

Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 2, 2021

R. Li
X. Zhang, Ed.
J. Fan
Inner Mongolia University
December 29, 2020

Architecture for collecting traffic accident information based on
blockchain
draft-zhang-t2trg-accident-blockchain-00

Abstract

Blockchain is a distributed technology, and it uses cryptography and hash functions to store data in a chain to ensure that data are tamper-resistant and traceable. So, this document proposes an architecture for collecting traffic accident information based on blockchain. At the same time, this document describes the working method of collecting traffic accident information under this architecture.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 2, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2

2. Relate work 4

3. System structure 5

 3.1. Perception layer 6

 3.2. Edge computing layer 6

 3.3. Service layer 6

4. Scheme design 7

 4.1. Traffic accident information query 7

 4.2. Traffic accident information return 7

 4.2.1. Resource fragmenting method 7

 4.2.2. Resource Naming Method 8

 4.3. RSUs consensus 8

 4.4. Traffic accident information storage 9

5. Discuss 10

6. IANA Considerations 10

7. Security Considerations 10

8. Conclusion 10

9. Acknowledgements 11

10. Informative References 11

Authors' Addresses 12

1. Introduction

With the development of society, there are more and more vehicles on the road, and a problem that follows is that the incidence of traffic accidents is also increasing. The frequent occurrence of traffic accidents has brought a serious impact on human life, and has brought certain pressure on the relevant traffic departments to deal with traffic accidents. The handling of traffic accidents must be timely, and the evidence must be obtained correctly, so as to avoid traffic jams, secondary accidents and legal disputes. Therefore, how to use the existing technology to quickly, correctly and effectively deal with traffic accidents has become a very important issue.

The most important thing to deal with traffic accidents is to collect traffic accident information (also known as "resources"). At present, the main methods of collecting traffic accident information are manual and automatic. Among them, manual methods include measuring tape, witness investigation, and on-site photographing. The automatic method is to use the camera at the intersection. These methods require a long time, and cause certain difficulties for rapid

recording, rapid evacuation of traffic, subsequent accident analysis and liability determination.

In the past few years, with the development of wireless communication technology and the automobile industry, the Vehicular Ad Hoc Network (VANET) has developed significantly [Misra2009]. Based on the VANET researchers have proposed a large number of related applications, which are divided into safety-related applications and comfort-related applications [Eze2014]. These applications mainly use the cooperation between vehicles to transmit messages. The driving recorder is an instrument that records the video image and sound of the vehicle during driving. If a traffic accident occurs in front of the vehicle, it can provide strong evidence for handling the traffic accident. Resources can also be collected through cooperation between vehicles. It can be seen that the use of vehicle-to-vehicle collaboration in the VANET can transmit driving recorder's data to relevant departments, which is beneficial to better handling of traffic accidents.

Most of the resources transmitted is used as evidence. It is necessary to ensure that the data transmitted to the relevant transportation department are true, confidential, and not tampered, and traceable. However, in the communication process, resources security is the main concern, including the safety protection issues in transmission process, the security issues of centralized storage in the data center, the access control and privacy protection.

Blockchain is a distributed technology. It uses cryptography and hash functions to store data in a chain to ensure that data are tamper-resistant and traceable. And the technology uses a consensus protocol to ensure data consistency. Therefore, blockchain technology can be applied to the VANET environment to solve the security problem and remove the dependence on trusted central entities. However, the process of consensus has to solve the large computational problem which cannot be done on computing resources constrained vehicles. As a new type of technology, Mobile Edge Computing (MEC) can be used not only to offload computationally intensive tasks from mobile devices to edge networks, but also to optimize processing before sending data to the core network, and to provide edge cloud services for mobile users at the edge.

Therefore, this document proposes an architecture for collecting traffic accident information based on blockchain. It uses blockchain to ensure that resources are tamper-resistant and traceable, and uses edge computing to solve the large computational problem of blockchain consensus process.

In section 2, some current researches on collecting transaction accident information are described, and their shortcomings are analyzed. Section 3 proposes the structure of this document. Section 4 describes the working method of collecting traffic accident information in the framework proposed in this document. Section 5 discusses how the architecture guarantees the security of VANET. Section 6 summarizes the full document.

2. Related work

With the increase of vehicles on the road, the number of traffic accidents has also increased. The traditional methods of collecting traffic accident information are manual methods—pulling a measuring tape, witnessing investigation, and taking pictures on the spot, which takes a long time and is not conducive to the rapid evacuation of traffic and rapid recording of the scene. Therefore, there are a large number of researchers in collecting traffic accident information.

Among these studies, one type of research is to use web-based methods to obtain accident information. Users upload the accident information to the server of the relevant transportation department through the browser, and the relevant transportation department obtains the traffic accident information from the server as the basis for handling the traffic accident. Lobont et al. collect basic information of accidents in a web-based traffic accident collection system, including time and location [Lobont2013]. In a web-based traffic accident collection system, Williams et al. collect information on the severity of accidents, vehicle types, casualties, road conditions, weather conditions, and light conditions [Williams2015]. Another form of such research is the use of smart phones. CrashData [Derdus2014] proposed by Derdus et al. is an application based on mobile smart phones. The application can upload the basic information of the traffic accident to the server. This type of research must be connected to the Internet and requires users to participate in actively uploading information, but users may not upload resources voluntarily.

Another type of research is to install fixed infrastructure on both sides of the road to obtain traffic accident information. In the traffic accident investigation and management system based on GPS VRS, GIS road database and stereo vision technology proposed by Qingwu H et al. [Hu2011], the traffic accident information is mainly obtained through GPS VRS and GIS road database, and then restored using stereo vision technology. In the system for collecting traffic accident information based on ultrasound and ZigBee wireless transmission technology proposed by Song H et al. [Song2014], the state of the vehicle during a traffic accident is measured by

ultrasound, including information such as speed and direction. This type of research is limited by the location of fixed infrastructure, and traffic accident information cannot be collected where there is no fixed infrastructure.

Other research is firstly obtaining traffic accident information through various sensors on the vehicle, and then using the VANET to transmit the traffic accident information to the relevant traffic department. In the literature [Abduljalil2012], Abduljalil FM et al. use on-board angle sensors, airbag sensors, cameras, GPS sensors, etc. to obtain traffic accident information, and then use Wi-Fi, GPRS, 3G, WIMAX, 4G-LTE wireless transmission technology to transfer traffic accident information to the relevant department. In the VWaaS service architecture proposed by Hussain R et al. [Hussain2013], when a traffic accident occurs, the surrounding vehicles use the car's camera to capture the traffic accident information, and then send the captured content to the centralized server facility. In this process, the vehicle directly sends traffic accident information to the server via 3G/4G or transmits the traffic accident information to the RSUs (Road Side Units) via DSRC, and then the RSU transmits the information to the RSUs server.

Among the above methods for collecting traffic accident information, the web-based method requires users to upload traffic accident information to a server, which must be connected to the Internet, and the time for collecting information is relatively long. Based on the way roadside infrastructure collects traffic accident information, limited by the fixed location of the infrastructure, it is impossible to collect traffic accident information in areas not covered by the infrastructure. The method of collecting traffic accident information based on vehicle sensors and the VANET requires the participation of RSUs. In the above three methods of collecting traffic accident information, only the information after the traffic accident can be collected, and the information before the traffic accident cannot be obtained. The analysis of the accident and the determination of responsibility after the accident have certain difficulties. And there is no guarantee that the collected traffic accident information is not been tampered with and can be traced to the source.

3. System structure

This document proposes a security architecture for collecting traffic accident information based on blockchain. The architecture consists of three layers, namely perception layer, edge computing layer, and service layer. The perception layer comprises vehicle and RSU, together forming blockchain network. The edge computing layer provides computing resources and edge cloud services for the

perception layer. The service layer includes cloud services and blockchain.

3.1. Perception layer

A driving recorder is installed on the vehicle, which can record the traffic accident information of the vehicle passing position. Because of the constraint of computing resource and the mobility, the vehicle cannot perform all blockchain functions, including wallet (save address and private key), miner (mining), complete blockchain (save all blockchain data), network routing (validate and propagate transaction block information, discover and maintain connections to peer nodes). In this document, vehicle performs the functions of wallet and network routing.

The RSU connects each other by wired communication, forming stable blockchain network which can ensure a unique ledger for collecting traffic accident information. Therefore, all blockchain functions are performed on the RSU. Even while one vehicle is moving, it can communicate with RSU directly or through other vehicles.

3.2. Edge computing layer

There are lots of transactions occurred for collecting traffic accident information. If all the consensus work of the blockchain transaction is completed in RSU, it will inevitably affect the network performance and bring high delay. Therefore, this document offloads the computationally intensive work to MEC, and the result is returned to the RSU after completion. MEC is also responsible for handling other computationally intensive work, such as video or image processing, etc.

3.3. Service layer

The traffic accident information recorded by the driving recorder is video, which has a large amount of data and is not suitable for storage in blockchain of RSUs. Because the blockchain is distributed storage, each blockchain node stores all the data, which consumes lots of storage resources. So, the document stores the traffic accident information on the cloud server, which can not only store the data permanently, but also facilitate the inspection and evidence collection by the traffic police department.

So, for data stored in the service layer, part of the data which are tamper-resistant and traceable, such as traffic accident data, traffic violation data, etc. are stored using blockchain. The other part of data is stored on the cloud service.

4. Scheme design

Based on the above architecture, the working method of collecting traffic accident information includes 4 steps, including traffic accident information query, traffic accident information return, RSUs consensus, and traffic accident information storage. The working methods of collecting traffic accident information are as follows.

4.1. Traffic accident information query

The traffic police department initiates a traffic accident information inquiry request based on the time and location of the traffic accident. The query request is sent to the vehicles driving on the road through the RSUs. Because it is uncertain which vehicles have captured the traffic accident information, in order to enable more vehicles within the communication range of the RSU to receive the traffic accident information query request, the document uses the flooding method to send the query request. At the same time, delay tolerant network technology is used to forward query requests to vehicles that are not within the communication range of RSU by using moving vehicles.

4.2. Traffic accident information return

The vehicle receives the traffic accident information query request and checks whether the traffic accident information is recorded locally. If recording, extract the traffic accident information from the driving recorder and transmit it to the nearest RSU. If the vehicle does not directly communicate with the RSUs in a single hop, it is forwarded through the intermediate vehicle.

The vehicle is in a moving state. If the traffic accident information recorded by the driving recorder is directly disseminated on the network, the probability of transmission failure will be very high, and the network performance will be affected. Therefore, this document processes the traffic accident information in fragments, and then transmits the fragmented traffic accident information, and finally aggregates it through the RSUs.

4.2.1. Resource fragmenting method

The resources need to be transmitted in fragments. However, the size of the fragments must ensure that a complete resource can be transmitted within the shortest communication time between vehicles. Therefore, this document determines the size of resource fragments according to the shortest communication time of vehicles on urban roads. First, determine the shortest time for vehicle communication on urban roads. The movement of vehicles on urban roads can be

divided into two types: same direction driving and reverse direction driving. When two vehicles are driving in the same direction and in the reverse direction on the city road at the same speed, the communication time for them when driving in the reverse direction is shorter.

Generally, vehicles on urban roads are not allowed to exceed the prescribed speed. When the vehicle is traveling at the maximum speed specified on the city road, the communication time between them is the shortest. Therefore, the fragment size of the resource is defined as the data size that can be transmitted in the shortest communication time between vehicles, which can ensure that any resource can be transmitted within the vehicle communication time range.

4.2.2. Resource Naming Method

The traffic accident information after fragmentation is named according to certain rules, which is convenient to distinguish from other vehicles and to facilitate aggregation. The naming rules are as follows:

NodeID_SerialNum_TotalNum_Time_Location

Among them, NodeID represents the ID of the node, that is, the license plate number of the vehicle; SerialNum represents the serial number of the traffic accident information fragment; TotalNum represents the total number of traffic accident information fragments; Time represents the time when the traffic accident occurred; Location represents the location of the traffic accident, that is, the latitude and longitude.

For the same traffic accident resource, the node ID can distinguish which vehicle provides the resource, and the resource sequence number and the total number of resource fragments can distinguish each fragment of the resource provided by the vehicle. For the same car (same node ID), even if the resources of multiple traffic accidents are captured, different traffic accidents can be distinguished by the time and location of the traffic accident. Moreover, each fragment of the same traffic accident resource can be distinguished by the resource sequence number and the total number of resource fragments.

4.3. RSUs consensus

The traffic accident information needs to be verified, agreed, and added to the blockchain. The specific process is as follows:

- a. When RSUs receive traffic accident information, they generate a transaction based on the basic information and hash value of the traffic accident information (NodeID, SerialNum, TotalNum, Time, Location) and forward it to other RSUs.
- b. Other RSUs in the blockchain network receive the transaction and check whether the transaction is valid and the format is correct. If the inspection meets the requirements, it is placed in the transaction storage pool and forwarded to other RSUs. The other RSUs that receive the transaction repeat the process.
- c. The RSU that obtains the right to packaging the transactions in the transaction storage pool into a block, and then mines the block. The mining process needs to complete a large number of calculations, and RSUs generally do not have the ability to complete a large number of calculations, and the calculation tasks need to be offloaded to edge computing. Edge computing completes the calculation task and returns the result to the RSUs. The RSUs sends the block to other RSUs to spread across the entire network.
- d. After receiving the block, other RSUs verify the block. If the block is verified, the RSUs deletes the completed consensus transaction from the transaction storage pool and the block being mined, and at the same time adds it to the blockchain.

4.4. Traffic accident information storage

The RSUs aggregate the traffic accident information fragmented in the blockchain. The aggregating process involves video processing, so this process is also offloaded to edge computing to reduce the workload of RSUs and increase its effectiveness. After the edge computing completes the aggregation of the traffic accident information, it sends the complete traffic accident information to the RSUs.

The blockchain in RSUs cannot store all traffic accident information. So it is uploaded to the cloud for storage, and the blockchain in the RSUs only store the digest of traffic accident information. In order to ensure the security of data in cloud, the data which are tamper-resistant and traceable are stored using blockchain. While, other data adopt the original storage method of the cloud, guaranteeing security by cloud computing architecture.

5. Discuss

This section focuses on how the architecture guarantees the security for collecting traffic accident information.

In this security architecture, vehicles and RSUs in the perception layer together form blockchain network to improve the security for collecting traffic accident information. However, traffic accident information generated by the vehicle generally are stored in the cloud or a centralized platform so as to provide data support for related department. Considering a large amount of traffic accident information, the perception layer does not have enough space to store. Therefore, in this security architecture, the traffic accident information is still stored in the cloud of the service layer. In order to ensure the security of data in cloud, the data which are tamper-resistant and traceable are stored using blockchain. While, other data adopt the original storage method of the cloud, guaranteeing security by cloud computing architecture.

At the perception layer, the main challenge is security of traffic accident information during transmission. So, blockchain in the perception layer is used to solve the security problem in the transmission process. And the data solving the security problem in transmission process need to be stored in perception layer blockchain. By combining MEC, the perception layer can ensure the security of traffic accident information in transmission process.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

There are no Security Considerations related to this document.

8. Conclusion

This document proposes an architecture for collecting traffic accident information based on blockchain. The architecture includes three layers, namely perception layer, edge computing layer and service layer. The perception layer ensures the security of VANET data in the transmission process through the blockchain. The edge computing layer provides computing resources and edge cloud services for the perception layer. The service layer uses the combination of traditional cloud storage and blockchain to ensure the security of data.

9. Acknowledgements

This work was supported by the Inner Mongolia Autonomous Region Science and Technology Achievements Transformation Project (No. CGZH2018124).

10. Informative References

[Abduljalil2012]

Abduljalil, F., "A framework for vehicular accident management using wireless networks", 2012 IEEE 13th International Conference on Information Reuse & Integration (IRI), 2012.

[Derdus2014]

Derdus, K. and V. Ozianyi, "A mobile solution for road accident data collection", Proceedings of the 2nd Pan African International Conference on Science, Computing and Telecommunications (PACT 2014), 2014.

[Eze2014]

Eze, E., Zhang, S., and E. Liu, "Centralized Conferencing (XCON) Media Models", 2014 20th International Conference on Automation and Computing, 2014.

[Hu2011]

Hu, Q. and H. Wang, "A Framework for Traffic Accident Scene Investigation with GPS VRS, Road Database and Stereo Vision Integration", 2011 International Workshop on Multi-Platform/Multi-Sensor Remote Sensing and Mapping, 2011.

[Hussain2013]

Hussain, R., Abbas, A., Son, S., Kim, K., Kim, K., and O. Oh, "Vehicle witnesses as a service: Leveraging vehicles as witnesses on the road in vanet clouds", 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013.

[Lobont2013]

Lobont, L., FILICHI, A., and L. POPESCU, "Improving traffic safety using modern methods for accident data collection", ANNALS OF THE ORADEA UNIVERSITY Fascicle of Management and Technological Engineering, 2013.

[Misra2009]

Misra, S., Zhang, I., and S. Misra, "Guide to wireless ad hoc networks", Springer Science & Business Media, 2009.

[Song2014]

Song, H., Ming, J., Tang, J., Zeng, D., Duan, w., and Z. Yin, "Wireless Positioning System for Investigation of Road Traffic Accidents", Proceedings of the International Conference on Logistics, Engineering, Management and Computer Science, 2014.

[Williams2015]

Williams, K., Idowu, P., and E. Olonade, "Online Road Traffic Accident Monitoring System for Nigeria", Transactions on Networks and Communications, 2015.

Authors' Addresses

Ru Li
Inner Mongolia University
Hohhot 010021
China

Phone: +86 15804712558
Email: csliru@imu.edu.cn

Xiaodong Zhang (editor)
Inner Mongolia University
Hohhot 010021
China

Phone: +86 15247168840
Email: cszxd@imu.edu.cn

Jun Fan
Inner Mongolia University
Hohhot 010021
China

Phone: +86 18686016307
Email: 250832228@qq.com