(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107465673 A
(43)申请公布日 2017.12.12

(21)申请号 201710637506.7

(22)申请日 2017.07.27

(71)申请人 深圳市易成自动驾驶技术有限公司
地址 518000 广东省深圳市南山区西丽街道高新科技产业园北区朗山路16号华瀚创新园

(72)发明人 刘新 单单 周军

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国 赵爱蓉

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/06(2009.01)
G08G 1/017(2006.01)

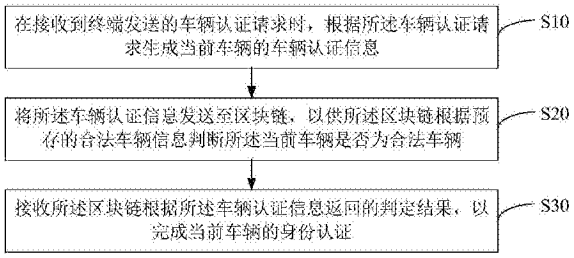
权利要求书2页 说明书9页 附图3页

(54)发明名称

车辆的身份认证方法、装置及计算机可读存储介质

(57)摘要

本发明提供一种车辆的身份认证方法、装置及计算机可读存储介质，所述车辆的身份认证方法通过在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；将所述车辆认证信息发送至区块链，以供所述区块链根据预存的合法车辆信息判断所述当前车辆是否为合法车辆；接收所述区块链根据所述车辆认证信息返回的判定结果，以完成当前车辆的身份认证。通过上述方式，本发明可安全、便捷地对车辆进行身份验证，提升了对待认证车辆身份认证的精确度，避免了接收非法车辆发送的信息，从而增加了系统内车辆之间通信的抗干扰能力，解决了CACC中的车辆之间的通信容易被干扰的技术问题。



CN 107465673 A

1.一种车辆的身份认证方法，其特征在于，所述车辆的身份认证方法应用于协同式自适应巡航控制系统CACC，所述车辆的身份认证方法包括以下步骤：

在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

2.如权利要求1所述的车辆的身份认证方法，其特征在于，所述在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息的步骤之前，还包括：

接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息；

将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

3.如权利要求1所述的车辆的身份认证方法，其特征在于，所述根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证的步骤包括：

若所述区块链中，存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为合法车辆；

在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记。

4.如权利要求3所述的车辆的身份认证方法，其特征在于，所述根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证的步骤还包括：

若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

5.如权利要求1-4中任意一项所述的车辆的身份认证方法，其特征在于，所述在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息的步骤包括：

在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

6.一种车辆的身份认证装置，其特征在于，所述车辆的身份认证装置包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的车辆的身份认证程序，其中所述车辆的身份认证程序被所述处理器执行时实现以下步骤：

在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

7.如权利要求6所述的车辆的身份认证装置，其特征在于，所述车辆的身份认证程序被

所述处理器执行时，还实现以下步骤：

接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息；

将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

8.如权利要求6所述的车辆的身份认证装置，其特征在于，所述车辆的身份认证程序被所述处理器执行时，还实现以下步骤：

若所述区块链中，存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为合法车辆；

在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记；

若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

9.如权利要求6-8中任意一项所述的车辆的身份认证装置，其特征在于，所述车辆的身份认证程序被所述处理器执行时，还实现以下步骤：

在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有车辆的身份认证程序，所述车辆的身份认证程序被处理器执行时实现如权利要求1-5中任意一项所述的车辆的身份认证方法的步骤。

车辆的身份认证方法、装置及计算机可读存储介质

技术领域

[0001] 本发明涉及自动驾驶技术领域，尤其涉及一种车辆的身份认证方法、装置及计算机可读存储介质。

背景技术

[0002] 随着车辆附加功能的增加，用于提高车辆安全性能的智能巡航控制系统(SCC)的安装率也越来越高。SCC用于使当前车辆与前方车辆保持恒定距离的同时提供巡航功能，即车辆可以通过SCC系统以驾驶者设定的恒定速度自动行驶。协同式自适应巡航控制系统(CACC)将车辆与外界的通信系统(V2X)添加到SCC中来进一步提高SCC的系统性能。具体地，CACC通过车辆与基础设施的通信系统(V2I)来确定道路的限制速度，通过车辆与车辆的通信系统(V2V)来接收关于在同一车道中行驶的前方车辆的信息，最后基于所接收到的信息提高来进一步提高SCC的系统性能。车辆与车辆的通信系统(V2V)中，车辆之间进行通信之前，需要对系统内的成员身份进行认证，以保证通信的车辆为系统内的合法成员。传统的V2V成员身份认证方法是使用CA公钥进行验证。由于使用CA公钥进行验证为第三方认证，如果第三方认证服务器出现信息泄露或者信息被篡改，则无法对待认证车辆身份进行精准认证，从而导致CACC中的车辆之间的通信容易被干扰。

发明内容

[0003] 本发明的主要目的在于提出一种车辆的身份认证方法、装置及计算机可读存储介质，旨在解决CACC中的车辆之间的通信容易被干扰的技术问题。

[0004] 为实现上述目的，本发明提供一种车辆的身份认证方法，所述车辆的身份认证方法应用于协同式自适应巡航控制系统CACC，所述车辆的身份认证方法包括以下步骤：

[0005] 在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

[0006] 根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

[0007] 根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

[0008] 可选地，所述在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息的步骤之前，还包括：

[0009] 接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息；

[0010] 将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

[0011] 可选地，所述根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证的步骤包括：

[0012] 若所述区块链中，存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为合法车辆；

[0013] 在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记。

[0014] 可选地，所述根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证的步骤还包括：

[0015] 若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

[0016] 在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

[0017] 可选地，所述在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息的步骤包括：

[0018] 在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

[0019] 根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

[0020] 此外，为实现上述目的，本发明还提供一种车辆的身份认证装置，所述车辆的身份认证装置包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的车辆的身份认证程序，其中所述车辆的身份认证程序被所述处理器执行时实现以下步骤：

[0021] 在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

[0022] 根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

[0023] 根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

[0024] 可选地，所述车辆的身份认证程序被所述处理器执行时，还实现以下步骤：

[0025] 接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息；

[0026] 将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

[0027] 可选地，所述车辆的身份认证程序被所述处理器执行时，还实现以下步骤：

[0028] 若所述区块链中，存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为合法车辆；

[0029] 在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记；

[0030] 若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

[0031] 在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

[0032] 可选地，所述车辆的身份认证程序被所述处理器执行时，还实现以下步骤：

[0033] 在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

[0034] 根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

[0035] 此外，为实现上述目的，本发明还提供一种计算机可读存储介质，所述计算机可读

存储介质上存储有车辆的身份认证程序，所述车辆的身份认证程序被处理器执行时实现如上所述的车辆的身份认证方法的步骤。

[0036] 本发明提供一种车辆的身份认证方法、装置及计算机可读存储介质，所述车辆的身份认证方法通过在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。通过上述方式，本发明利用区块链中数据不可篡改的特性，通过区块链保存合法车辆信息，然后根据区块链中存储的合法车辆信息对待认证的当前车辆的车辆认证信息进行验证。由此，本发明可安全、便捷地对车辆进行身份验证，提升了对待认证车辆身份认证的精确度，避免了接收非法车辆发送的信息，从而增加了系统内车辆之间通信的抗干扰能力，解决了CACC中的车辆之间的通信容易被干扰的技术问题。

附图说明

[0037] 图1为本发明实施例方案涉及的车辆的身份认证方法执行终端的终端结构示意图；

[0038] 图2为本发明车辆的身份认证方法第一实施例的流程示意图；

[0039] 图3为本发明车辆的身份认证方法第二实施例的流程示意图；

[0040] 图4为本发明车辆的身份认证方法第三实施例的流程示意图。

[0041] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0042] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0043] 本发明实施例方案的主要思路是：车辆的身份认证装置通过在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证，解决了CACC中的车辆之间的通信容易被干扰的技术问题。

[0044] 参照图1，图1为本发明实施例方案涉及的车辆的身份认证方法执行终端的终端结构示意图。

[0045] 本发明实施例的运行终端可以是PC，也可以是智能手机、平板电脑、电子书阅读器、便携计算机等具有显示功能的可移动式终端设备。

[0046] 如图1所示，该终端可以包括：处理器1001，例如CPU，通信总线1002、用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0047] 本领域技术人员可以理解，图1中示出的终端结构并不构成对运行终端的限定，可

以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0048] 继续参照图1，图1中作为一种计算机存储介质的存储器1005可以包括操作系统、网络通信模块、用户接口模块以及程序。其中，操作系统是管理和控制车辆的身份认证装置与软件资源的程序，支持网络通信模块、用户接口模块、车辆的身份认证程序以及其他程序或软件的运行；网络通信模块用于管理和控制网络接口1002；用户接口模块用于管理和控制用户接口1003。

[0049] 在图1所示的终端中，网络接口1004主要用于连接云服务器，与云服务器进行数据通信。用户接口1003还可以连接客户端(用户端)，与客户端进行数据通信；本发明终端中的处理器1001、存储器1005可以设置在车辆的身份认证装置中，所述车辆的身份认证装置通过处理器1001调用存储器1005中存储的车辆的身份认证程序，并执行以下操作：

[0050] 在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

[0051] 本实施例中，为了解决CACC中的车辆之间的通信容易被干扰的技术问题，本发明利用区块链中数据不可篡改的特性，通过区块链进行车辆的认证，提高车辆身份认证的精准度，从而屏蔽非法车辆发送的信息。本发明可应用于物流自动驾驶车队、婚礼自动驾驶车队等。为了便于说明，本实施例中选定自动驾驶车队进行描述，但本发明不仅仅限于自动驾驶车队。自动驾驶车队在行驶中发生变动情况时，需要给系统内的车辆发送信息，以便各个车辆能及时根据变动情况进行对应调整。具体地，待认证的当前车辆可通过终端向服务器发送车辆认证请求，其中所述终端可以是手机、pad等移动终端。服务器在接收到车辆发送的车辆认证请求时，将所述车辆认证请求进行解析，以获取需要的信息。并根据需要的信息生成所述当前车辆对应的车辆认证信息，该车辆认证信息可用于对所述当前车辆的身份是否属于系统内登记的合法车辆进行验证。

[0052] 根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

[0053] 具体地，服务器在生成对应的车辆认证信息后，将所述车辆认证信息根据预先保存的路径，发送至区块链。区块链在接收到服务器发送的车辆认证信息后，将所述车辆认证信息进行解析，获取当前车辆对应的车辆信息，将所述车辆信息与预先存储的合法车辆信息进行比对，并将比对结果反馈至服务器。服务器根据区块链的反馈结果，即区块链中是否存在与所述当前车辆的车辆信息匹配的合法车辆信息，来判断所述车辆认证信息对应的当前车辆是否为合法车辆。具体实施例中，可进一步获取区块链中匹配到的合法车辆信息对应的编号，将从所述车辆认证信息中解析获取得到的认证因子与所述编号进行匹配，判断是否一致。一致时，则区块链判定当前车辆为系统内已登记的合法车辆。否则，区块链判定当前车辆为系统内未登记的非法车辆。

[0054] 根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

[0055] 具体地，服务器在根据区块链反馈的信息在根据车辆认证信息判定当前车辆的身份后，将判定结果根据所述车辆认证请求对应的终端地址和/或服务器地址，将所述判定结果发送至对应至终端和/或服务器。终端和/或服务器在接收到该判定结果时，根据该判定结果将当前车辆进行标记，完成当前车辆的身份认证。系统会根据当前车辆的标记，对所述当前车辆发送的消息进行对应处理。

[0056] 本实施中提供一种车辆的身份认证方法、装置及计算机可读存储介质，所述车辆的身份认证方法通过在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。通过上述方式，本发明利用区块链中数据不可篡改的特性，通过区块链保存合法车辆信息，然后根据区块链中存储的合法车辆信息对待认证的当前车辆的车辆认证信息进行验证。由此，本发明可安全、便捷地对车辆进行身份验证，提升了对待认证车辆身份认证的精确度，避免了接收非法车辆发送的信息，从而增加了系统内车辆之间通信的抗干扰能力，解决了CACC中的车辆之间的通信容易被干扰的技术问题。

[0057] 进一步的，本发明终端中的处理器1001、存储器1005可以设置在车辆的身份认证装置中，所述车辆的身份认证装置通过处理器1001调用存储器1005中存储的车辆的身份认证程序，执行以下操作：

[0058] 接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息；

[0059] 将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

[0060] 进一步的，本发明终端中的处理器1001、存储器1005可以设置在车辆的身份认证装置中，所述车辆的身份认证装置通过处理器1001调用存储器1005中存储的车辆的身份认证程序，执行以下操作：

[0061] 若所述区块链中，存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为合法车辆；

[0062] 在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记。

[0063] 进一步的，本发明终端中的处理器1001、存储器1005可以设置在车辆的身份认证装置中，所述车辆的身份认证装置通过处理器1001调用存储器1005中存储的车辆的身份认证程序，执行以下操作：

[0064] 若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

[0065] 在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

[0066] 进一步的，本发明终端中的处理器1001、存储器1005可以设置在车辆的身份认证装置中，所述车辆的身份认证装置通过处理器1001调用存储器1005中存储的车辆的身份认证程序，执行以下操作：

[0067] 在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

[0068] 根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

[0069] 基于上述硬件结构，提出本发明车辆的身份认证方法实施例。

[0070] 参照图2，图2为本发明车辆的身份认证方法第一实施例的流程示意图。

[0071] 本实施例中，所述车辆的身份认证方法应用于协同式自适应巡航控制系统CACC，所述车辆的身份认证方法包括以下步骤：

[0072] 步骤S10，在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息；

[0073] 本实施例中，为了解决CACC中的车辆之间的通信容易被干扰的技术问题，本发明利用区块链中数据不可篡改的特性，通过区块链进行车辆的认证，提高车辆身份认证的精准度，从而屏蔽非法车辆发送的信息。本发明可应用于物流自动驾驶车队、婚礼自动驾驶车队等。为了便于说明，本实施例中选定自动驾驶车队进行描述，但本发明不仅仅限于自动驾驶车队。自动驾驶车队在行驶中发生变动情况时，需要给系统内的车辆发送信息，以便各个车辆能及时根据变动情况进行对应调整。具体地，待认证的当前车辆可通过终端向服务器发送车辆认证请求，其中所述终端可以是手机、pad等移动终端。服务器在接收到车辆发送的车辆认证请求时，将所述车辆认证请求进行解析，以获取需要的信息。并根据需要的信息生成所述当前车辆对应的车辆认证信息，该车辆认证信息可用于对所述当前车辆的身份是否属于系统内登记的合法车辆进行验证。

[0074] 进一步地，步骤S10包括：

[0075] S11，在接收到所述终端发送的车辆认证请求时，其中，所述车辆认证请求包括所述当前车辆的车辆信息和认证因子；

[0076] 具体地，所述车辆认证请求中包括当前车辆对应的车辆信息和认证因子。所述车辆信息包括车牌信息和车主信息等车辆的必要信息，认证因子可以包括以下一项或者多项：用户名信息、用户密码信息、设备指纹信息、动态码和车辆标记信息等。更多实施例中，认证因子还可包括其他可用于认证身份的信息。

[0077] S12，根据所述车辆信息和认证因子，生成所述当前车辆对应的车辆认证信息。

[0078] 具体地，服务器在根据终端发送的车辆认证请求解析获取到多赢的车辆信息和认证因子后，根据所述车辆信息和认证因子生成用于进行身份验证的车辆认证信息。

[0079] 步骤S20，根据所述车辆认证信息和区块链中预存的合法车辆信息，判断所述车辆认证信息对应的当前车辆是否为合法车辆；

[0080] 具体地，服务器在生成对应的车辆认证信息后，将所述车辆认证信息根据预先保存的路径，发送至区块链。区块链在接收到服务器发送的车辆认证信息后，将所述车辆认证信息进行解析，获取当前车辆对应的车辆信息，将所述车辆信息与预先存储的合法车辆信息进行比对，判断是否存在与所述当前车辆的车辆信息匹配的合法车辆信息。并获取匹配到的合法车辆信息对应的编号，将从所述车辆认证信息中解析获取得到的认证因子与所述编号进行匹配，判断是否一致。一致时，则区块链判定当前车辆为系统内已登记的合法车辆。否则，区块链判定当前车辆为系统内未登记的非法车辆。

[0081] 步骤S30，根据所述车辆认证信息对应的判定结果，完成当前车辆的身份认证。

[0082] 具体地，区块链在根据车辆认证信息判定当前车辆的身份后，将判定结果根据所述车辆认证请求对应的终端地址和/或服务器地址，将所述判定结果发送至对应至终端和/或服务器。终端和/或服务器在接收到该判定结果时，根据该判定结果将当前车辆进行标记，完成当前车辆的身份认证。系统会根据当前车辆的标记，对所述当前车辆发送的消息进行对应处理。

[0083] 本实施中提供一种车辆的身份认证方法、装置及计算机可读存储介质，所述车辆的身份认证方法通过在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当

前车辆的车辆认证信息;根据所述车辆认证信息和区块链中预存的合法车辆信息,判断所述车辆认证信息对应的当前车辆是否为合法车辆;根据所述车辆认证信息对应的判定结果,完成当前车辆的身份认证。通过上述方式,本发明利用区块链中数据不可篡改的特性,通过区块链保存合法车辆信息,然后根据区块链中存储的合法车辆信息对待认证的当前车辆的车辆认证信息进行验证。由此,本发明可安全、便捷地对车辆进行身份验证,提升了对待认证车辆身份认证的精确度,避免了接收非法车辆发送的信息,从而增加了系统内车辆之间通信的抗干扰能力,解决了CACC中的车辆之间的通信容易被干扰的技术问题。

[0084] 参照图3,图3为本发明车辆的身份认证方法第二实施例的流程示意图。

[0085] 本实施例中,基于上述图2所示实施例,所述车辆的身份认证方法的步骤S10之前,还包括:

[0086] 步骤S01,接收终端发送的车辆登记请求,获取所述车辆登记请求中的车辆身份信息;

[0087] 具体地,在终端向服务器发送车辆认证请求之前,需要将当前车辆的车辆信息加入区块链中进行存储,即终端向服务器发送当前车辆对应的车辆登记请求。服务器将所述车辆登记请求进行解析以获取其中的车辆身份信息。具体实施例中,终端还可以直接将车辆登记请求发送至区块链,以供区块链将所述车辆登记请求进行解析以获取其中的车辆身份信息。

[0088] 步骤S02,将所述车辆身份信息发送至所述区块链,以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储。

[0089] 具体地,区块链在接收到服务器发送的车辆身份信息或解析出车辆身份信息时,将所述车辆身份信息标记为合法车辆信息,并将所述合法车辆信息进行存储。并根据所述合法车辆信息生成对应的编号,并发送至对应终端。具体实施例中,还可以将所述编号发送至服务器,由服务器发送至对应终端,由对应终端将所述编号与车辆信息进行对应关联存储。以供后续生成认证因子。

[0090] 本实施中提供一种车辆的身份认证方法、装置及计算机可读存储介质,本实施例中进行提供合法车辆信息登记的渠道。本发明通过利用区块链中数据不可篡改的特性,通过区块链保存合法车辆信息,然后通过区块链中存储的合法车辆信息对待认证的当前车辆的车辆认证信息进行验证,以完成当前车辆的身份认证。由此,本发明可安全、便捷地对车辆进行身份验证,提升了对待认证车辆身份认证的精确度,避免了接收非法车辆发送的信息,从而增加了系统内车辆之间通信的抗干扰能力,解决了CACC中的车辆之间的通信容易被干扰的技术问题。

[0091] 参照图4,图4为本发明车辆的身份认证方法第三实施例的流程示意图。

[0092] 本实施例中,基于上述图2所示实施例,所述车辆的身份认证方法的步骤S20还包括:

[0093] 步骤S21,若所述区块链中,存在与所述车辆认证信息匹配的合法车辆信息,则判定所述车辆认证信息对应的当前车辆为合法车辆;

[0094] 具体地,若服务器在所述区块链中,获取到与所述车辆认证信息匹配的合法车辆信息,即表示该车辆认证信息与区块链中某一条合法车辆信息相匹配,则判定所述车辆认证信息对应的当前车辆为合法车辆。具体实施例中,服务器还可以直接通过接收到区块链

分局对应的车辆认证信息反馈的判定结果，并根据预先存储的对应信息，来判定所述判定结果是否为合法判定结果。如合法判定结果为0，非法判定结果为1等。

[0095] 步骤S22，在判定所述当前车辆为合法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行合法车辆标记。

[0096] 具体地，服务器在判定所述车辆认证信息对应的当前车辆为合法车辆，在所述当前车辆所属的CACC系统中，将所述当前车辆标记为合法车辆。标记为合法车辆之后，所述当前车辆所属的CACC系统在接收到当前车辆发送的指令时，将该指令判定为合法指令，并根据该指令对其他车辆进行对应的调整。更多实施例中，服务器还可以在将所述判定结果匹配到合法判定结果对应的信息时，如匹配到0，即当前车辆通过区块链认证，为合法车辆。将所述当前车辆标记为合法车辆，完成当前车辆的身份验证。

[0097] 步骤S23，若所述区块链中，不存在与所述车辆认证信息匹配的合法车辆信息，则判定所述车辆认证信息对应的当前车辆为非法车辆；

[0098] 具体地，若服务器在所述区块链中，查找不到与所述车辆认证信息匹配的合法车辆信息，即表示该车辆认证信息与区块链中任意一条合法车辆信息均不匹配，则判定所述车辆认证信息对应的当前车辆为非法车辆。具体实施例中，服务器可以在所述判定结果匹配到非法判定结果对应的信息时，如匹配到1，即当前车辆通过区块链认证，为非法车辆。

[0099] 步骤S24，在判定所述当前车辆为非法车辆时，在所述协同式自适应巡航控制系统CACC中将所述当前车辆进行非法车辆标记。

[0100] 具体地，服务器在判定所述车辆认证信息对应的当前车辆为非法车辆，在所述当前车辆所属的CACC系统中，将所述当前车辆标记为非法车辆。标记为非法车辆之后，所述当前车辆所属的CACC系统在接收到当前车辆发送的指令时，将该指令判定为非法指令，可直接屏蔽该指令，不作出回应措施。

[0101] 本实施中提供一种车辆的身份认证方法、装置及计算机可读存储介质，通过利用区块链中数据不可篡改的特性，通过区块链保存合法车辆信息，然后根据区块链预存的合法车辆信息对待认证的当前车辆的车辆认证信息进行验证，以完成当前车辆的身份认证。由此，本发明可安全、便捷地对车辆进行身份验证，提升了对待认证车辆身份认证的精确度，避免了接收非法车辆发送的信息，从而增加了系统内车辆之间通信的抗干扰能力，解决了CACC中的车辆之间的通信容易被干扰的技术问题。

[0102] 本发明还提供一种计算机可读存储介质。

[0103] 本发明计算机可读存储介质上存储有车辆的身份认证程序，所述车辆的身份认证程序被处理器执行时实现如上述车辆的身份认证方法的步骤。

[0104] 其中，车辆的身份认证程序被执行时所实现的方法可参照本发明车辆的身份认证方法的各个实施例，此处不再赘述。

[0105] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0106] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0107] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0108] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

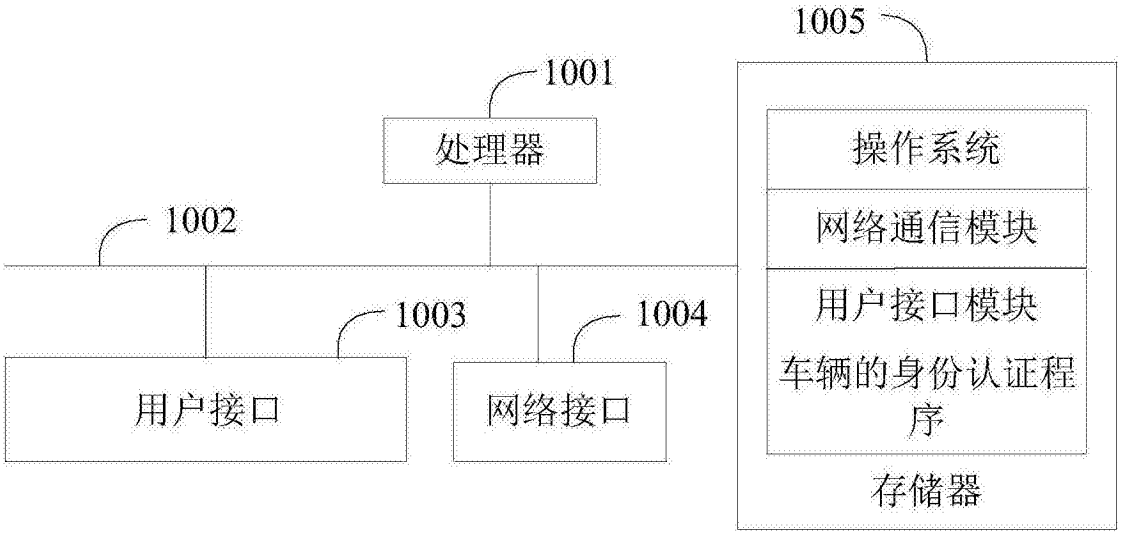

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
车辆的身份认证程序
1003
1004
用户接口
网络接口
存储器

图1

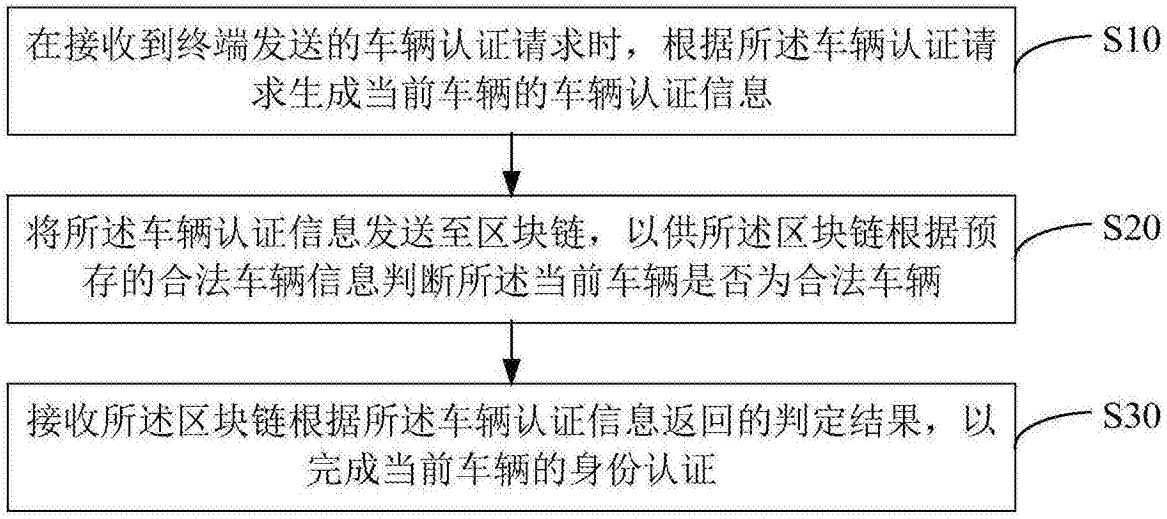

在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息
S10
将所述车辆认证信息发送至区块链，以供所述区块链根据预存的合法车辆信息判断所述当前车辆是否为合法车辆
S20
接收所述区块链根据所述车辆认证信息返回的判定结果，以完成当前车辆的身份认证
S30

图2

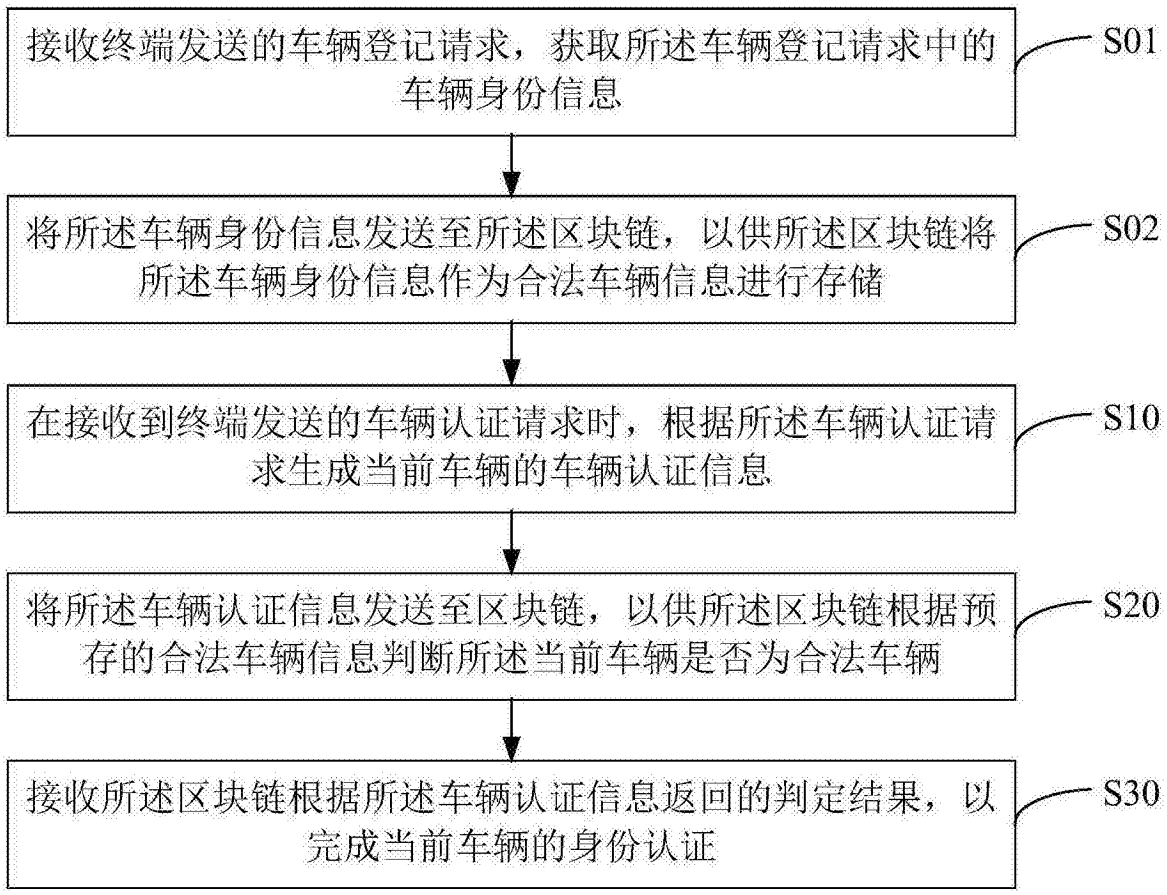

接收终端发送的车辆登记请求，获取所述车辆登记请求中的车辆身份信息
S01
将所述车辆身份信息发送至所述区块链，以供所述区块链将所述车辆身份信息作为合法车辆信息进行存储
S02
在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息
S10
将所述车辆认证信息发送至区块链，以供所述区块链根据预存的合法车辆信息判断所述当前车辆是否为合法车辆
S20
接收所述区块链根据所述车辆认证信息返回的判定结果，以完成当前车辆的身份认证
S30

图3

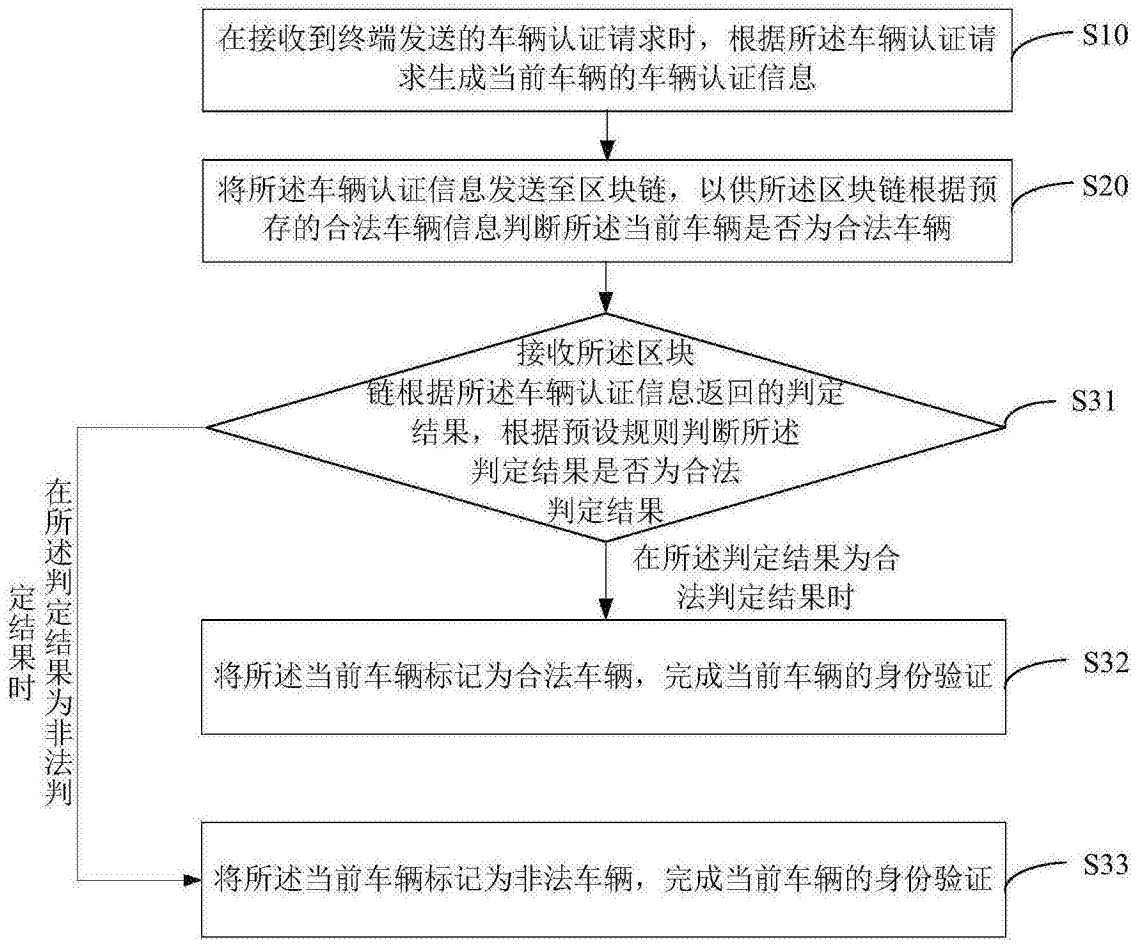

在接收到终端发送的车辆认证请求时，根据所述车辆认证请求生成当前车辆的车辆认证信息
S10
将所述车辆认证信息发送至区块链，以供所述区块链根据预存的合法车辆信息判断所述当前车辆是否为合法车辆
S20
接收所述区块链根据所述车辆认证信息返回的判定结果，根据预设规则判断所述判定结果是否为合法判定结果
S31
在所述判定结果为合法判定结果时
在所述判定结果为非法判定结果时
将所述当前车辆标记为合法车辆，完成当前车辆的身份验证
S32
将所述当前车辆标记为非法车辆，完成当前车辆的身份验证
S33

图4