Journal of Computer Applications
计算机应用,2021,41(7):1989 - 1995
ISSN 1001-9081
CODEN JYIIDU
2021-07-10
http://www.joca.cn

文章编号:1001-9081(2021)07-1989-07
DOI:10.11772/j.issn.1001-9081.2020081205

基于区块链的车联网电子取证模型

陈葳葳,曹　利*,顾　翔
(南通大学 信息科学技术学院,江苏 南通 226019)
(*通信作者电子邮箱cl@ntu.edu.cn)

摘　要:针对车辆交通事故取证困难、责任归属难以判定等问题,提出一种车联网(IOV)通信架构下基于区块链的电子取证方案。该方案利用区块链去中心化存储机制实现电子证据的远程存储,并利用智能合约机制完成电子证据的快速检索和相关证据链的有效追溯;而为有效保护车辆身份的隐私,提出一种令牌机制来对数据进行访问控制;同时,为满足IOV的实时取证要求,提出了一种高效批量共识机制。实验仿真表明,所提方案中的新型共识算法效率优于传统委托权益证明(DPOS)共识算法,且取证速度满足IOV环境的需求,保证了电子证据的不可篡改、不可否认及永久保存等特性,实现了区块链技术在司法存取证方面的应用。

关键词:车联网;区块链;电子取证;共识算法;智能合约
中图分类号:TP393; TP309　　**文献标志码**:A

E-forensics model for internet of vehicles based on blockchain

CHEN Weiwei, CAO Li*, GU Xiang
(*College of Information Science and Technology*, *Nantong University*, *Nantong Jiangsu* 226019, *China*)

Abstract: To resolve the difficulties of forensics and determination of responsibility for traffic accidents, a blockchain-based e-forensics scheme under Internet Of Vehicles (IOV) communications architecture was proposed. In this scheme, the remote storage of digital evidence was implemented by using the decentralized storage mechanism of blockchain, and the fast retrieval of digital evidence and effective tracing of related evidence chain were realized by using the smart contracts. The access control of data was performed by using the token mechanism to protect the privacy of vehicle identities. Meanwhile, a new consensus mechanism was proposed to meet real-time requirements of IOV for forensics. Simulation results show that the new consensus algorithm in this proposed scheme has higher efficiency compared with the traditional Delegated Proof Of Stake (DPOS) consensus algorithm and the speed of forensics meets the requirements of IOV environment, which ensures the characteristics of electronic evidence such as non-tampering, non-repudiation and permanent preservation, so as to realize the application of blockchain technology in judicial forensics.

Key words: Internet Of Vehicles (IOV); blockchain; e-forensics; consensus algorithm; smart contract

0　引言

交通事故认定是指交管部门对事故现场勘验、调查,并对事故原因做出认定,最后根据当事人过错的程度,归属其责任[1]。事故的鉴定依赖于现场证据,但取证面临诸多困难,如:现场遭到破坏,责任人故意掩盖或者伪造证据等。交通事故取证困难影响司法机关对事故责任的判决。在车联网环境下,车内传感器网络采集其行驶过程中的状态数据(行驶时间、车速、加速度、行驶轨迹等),通过控制器局域网络(Controller Area Network, CAN)总线汇总至黑匣子[2]。事故发生后,分析黑匣子数据即可建立较为精确的事故模型,分析原因、判定责任归属。根据《民事诉讼法》《刑事诉讼法》《行政诉讼法》的定义,汽车黑匣子是司法定义中的8大类证据之一。但黑匣子在取证时也存在脆弱一面,如对外界高度暴露,只要掌握黑匣子内部工作方式,便可通过外部设备与其连接,篡改、伪造证据以逃避责任;另外,在一些事故中,车辆因焚烧、掩埋等严重损毁,导致无法获取黑匣子中的电子数据,从而无法进行责任鉴定。文献[3]中提出了一种智能云取证方法,利用移动通信技术实现了车联网环境下车、路、处理平台的互通互联,对黑匣子内的数据远程云化处理,提高了取证的安全性和准确度;但云取证存在存放中心化、易受攻击的问题,同时取证效率比较低。

区块链技术本质是一种信任机制,它为电子证据的司法应用提供了一种新的理想化技术支撑[4-6]。目前,关于区块链和电子取证结合方面已经有一些研究:Zhang等[7]提出了一个基于区块链的云取证方案,该方案在提供证据的同时可实现身份的隐私保护;但方案的效率和安全均受限于中心信任节点。Pourvahab等[8]提出了一种基于移动物联网的取证框架,利用区块链轻量证明及智能合约获取证据,能保证证据完整性和可靠性;但密钥管理技术繁琐,无法适用车联网场景。Meheran等[9]利用区块链技术实现了物联网新型取证框架,但

收稿日期:2020-08-10;**修回日期**:2020-10-22;**录用日期**:2020-12-02。　**基金项目**:南通市科技项目(JC2018131)。
作者简介:陈葳葳(2000—),女,江苏南通人,主要研究方向:网络与信息安全、区块链、物联网;　曹利(1974—),男,江苏宜兴人,副教授,硕士,主要研究方向:网络与信息安全、区块链、边缘计算;　顾翔(1973—),男,江苏南通人,教授,博士,主要研究方向:网络通信协议、车联网、边缘计算。

方案存在时延问题。曹迪迪等[10]利用智能合约实现了一种分布式存证方法和区块的查询取证方法，可实现去中心化的可信证据存取；但存在共识机制周期较长、主链负荷过重等问题。黄晓芳等[11]提出了一种基于区块链技术的云计算电子取证模型，可以防止取证方的共谋篡改；但无法满足并发请求，算法效率需要进一步优化。Oham等[12]利用区块链存取证据，提出了一种自动车辆责任归属框架，能解决交通事故中车辆与制造商、保险公司、司法部门之间的信任问题，但存在低吞吐量和高延迟问题。

综上所述，区块链技术应用于车联网电子取证具有可行性，但存在低吞吐量、高延迟和共识算法慢等问题。针对上述问题，本文提出一种基于区块链的新型车联网电子取证方案，该方案根据汽车黑匣子数据记录方式设计了新的区块链储存结构，利用区块链在隐私保护和数据防篡改上的优势，安全存储汽车状态记录；优化入链算法，改进委托权益证明(Delegated Proof Of Stake，DPOS)共识算法，克服现有共识算法在执行效率上的不足；利用智能合约机制设计了电子证据的高效存取方案。

1 相关知识

1.1 车联网架构

车联网(Internet Of Vehicles，IOV)以每辆车为基本元素，通过传感器技术采集原始数据，再利用无线通信技术，实现车-路-处理平台的信息数据传播和通信交流。典型车联网结构主要由三类节点组成，如图1所示。

1)车辆节点(On Board Unit，OBU)：车辆节点作为具有移动属性的通信实体，通过部署各类智能传感器装置、计算装置及无线通信装置，实现信息的感知、采集、计算和通信功能。

2)路侧单元(Road Side Unit，RSU)：路侧单元作为固定通信节点，相对车辆节点具有更强的计算和存储能力，为车辆节点接入网络提供服务，并转发路况信息。

3)可信中心(Trust Center，TC)：此节点是网络结构中让所有节点无条件信任的基础服务设施，主要为接入节点颁发证书、存储密钥、完成身份认证。

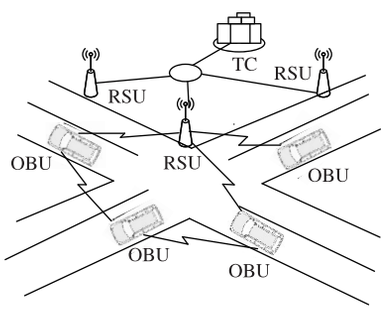

图1 车联网结构示意图

Fig. 1 Schematic diagram of IOV structure

1.2 区块链技术

区块链是一种按照时间顺序将数据区块以链条的方式组合而成的特定数据结构，并以密码学方式保证不可篡改和不可伪造性的去中心化共享总账。

区块链每一个数据区块主要由区块头和区块体组成：区块头用来记录当前区块的元数据，主要封装了当前版本号、前一个区块的地址、当前区块的目标哈希值、Merkle根等；区块体记录具体的数据，数据结构为Merkle树，数据记录在叶子节点，非叶子节点的值为所有叶子节点数据的哈希值而不是具体数据，减少了区块容量，便于同步与备份。区块体中数据经过哈希运算得到Merkle根，当某个区块的值发生变化，会造成整个区块链发生变化。另外，每个区块的时间戳确保了区块链中交易数据的不可篡改和可追溯。

一个区块从产生到成功入链经历交易分发、区块验证、区块同步三个阶段，共识算法是核心问题。传统的工作量证明(Proof of Work，PoW)、权益证明(Proof of Stake，PoS)、DPOS[13]等算法中矿工节点竞争效率低，交易传播和区块验证过程均需要在全网进行广播，如果网络中的节点数较多，将会占用大量的网络带宽，无法满足车联网时空型交易数据[14]的时效性。

2 车联网电子取证

2.1 方案架构

基于区块链的车联网电子取证整体架构如图2所示。在车联网环境下，车辆、RSU、交管部门、司法部门、保险公司组成联盟链。其中车辆、司法部门和保险公司为轻节点，存有各区块头部信息；辖区内各RSU和交管部门为全节点，负责全链存储和新区块入链。

1)RSU：在本方案中除了实现车联网传统的功能，还作为区块链全节点存储相关完整证据数据，完成网络路由、共识达成、交易记录等功能。在安全上，RSU通过第三方可信机构认证车辆身份。

2)交管部门：发生交通事故需要责任鉴定时，进行电子取证。在方案的共识机制改进算法中，各地区交管部门投票选取RSU共识节点，提高共识效率。

3)司法部门：由执法机构(交通警察和法院)组成，可查询并分析链中争端实体所存证据并进行责任判决；并向保险公司提供证据，以方便保险公司支付赔偿金。

4)保险公司：查询证据或者接受司法部门提供相关证据，决定赔偿方案。

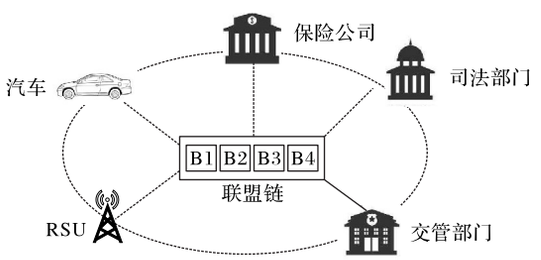

图2 基于区块链的车联网电子取证方案架构

Fig. 2 Framework of e-forensics scheme for IOV based on blockchain

基于区块链的车联网电子证据存取过程为：车辆线下向交管部门注册，获得初始化认证参数；在认证入网后，将行驶过程中采集的状态数据周期性发送至附近RSU；RSU验证数据可靠性后，进行新证据入链工作；当发生交通事故，需要责任认定时，司法部门和保险公司向交管部门申请查询权限，进行区块链查证，获得相关车辆的行驶状态数据，还原事故现场，进而进行责任判定。

2.2 快速共识算法

DPOS算法一般以共识21个区块为周期，21个区块生产者被投票选出，出块者100%在线的特性，保证了共识节点在1.5 s内必知晓一笔交易，轮流进行出块。但由于只有轮到节

点发言时才可发送交易确认信息,导致交易确认时间较长,从而使共识速度变慢,不适合车联网实时存证需求。新的快速共识算法以车辆、RSU、交管部门、保险公司、司法部门共同构成联盟链,其中RSU和交管部门为全节点,参与共识。

共识过程如图3所示:各地方交管部门投票选出21个RSU参与出块(1个RSU节点为主节点,剩余20个RSU节点进行区块的打包)。

1)RSU_j记满3个区块,先向主节点RSU_i发送共识请求;

2)主节点收到共识请求向其他19个RSU广播准备认证的请求消息,其他RSU进入认证准备状态;

3)RSU_j广播区块,其余RSU返回验证结果并继续打包区块;

4)RSU_j待收到认证通过消息后,将区块加入区块链。

本共识算法可以有效提高共识速度,优势在于:

1)实现本共识算法的节点存在联盟链中,所有共识节点均可信且在线;

2)主节点的存在使区块链不会产生分叉;

3)共识节点由多方交管部门投票选举,其随机性保证共识机制的可靠;

4)共识节点可随时发送验证结果无需等待发言权,且进行批量共识,大大提高共识速度,确保证据的时效性。

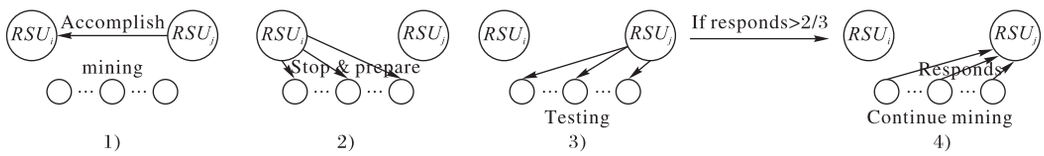

图3　共识过程

Fig. 3　Consensus process

2.3　区块存储结构和检索

方案定义的区块存储结构如图4所示:以key-value键值对存储交易信息。其中,key是由根结点到叶子节点路径拼接而成,路径上的key值依次为证据的上传时间、RSU的ID号、车辆ID号。所有数据按照“小时”为单位,同一小时上传的数据成为一条路径,再以“分”构成分支,在时间形成的分支下按照RSU和车辆的ID编码,以省、市、县进行归纳划分。数据的有序整合可快速定位到相应路径,提高查询效率。value值存储车辆状态数据。

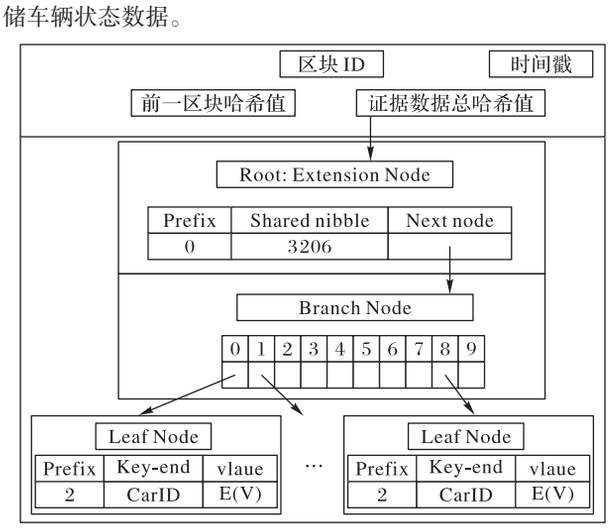

图4　区块存储结构

Fig. 4　Structure of block storage

区块检索采用Bloom Filter算法,算法通过哈希函数将交易数据压缩并存储为向量中的一点。如图5所示,设集合$X=\{x_0,x_1\}$经过哈希映射为$H(x_0)=(2,3,7)$和$H(x_1)=(4,7,9)$,则将向量$\boldsymbol{B}$第2、3、4、7、9处置为1。当查询y_0元素是否存在,由于$H(y_0)=(1,4,7)$,第一位为0,则表明y_0不在集合X中。

2.4　方案实现

电子取证方案的实现分为三个阶段:身份注册、实时存证和查询取证。车辆身份注册阶段分为线上及线下注册部分,部分思想引用文献[15]中预注册阶段方法。表1为方案符号说明。

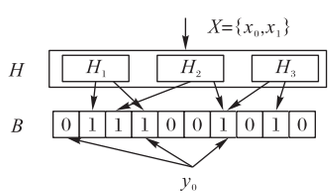

图5　Bloom Filter检索

Fig. 5　Retrieval of Bloom Filter

表1　符号及其含义

Tab. 1　Symbols and their meanings

符号	表示含义	符号	表示含义
G_1, G_2	满足双线性映射的群	V	证据
q, α	群中素数	N	随机数
$H()$	哈希加密函数	M	查询令牌
P_x	公钥	$Sign_x()$	签名算法
S_x	私钥	$E_x()$	加密算法
IM_i	身份唯一标识		

2.4.1　身份注册

车管所为可信第三方,进行RSU、车辆的初始化,产生初始参数:选择满足双线性映射的群G_1和G_2,生成随机数$s \in \mathbf{Z}_q^*$作为主密钥,其中$\mathbf{Z}_q^*$代表正整数集中的素数。计算公钥$P_{pub}=sq, n=\alpha q$。公开的参数有$\{G_1, G_2, n, P, P_{pub}, H_1, g\}$。其中$H_1:\{0,1\}^* \rightarrow G_1$代表单项哈希加密函数;$g$代表双线性映射;$G_1$、$G_2$分别是阶数为素数的加法群和乘法群;$P$为$G_1$的生成元。

身份注册由线下注册和线上注册两部分组成:线下实现车辆和RSU身份认证的参数初始化;线上实现临时身份注册,保证车辆通信的隐私安全。

1)线下注册。

车辆上牌照或年检时,车管所检验车辆状态,并根据车主提供的身份信息$INP_i \in \{0,1\}^*$(如手机号码、身份证号码)和车辆信息INC_i(如车牌号)设置共享密钥$x_i \in \mathbf{Z}_q^*$,并建立关联$R_i = H_1(INP_i) \oplus x_i$($\oplus$代表异或运算)。计算全局唯一标识$IM_i = H_1(INP_i \| x_i \| TS_{reg}) \in G_1$($TS_{reg}$表示注册时间),并根据所在地行政编号和车牌号形成车辆ID_i(如**市**区车辆ID_i为226001xx)。

部署RSU前，车管所统一购进RSU设备并为其初始化。车管所根据RSA公钥密码体制为RSU生成整数e满足$\gcd(\phi(n),e)=1$，生成公私钥对$\{P_R\{e,n\},S_R\{d,n\}\}$，其中$d=e^{-1}(\mathrm{mod}\,\phi(n))$。并分配$ID_r$为RSU的唯一标识（标识根据RSU所部属地区行政编号设计）。存储车管所与RSU的共享密钥k。RSU随机选择整数$r_r\in\mathbf{Z}_q^*$并且广播参数r_rP_R。

车管所存有ID_i—IM_i及ID_r—k映射数据。

交管部门为区块链中可信全节点，负责司法部门与保险公司身份信息的注册及认证。司法部门与保险公司于交管部门登记其合法身份信息，交管部门以同样方式初始化参数，为其分配ID_x及公私钥对$\{P_x,S_x\}$，并存有ID_x—P_x映射数据。

2）线上注册。

车辆行驶时入网过程：

a）利用RSA算法自行生成公私钥对$\{P_{\mathrm{Token}},S_{\mathrm{Token}}\}$。

b）根据临时公钥生成临时身份凭证Token，其结构如图6所示。

区域号	P_{Token}	时间戳

图6 Token结构

Fig. 6 Structure of Token

c）驶入某路段RSU覆盖范围时，接收RSU周期性广播的信息，向其发送消息$m_0=\{A_i,TS_i,P_{\mathrm{pub}}\}$。其中$A_i$表示$\{ID_i\|P_{\mathrm{pub}}\|IM_i\|\mathrm{Token}\|TS_i\}$用RSU公钥$P_R$加密信息的结果。

d）RSU收到m_0，先验证时间戳$|T-TS_i|<\Delta T$是否有效，若有效则用S_R解密A_i，获得ID_i和P_{pub}，并验证参数P_{pub}是否与m_0中明文相一致。确保信息的有效性和完整性后，向车管所请求车辆身份验证：生成消息$m_1=\{C,\mathrm{MAC},TS_r,P_R\}$。其中$C=E_k(IM_i\|ID_i)$，$k$为RSU与车管所的共享密钥。

e）车管所检查$|T-TS_r|<\Delta T$是否成立，并利用验证码MAC验证消息完整性，使用共享密钥解密消息得IM_i和ID_i，检验车辆身份的合法性；最后将车辆的身份合法性告知RSU。

f）RSU收到车管所响应的验证通过消息后，将车辆Token与ID_i、IM_i映射关系存入区块链，车辆获得临时公私钥使用权。

车辆用此临时公私钥代替长期身份标识IM_i实现车辆的本次匿名存证，同时在Token时间戳有效期间，使得车辆在跨RSU通信时无需再进行匿名身份的注册。

2.4.2 实时存证

车辆黑匣子将行驶过程中记录的车辆状态信息发送至RSU，RSU验证车辆身份的同时产生会话密钥（使得向同一个RSU存证时无需频繁身份认证），车辆用此会话密钥加密上传证据；RSU调用智能合约存入证据。具体流程如图7所示。

1）会话建立。

a）车辆计算会话密钥$key=H_1(g(r_rP_r,P_{\mathrm{pub}})^{ri})$，车辆接受RSU广播数据，生成随机整数$r_r\in\mathbf{Z}_q^*$，计算会话密钥$key$。

b）车辆向RSU发送握手请求req_1：$E_{PR}(\mathrm{Token},r_iP,N_1,Sign_{STOken})$，车辆用私钥生成签名$Sign_{STOken}$；请求消息用RSU的公钥$P_R$加密发送。

c）RSU→车：res_1：$E_{key}(\mathrm{Success},Sign_{SR}(N_1))$。

① 验证车辆身份：

私钥解密消息$req_1{}^{SR}\,\mathrm{mod}\,n$，并验证签名$(Sign_{STOken})^{P_{\mathrm{Token}}}\ \mathrm{mod}\ n=(\mathrm{Token}\|N_1\|r_iP)$是否正确，调用智能合约，在区块链中检索定位到Token所对应的key-value分支，即认可车辆身份合法，同时获取value：车辆ID_i。若未找到分支，丢弃此消息。

②响应握手请求：

RSU生成会话密钥$key=H_1(g(r_rS_r,r_iP))$。对选取随机数N_1的签名$Sign_{SR}(N_1)$、认证结果Success用会话密钥加密作为消息$res_1=E_{key}(\mathrm{Success},Sign_{SR}(N_1))$发送至车辆。

2）存证。

a）车辆身份授权：车辆接收RSU握手响应，使用会话密钥解密得Success，验证签名$(Sign_{SR})^{P_R}\,\mathrm{mod}\,n=N_1'$，确认$N_1=N_1'$，得到临时公私钥使用权。

b）车辆证据上传：req_2：$E_{key}(V,Sign_{STOken}(N_1))$，证据数据结构$V$定义如图8所示，包含数据上传时间、接入$RSU_{ID}$、车辆$ID$、当前状态数据、签名字段。附加随机数$N_1$签名后加密发送至RSU。

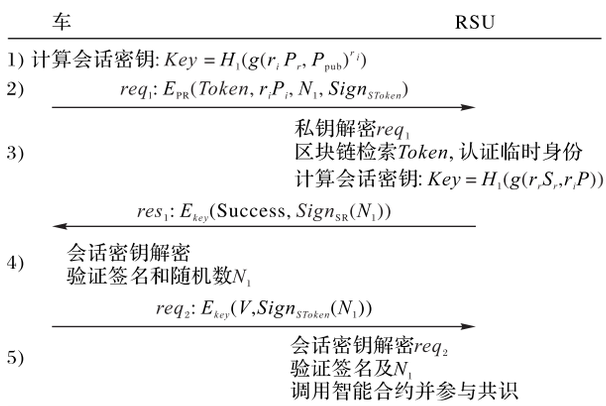

图7 存证流程

Fig. 7 Process of log evidences

时间	RSU_{ID}	Car_{ID}	车辆状态数据	$Sign_{Sv}$

图8 证据数据结构

Fig. 8 Data structure of evidence

c）RSU接收密文证据：会话密钥解密得明文V，验证签名和随机数N_1的正确性，触发智能合约Save Evidence算法，建立key（时间、RSU_{ID}、车辆ID）与value（电子证据）的区块链键值对，存储车辆-证据映射关系。RSU签名此映射广播至全网。

```
Algorithm 1:Save Evidence
Input:RSU_ID,Car_ID,evidences
Output:RSU_ID+Car_ID                    //与加密的evidences的映射关系
begin
  let stack = new Stack()
                          //存入RSU、车辆ID与加密证据映射的栈
  If RSU_ID && Car_ID are valid then{
    return stack.push(RSU_ID,Car_ID,evi)
  }else{
    return fail
  }
end
```

4）证据入链。

参与共识的RSU通过验证签名将映射关系记入区块，并使用新共识算法对记满的区块快速达成共识，加入区块链尾部。

2.4.3　查询取证

交通事故发生后,需要电子取证进行责任认定。保险公司先查询本地轻节点,判断电子证据在区块链中的存在性。若存在,向交管部门全节点申请查询权限令牌,利用该令牌激活查询智能合约,执行区块链数据检索。具体流程如图9所示。

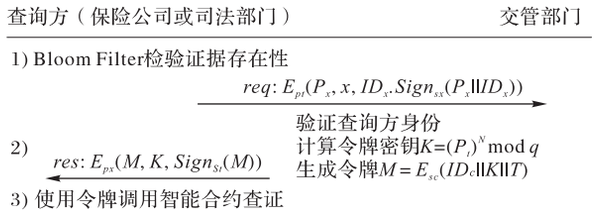

图9　查证流程

Fig. 9　Process of searching evidence

1)查询方向交管部门申请取证。

$req = E_{pt}(P_x, ID_x, Sign_{Sx})$

查询方为轻节点,首先使用Bloom Filter算法,查询本节点中存储的区块头,根据哈希映射判断证据的存在性,若存在则对全节点申请查询权限,申请消息如下:

$req = E_{pt}(P_x, ID_x, Sign_{Sx})$

其中,$Sign_{Sx}$表示交管部门对信息P_x和ID_x的签名。申请消息使用交管部门公钥P_t加密。

2)交管部门颁发查询令牌。

$res = E_{Px}(M, K^*, Sign_{St}(M))$

交管部门在本地数据库检索ID_x—P_x,验证查询方身份合法性。使用自身公钥P_t,结合随机数N,计算令牌密钥$K^* = (P_t)^N \bmod q$。由令牌密钥生成查询令牌:$M = E_{St}(ID_t \| K^* \| TS_{reg})$,其中$TS_{reg}$为令牌注册时间戳,用于限制查询时间;$ID_t$为交管部门身份标识。最后加密令牌生成消息$res$传输给查询方。

3)取证。

查询方用私钥解密res,验证签名$Sign_{St}$正确性后,提取令牌M、密钥K^*。

查询方获得令牌M,激活智能合约,以(车辆ID,肇事时间T_0,待查时间范围T_{ran})为参数,调用取证算法Search Evidence查找对应区块中车辆证据数据。

```
Algorithm 2: Search Evidence
Input: T0, Tran, Car_ID
Output: Ek(evi)
begin
  decrypt RSA(M)                                    //解密M
  let RSU = new stack()
  function Searchevi(){
    if ID == 'legal' && T - TS_reg < ΔT{
      while(Block = Bloom Filter(Car_ID)){
        Branch[][] = travel(Block)
        while(Branch[i++] ! = null){
          if(Time ≤ T0 - Tran||Time ≥ T0 + Tran)
            if(CAR == Car_ID)
                CARe == value.get()                 //肇事车辆证据
                let RSU_ID == Branch[i].length()
                                                    //提取区块链中RSU_ID
                RSU.push(RSU_ID)
        }
        while(Block = Bloom Filter(RSU_ID.top())){
          Branch[] = travel(Block)
          while( Branch[i++] ! = null ){
            if(Time ≤ T0 - Tran||Time ≥ T0 + Tran)
              if(RSU == RSU_ID)
                  RSUe = value.get()}               //肇事车辆证据
          RSU_ID.pop()
        }
      } else {return fail }
      evi=CARe.concat(RSUe)
      return Ek(evi)
    }
    function travel(Block){
      let Branch[i][j++]=node
      return Branch
    }
  end
```

算法步骤如下:

a)判断令牌有效性。交管部门解密令牌$M^{Pt} \bmod n$,得到数据$ID_t \| K^* \| TS_{reg}$,存在ID_t则表明查询者已获得权限。

b)判断令牌时效性。若$T - TS_{reg} > \Delta T$,令牌时效已过,无权查询,否则执行步骤c)。

c)定位证据所在区块。调用Bloom Filter算法计算车辆ID_x的哈希映射,查询对应区块,执行步骤d)。

d)travel函数遍历定位的区块。对每一条分支,执行步骤e)。

e)匹配待查车辆在$T_0 \pm T_{ran}$时间范围内对应存储路径,对每一条符合条件路径,执行步骤f);

f)获取路径键值中的RSU_{ID}值,以(RSU_{ID},T_0,T_{ran})为参数,重复c)~d)步骤查找同时段同一RSU下车辆的证据。

g)使用令牌密钥加密证据(结构如图8),返回给查询方。

4)查询方接收证据信息。

查询方使用令牌公式密钥K^*解密:$D_k(evi)$,获得证据数据。

证据除了包含事故时段内,本车辆的状态数据外,还包含此时段内,与本车接入同一RSU的其他车辆状态数据。司法机关和保险公司可以根据查得数据全面有效地还原事故现场相关车辆的状态,从而判定责任归属。

3　仿真结果及分析

方案采用Hyperledger Fabric开源代码进行仿真实验,在Linux操作系统中利用docker搭建联盟链模型,模拟6个RSU作为节点进行共识,采用go语言编写智能合约,完成证据的存取操作。实验设计了电子存取证系统,分别模拟合法入网车辆进行证据的上传,及可信查询方进行证据的获取。实验结合吞吐量与取证响应时间对系统的可行性进行分析。

3.1　实验结果及可行性分析

方案在虚拟机中部署6个区块链节点,代表共识的节点RSU,负责车辆证据的入链及更新操作。表2显示RSU在1 h内的测试情况,结果表明6个共识节点均保持在线状态,且进行证据的更新操作。

表2 可行性分析

Tab. 2 Feasibility analysis

节点	在线状态/min	是否更新
R1	48/60	是
R2	54/60	是
R3	56/60	是
R4	60/60	是
R5	57/60	是
R6	59/60	是

3.2 安全性分析

1)证据存储的不可篡改与可追溯性。

在传统车联网电子取证模型中,车辆将证据全部发送至云数据中心进行处理存在较大风险——实时性和安全性。高速行驶的车辆需要在毫秒时间内得到响应,一旦由于数据传输、网络攻击等问题,车辆状态数据将无法记录,从而带来责任归属难题。另外,由于中心云服务器面临高负荷数据处理工作,且极易遭到篡改、窃听及拒绝服务等攻击,证据的破坏将对车联网用户造成巨大的损失。本文方案结合区块链技术存储车辆的电子证据,将存取证服务移至车辆就近的RSU,进行边缘处理,满足低时延、大连接需求。区块链以区块头部中的哈希值串联而成,利用了哈希函数的不可逆性与极难碰撞性(一旦修改一个数据,整条链的哈希值随之发生变化),加大攻击难度,使得存储在区块链中的证据无法篡改且不可否认。由于区块链永久存在,并按照时间顺序排列,故每条记录都可通过时间追溯。

2)证据访问控制和身份隐私保护。

保险公司、司法部门、车辆都为轻节点,只存储区块头部信息,无法查看区块链中完整证据,完整证据的获取需要向交管部门申请令牌,只有在交管部门授权条件下可查询证据。令牌可根据需要规定有效期限,由随机数构成一次一密,保护了证据隐私。

车辆使用临时匿名私钥进行证据的签名,临时身份Token带有时间戳,可在不定时间内进行更新,保护车辆身份的隐私。

3)会话过程的安全性。

a)会话密钥产生安全性。

车辆计算会话密钥:$\text{key} = H_1(g(r_rP_r, P_{pub})^{r_i})$;

RSU计算会话密钥:$\text{key} = H_1(g(r_rS_r, r_iP))$;

car:$H_1(g(r_rP_r, P_{pub})^{r_i}) = H_1(g(r_rp_r, sP)^{r_i}) = H_1(g(P_r, P)^{r_rr_is})$;

RSU:$H_1(g(r_rSP_r, r_iP)) = H_1(g(r_rS_r, r_iP))$。

单项哈希函数加密,保证会话密钥的安全,同时采用随机数抵御中间人攻击。

b)会话过程安全性。

会话明文以分组为单位进行加密,每个分组的二进制均小于n,设$P_R = \{e, n\}$,$S_R = \{d, n\}$,明文为m。

①加密:$C = m^e \bmod n$;

②解密:$M = C^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$。

数学攻击的途径:分解n为两个素因子。计算出$\phi(n) = (p-1)(q-1)$,从而确定$d \equiv e^{-1}(\bmod \phi(n))$。由给定的$n$来确定$\phi(n)$等价于因子分解$n$,基于大整数的因式分解难题无法破解私钥。对于选择密文攻击(Chosen Ciphertext Attack, CCA),由于$E_{P_x}(M_1) \times E_{P_x}(M_2) = E_{P_x}([M_1, M_2])$,利用如下方法解密:

①计算$X = (C \times 2^e) \bmod n$;

②将X作为选择明文提交,并收到:

$Y = X^d \bmod n$

③$X = (C \bmod n) \times (2^e \bmod n) = (M^e \bmod n) \times (2^e \bmod n) = (2M)^e \bmod n$

因此,得到M。为防止此类攻击,在加密前对明文进行随机填充。使得密文随机化,从而性质不成立。使之无法破解。

同时因为私钥只有本地可知,对于公钥加密信息只有对应私钥可解,只有私钥拥有者才可进行数字签名,保证传输数据的保密性、完整性和可靠性。

c)查证安全性。

查证时,令牌密钥由交管部门私钥和随机数计算得到,实现一次一密,保证令牌的不可伪造性与安全性,从而实现可靠证据传输。

3.2 功能对比

和其他已知电子存证方法的功能对比如表3所示。

表3 电子存证方法的功能对比

Tab. 3 Functional comparison of electronic deposition methods

性能	智能合约可信存证	云计算电子取证模型	自动驾驶车辆责任归属	本文方案
存证高效	√			√
证据完整可信	√	√	√	√
操作简便	√	√		√
隐私保密性				√
快速共识				√

3.3 性能分析

3.3.1 共识算法的改进

本文方案基于DPOS设计了新型共识机制,改进后的算法可批量验证区块,改善了DPOS原有轮流出块高时延缺陷,提高了存证效率,确保证据的第一时效性。方案模拟了400个车辆存证情况下,在10 min内RSU出块时延的变化,如图10所示,传统DPOS算法和本文方案由于频繁交互均出现先增高后降低的趋势,在6~8 s时,系统性能较稳定,本文方案的新共识算法在吞吐量方面的性能优于传统DPOS。

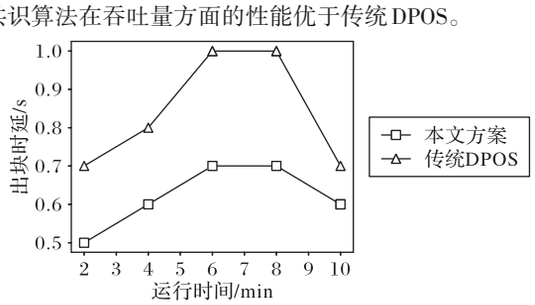

图10 系统吞吐量分析

Fig. 10 System throughput analysis

3.3.2 取证响应时间测试

方案为测试取证时延,分别模拟400~600次查询方调用智能合约进行车辆状态数据的获取,计算取证平均响应时间。结果如图11所示,随着请求次数的增加,时延呈上升趋势,但响应时间均维持在4 s内。传统的电子取证多为远程中心化,由于带宽及距离因素,存证时延在10 s左右。本文方案设计了适用于车联网的电子取证方案,将存取证任务边缘化,减少了远程传输时延,可满足车联网取证需求。

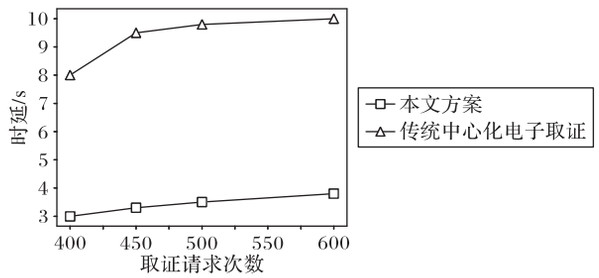

图11　响应时间测试

Fig. 11　Test of response time

另外,由于本文方案设计的查证方都属于区块链的轻节点(保险公司、司法部门),事先通过Bloom Filter可得知证据是否存在于区块链,减轻智能合约负荷,再使用travel函数定位完整证据,提高查询效率。

综上所述,本文方案采取改进的DPOS共识机制,能有效提高存证共识效率,同时取证响应速度可满足场景需求,说明了本文方案是高效可行的。

4　结语

为了更有效地进行机动车责任认定,本文设计了基于区块链的车联网环境下电子取证方案,利用区块链技术实现了电子证据的不可篡改、不可否认及永久保存;并提出新的高效率批量共识机制,以满足车联网实时性要求。方案通过令牌授权技术实现查询权限控制,结合智能合约完成快速的证据检索。通信过程使用公钥密码体制,保证车辆用户身份的匿名、数据传输的保密性与完整性。目前对于电子证据的存证问题,国内外研究不多,希望通过引入区块链技术,能为车联网的电子存证探索一种新的思路,以期抛砖引玉。

参考文献 (References)

[1] 陈小优. 交通肇事逃逸行为研究[D]. 广州:华南理工大学, 2012:20-23. (CHEN X Y. Escaping behavior after causing a traffic accident research [D]. Guangzhou: South China University of Technology, 2012:20-23.)

[2] 刘潇. 为车辆保驾护航的智能黑匣子探密[J]. 交通与运输, 2016, 32(5):58-59. (LIU X. Exploring the secret of the intelligent black box that protects vehicles [J]. Traffic and Transportation, 2016, 32(5):58-59.)

[3] 刘雪花,丁丽萍,刘文懋,等. 一种基于软件定义安全和云取证趋势分析的云取证方法[J]. 计算机研究与发展, 2019, 56(10): 2262-2276. (LIU X H, DING L P, LIU W M, et al. A cloud forensics method based on SDS and cloud forensics trend analysis [J]. Journal of Computer Research and Development, 2019, 56 (10):2262-2276.)

[4] 沈鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): No. 00107. (SHEN X, PEI Q Q, LIU X F. Survey of block chain [J]. Chinese Journal of Network and Information Security, 2016, 2(11): No. 00107.)

[5] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4):481-494. (YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4):481-494.)

[6] 胡铭. 用区块链技术解决刑事诉讼证明难题[N]. 民主与法制时报, 2020-05-14(6). (HU M. Using blockchain technology to solve the proving problem of criminal proceedings [N]. Democracy and Law Times, 2020-05-14(6).)

[7] ZHANG Y, WU S, JIN B, et al. A blockchain-based process provenance for cloud forensics [C]// Proceedings of the 3rd IEEE International Conference on Computer and Communications. Piscataway: IEEE, 2017: 2470-2473.

[8] MALAMAS V, DASAKLIS T, KOTZANIKOLAOU P, et al. A forensics-by-design management framework for medical devices based on blockchain [C]// Proceedings of the 2019 IEEE World Congress on Services. Piscataway: IEEE, 2019:35-40.

[9] POURVAHAB M, EKBATANIFARD G. An efficient forensics architecture in software-defined networking-IoT using blockchain technology[J]. IEEE Access, 2019, 7: 99573-99588.

[10] 曹迪迪,陈伟. 基于智能合约的以太坊可信存证机制[J]. 计算机应用, 2019, 39(4): 1073-1080. (CAO D D, CHEN W. Mechanism of trusted storage in Ethereum based on smart contract [J]. Journal of Computer Applications, 2019, 39(4): 1073-1080.)

[11] 黄晓芳,徐蕾,杨茜. 一种区块链的云计算电子取证模型[J]. 北京邮电大学学报, 2017, 40(6):120-124. (HUANG X F, XU L, YANG X. Blockchain model of cloud forensics [J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40 (6):120-124.)

[12] OHAM C, KANHERE S S, JURDAK R, et al. A blockchain based liability attribution framework for autonomous vehicles [EB/OL]. [2020-05-31]. https://arxiv.org/pdf/1802.05050.pdf.

[13] 丁越. 基于区块链的共识机制研究[D]. 南京:南京邮电大学, 2019:12-13. (DING Y. Research on consensus mechanism based on blockchain [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2019:12-13.)

[14] 傅易文晋,陈华辉,钱江波,等. 面向时空数据的区块链研究综述[J]. 计算机工程, 2020, 46(3):1-10. (FU Y W J, CHEN H H, QIAN J B, et al. Survey of blockchain research for spatiotemporal data [J]. Computer Engineering, 2020, 46(3): 1-10.)

[15] 陈葳葳,曹利,邵长虹. 基于区块链技术的车联网高效匿名认证方案[J]. 计算机应用, 2020, 40(10):2992-2999. (CHEN W W, CAO L, SHAO C H. Blockchain based efficient anonymous authentication scheme for IOV [J]. Journal of Computer Applications, 2020, 40(10):2992-2999.)

This work is partially supported by the Science Research Program of Nantong (JC2018131).

CHEN Weiwei, born in 2000. Her research interests include network and information security, blockchain, internet of things.

CAO Li, born in 1974, associate professor, M.S. His research interests include network and information security, blockchain, edge computing.

GU Xiang, born in 1973, professor, Ph. D. His research interests include network communication protocol, internet of vehicles, edge computing.