*, the better the network performance of the corresponding algorithm, the fewer network resources that are occupied and the lower the number of additional nodes that are occupied. However, the larger the *Or*, the worse the corresponding algorithm network performance, indicating that more network resources are occupied and more additional nodes are occupied.

5.3. Simulation Software and Simulation Environment

5.3.1. Simulation Software

Simulation software: the ONE

The ONE is a discrete-time engine open-source simulation platform written in the Java language. This is a simulation software, which is mainly used to design and evaluate the

routing mechanism of data forwarding and message communication in the Internet of Vehicles. The real-time interactive graphical interface of the ONE simulation is shown in Figure 2.

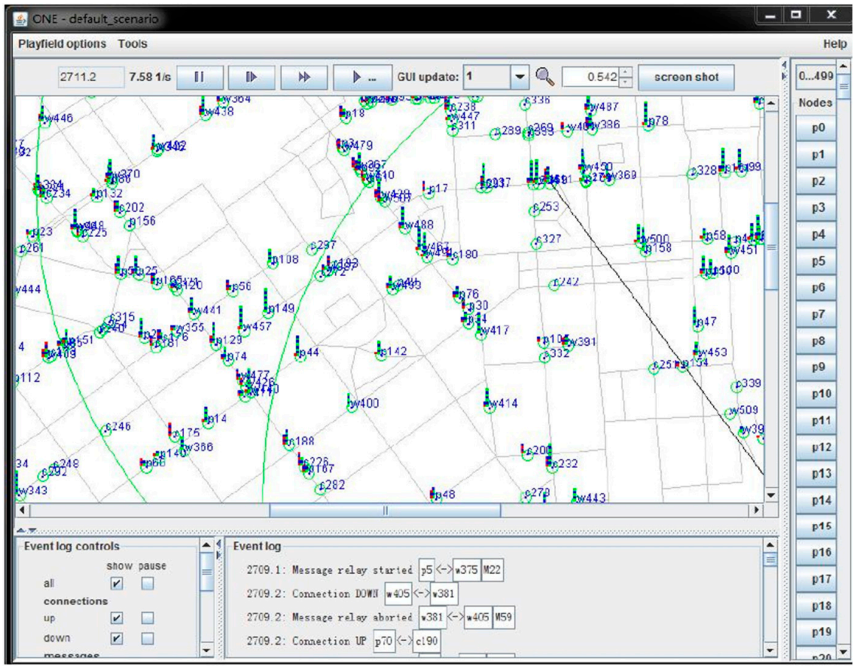

Figure 2. Interactive graphical interface of the emulator.

The emulator involves the classification and number of node types in the network, the path model of node movement, and the number of messages generated by the interaction, which are all displayed in real time in the interface. The ONE simulation platform contains a variety of simulation modules, which will be updated in each simulation process to realize the whole simulation function. The main functions of the ONE simulation platform include: mobile modeling of nodes, sending, receiving and processing routing messages, node communication, visual representation of results, etc. In this simulation platform, various different communication protocols simulate message transmission, and generate the trajectory information during the transmission process. All of ONE's components are independent of each other. The main structure and modules of the ONE simulation platform are shown in Figure 3.

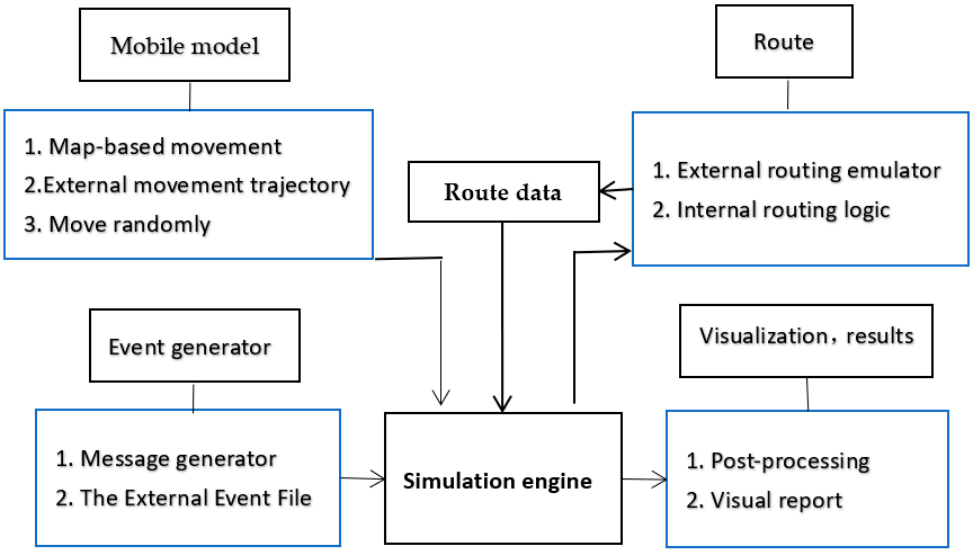

Figure 3. Simulation platform architecture.

5.3.2. Simulation Environment

ONE is used to simulate the network simulation environment to test and optimize the performance of the security scheme. In simulation experiments, a motion model based on the shortest map path was used in ONE to simulate vehicle behavior on the road. The model initially places nodes at random locations, but selects a specific destination for all nodes in the map and generates the shortest path from the start to end point using the Dijkstra algorithm. This experiment was implemented on the Helsinki city map, and a scene size of 4500 m × 3400 m was selected for the simulation experiments, as shown in Figure 4.

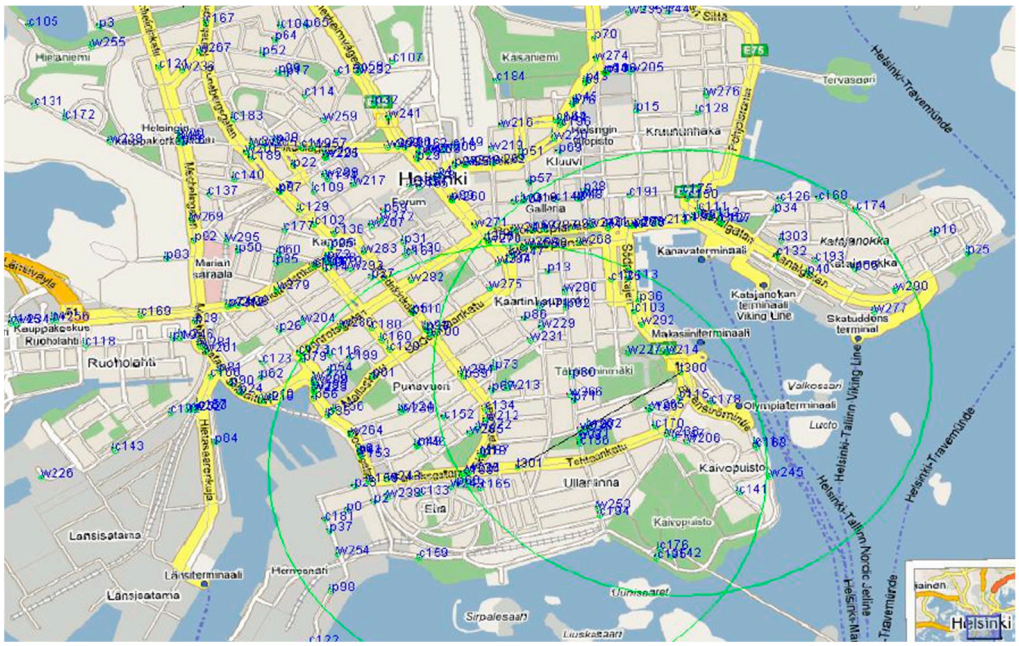

Figure 4. City map of Helsinki, Finland.

In the simulation experiment, the vehicle nodes communicate messages through the IEEE 802.11p communication protocol. The specific experimental simulation parameters are shown in Table 2.

Table 2. Experimental simulation parameters are set.

The Parameter Name	Parameter Values
Simulation Scene Range (m^2)	4500 × 3400
Simulation Time (s)	0–43,200
Vehicle mobility model	Shortest path movement model
Vehicle node type grouping (group)	11
Total number of vehicle nodes (individual)	200–600
Vehicle communication range (m)	10
Node speed (m/s)	2
RSU quantity (s)	10
Vehicle Cache Size (M)	40
Packet lifecycle (min)	15

There are two scenarios in the simulation experiments: low flow density and high flow density. Each simulation was run 20 times on average. In the experiment, the number of the malicious vehicles that sent forged messages or forged messages in VANET ranged from 10% to 45%. When malicious vehicles exceed 45%, VANET's efficiency will dramatically

decline, and it will be unable to provide any reliable services. Therefore, this extreme case is not considered in this paper.

The locations of all nodes are shown in Figure 5.

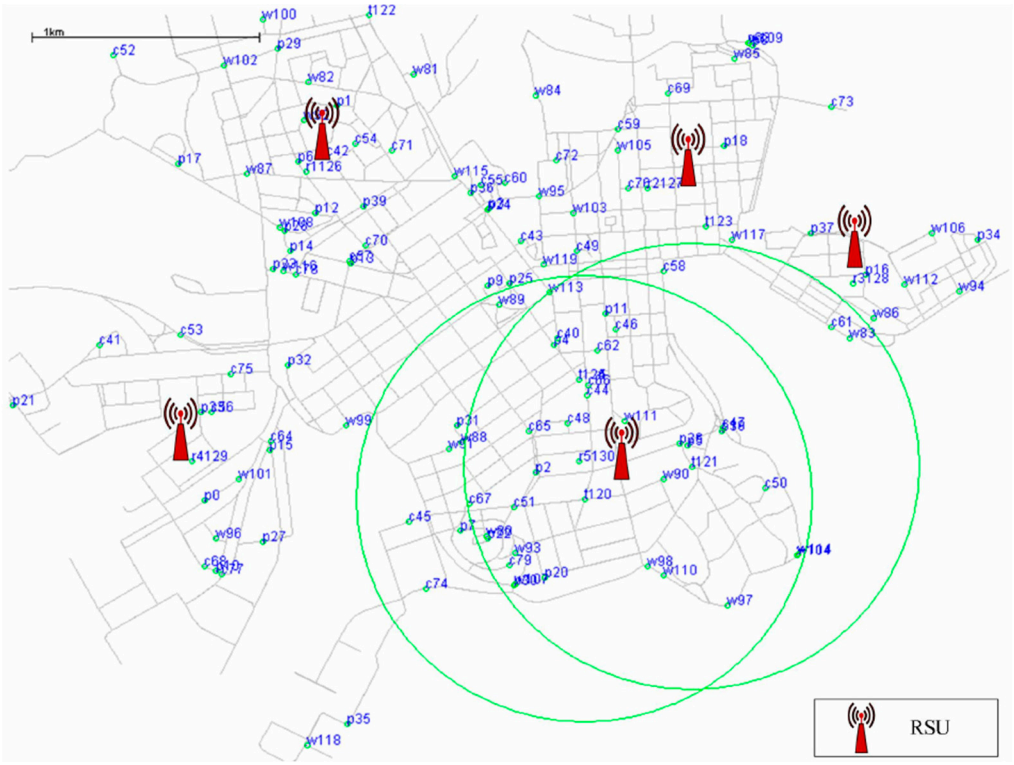

Figure 5. The location of all nodes.

To smooth the simulation experiment, some necessary assumptions in the theoretical algorithm and simulation experiments are presented as the basis of the proposed scheme.

- Suppose that an attacker cannot attack more than half of the vehicles in the network.
- Authorities and the RSU are equipped with customized hardware with high computing abilities.
- Certification bodies and RSU are equipped with custom hardware with a much higher computing power than general computers.
- As long as the public or private keys are not stolen, encryption technology can be used to provide secure communication channels between entities.

5.4. Simulation Results

To objectively and effectively analyze the malicious node detection mechanism algorithm based on blockchain, the simulation experiment is divided into two groups, looking at the number of vehicles for low-flow-density and high-flow-density scenarios. The results of each experiment are the average of the data obtained from 20 simulations. The simulation experiment takes the proportion of malicious vehicle nodes in the network as the independent variable and analyzes the algorithm's performance under low and high traffic flow densities. The experimental simulation results are as follows (See Table 3).

Overall, high-density scenarios outperform low-density scenarios using this algorithm. The proposed algorithm has a low *FAR* at both high and low densities. This is because this algorithm uses the blockchain to jointly verify the legitimacy of the sending nodes, determine the integrity and reliability of the VANET transmission messages, and greatly improve the identification rate of malicious messages.

Dr, *Ad* and *Or* were used to evaluate and analyze the performance, and each experiment was the average of the data obtained from 20 simulations. The simulation experiment

also takes the proportion of all vehicles of malicious vehicle nodes in the network as the independent variable and analyzes the algorithm's performance in the case of low traffic density and high flow density, respectively. The experimental simulation results are as follows (See Table 4).

Table 3. The *FAR* versus *MDR* comparison results.

Number of Malicious Vehicle Nodes in the Network	*FAR*		*MDR*	
	Low Flow Density	High Flow Density	Low Flow Density	High Flow Density
15%	0.156	0.112	0.100	0.105
25%	0.168	0.125	0.125	0.119
35%	0.171	0.135	0.129	0.120
45%	0.182	0.152	0.130	0.125

Table 4. Comparative results of the D, A, and O.

Number of Malicious Vehicle Nodes in the Network	*Dr* (%)		*Ad* (s)		*Or* (KB/S)	
	Low Flow Density	High Flow Density	Low Flow Density	High Flow Density	Low Flow Density	High Flow Density
10%	70.02	94.25	0.102	0.118	29.52	129.20
15%	69.52	90.21	0.161	0.156	40.20	134.56
20%	68.65	88.68	0.175	0.167	43.25	142.30
25%	67.25	86.98	0.201	0.210	50.20	149.52
30%	66.82	86.70	0.214	0.234	53.29	150.29
35%	66.30	84.02	0.226	0.301	58.63	167.98
40%	65.48	80.20	0.238	0.365	61.30	165.32
45%	65.00	78.68	0.262	0.402	67.05	172.02

In general, comprehensive experimental performance analysis can conclude with an increase in experimental simulation time and the gradual increase of malicious nodes in the network. If faced with the experimental simulation time and the high density of malicious vehicle nodes, the above algorithm can still play a significant role, and it has been verified by many scholars.

6. Conclusions

After a series of performance tests and verification of the results of the malicious node identification algorithm based on blockchain technology, the algorithm proposed in this paper can identify vehicle information in either low- or high-density vehicle scenarios. Based on the judgment of *FAR*, *MDR* and other indicators, the Internet of Vehicles' malicious node identification algorithm based on blockchain technology has a very significant false alarm rate and missing detection rate when identifying vehicle information. In this paper, *Dr*, *Ad*, *Or* and other indicators were selected to reveal malicious node identification algorithm's performance in the Internet of Vehicles. In general, the computing system based on blockchain technology is feasible, and ITS network performance is superior to other algorithms.

In the face of the increasingly prominent security needs and the complex diversity of malicious node attacks in the Internet of Vehicles, to further improve the detection of malicious nodes, the following perspectives could be the focus of future research work. First, the malicious node recognition algorithm model could be optimized to improve the system availability. The algorithm presented here is a result of the limited experimental conditions. A transportation service platform should be considered to evaluate the performance of this plan in real-world transportation networks. Second, the evaluation indicators should be

increased to improve system comprehensiveness. The application of blockchain technology in car networking applications is relatively low at present. Although the application of blockchain technology in the field of car networking has shown a good effect in this paper, the article used in the network evaluation index is not comprehensive. In future, other security metrics will need to be performance evaluated to integrate blockchain technology more comprehensively with automotive networks. Third, traffic scenarios should be enriched to improve the robustness of the system.

This blockchain, car networking, malicious-node-detection mechanism used a ONE simulation platform simulation experiment, looking at high-density and low-density scenario car scenarios to analyze the networking and malicious node identification algorithm performance. The malicious node detection performance of *FAR* and *MDR*, for algorithm models *Dr*, *Ad*, *Or* were also looked at, to conduct a comparative analysis of the algorithm performance. The final experimental results show that the proposed trust detection mechanism is feasible, and the ITS network performance is superior to that of other algorithms.

The blockchain-based malicious node detection mechanism proposed in this paper has a very significant application effect. The aim was build a model in more diversified traffic scenarios to test the security and trust mechanism, which can further improve the detection rate of malicious nodes and optimize the algorithm performance. In the future, this mechanism can be applied to richer traffic scenarios to improve its expansion and robustness.

Author Contributions: Conceptualization, J.C.; Project administration, T.L.; Resources, T.L.; Writing—original draft, J.C.; Writing—review & editing, R.Z. All authors have read and agreed to the published version of the manuscript.

Funding: Authors received funding from Yunnan Province's major science and technology special plan project "Research and application demonstration of key technologies of blockchain serving key industries": 202002AD080002.

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. Abboud, K.; Omar, H.A.; Zhuang, W. Inter working of DSRC and Cellular Network Technologies for V2X Communications: A Survey. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9457–9470. [CrossRef]
2. Zhongmei, L.; Wei, C.; Jie, W.; Haitao, Y. Very low latency and high reliability communication of Internet of Vehicles: Status and Outlook. *Signal Process.* **2019**, *35*, 1773–1783.
3. Nasrollahi, M.; Fathi, M.R. Modeling Big Data Enablers for Service Operations Management. In *Big Data and Blockchain for Service Operations Management*; Springer: Cham, Switzerland, 2022; pp. 49–94.
4. Ravari, S.S.M.; Fathi, M.R.; Mohammadi, M.; Bandarian, R. Investigating the concept of effectiveness in technology development projects in a research and technology organizations; evaluating eight technology development projects in the Research Institute of Petroleum Industry (RIPI). *Pet. Bus. Rev.* **2020**, *4*, 21–41. [CrossRef]
5. Yu, H.; Zhao, C.; Li, S.; Wang, Z.; Zhang, Y. Pre-Work for the Birth of Driver-Less Scraper (LHD) in the Underground Mine: The Path Tracking Control Based on an LQR Controller and Algorithms Comparison. *Sensors* **2021**, *21*, 7839. [CrossRef]
6. Parsajoo, M.; Armaghani, D.J.; Mohammed, A.S.; Khari, M.; Jahandari, S. Tensile strength prediction of rock material using non-destructive tests: A comparative intelligent study. *Transp. Geotech.* **2021**, *31*, 100652. [CrossRef]
7. Arushi, A.; Kumar, Y.S. Block Chain Based Security Mechanism for Internet of Vehicles (IoV). In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India, 26–27 March 2018; pp. 267–272.
8. Wagner, M.; Mcmillin, B. Cyber-Physical Transactions: A Method for Securing VANETs with Blockchains. In Proceedings of the IEEE Pacific Rim International, Symposium on Dependable Computing, Taipei, Taiwan, 4–7 December 2018; pp. 64–73.
9. Yu, H.; Li, S. The Function Design for the Communication-Based Train Control (CBTC) System: How to Solve the Problems in the Underground Mine Rail Transportation? *Appl. Syst. Innov.* **2021**, *4*, 31. [CrossRef]
10. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Inf. Process. Manag.* **2021**, *58*, 102511. [CrossRef]
11. Chen, W.; Yuan, L.; Wei, L. Progress of Internet of Vehicles Industry and Key Technology Analysis. *Zte Technol.* **2020**, *26*, 5–11.

12. Lin, L.; Lu, L.; Yuming, G. Analysis of Internet of Vehicles Communication Standardization and Industry Development. *Telecommun. Sci.* **2020**, *36*, 15–26.
13. Rongyue, Y.; Pengzhou, Z.; Qing, S. Research and Outlook of Intelligent Internet of Vehicles based on 5G Technology. *Telecommun. Sci.* **2020**, *36*, 106–114.
14. Jiahui, Q.; Zhichao, Z.; Xiaobo, L.; Yu, X.; Chao, C.; Liu, L. Research and Application of Internet of Vehicles Technology based on MEC. *Telecommun. Sci.* **2020**, *36*, 45–55.
15. Junhao, Y.; Zongpu, J.; Dongying, L. Intelligent Mine Internet of Vehicles System Architecture and Key Technologies. *Coal Sci. Technol.* **2020**, *48*, 249–254.
16. Rundong, W.; Wanwei, L.; Xiuliang, M.; Wenjun, Y. Summary of Mutual trust Certification and safe Communication of Internet of Vehicles. *Comput. Sci.* **2020**, *47*, 1–9.
17. Xiaolong, X.; Zijie, F.; Lianyong, Q.; Wanchun, D.; Qiang, H.; Yucong, D. Distributed service uninstallation method based on deep reinforcement learning in the edge computing environment of Internet of Vehicles. *J. Comput. Sci.* **2021**, *44*, 2382–2405.
18. Li, S.; Wang, G.; Yu, H.; Wang, X. Engineering Project: The Method to Solve Practical Problems for the Monitoring and Control of Driver-Less Electric Transport Vehicles in the Underground Mines. *World Electr. Veh. J.* **2021**, *12*, 64. [CrossRef]
19. Momeni, E.; Nazir, R.; Armaghani, D.J.; Maizir, H. Prediction of pile bearing capacity using a hybrid genetic algorithm-based ANN. *Measurement* **2014**, *57*, 122–131. [CrossRef]
20. Tao, S.; Xiuhua, L.; Hui, L.; Junhao, W.; Qingyu, X.; Jie, C. Summary of research on the car network security encryption authentication technology in the era of big data. *Comput. Sci.* **2022**, *49*, 340–353.
21. Xiao, W.; Tingting, T.; Shuangshuang, H.; Dongpu, C.; Feiyue, W. Parallel vehicle networking: Intelligent vehicle network management and control based on ACP. *J. Autom.* **2018**, *44*, 1391–1404.
22. Xinghua, L.; Cheng, Z.; Ying, C.; Huilin, Z.; Jian, W. A Review of Internet of Vehicles Security. *J. Inf. Secur.* **2019**, *4*, 17–33.
23. Wang, R.; Deng, X.; Xu, Z.; Zhao, X. Review of Simulation Test and Evaluation Technology of Internet of Vehicles. *Comput. Appl. Res.* **2019**, *36*, 1921–1926, 1939.
24. Paschek, D.; Mocan, A.; Draghici, A. Industry 5.0–The Expected Impact of Next Industrial Revolution. In *Thriving on Future Education, Industry, Business and Society, Proceedings of the MakeLearn and TIIM International Conference, Piran, Slovenia, 15–17 May 2019*; ToKnowPress: Bangkok, Thailand, 2019.
25. Hasanipanah, M.; Monjezi, M.; Shahnazar, A.; Armaghani, D.J.; Farazmand, A. Feasibility of indirect determination of blast induced ground vibration based on support vector machine. *Measurement* **2015**, *75*, 289–297. [CrossRef]
26. Garg, S.; Singh, A.; Aujla, G.S.; Kaur, S.; Batra, S.; Kumar, N. A Probabilistic Data Structures-Based Anomaly Detection Scheme for Software-Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3557–3566. [CrossRef]
27. Junejo, M.H.; Ab Rahman AA, H.; Shaikh, R.A.; Mohamad Yusof, K.; Memon, I.; Fazal, H.; Kumar, D. A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks. *Sci. Program.* **2020**, *2020*, 1–21. [CrossRef]
28. Lamba, K.; Singh, S.P. Modeling Big Data Enablers for Operations and Supply Chain Management. *Int. J. Logist. Manag.* **2018**, *29*, 629–658. [CrossRef]
29. Chen, J.M.; Li, T.T.; Panneerselvam, J. TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles. *IEEE Access* **2018**, *7*, 148913–148922. [CrossRef]
30. Farooq, S.M.; Hussain, S.M.S.; Ustun, T.S. A Survey of Authentication Techniques in Vehicular Ad-Hoc Networks. *IEEE Intell. Transp. Syst. Mag.* **2021**, *13*, 39–52. [CrossRef]