(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114866261 B
(45)授权公告日 2022.09.09

(21)申请号 202210785948.7

(22)申请日 2022.07.06

(65)同一申请的已公布的文献号
申请公布号 CN 114866261 A

(43)申请公布日 2022.08.05

(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号

(72)发明人 张卫平 丁烨 张思琪 黄筱雨 丁园

(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
专利代理师 马肃 林淡如

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
G08G 1/00(2006.01)
G06Q 50/30(2012.01)

(56)对比文件
CN 110647763 A,2020.01.03
CN 108200159 A,2018.06.22
US 2018174446 A1,2018.06.21

审查员 何德超

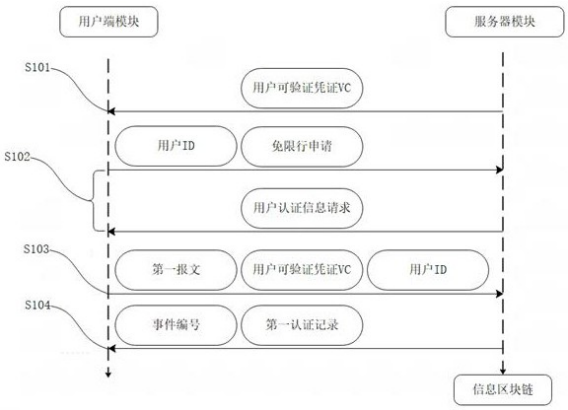
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种基于区块链技术的免限行申请处理系统

(57)摘要

本发明涉及一种基于区块链技术的免限行申请处理系统,所述处理系统包括运行一信息区块链,用于存储以及向所述处理系统提供用户、车辆的可验证信息;同时所述处理系统包括一种基于区块链技术的免限行申请处理方法;该方法通过分别对用户、用户-车辆以及车辆的三个阶段的合法性判断,从而判定用户及其驾驶的车辆是否合乎限行的豁免条件;进一步的,该处理方法更适合使用于汽车租凭、汽车共享等车辆不属于用户的使用场景下。



CN 114866261 B

1.一种基于区块链技术的免限行申请处理方法,所述处理方法应用于一种基于区块链技术的免限行申请处理系统,其特征在于,所述处理系统包括:

用户端模块,被配置为验证用户身份,生成并存储用户的用户ID、公钥PK和私钥SK;存储与所述用户ID对应的用户公开信息;其中所述用户公开信息包括公钥PK;接收用户的免限行申请,并生成相应的免限行申请信息;

服务器模块,包括用户认证子模块、申请认证子模块以及车辆认证子模块;所述用户认证子模块被配置为接收、处理用户的注册申请和用户认证信息请求;所述申请认证子模块被配置为用于接收、审核用户模块发出的免限行申请,并反馈免限行申请的审核结果;所述车辆认证子模块被配置为接收、处理车辆的车辆认证记录请求;

限行模块,多个所述限行模块被配置在限行区域的多个入口位置;所述限行模块用于记录用户在所述限行区域的通行记录,并且根据免限行申请的审核结果判断用户的通行记录是否违反限行规定;

其中,所述处理系统还包括信息区块链,多个所述限行模块以及所述服务器模块均作为所述信息区块链的节点,共同维护并参与该区块链的运行以及新区块的生成;所述用户端模块以及多个所述限行模块均与所述服务器模块通讯连接以进行数据传输;同时所述用户端模块由用户控制其与多个所述限行模块中的其中一个进行通讯连接;

所述处理方法包括执行以下用户认证步骤:

S101:由所述用户端模块将用户的用户ID以及所述用户公开信息在所述信息区块链中注册,由运行所述用户认证子模块的节点认证后,所述用户认证子模块向用户颁发用户可验证凭证VC,并将该用户可验证凭证VC发行于所述信息区块链;并且所述用户可验证凭证VC亦存储于所述用户端模块;

S102:由所述用户端模块将免限行申请以及用户ID发送到所述申请认证子模块;所述申请认证子模块在接收到一个免限行申请后,根据用户ID向对应的所述用户端模块发送用户认证信息请求,请求获取和认证该免限行申请的用户的信息;

S103:响应于来自所述申请认证子模块的用户认证信息请求,所述用户端模块将用户可验证凭证VC使用私钥SK进行数字签名后获得第一报文,将所述第一报文、所述用户可验证凭证VC以及用户ID传输到所述申请认证子模块;所述申请认证子模块根据用户ID从信息区块链获取对应的公钥PK,使用公钥PK解密所述第一报文从而获得解密后的用户可验证凭证VC,将解密后的用户可验证凭证VC与申请认证子模块接收的来自用户端模块的原始的用户可验证凭证VC进行校对验证,从而确认用户可验证凭证VC在传输过程中未被修改;

S104:所述申请认证子模块根据限行规定对用户可验证凭证VC进行判定是否合乎免限行条件;并当认证通过后,生成对应所述免限行申请的事件编号以及属于该事件编号的第一认证记录;将所述事件编号以及所述第一认证记录写入所述信息区块链的区块;并且包括将所述事件编号以及所述第一认证记录返回到所述用户端模块。

2.如权利要求1所述一种基于区块链技术的免限行申请处理方法,其特征在于,所述处理方法还包括执行以下用户-车辆认证步骤:

S201:用户通过所述用户端模块将待驾驶的车辆ID以及用户ID发送到所述车辆认证子模块;

S202:所述车辆认证子模块根据用户ID从信息区块链获取对应的公钥PK,并根据车辆

ID从信息区块链获取对应的车辆可验证凭证VC；

S203：所述车辆认证子模块将所述车辆可验证凭证VC通过公钥PK加密后生成第二报文，并将所述第二报文发送到所述用户端模块，由所述用户端模块通过私钥SK解密所述第二报文，从而获得车辆可验证凭证VC；

S204：所述用户端模块保存所述车辆可验证凭证VC。

3.如权利要求2所述一种基于区块链技术的免限行申请处理方法，其特征在于，所述处理方法还包括执行以下通行认证步骤：

S301：当用户驾驶车辆通过其中一个所述入口进入所述限行区域时，令所述用户端模块与位于该限行区域的入口的所述限行模块建立通讯；其后，所述用户端模块执行将所述第一认证记录以及车辆可验证凭证VC进行哈希函数运算生成第一认证摘要；将所述事件编号、所述第一认证摘要发送到所述限行模块；

S302：所述限行模块执行：识别用户驾驶车辆的车辆ID；将车辆ID、所述事件编号以及所述第一认证摘要发送到所述申请认证子模块；

S303：所述申请认证子模块在接收到所述限行模块发送的车辆ID、所述事件编号以及所述第一认证摘要，执行：记录所述限行模块的位置；根据所述事件编号从所述信息区块链获得第一认证记录；根据车辆ID从所述信息区块链获得车辆可验证凭证VC；使用哈希函数对获得的所述第一认证记录以及车辆可验证凭证VC进行哈希运算，生成第二认证摘要；比对所述第一认证摘要与所述第二认证摘要是否相同；根据限行规定对车辆可验证凭证VC进行判定是否合乎免限行条件。

4.如权利要求3所述一种基于区块链技术的免限行申请处理方法，其特征在于，所述用户ID以及所述车辆ID均由所述处理系统以分布式生成。

5.如权利要求4所述一种基于区块链技术的免限行申请处理方法，其特征在于，在所述信息区块链中对车辆进行注册，注册成功后的车辆在所述信息区块链中拥有一个唯一的车辆ID，并由所述车辆认证子模块根据车辆的具体信息生成车辆可验证凭证VC，并将该车辆可验证凭证VC发行于所述信息区块链；其中，所述车辆ID向所有用户以及所述信息区块链的所有节点公开。

6.如权利要求5所述一种基于区块链技术的免限行申请处理方法，其特征在于，当所述服务器模块无法完成所述用户认证步骤、所述用户-车辆认证步骤以及所述通行认证步骤中一个或多个步骤时，记录该用户驾驶车辆进入限行区域的行为属于非认证行为。

一种基于区块链技术的免限行申请处理系统

技术领域

[0001] 本发明涉及交通管理系统技术领域。具体而言，涉及一种基于区块链技术的免限行申请处理系统。

背景技术

[0002] 随着当前城市交通发展越加迅速，城市各类型的交通工具大量在道路上运行，造成道路在高峰时期出现巨大通行压力；为了缓解交通的拥堵，保证公共交通的顺畅，交管部门会根据实际需要对部分区域以及道路实施限行措施。而基于人性化管理以及动态的交通管理原则，在符合放宽限行措施的条件下，理应实施对部分交通参与者以及其驾驶的交通工具，在预先提交并获取免限行的申请下，有条件地进入并通过管制区域。然而该类型的申请由于数量庞大，且交通参与者以及其使用的交通工具条件各异，令审批处理的工作量巨大，需要提出一种有效的处理系统和处理办法。

[0003] 查阅相关已公开的技术方案，公开号为CN105023431B的技术方案提出一种确定交通限行信息的方法及装置，通过获取多辆浮动车的轨迹点信息，确定多辆浮动车的允许通过的道路以及允许通过的时段，从而使道路上多辆车辆的实施错峰通过；公开号为US20050267658A1的技术方案，基于执行法律交通速度限制和停止，在进入具有限行措施的道路或区域时，自动接收来自该道路或区域的限行规定，并以图形或声音通知交通工具内的驾驶人员执行该限行规定；公开号为JPWO2013128486A1的技术方案提出一种交通量预测系统，通过探测道路的自由速度、临界速度、饱和密度和临界密度等道路特性，对道路进行集群分类并为每个集群创建一个驱动模式，从而根据探测数据设置道路的可适应的交通量以及适合的限行模式。

[0004] 背景技术的前述论述仅意图便于理解本发明。此论述并不认可或承认提及的材料中的任一种公共常识的一部分。

发明内容

[0005] 本发明的目的在于，提供本发明涉及一种基于区块链技术的免限行申请处理系统，所述处理系统包括运行一信息区块链，用于存储以及向所述处理系统提供用户、车辆的可验证信息；同时所述处理系统包括一种基于区块链技术的免限行申请处理方法；该方法通过分别对用户、用户-车辆以及车辆的三个阶段的合法性判断，从而判定用户以其驾驶的车辆是否合乎限行的豁免条件；进一步的，该处理方法更适合使用于汽车租凭、汽车共享等车辆不属于用户的使用场景下。

[0006] 本发明采用如下技术方案：

[0007] 一种基于区块链技术的免限行申请处理系统，所述处理系统包括：

[0008] 用户端模块，被配置为验证用户身份，生成并存储用户的用户ID、公钥PK和私钥SK；存储与所述用户ID对应的用户公开信息，其中所述用户公开信息包括公钥PK；接收用户的免限行申请，并生成相应的免限行申请信息；

[0009] 服务器模块,包括用户认证子模块、申请认证子模块以及车辆认证子模块;所述用户认证子模块被配置为接收、处理用户的注册申请和用户认证信息请求;所述申请认证子模块被配置为用于接收、审核用户模块发出的免限行申请,并反馈免限行申请的审核结果;所述车辆认证子模块被配置为接收、处理车辆的车辆认证记录请求;

[0010] 限行模块,多个所述限行模块被配置在限行区域的多个入口位置;所述限行模块用于记录用户在所述限行区域的通行记录,并且根据免限行申请的审核结果判断用户的通行记录是否违反限行规定;

[0011] 其中,所述处理系统还包括信息区块链,多个所述限行模块以及所述服务器模块均作为所述信息区块链的节点,共同维护并参与该区块链的运行以及新区块的生成;所述用户端模块以及多个所述限行模块均与所述服务器模块通讯连接以进行数据传输;同时所述用户端模块由用户控制其与多个所述限行模块中的其中一个进行通讯连接;

[0012] 可选地,所述处理系统包括一种基于区块链技术的免限行申请处理方法,该方法包括执行以下用户认证步骤:

[0013] S101:由所述用户端模块将用户的用户ID以及所述用户公开信息在所述信息区块链中注册,由运行所述用户认证子模块的节点认证后,所述用户认证子模块向用户颁发用户可验证凭证VC,并将该用户可验证凭证VC发行于所述信息区块链;并且所述用户可验证凭证VC亦存储于所述用户端模块;

[0014] S102:由所述用户端模块将免限行申请以及用户ID发送到所述申请认证子模块;所述申请认证子模块在接收到一个免限行申请后,根据用户ID向对应的所述用户端模块发送用户认证信息请求,请求获取和认证该免限行申请的用户的信息;

[0015] S103:响应于来自所述申请认证子模块的用户认证信息请求,所述用户端模块将用户可验证凭证VC使用私钥SK进行数字签名后获得第一报文,将所述第一报文、所述用户可验证凭证VC以及用户ID传输到所述申请认证子模块;所述申请认证子模块根据用户ID从信息区块链获取对应的公钥PK,使用公钥PK解密所述第一报文从而获得解密后的用户可验证凭证VC,将解密后的用户可验证凭证VC与申请认证子模块接收的来自用户端模块的原始的用户可验证凭证VC进行校对验证,从而确认用户可验证凭证VC在传输过程中未被修改;

[0016] S104:所述申请认证子模块根据限行规定对用户可验证凭证VC进行判定是否合乎免限行条件;并当认证通过后,生成对应所述免限行申请的事件编号以及属于该事件编号的第一认证记录;将所述事件编号以及所述第一认证记录写入所述信息区块链的区块;并且包括将所述事件编号以及所述第一认证记录返回到所述用户端模块;

[0017] 可选地,所述处理方法还包括执行以下用户-车辆认证步骤:

[0018] S201:用户通过所述用户端模块将待驾驶的车辆ID以及用户ID发送到所述车辆认证子模块;

[0019] S202:所述车辆认证子模块根据用户ID从信息区块链获取对应的公钥PK,并根据车辆ID从信息区块链获取对应的车辆可验证凭证VC;

[0020] S203:所述车辆认证子模块将所述车辆可验证凭证VC通过公钥PK加密后生成第二报文,并将所述第二报文发送到所述用户端模块,由所述用户端模块通过私钥SK解密所述第二报文,从而获得车辆可验证凭证VC;

[0021] S204:所述用户端模块保存所述车辆可验证凭证VC;

[0022] 可选地,所述处理方法还包括执行以下通行认证步骤:

[0023] S301:当用户驾驶车辆通过其中一个所述入口进入所述限行区域时,令所述用户端模块与位于该限行区域的入口的所述限行模块建立通讯;其后,所述用户端模块执行将所述第一认证记录以及车辆可验证凭证VC进行哈希函数运算生成第一认证摘要;将所述事件编号、所述第一认证摘要发送到所述限行模块;

[0024] S302:所述限行模块执行:识别用户驾驶车辆的车辆ID;将车辆ID、所述事件编号以及所述第一认证摘要发送到所述申请认证子模块;

[0025] S303:所述申请认证子模块在接收到所述限行模块发送的车辆ID、所述事件编号以及所述第一认证摘要,执行:记录所述限行模块的位置;根据所述事件编号从所述信息区块链获得第一认证记录;根据车辆ID从所述信息区块链获得车辆可验证凭证VC;使用哈希函数对获得的所述第一认证记录以及车辆可验证凭证VC进行哈希运算,生成第二认证摘要;比对所述第一认证摘要与所述第二认证摘要是否相同;根据限行规定对车辆可验证凭证VC进行判定是否合乎免限行条件;

[0026] 可选地,所述用户ID以及所述车辆ID均由所述处理系统以分布式生成;

[0027] 进一步的,在所述信息区块链中对车辆进行注册,注册成功后的车辆在所述信息区块链中拥有一个唯一的车辆ID,并由所述车辆认证子模块根据车辆的具体信息生成车辆可验证凭证VC,并将该车辆可验证凭证VC发行于所述信息区块链;其中,所述车辆ID向所有用户以及所述信息区块链的所有节点公开;

[0028] 可选地,当所述服务器模块无法完成所述用户认证步骤、所述用户-车辆认证步骤以及所述通行认证步骤中一个或多个步骤时,记录该用户驾驶车辆进入限行区域的行为属于非认证行为。

[0029] 本发明所取得的有益效果是:

[0030] 1.本发明的处理方法基于区块链技术以及非对称加密技术,实现用户的信息可以通过加密传输的方式提交用户验证,有效保护了用户在需要进行验证时的信息私隐;

[0031] 2.本发明的处理系统基于区块链技术实现和运行,能够有效保证多信息源的可靠性,并且保证储储于区块链上的信息不被某个单位或个人私自篡改;

[0032] 3.本发明的处理方法能够利用分布式系统的高并发以及多分支的高效处理特点,因此特别适用于在高处理量需求的免限行申请实施条件中;

[0033] 4.本发明的处理系统其硬件模块以及装置采用模块化设计和配合,后期可通过软件、硬件进行灵活优化和变更,节省了大量后期维护升级成本。

附图说明

[0034] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制,而是将重点放在示出实施例的原理上。在不同的视图中,相同的附图标记指定对应的部分。

[0035] 图1为本发明所述处理系统的组成原理示意图;

[0036] 图2为本发明中用户认证步骤的示意图;

[0037] 图3为本发明中用户-车辆认证步骤的示意图;

[0038] 图4为本发明中通行认证步骤的示意图。

具体实施方式

[0039] 为了使得本发明的目的技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明;应当理解,此处所描述的具体实施例仅用于解释本发明 ,并不用于限定本发明。对于本领域技术人员而言,在查阅以下详细描述之后,本实施例的其它系统.方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内.包括在本发明的范围内,并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征,并且这些特征根据以下将详细描述将是显而易见的。

[0040] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件;在本发明的描述中,需要理解的是,若有术语上、下、左、右等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或组件必须具有特定的方位.以特定的方位构造和操作,因此附图中描述位置关系的用语仅用于示例性说明,不能理解为对本专利的限制,对于本领域的普通技术人员而言,可以根据具体情况理解上述术语的具体含义。

[0041] 实施例一:

[0042] 基于当前的免限行申请系统,用户需要提前向申请系统提供用户以及所驾驶车辆的信息证明,包括通过在线或离线要求提交身份证或者驾驶证件的编号、复印件或者其他身份记录证明;又或者,在临近限行路口时,才向管理人员出示驾驶人以及车辆的身份记录证明;因此与身份证对应的本人,如果想证明自己或者车辆的合法信息时,必须亲自拿出实物证件出示,所以总是有单独携带实物证件的麻烦;

[0043] 此外,在传统上,在验证身份的过程中,存在不必要地向第三方公开身份证中包含的所有信息的问题;例如,驾驶执照包括有关本人照片、姓名、社会保险号、地址、签发日期、签发机构信息、许可证类型、有效期等信息,很多信息是不必要地暴露给第三方的;

[0044] 因此需要提出一种技术方案,不仅可以令免限行的申请人能够方便而且具有更强保密性地提交身份证明文件、车辆证明文件,同时亦令免限行申请的审核方能够有效保证申请人、车辆的合法证身份,避免出现申请人私自更改证明文件的非法行为;

[0045] 作为一种实施方式,提出以下实施方法:

[0046] 一种基于区块链技术的免限行申请处理系统,所述处理系统包括:

[0047] 用户端模块,被配置为(1)验证用户身份,生成并存储用户的用户ID、公钥PK和私钥SK;(2)存储与所述用户ID对应的用户公开信息,其中所述用户公开信息包括公钥PK;(3)接收用户的免限行申请,并生成相应的免限行申请信息;

[0048] 服务器模块,包括用户认证子模块、申请认证子模块以及车辆认证子模块;所述用户认证子模块被配置为接收、处理用户的注册申请和用户认证信息请求;所述申请认证子模块被配置为用于接收、审核用户模块发出的免限行申请,并反馈免限行申请的审核结果;所述车辆认证子模块被配置为接收、处理车辆的车辆认证记录请求;

[0049] 限行模块,多个所述限行模块被配置在限行区域的多个入口位置;所述限行模块用于记录用户在所述限行区域的通行记录,并且根据免限行申请的审核结果判断用户的通行记录是否违反限行规定;

[0050] 其中,所述处理系统还包括信息区块链,多个所述限行模块以及所述服务器模块均作为所述信息区块链的节点,共同维护并参与该区块链的运行以及新区块的生成;所述

用户端模块以及多个所述限行模块均与所述服务器模块通讯连接以进行数据传输;同时所述用户端模块由用户控制其与多个所述限行模块中的其中一个进行通讯连接;

[0051] 可选地,所述处理系统包括一种基于区块链技术的免限行申请处理方法,该方法包括执行以下用户认证步骤:

[0052] S101:由所述用户端模块将用户的用户ID以及所述用户公开信息在所述信息区块链中注册,由运行所述用户认证子模块的节点认证后,所述用户认证子模块向用户颁发用户可验证凭证VC,并将该用户可验证凭证VC发行于所述信息区块链;并且所述用户可验证凭证VC亦存储于所述用户端模块;

[0053] S102:由所述用户端模块将免限行申请以及用户ID发送到所述申请认证子模块;所述申请认证子模块在接收到一个免限行申请后,根据用户ID向对应的所述用户端模块发送用户认证信息请求,请求获取和认证该免限行申请的用户的信息;

[0054] S103:响应于来自所述申请认证子模块的用户认证信息请求,所述用户端模块将用户可验证凭证VC使用私钥SK进行数字签名后获得第一报文,将所述第一报文、所述用户可验证凭证VC以及用户ID传输到所述申请认证子模块;所述申请认证子模块根据用户ID从信息区块链获取对应的公钥PK,使用公钥PK解密所述第一报文从而获得解密后的用户可验证凭证VC,将解密后的用户可验证凭证VC与申请认证子模块接收的来自用户端模块的原始的用户可验证凭证VC进行校对验证,从而确认用户可验证凭证VC在传输过程中未被修改;

[0055] S104:所述申请认证子模块根据限行规定对用户可验证凭证VC进行判定是否合乎免限行条件;并当认证通过后,生成对应所述免限行申请的事件编号以及属于该事件编号的第一认证记录;将所述事件编号以及所述第一认证记录写入所述信息区块链的区块;并且包括将所述事件编号以及所述第一认证记录返回到所述用户端模块;

[0056] 可选地,所述处理方法还包括执行以下用户-车辆认证步骤:

[0057] S201:用户通过所述用户端模块将待驾驶的车辆ID以及用户ID发送到所述车辆认证子模块;

[0058] S202:所述车辆认证子模块根据用户ID从信息区块链获取对应的公钥PK,并根据车辆ID从信息区块链获取对应的车辆可验证凭证VC;

[0059] S203:所述车辆认证子模块将所述车辆可验证凭证VC通过公钥PK加密后生成第二报文,并将所述第二报文发送到所述用户端模块,由所述用户端模块通过私钥SK解密所述第二报文,从而获得车辆可验证凭证VC;

[0060] S204:所述用户端模块保存所述车辆可验证凭证VC;

[0061] 可选地,所述处理方法还包括执行以下通行认证步骤:

[0062] S301:当用户驾驶车辆通过其中一个所述入口进入所述限行区域时,令所述用户端模块与位于该限行区域的入口的所述限行模块建立通讯;其后,所述用户端模块执行(1)将所述第一认证记录以及车辆可验证凭证VC进行哈希函数运算生成第一认证摘要;(2)将所述事件编号、所述第一认证摘要发送到所述限行模块;

[0063] S302:所述限行模块执行:(1)识别用户驾驶车辆的车辆ID;(2)将车辆ID、所述事件编号以及所述第一认证摘要发送到所述申请认证子模块;

[0064] S303:所述申请认证子模块在接收到所述限行模块发送的车辆ID、所述事件编号以及所述第一认证摘要,执行:(1)记录所述限行模块的位置;(2)根据所述事件编号从所述

信息区块链获得第一认证记录;(3)根据车辆ID从所述信息区块链获得车辆可验证凭证VC;(4)使用哈希函数对获得的所述第一认证记录以及车辆可验证凭证VC进行哈希运算,生成第二认证摘要;(5)比对所述第一认证摘要与所述第二认证摘要是否相同;(6)根据限行规定对车辆可验证凭证VC进行判定是否合乎免限行条件;

[0065] 可选地,所述用户ID以及所述车辆ID均由所述处理系统以分布式生成;

[0066] 进一步的,在所述信息区块链中对车辆进行注册,注册成功后的车辆在所述信息区块链中拥有一个唯一的车辆ID,并由所述车辆认证子模块根据车辆的具体信息生成车辆可验证凭证VC,并将该车辆可验证凭证VC发行于所述信息区块链;其中,所述车辆ID向所有用户以及所述信息区块链的所有节点公开;

[0067] 可选地,当所述服务器模块无法完成所述用户认证步骤、所述用户-车辆认证步骤以及所述通行认证步骤中一个或多个步骤时,记录该用户驾驶车辆进入限行区域的行为属于非认证行为。

[0068] 实施例二:

[0069] 本实施例应当理解为至少包含前述任意一个实施例的全部特征,并在其基础上进一步改进;

[0070] 作为一种实施方式,所述用户端模块可以包括处理器,使用基于区块链网络的分布式身份的用户ID,将用户ID存储在存储器中,并允许执行提取该用户ID并将用户ID进行图像化显示、以数字信号形式传输等形式,以实施用户身份的认证服务;此时,所述用户端模块可以包括个人计算机、移动计算机、PDA/EDA、手机、智能手机、平板电脑、物联网设备等;此外,所述用户端模块不限于此,可以包括任何设备,如便携式游戏机、数码相机、个人导航等具有有线和无线网络功能的电子设备;

[0071] 具体来说,用户端模块通常包括:计算机的组件单元/模块,例如,计算机处理器、内存、存储、输入设备和输出设备,其他传统计算设备的组件;电子通信组件单元/模块,如路由器、交换机等;网络连接存储(NAS)和电子信息存储系统,如存储区域网络(SAN)和计算机软件(即,通过计算机的组件单元/模块以特定方式运作的仪器)的组合,从而可以实现所需的系统性能;

[0072] 此外,计算设备的处理器可以包括硬件配置,如 MPU(微处理器单元)或 CPU(中心处理器单元)、缓存内存(缓存内存)、数据总线(数据总线);此外,计算设备还可以包括操作系统、执行特定目的的应用程序的软件配置;

[0073] 然而,这并不排除计算设备包括集成了中端、处理器和内存的集成形式的集成处理器,以实施本发明中所述用户端模块所包括的功能;

[0074] 进一步的,所述用户端模块可以通过验证用户的生物认证信息作为用户身份验证的方式;只有当用户身份被成功验证,才允许存储在所述用户端中的用户公开信息向外部传输,或者修改存储在所述用户端模块中的用户公开信息;进一步包括,当用户身份被成功验证时,才允许通过E2E加密通道从所述服务器模块获得所述用户可验证凭证VC;

[0075] 其中,上述用户的生物认证信息,包括虹膜信息、静脉信息、指纹信息、视网膜信息、面部信息、语音信息、DNA模式信息或/和其他用户的特有生物特征的信息;

[0076] 进一步的,用户存储在所述用户端模块的所述用户公开信息包括:用户本人照片、姓名、社会保险号、地址、签发日期、签发机构信息、许可证类型、有效期等信息;

[0077] 进一步的，所述用户端模块存储的公钥PK和私钥SK，目的在于使用非对称加密的方式，实现在所述信息区块链中的信息加密和解密，保证在本处理系统以及处理方法在信息传输过程中，信息即使被泄露于第三方，而第三方亦无法获取加密信息中的有效信息；

[0078] 关于非对称加密，以及上述内容中提及的数字签名，以及通过数字签名所生成的所述第一报文、所述第二报文、所述第一认证摘要以及所述第二认证摘要，均基于相关的非对称加密技术实现，应为相关技术领域人员所熟知，在此不作赘述。

[0079] 实施例三：

[0080] 本实施例应当理解为至少包含前述任意一个实施例的全部特征，并在其基础上进一步改进；

[0081] 在一种实施方式中，车辆ID可以包括标示于车辆本身的牌照号、二维码或者其它用于进行车辆身份唯一性的标识；

[0082] 而在另外一种实施方式中，车辆ID可以包括配置于车辆上的近场通讯装置，例如基于NFC、蓝牙等非接触式近场通讯技术的可读取装置；并且配置于车辆上的可读取装置同时可用于存储所述车辆可验证凭证VC；该可读取装置可以由所述车辆认证子模块发放到车辆，或者该可读取装置通过连接到一E2E加密通道，并通过该E2E加密通道通讯连接到所述车辆认证子模块从而获得所述车辆可验证凭证VC；

[0083] 进一步的，当车辆到达所述限行模块前时，配置于车辆上的所述近场通讯装置与最靠近车辆的所述限行模块进行通讯连接；通讯连接的方式工作模式可为被动模式和主动模式；在被动模式中，近场通讯发起设备(也称为主设备)可以由所述近场通讯装置或者所述限行模块担任；其中主设备需要由外部供电设备提供能量，主设备利用供电设备的能量来提供射频场，并将数据发送到NFC目标设备(也称作从设备)，传输速率需在106kbps、212kbps或424kbps中选择其中一种；相对的，从设备不产生射频场，可以不需要供电设备，而是利用主设备产生的射频场转换为电能，为从设备的电路供电，接收主设备发送的数据，并且利用负载调制技术，以相同的速度将从设备数据传回主设备；因为此在被动模式下，从设备不产生射频场，而是被动接收主设备产生的射频场；在此模式下，主设备可以检测非接触式卡或NFC目标设备，与之建立连接；优选地，基于电能的获取难易度考虑，一般将所述限行模块作为主设备，而为于车辆上的所述近场通讯装置作为从设备；

[0084] 而在一种实施方式中，可以使用主动模式部署所述限行模块与所述近场通讯装置的通讯连接；该模式下，发起设备和目标设备在向对方发送数据时，都必须主动产生射频场；两者都需要供电设备来提供产生射频场的能量。这种通信模式是对等网络通信的标准模式，可以获得非常快速的连接速率，并且允许两者相距较大距离；

[0085] 进一步的，所述限行模块包括配置有摄像头设备，由摄像头设备同时获得车辆的外观信息、驾驶人信息或者其他与车辆相关的信息；并将该部分获取的信息与记录区信息区块链上所述车辆可验证凭证VC所登记的信息进行比对；

[0086] 其中所述车辆可验证凭证VC基于车辆的具体信息生成并通过所述车辆认证子模块的验证；其中车辆的具体信息包括：号牌号码、车辆类型、使用性质、所有人、住址、品牌型号、发动机号码、车辆识别代号、注册日期、发证日期等文字；并可以进一步包括核定载人数、档案编号、整备质量、 总质量、核定载质量、外廓尺寸、准牵引总质量、备注、检验记录等；

[0087] 进一步，所述免限行申请可以包括以上所述的用户公开信息、车辆的具体信息，并进一步由所述服务器模块根据限行区域的具体限行规定，例如禁止大型车进入，或者禁止特定车辆进入，或者禁止特定人员进入等条件，审核所述免限行申请的内容，从而对特定的驾驶人、特定的车辆进行拦截或者放行；

[0088] 并且基于区块链技术，以上提到的所有信息、规定、执行步骤均具有去中心化主管理、不可篡改、高自主性的特点，避免了以往审核过程中的多种弊病。

[0089] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0090] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0091] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0092] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

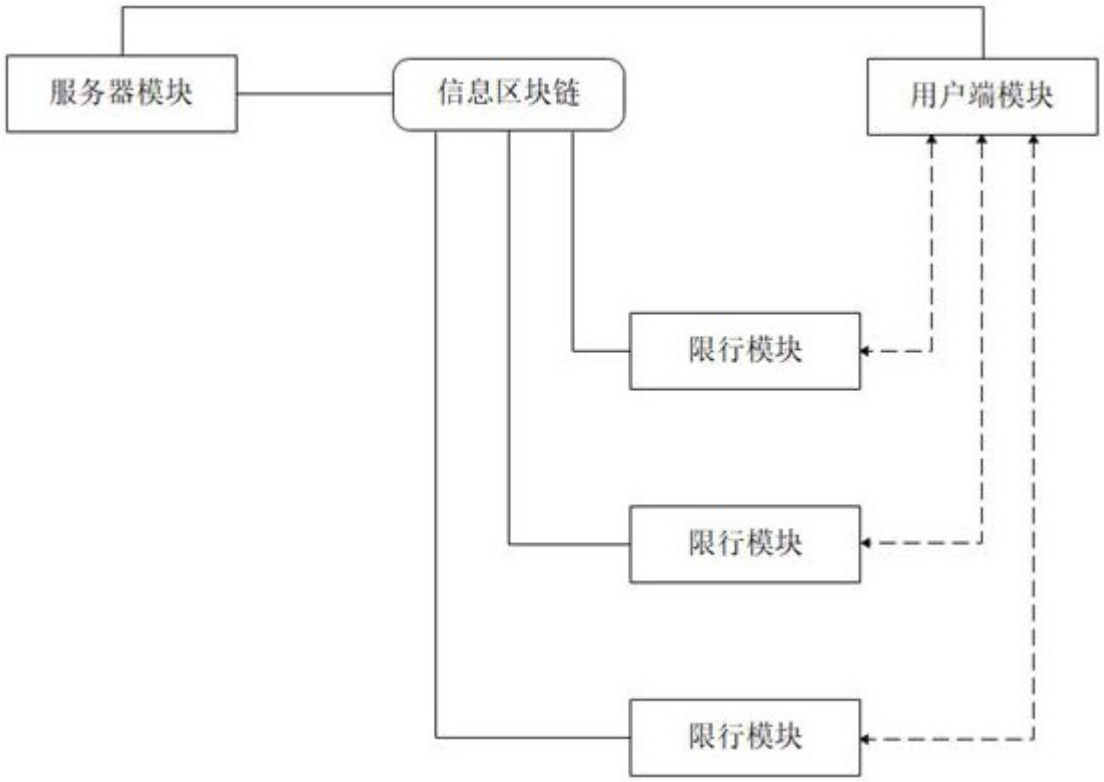


图1

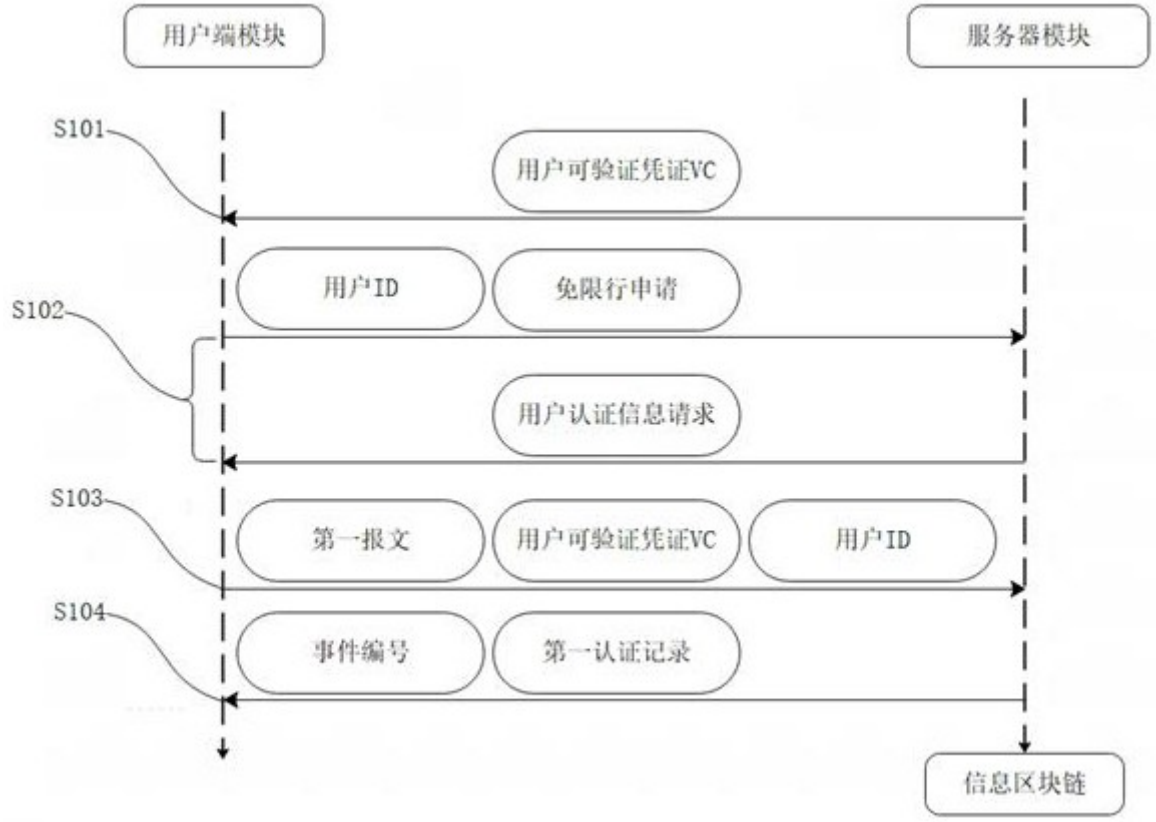

用户端模块
服务器模块
S101
用户可验证凭证VC
用户ID
免限行申请
S102
用户认证信息请求
S103
第一报文
用户可验证凭证VC
用户ID
S104
事件编号
第一认证记录
信息区块链

图2

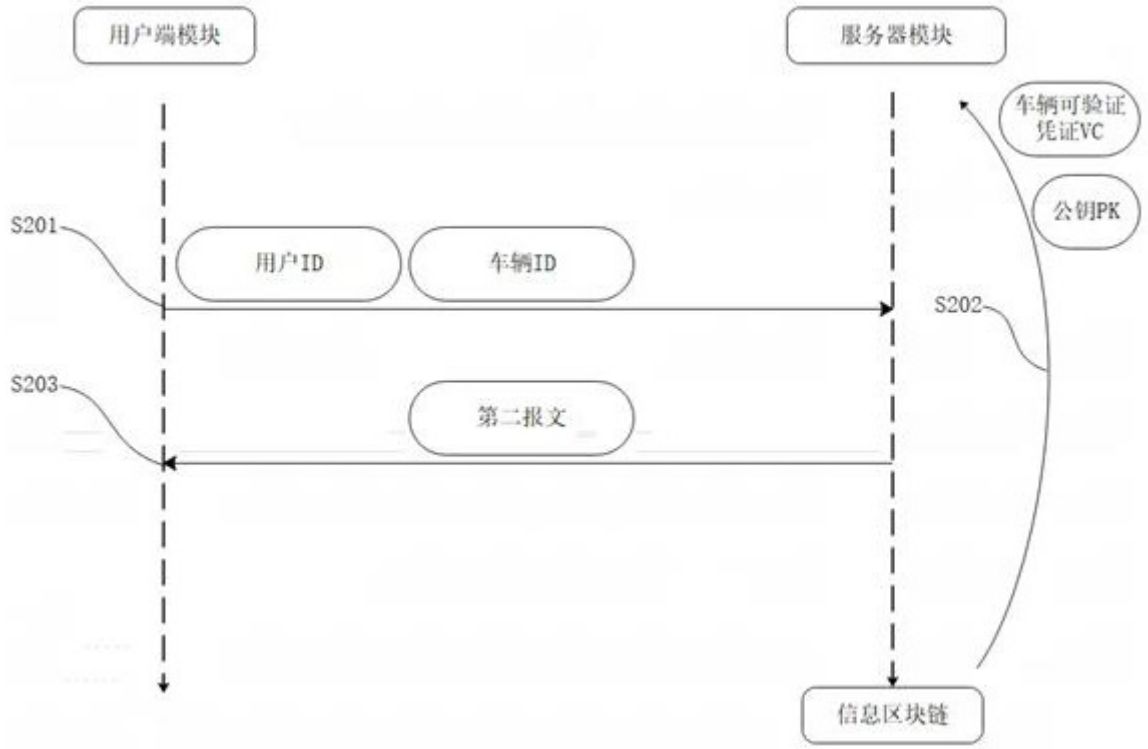

用户端模块
服务器模块
车辆可验证凭证VC
公钥PK
S201
用户ID
车辆ID
S202
S203
第二报文
信息区块链

图3

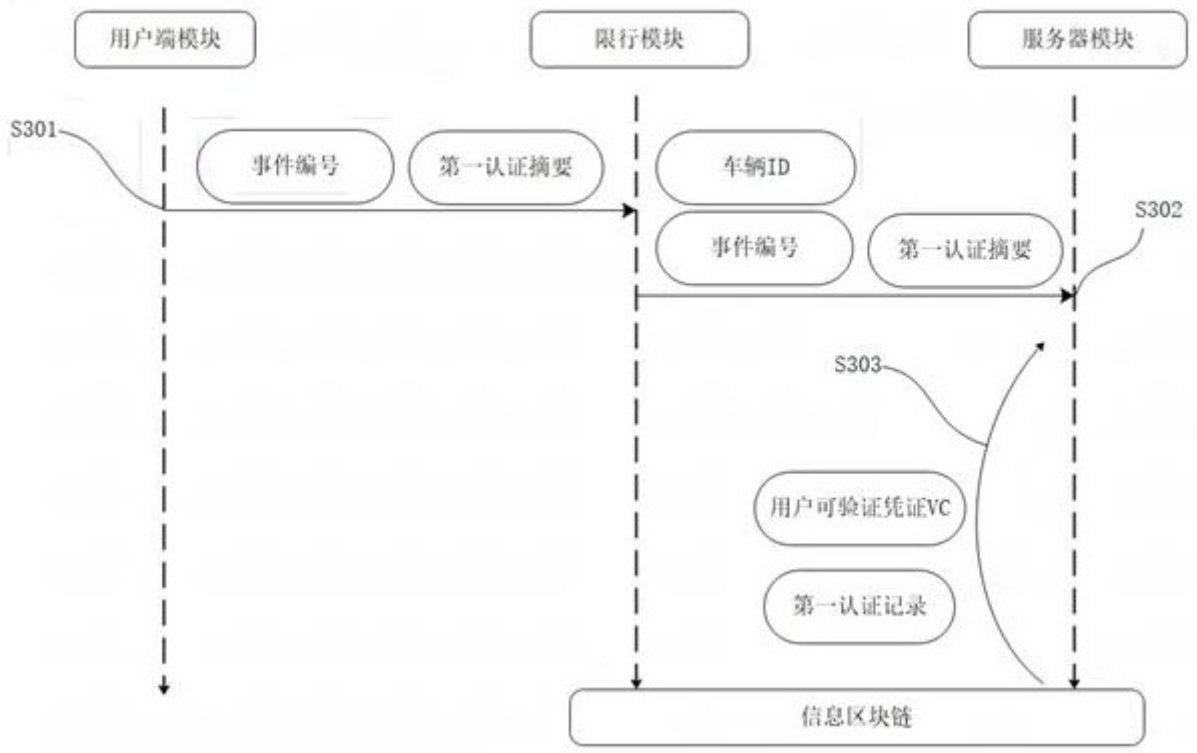

用户端模块
限行模块
服务器模块
S301
事件编号
第一认证摘要
车辆ID
事件编号
第一认证摘要
S302
S303
用户可验证凭证VC
第一认证记录
信息区块链

图4