Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.048903

ARTICLE

FADSF: A Data Sharing Model for Intelligent Connected Vehicles Based on Blockchain Technology

Yan Sun, Caiyun Liu, Jun Li and Yitong Liu*

Data Security Institute, China Industrial Control Systems Cyber Emergency Response Team, Beijing, 100040, China

*Corresponding Author: Yitong Liu. Email: 13322470268@163.com

Received: 21 December 2023 Accepted: 21 May 2024 Published: 15 August 2024

ABSTRACT

With the development of technology, the connected vehicle has been upgraded from a traditional transport vehicle to an information terminal and energy storage terminal. The data of ICV (intelligent connected vehicles) is the key to organically maximizing their efficiency. However, in the context of increasingly strict global data security supervision and compliance, numerous problems, including complex types of connected vehicle data, poor data collaboration between the IT (information technology) domain and OT (operation technology) domain, different data format standards, lack of shared trust sources, difficulty in ensuring the quality of shared data, lack of data control rights, as well as difficulty in defining data ownership, make vehicle data sharing face a lot of problems, and data islands are widespread. This study proposes FADSF (Fuzzy Anonymous Data Share Frame), an automobile data sharing scheme based on blockchain. The data holder publishes the shared data information and forms the corresponding label storage on the blockchain. The data demander browses the data directory information to select and purchase data assets and verify them. The data demander selects and purchases data assets and verifies them by browsing the data directory information. Meanwhile, this paper designs a data structure Data Discrimination Bloom Filter (DDBF), making complaints about illegal data. When the number of data complaints reaches the threshold, the audit traceability contract is triggered to punish the illegal data publisher, aiming to improve the data quality and maintain a good data sharing ecology. In this paper, based on Ethereum, the above scheme is tested to demonstrate its feasibility, efficiency and security.

KEYWORDS

Blockchain; connected vehicles; data sharing; smart contracts; credible traceability

1 Introduction

The accelerated integration of the digital economy has spurred the development of intelligent connected vehicles (ICV) equipped with advanced onboard sensors, controllers, actuators and other devices. This sophisticated integration of modern communication and network technology enables intelligent information exchange and sharing between vehicles and various entities including other vehicles, roads, people, and clouds-a process encompassing complex environment perception, smart decision-making, and collaborative control. Consequently, ICVs facilitate safe, efficient, comfortable, energy-saving driving, thereby heralding a new generation of automobiles that can autonomously

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

function, hence becoming a pivotal direction for innovative progression in the automotive industry [1]. The product form, industrial ecology, and development concept of ICV deviate substantially from those of the traditional automobile industry, thus promising vast developmental prospects. Externally, ICV is a transportation vehicle, internally, it serves as a powerful information terminal and energy storage unit. Therefore, ICV [2] amalgamates logistics, information, and energy networks. Data plays an instrumental role in organically linking these three networks and harnessing their efficiencies, forming the core of future ICVs for improved intelligence, business model creation, and applications [3]. Throughout their design, research and development, usage, operation, and maintenance, ICVs will collect, process, transmit, and utilize copious amounts of personal, vehicle, road, and environmental data. The sharing and exchange of data are essential prerequisites for the advancement of the automobile industry in this big data era. Such data-sharing practices also exhibit urgent market demand in fields such as autonomous driving model [4] analysis, second-hand car trading, and automobile insurance. However, ensuring the safe and orderly flow of automotive data presents certain challenges. The question then arises: how can we secure the compliance of vehicle data?

For organized ICV data sharing and optimal data value realization, the National Highway Traffic Safety Administration [5] of the United States launched the "AV TEST Initiative" as an online, public platform for disseminating road testing activities of autonomous drive systems. Autonomous vehicles that were previously tested can voluntarily submit information to NHTSA (National Highway Traffic Safety Administration) under the AV TEST Initiative, and NHTSA [6] will provide information viewing services. Meanwhile, Oxbotica, a global autonomous vehicle software company, is collaborating with Cisco to develop an open roaming platform. The platform facilitates autonomous driving fleets to share large volumes of data safely and cost-effectively. It is designed to be fully scalable and can be deployed in a variety of fleet networks, allowing safe and inexpensive data downloading irrespective of fleet size or location. Furthermore, GM is teaming up with BMW to research and implement blockchain technology for sharing autonomous vehicle data among themselves and other automotive manufacturers. Under the auspices of the Mobile Open Blockchain Initiative (MOBI), exploratory work on data sharing in this field is ongoing [7]. However, every scheme has its distinct characteristics and weaknesses. NHTSA introduces third-party organizations that pose centralized risks. GM and BMW's solutions involve data encryption and storage, as well as decryption and verification each time data is read, which is inefficient. The roaming platform depends on the honesty of the data requester-malicious attackers could issue numerous data acquisition requests and potentially block the network, disrupting regular data flow. None of these schemes consider the reputability of the data holder [8]. This study proposes a decentralized car data sharing scheme based on blockchain technology, linking data sharing behavior with the reputation of the data publisher, aiming to secure data quality and preserve a healthy data sharing ecosystem [9].

The main contributions of this study are as follows:

1) This study proposes a data quality evaluation model based on the concept of the Bloom filter. For each shared data, DDBF is utilized to record the frequency of data complaints. If the number of complaints exceeds a certain threshold, the data is deemed illegal.
2) A decentralized vehicle data sharing method is proposed based on blockchain technology. Trusted interaction of data is achieved without the need for a trusted location. In addition, blockchain is used to record the data flow path.
3) An experimental simulation using Ethereum demonstrates the security and efficiency of the scheme. By comparing the time efficiency with the industrial Internet data trusted exchange and sharing service platform, the feasibility and effectiveness of the approach are verified.

The structure of this paper is arranged as follows: Section 2 introduces the automobile data quality evaluation scheme. Building upon blockchain technology, Section 3 delineates the data sharing strategy for intelligent network-connected vehicles. Section 4 employs experimental analyses to demonstrate the viability and efficiency of the proposed scheme. Finally, Section 5 provides a comprehensive summary of the entire paper and discusses potential future work and areas for enhancement.

2 Data Discrimination Bloom Filter

2.1 DDBF Construction

To ensure the quality of shared data, standardize data sharing activities, and maintain a good data ecology, the data demander can complain about the illegal data it has obtained. When the number of complained data reaches a certain threshold, the data holder will be punished. To improve the time efficiency, based on the idea of Bloom filter, this study designs DDBF to record the number of complaints against each data. Its structure is shown in the Fig. 1, where S represents the length of array V, $V[i] = 0, i \in \{0, 1, 2, \ldots, S-1\}$. Each user a will be randomly assigned a collection P_a, P_a is a subset of $\{0, 1, 2, \ldots, S-1\}$, and a collection Q_i will be randomly assigned after the data holder publishes the data information i and stores the label in the blockchain; Q_i is a subset of $\{0, 1, 2, \ldots, S-1\}$.

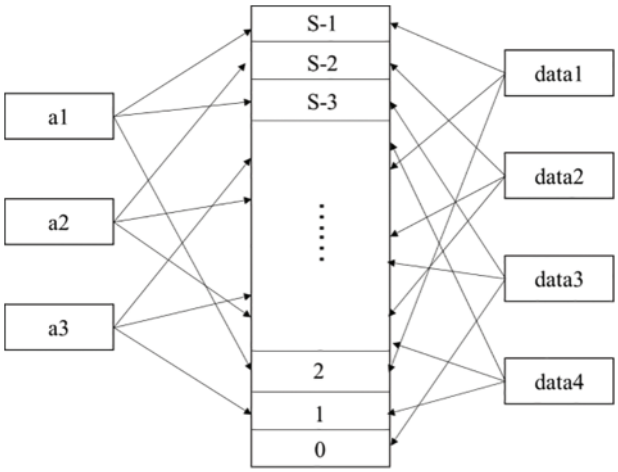

Figure 1: Data complaints structre

When user a wants to complain data i, he will set an element in array V from 0 to 1. The operation steps are presented as follows:

Algorithm 1: Illegal data complaint algorithm

input: complaint users a, illegal data i
output: null
1. Initialize the set P_a corresponding to a, and the set Q_i corresponding to i;
2. $V_a = \{m \in P_a \mid V[m] = 0\}$
3. **if** $V_a == \Phi$
4. The number of complaints made by user a has reached the upper limit;
5. goto final;
6. **else if** $V_a \cap Q_i \neq \Phi$

(Continued)

Algorithm 1 (continued)

```
7.        user a randomly selects an n, n ← V_a ∩ Q_i;
8.  else
9.        user a randomly selects an n, n ← V_a;
10.  V[n] = 1;
11. final;
12. return;
```

After each epoch in a time period, the system calculates whether the complaint number of each shared data in that time period exceeds the threshold μ. If the threshold value is exceeded, the data holder will be punished, and the operation steps are as follows:

Algorithm 2: Data quality evaluation algorithm

```
input: evaluation data i, threshold μ
output: legal data is true, illegal data is false
1.  Initializes the set Qi corresponding to data i
2.  count ← 0, legal;
3.  repeat
4.     for each m in Q_i do
5.        if V[m] == 1
6.           Count++;
7.    end for
8.  if count > μ then
9.     legal = false;
10.   goto final;
11. else
12.   legal = true;
13. final;
14. return legal;
```

2.2 Data Quality Threshold Measurement Model

Data quality threshold is the critical number of complaints for a certain illegal data. At first, this study firstly calculates the probability of intersection of any two subsets of {*0, 1, 2, . . . , S−1*}. Based on this probability, the critical value is calculated recursively, and the integer closest to the critical value is obtained with the dynamic strategy as the threshold.

Suppose *P, Q* are two subsets of {*0, 1, 2, . . . , S−1*}, $|P| = m$, $|Q| = n$, $x \le m \le n \le s$, the probability that any two subsets have an intersection is calculated as follows:

$$m(n) = \frac{m!}{(m-n)!} = m * (m-1) * (m-2) * \ldots\ldots * (m-n+1) \tag{1}$$

$$P(|P \cap Q| = x) = \frac{m(x) * n(x) * (s-n)(m-x)}{s(m) * x!} \tag{2}$$

For any piece of data, $\xi \leq |\, Q_{data}\,|$ is defined as the number of 0 in Q_{data}, and count is the number of complaints that data has received. The probability that any user a can set a *0* in Q_{data} to 1 is as follows:

$$P_{\xi} = 1 - \frac{(s - |Pa|)(\xi)}{s(\xi)} \tag{3}$$

It is assumed that the number of 0 in Q_{data} is ξ. After data is complained for count times, the number of 0 in Q_{data} is DR_{ξ}. Count, if ξ equals 0, and all elements in Q_{data} are 1. If count equals 0, the number of 0 in Q_{data} is ξ. Otherwise, the first complaint has a P_{ξ} probability, making the number of 0 in Q_{data} be $\xi - 1$, or $1 - P_{\xi}$ probability, making the number of 0 be ξ. DR_{ξ}; count is calculated as follows:

$$\mathrm{DR}_{\xi,\,count} = \begin{cases} 0, & \xi = 0 \\ \xi, & count = 0 \\ P_{\xi} * \mathrm{DR}_{\xi-1,\,count-1} + \left(1 - P_{\xi}\right) * \mathrm{DR}_{\xi,\,count-1} & else \end{cases} \tag{4}$$

Data quality threshold μrepresents the number of 1 in $Q_{\,data}$ after data is complained t times, which can be calculated by the sum of $\mathrm{DR}_{\xi,\,count}$ under all possible values of ξ. After λ of complaints about other data, the probability that the number of 0 in Q_{data} is ξ is $H_{\xi,}$ which is the probability that a subset with the number of elements λ and a subset with the number of elements Q_{data} have an intersection of $Q_{data} - \lambda$ elements. It can be calculated as follows:

$$H_{\xi} = \frac{\lambda\,(|Q_{data}| - \xi)\ *\ |Q_{data}|\,(|Q_{data}| - \xi)\ *\ (s - \lambda)(\xi)}{s\,(|Q_{data}|)\ *\ (|Q_{data}| - \xi)\,!} \tag{5}$$

After obtaining P_{ξ}, $\mathrm{DR}_{\xi,\,count}$ and H_{ξ}, we can calculate the data quality threshold μ. The calculation method is as follows:

$$\mu = |Q_{data}| - \sum\nolimits_{\xi=0}^{|Q_{data}|} H_{\xi} * \mathrm{DR}_{\xi,\,count} \tag{6}$$

3 Fuzzy Anonymous Data Share Frame

The architecture of the connected vehicle data sharing scheme [10] based on blockchain [11] technology proposed in this study is shown in the Fig. 2. The data holder initiates the data sharing request, uploading the data category, size, format, acquisition method and other information to the off-chain storage model. The data demander browses the data information [12] and initiates the data reading request. The data holder sends the requested data to the data demander, and synchronously generates data labels to be packaged and stored in the blockchain. When the data information received is illegal [13], the data demander calls the data complaint smart contract to complain about the data [14]. After each epoch, the audit traceability smart contract checks the data information exceeding the threshold μ, and the data is taken off the shelf, reducing the credibility of the data holder. When the reputation of the automobile data processor is lower than a certain threshold, the request for data sharing or data demanding cannot be initiated within a limited time [15].

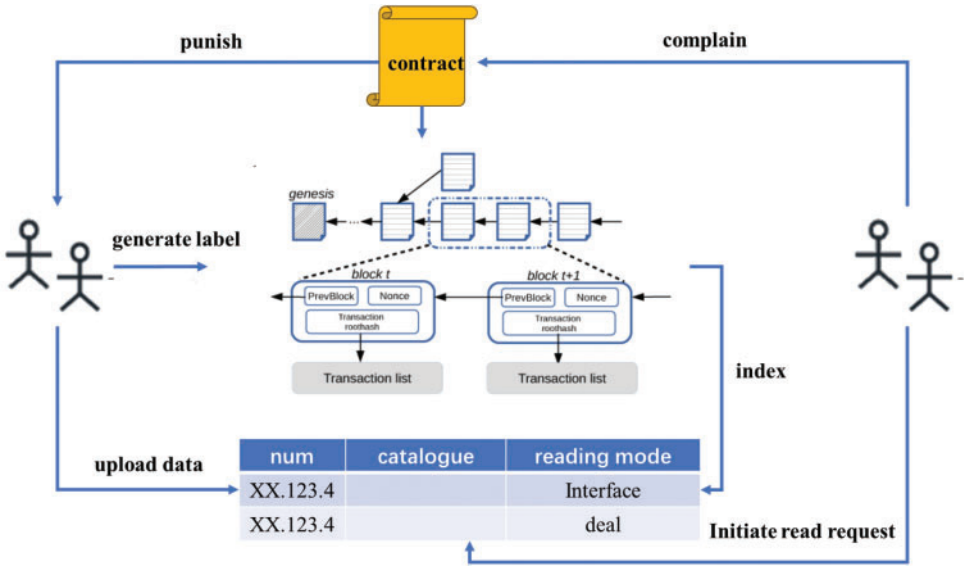

Figure 2: ICV data sharing scheme

3.1 Vehicle Data Exchange and Sharing

To bind the data with the identity [16] of the publisher and prevent the data integrity and availability from being damaged by attackers in the subsequent circulation process, the data holder sharer will generate a label $MARK_{data}$ to be packaged and stored in the blockchain after initiating the data sharing request. This study employs smart contracts ProduceCon to ensure the security and transparency of the label generation process [17]. The specific generation steps are as follows:

Algorithm 3: Shared data label generation contract

input: data holder *sharer*, sharing data *data*
output: data label $MARK_{data}$
1. *Sharer* generate random number $б \leftarrow \{0,1\}^{\Omega}$;
2. *Sharer* generate a message digest of shared data, $hash = \text{sha1}\,(data \,\|\, б)$;
3. $r \leftarrow Enc_{PK_{CON}}(sharer)$;
4. $\eta \leftarrow Sig_{sk_{con}}(hash||r)$;
5. $\text{MARK}_{\text{data}} = (r, \eta, б)$;
6. **return** $MARK_{data}$;

When the data holder receives [18] the read request from the data demander, the data holder generates a shared data label through the contract. If the data is generated by the holder, the data is sent to the data demander along with the label. If the data is retransmitted twice, the data label generated this time is discarded, and the data is sent to the data demander along with the original label. The specific steps are presented as follows:

When the data demander receives the data [19], it verifies the data, including the signature of the label generation contract and checks whether the data content is consistent with the description information in the off-chain storage model, whether there is dirty data, and whether the data tag is legal. The specific steps are as follows:

Algorithm 4: Vehicle data sharing algorithm

input: data holder *sharer*, sharing data *data*
output: null
1. Initialize the $MARK_{data}$ label;
2. **if** $\mathrm{MARK}_{\mathrm{data}} == \Phi$
3. $MARK_{data} \leftarrow$ ProduceCon(*sharer*, *data*);
4. *Sharer* send (*data*, $MARK_{data}$) to data demander;
5. **final;**
6. **return;**

Algorithm 5: Vehicle data check algorithm

input: data demander *acquirer*, sharing data *data*
output: legal data returns true, illegal data returns false
1. parsed response data, $MARK_{data} \leftarrow (r, \eta, б)$
2. calculate hash = sha1 ($data \parallel б$);
3. calculate $Ver_{PK_{con}}(б, (hash||\eta))$
4. check whether the data content is consistent with the description of the off-chain storage model;
5. check whether dirty data exists;
6. **return**;

3.2 Vehicle Data Complaints and Audit

The data complainer calls the illegal data complaint algorithm, and sets an element in array V from 0 to 1. To prevent malicious attackers from madly initiating data complaints and conducting denial of service attacks on the system, in the scheme proposed in this study, the data complainer can only set the elements assigned to the subset from 0 to 1. In a time period epocah, the number of complaints is limited. Meanwhile, each data complaint operation is a write operation to group V. To avoid competition conditions and improve the security and transparency of the system, the illegal data complaint algorithm is implemented using smart contracts. It is essential to queue according to the timestamp information carried by each data complaint operation, and linearly execute all complaint requests.

Algorithm 6: Data complaint algorithm

input: data complainer *complainer*, sharing data *data*
output: null
1. analyze the complained data, $MARK_{data} \leftarrow (r, \eta, б)$;
2. invoke the illegal data complaint algorithm;
3. **return**;

After a time period epocah, the system will check whether the number of complaints about data released in this period reaches the threshold. If the number reaches the threshold, the system will take the data off, decrypt the data label information to obtain the identity of the data holder, and reduce the credit value of the data holder as a punishment. In addition, the above operation does not involve write operation. Therefore, the audit operation can be distributed and concurrently executed by multiple machines, aiming to ensure the system time efficiency.

Algorithm 7: Illegal data audit algorithm

input: illegal data *data*
output: null
1. parse data information to be verified, $MARK_{data} \leftarrow (r, \eta, б)$;
2. invoke data quality evaluation algorithm;
3. **if** the number of data complaints exceeds the threshold
4. calculate $hash = \text{sha1}(data \| б)$;
5. calculate $Ver_{PK_{con}}(б, (hash||\eta))$;
6. **if** invalid label information
7. **goto** final;
8. **else**
9. disclosure of *data* holder information;
10. sharer $= Dec_{SK_{CON}}(\eta)$;
11. final;
12. **return**;

3.3 Measurement the Credit Value of Participants in Data Sharing

Based on the logistic regression model, this study proposes an algorithm to measure the credit value of data sharers, credit value measurement contract maintain the data sharing behavior record, and takes epocah as a measurement cycle. The measurement content includes six items. The parameter settings are shown in Table 1.

Table 1: Parameter settings

Parameter	Computing method
Data require number	Number of data demanders generating data exchange and sharing behavior
Data share number	Number of data sharing requests initiated in the current cycle
Legal data number	Number of legal data in the current cycle
Complaint number	Number of complaints made by the data demander in the current cycle
Data share old	Time of data exchange sharing (in *epocah*)
Credit	Periodic calculation through credit value calculation formula

The value of each field in the table is brought into formula (7) to calculate the credit value of the data sharing participant. All data sharing and data reading requests will be discarded when the credit value is less than the system minimum value.

$$credit_{\text{cur}}^{(a)} = \frac{1}{1 + e^{-\frac{\theta}{\alpha}\left(\sum_{x=1}^{\alpha} v_x - \sigma \sum_{x=1}^{\alpha} \mu_x\right)}} \tag{7}$$

$credit_{\text{cur}}^{(a)}$ is the trust degree of the data sharer according to the previous behavior of data processor a in a time period *epocah*; α indicates the number of times the data processor a acquires data in the current period; θ refers to the number of data sharing requests initiated by data processor a in the current period, and v_x suggests whether the data processor a is honest in the x data receiving behavior. Honesty is 1; otherwise, it is 0; μ_x indicates whether data sharer a is complained in the x round,

malicious is 1; otherwise, it is 0; ϭ indicates the penalty weight for malicious voting, which is set by the user. It indicates the greater the value, the greater the penalty for malicious voting of the node.

4 Experimental Results

4.1 Experimental Environment

In this study, two ECS servers are employed to build the experimental environment. Totally 15 data sharing participants are virtualized. These data nodes receive real-time data from BYD Dynasty automotive sensors in real time. Ethereum clients are installed to form a private chain. Smart contract scripts are written using solidity, and TLS1.3 is used for communication. The configuration of two servers and 15 virtual nodes is presented in Table 2.

Table 2: Servers configuration

Name	Type	CPU	Memory	Storage	System
Control node	Physics machine	8core 2.13 HZ	64 G	500 G	CentOS 7.5
Compute node	physics machine	8core 2.13 HZ	64 G	500 G	CentOS 7.5
Data node	virtual machine	1core 2.13 HZ	2 G	8 G	CentOS 7.5

4.2 Time Efficiency of Vehicle Data Sharing Based on Blockchain Technology

According to the experimental test, the time efficiency used by data holder A to share data with data demander B mainly includes the following four parts: data label generation time, data transmission time, data complaint time and audit traceability time. The data transmission time is associated with the specific data type, data volume and sharing method, which is independent of the sharing scheme proposed in this study. The audit traceability time, data label generation time and data complaint time change with the block out time and the number of data. The efficiency is shown in the following Figs. 3–6.

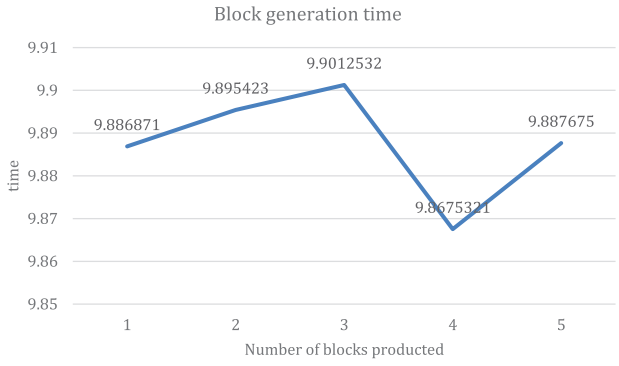

Figure 3: Block generation time

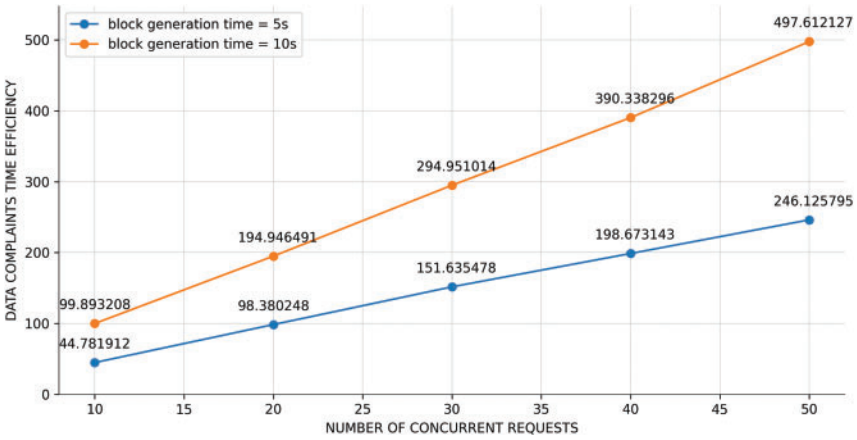

Figure 4: Audit traceability time efficiency

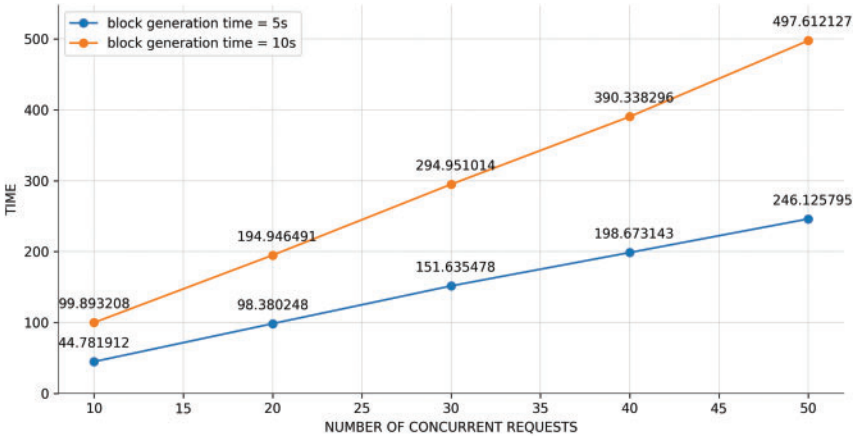

Figure 5: Data complaints time efficiency

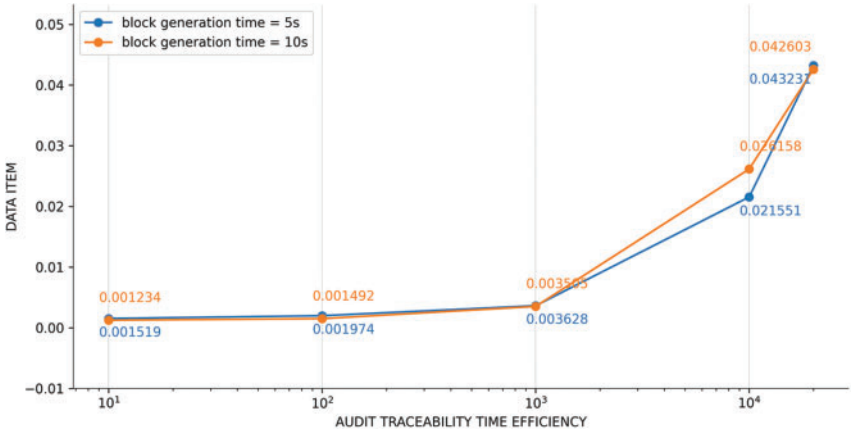

Figure 6: Data label generation time efficiency

Based on the experimental data in the table, we can find that the audit traceability operation is to read data through the smart contract. This is independent of the block out time and is very short, which can be ignored. However, the data complaint operation and data label generation operation aim to generate a piece of data through smart contract packaging. The time is basically equivalent to a block out time. The data set's write time is proportional to the concurrent requests and block out time. The above experiments demonstrate the feasibility of the scheme and the time efficiency is within the acceptable range.

5 Conclusion

To address the common problem of "data island" in the ICV network, this study proposes a connected vehicle data security sharing scheme based on blockchain technology. This scheme binds data with the identity of the data holder through smart contracts and preliminarily addresses the risk of data ownership confirmation and data secondary transfer. The scheme achieves the quality evaluation of shared data based on the data discrimination Bloom filter. By associating the data quality with the credit value of the data holder, the secure and efficient exchange and sharing of data can be realized without the need for a trusted third party. In addition, a good data sharing ecology is maintained. Finally, the Ethereum private chain is built to simulate the data exchange and sharing process proposed in this study. The experimental results demonstrate the feasibility and efficiency of the scheme. In the next stage, we will concentrate on the improvement of space efficiency and time efficiency of the scheme. Because the blockchain can only grow and cannot be deleted, when a piece of data is taken off the shelf, its label is still stored in the blockchain, which greatly wastes storage resources. The data acquirer needs to verify the integrity of the signature and summary when verifying the data quality, which is not beneficial for sharing scenarios with high real-time requirements. Finally, we will consider the business attributes of intelligent connected vehicles and propose a solution that does not influence the real-time performance of the business system in the event of data sharing system failures or hacker attacks. The above issues need to be further studied.

Acknowledgement: We wish to thank the timely help given by China Industrial Control Systems Cyber Emergency Response Team in experimental design, which greatly improved the quality of the work.

Funding Statement: This work was financially supported by the National Key Research and Development Program of China (2022YFB3103200).

Author Contributions: Conceptualization, Yan Sun, Yitong Liu; methodology, Yan Sun, Yitong Liu; formal analysis, Yan Sun, Caiyun Liu; investigation, Yan Sun, Jun Li; data curation, Yan Sun, Jun Li. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data are not publicly available due to their containing information that could compromise the privacy of research participants.

Conflicts of Interest: All authors have read and agreed to the published version of the manuscript.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," vol. 3, pp. 99, 2008. doi: 10.2139/ssrn.3440802.

[2] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019. doi: 10.1109/ACCESS.2019.2936094.
[3] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surv. & Tutor. 21*, vol. 4, pp. 3796–3838, 2019.
[4] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, 2018, pp. 45–54. doi: 10.1109/CVCBT.2018.00011.
[5] C. Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. New York City: Apress, 2017, pp. 1–39.
[6] S. Tikhomirov, "Ethereum: State of knowledge and research perspectives," in *Int. Symp. Found. Pract. Secur.*, Cham, Springer, 2017, pp. 206–221.
[7] G. Wood, Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.
[8] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," in *FSBC Working Paper*, 2017, vol. 8, pp. 1–8.
[9] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019. doi: 10.1109/ACCESS.2018.2890736.
[10] A. Parakh and S. Kak, "Space efficient secret sharing for implicit data security," *Inf. Sci.*, vol. 181, no. 2, pp. 335–341, 2011. doi: 10.1016/j.ins.2010.09.013.
[11] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, 2020. doi: 10.1109/JPROC.2019.2961937.
[12] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, "BDSS-FA: A blockchain-based data security sharing platform with fine-grained access control," *IEEE Access*, vol. 8, pp. 87552–87561, 2020. doi: 10.1109/ACCESS.2020.2992649.
[13] W. Li, J. Bu, X. Li, and X. Chen, "Security analysis of DeFi: Vulnerabilities," in *2022 IEEE Int. Conf. Blockchain (Blockchain)*, Espoo, Finland, 2022, pp. 488–493. doi: 10.1109/Blockchain55522.2022.00075.
[14] Y. Xue *et al.*, "A review on the security of the ethereum-based DeFi ecosystem," *Comput. Model. Eng. Sci.*, vol. 139, no. 1, pp. 1–101, 2024. doi: 10.32604/cmes.2023.031488.
[15] L. Wang, S. Huang, L. Zuo, J. Li, and W. Liu, "RCDS: A right-confirmable data-sharing model based on symbol mapping coding and blockchain," *Front. Inform. Technol. Electron. Eng.*, vol. 24, no. 8, pp. 1194–1213, 2023. doi: 10.1631/FITEE.2200659.
[16] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Vehicular Technol.*, vol. 69, no. 4, pp. 4298–4311, 2020. doi: 10.1109/TVT.2020.2973651.
[17] O. Serrano, L. Dandurand, and S. Brown, "On the design of a cyber security data sharing system," in *Proc. 2014 ACM Workshop Inform. Sharing & Collab. Secur.*, 2014, pp. 61–69.
[18] D. Xie, J. Yang, W. Bian, F. Chen, and T. Wang, "An improved identity-based anonymous authentication scheme resistant to semi-trusted server attacks," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 734–746, 2023. doi: 10.1109/JIOT.2022.3203991.
[19] T. Wang, H. Shen, J. Chen, F. Chen, Q. Wu and D. Xie, "A hybrid blockchain-based identity authentication scheme for mobile crowd sensing," *Future Gener. Comput. Syst.*, vol. 143, no. 6, pp. 40–50, 2023. doi: 10.1016/j.future.2023.01.013.