(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118138211 A
(43)申请公布日 2024.06.04

(21)申请号 202311555327.0
(22)申请日 2023.11.21
(30)优先权数据
18/073,456 2022.12.01 US
(71)申请人 福特全球技术公司
地址 美国密歇根州迪尔伯恩市
(72)发明人 V·斯特凡诺夫斯基
卡尔·南森·克拉克 R·乌拉
Z·穆罕默德
(74)专利代理机构 北京连和连知识产权代理有限公司 11278
专利代理师 刘小峰 杨帆
(51)Int.Cl.
H04L 9/00(2022.01)
H04L 9/40(2022.01)
H04L 67/1097(2022.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)

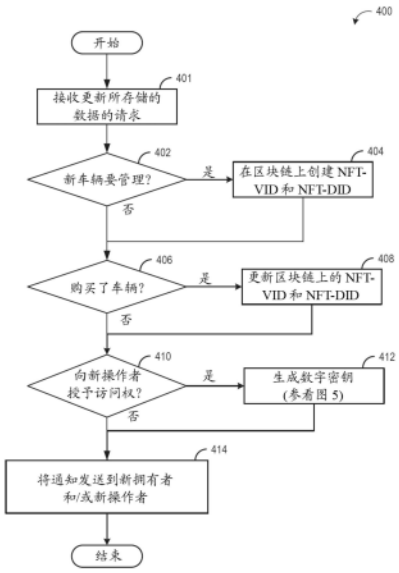
权利要求书3页 说明书26页 附图7页

(54)发明名称

区块链上的车辆数字密钥管理

(57)摘要

本公开提供了“区块链上的车辆数字密钥管理”。提供了用于将车辆数据、车辆拥有者数据和车辆操作者数据存储在区块链上的方法和系统，所述数据包括智能合约，其可被执行以经由可定制的权限控制对车辆的使用。在一个实施例中，一种车辆管理系统包括：区块链；流服务，其被配置为向嵌入区块链中的合约执行虚拟机(VM)实时提供事件数据；以及非暂时性存储器，其存储指令，所述指令在由车辆管理系统的处理器执行时致使车辆管理系统进行以下操作：针对车辆管理系统的车辆的操作者生成数字密钥，所述数字密钥基于一个或多个智能合约来控制操作者对车辆的访问和/或对车辆的一个或多个功能性的使用；以及将车辆、拥有者和操作者的数据存储在区块链上。



CN 118138211 A

1.一种车辆管理系统(102),所述车辆管理系统包括:

区块链(108);

流服务(134),所述流服务被配置为向嵌入所述区块链(108)中的合约执行虚拟机(VM)(109)实时提供事件数据;以及

非暂时性存储器(104),所述非暂时性存储器存储指令,所述指令在由所述车辆管理系统(102)的处理器(106)执行时致使所述车辆管理系统(102)进行以下操作:

基于来自所述车辆(130)的拥有者的输入针对所述车辆管理系统(102)的车辆(130)的操作者(350)生成数字密钥(306),所述数字密钥(306)基于一个或多个智能合约来控制所述操作者(350)对所述车辆(130)的访问和对所述车辆(130)的一个或多个功能性的使用;

将所述车辆(130)、所述拥有者和所述操作者(350)的数据存储在所述区块链(108)中,所述数据包括所述一个或多个智能合约;以及

将所述数字密钥(306)无线地传输到所述操作者(350)的计算装置。

2.如权利要求1所述的车辆管理系统(102),其中经由所述数字密钥(306)控制对所述车辆(130)的所述访问和/或对所述车辆(130)的所述一个或多个功能性的所述使用还包括:

将用于实施所述流服务(134)的版本的计算机应用程序包括在所述数字密钥(306)中;

响应于在所述车辆(130)处执行所述应用程序,经由所述流服务(134)的所述版本在所述车辆管理系统(102)处实时地接收所述车辆(130)的事件数据;

将所述车辆(130)的所述事件数据转发到嵌入所述区块链(108)中的所述合约执行VM(109);

响应于所述合约执行VM(109)执行所述一个或多个智能合约中的至少一个智能合约,从所述合约执行VM(109)接收控制对所述车辆(130)的所述访问和/或对所述车辆(130)的所述一个或多个功能性的所述使用的指令;以及

将所述接收到的指令发送到所述车辆(130)以由所述车辆(130)的电子控制单元(ECU)(132)执行。

3.如权利要求1所述的车辆管理系统(102),其中经由所述数字密钥(306)控制对所述车辆(130)的所述访问和/或对所述车辆(130)的所述一个或多个功能性的所述使用还包括:

将所述区块链(135)的副本包括在所述数字密钥(306)中,并且包括在第一次使用所述数字密钥(306)时将所述副本安装在所述车辆(130)处的指令;

将用于在所述车辆(130)处实施所述流服务(134)的版本的计算机应用程序包括在所述数字密钥(306)中,所述版本向嵌入所述车辆(130)处的所述区块链(135)的所述副本中的合约执行VM(136)提供实时事件数据,所述合约执行VM(136)被配置为基于所述实时事件数据自动执行存储在所述区块链(135)的所述副本中的所述一个或多个智能合约,所述一个或多个智能合约在被执行时向所述车辆(130)的ECU提供控制对所述车辆(130)的所述访问和/或对所述车辆(130)的所述一个或多个功能性的所述使用的代码以供执行;并且

其中包括所述数字密钥(306)的所述操作者(350)的所述计算装置和所述车辆(130)都不与所述车辆管理系统(102)通信以控制对所述车辆(130)的所述访问和/或对所述车辆(130)的所述一个或多个功能性的所述使用,并且嵌入所述车辆管理系统(102)的所述区块

链(108)中的所述合约执行VM(109)不执行智能合约。

4.如权利要求3所述的车辆管理系统(102),其中由所述车辆管理系统(102)在所述车辆(130)处周期性地更新所述区块链(135)。

5.如权利要求1所述的车辆管理系统(102),其中将所述车辆(130)、所述拥有者和所述操作者(350)的所述数据存储在所述区块链(108)上还包括:

将所述车辆(130)的所述数据写入到存储在所述区块链(108)上的所述车辆(130)的非同质化令牌(NFT)(200);

将所述拥有者的所述数据写入到存储在所述区块链(108)上的所述拥有者的NFT(250);以及

将所述操作者的所述数据写入到存储在所述区块链(108)上的所述操作者的NFT(250)。

6.如权利要求5所述的车辆管理系统(102),其中所述车辆(130)的所述NFT(200)包括以下各项中的至少一者:

所述车辆(204)的识别信息;

关于指派给所述车辆(218)的数字密钥的信息;

所述车辆(206)的一个或多个拥有者的标识信息(208);

所述车辆的一个或多个操作者(212)的标识信息(214)。

7.如权利要求5所述的车辆管理系统(102),其中所述拥有者的所述NFT包括以下各项中的至少一者:

所述拥有者(254)的识别信息;

关于指派给所述拥有者(268)的数字密钥的信息;

所述拥有者(256)所拥有的一辆或多辆车辆的标识信息(258);

所述拥有者(262)所操作的一辆或多辆车辆的标识信息(264)。

8.如权利要求5所述的车辆管理系统(102),其中所述操作者的所述NFT包括以下各项中的至少一者:

所述操作者(254)的识别信息;

关于指派给所述操作者(268)的数字密钥的信息;

所述操作者(256)所拥有的一辆或多辆车辆的标识信息(258);

所述操作者(262)所操作的一辆或多辆车辆的标识信息(264)。

9.如权利要求5所述的车辆管理系统(102),其中所述一个或多个智能合约存储在以下各项中的至少一者中:所述操作者(250)的所述NFT、所述车辆(200)的所述NFT和所述拥有者(250)的所述NFT。

10.如权利要求5所述的车辆管理系统(102),其中所述一个或多个智能合约存储在所述操作者(250)的所述NFT和所述车辆(200)的所述NFT中,并且所述一个或多个智能合约在所述操作者(350)的所述计算装置和所述车辆的ECU(132)中的至少一者处执行,而不在所述车辆管理系统(102)处执行。

11.如权利要求1所述的车辆管理系统(102),其中由所述车辆的所述拥有者经由所述车辆管理系统(102)的图形用户界面(GUI)创建所述数字密钥(306)。

12.如权利要求1所述的车辆管理系统(102),其中由所述车辆管理系统(102)经由所述

数字密钥(306)对所述操作者进行认证,之后授予访问权。

13.一种用于通过车辆管理系统管理对车辆的使用的方法,所述方法包括:

在制造所述车辆(404)时针对所述车辆创建包括所述车辆的数据的非同质化令牌(NFT),并且将所述车辆的所述NFT存储在所述车辆管理系统的区块链上;

在购买所述车辆之后,针对所述车辆的拥有者创建包括所述拥有者(408)的数据的NFT,并且将所述拥有者的所述NFT存储在所述区块链上;

针对所述车辆的操作者(506)创建包括所述操作者的数据的NFT,所述操作者是由所述车辆的所述拥有者指派,并且将所述操作者的所述NFT存储在所述区块链(510)上;以及

响应于由所述拥有者输入到所述车辆管理系统的应用程序中的数据,创建一个或多个智能合约(508),所述一个或多个智能合约控制对所述车辆的访问和对所述车辆的功能性的使用中的至少一者,所述一个或多个智能合约能够在包括所述区块链的副本的一个或多个计算装置处执行。

14.如权利要求13所述的方法,所述方法还包括:

针对所述操作者(412)生成数字密钥,所述数字密钥包括所述一个或多个智能合约,并且将所述数字密钥传输到所述操作者的计算装置;

在嵌入安装在所述车辆处的所述区块链的副本中的合约执行虚拟机(VM)处从所述车辆的流服务接收事件数据,所述合约执行VM被配置为基于所述事件数据执行所述一个或多个智能合约;以及

响应于由所述合约执行VM执行所述一个或多个智能合约中的智能合约,将所述合约执行VM的输出传输到所述车辆的电子控制单元(ECU)以供执行(720)。

15.如权利要求14所述的方法,所述方法包括:将用于在所述车辆(512)处实施所述流服务的应用程序包括在所述数字密钥中。

区块链上的车辆数字密钥管理

技术领域

[0001] 本说明书涉及用于基于存储在分布式账本中的智能合约经由数字密钥为车辆的不同用户自动启用不同功能性的方法和系统。

背景技术

[0002] 在各种场景中,车辆拥有者可能希望基于预先限定的一组规则将一个或多个可撤销数字密钥部署给一个或多个指定的人。例如,租赁汽车公司和车队运营商可能希望将临时和/或可撤销的数字密钥授予被授权访问和操作它们的车辆的某些个体。提供授权的条款可以取决于车辆拥有者规定的一个或多个因素。示例包括对操作者的身份、使用持续时间、有效驾驶执照等的认证。另外,拥有者可能希望在某些情况下启用或禁用车辆的各种功能性。例如,公司可能希望限制驾驶员可以操作公司送货车的连续小时数。另外或替代地,拥有者可能希望针对不同的操作者启用或禁用车辆的各种功能性。例如,车辆可以包括起重机,其中第一驾驶员可以被授权操作车辆并操作起重机,而第二驾驶员可以被授权操作车辆并且未被授权操作起重机。

[0003] 对于包括车辆的各种实物资产,存在可撤销数字密钥的各种实现方式。例如,U.S.9892584B1公开了用于使得拥有者能够将电子密钥分发给其他用户的技术,其中拥有者可以限制可以使用密钥的次数,建立使用时间窗口,或者要求借用人具有某些资格。U.S.10275956B1公开了用于接收生成和共享准许访问资源的电子密钥的请求的方法,其中可以采用诸如时间、位置和/或用户存在的约束,并且如果条件未满足,则可以自动拒绝/撤销密钥。U.S.9189900B1教导了将电子密钥授予具有用户账户的接收方以使用车辆,其中拥有者可以创建用户账户并设置持续时间、时间和/或对车辆的操作功能或车辆的用户界面的访问的权限。

发明内容

[0004] 本文的发明人已经识别出数字密钥管理系统的当前实现方式的问题。通常,密钥管理服务器在每次尝试使用时确定是否满足条件。然而,基于在使用期间可能发生的状况,密钥管理服务器可能不支持在使用车辆时灵活地改变权限。例如,在电力中断期间,密钥管理服务器可能变得不起作用,或者包括密钥的计算装置(例如,智能电话)与密钥管理服务器之间的连接可能失去,这可能导致权限的不执行和/或车辆变得不可用。另外,密钥管理服务器所依赖的存储器资源、处理能力和/或通信带宽的量可能较大,这可能导致关于使用车辆的响应性的缺乏和延迟,或其他技术问题,并且可能增加操作密钥管理服务器的成本。此外,密钥管理服务器可以控制对车辆的访问,但是可能控制不了车辆的不同功能性的使用,或者密钥管理服务器对其具有控制权的功能性范围可能是有限的。添加密钥管理服务器对其具有控制权的新功能性可能是缓慢且耗时的,并且可能进一步消耗密钥管理服务器的资源。

[0005] 在一个实施例中,上述问题可以通过一种车辆管理系统来解决,所述车辆管理系

统包括:区块链;流服务,所述流服务被配置为向嵌入所述区块链中的合约执行虚拟机(VM)实时提供事件数据;以及非暂时性存储器,所述非暂时性存储器存储指令,所述指令在由所述车辆管理系统的处理器执行时致使所述车辆管理系统基于来自车辆的拥有者的输入针对所述车辆管理系统的车辆的用户生成数字密钥,所述数字密钥基于一个或多个智能合约来控制所述用户对所述车辆的访问和/或对所述车辆的一个或多个功能性的使用;将所述车辆、所述拥有者和所述用户的数据存储在所述区块链上,所述数据包括所述一个或多个智能合约;以及将所述数字密钥无线地传输到所述用户的装置(例如,计算装置)。所述数字密钥可以包括用于实施一个版本的所述流服务的计算机应用程序,所述计算机应用程序可以在用户的装置上或在车辆的电子控制单元(ECU)中启动。在一些实施例中,所述数字密钥还可包括所述区块链的副本,所述副本可安装在所述装置上或所述ECU处。当实施所述流服务时,嵌入所述区块链中(例如,车辆管理系统处的主副本、安装在装置上的本地副本或安装在车辆中的本地副本中)的合约执行VM可从安装在车辆处的流服务接收事件数据。如果合约执行VM确定已经满足一个或多个智能合约的一个或多个条件,则可将控制对车辆的访问和/或车辆的一个或多个功能性的使用的指令从合约执行VM传输到车辆ECU进行执行。例如,所述指令可以包括在被执行时启用或禁用访问或功能性的计算机代码,或者所述指令可以在车辆ECU处被转换为计算机代码。通过这种方式,可以基于事件数据选择性地启用或禁用对车辆的访问和/或对车辆的各种功能性的使用。通过经由智能合约控制对各种功能性的访问和/或使用(所述智能合约可以由拥有者经由车辆管理系统的用户友好的图形用户界面(GUI)创建和定制),车辆的拥有者可以通过比当前数字密钥实现方式提供的方式更容易、更灵活且更可定制的方式来创建不同操作者使用车辆的定制条件。另外,通过跨区块链的多个副本以分布式方式存储智能合约,可以通过经由本领域已知的标准区块链操作查阅各种副本来随时验证智能合约的有效性,从而增加车辆的安全性,并且降低对车辆的未授权访问或使用的可能性。此外,在其中区块链的副本安装在车辆处的实施例中,可以在车辆处(例如,在数字密钥与车辆之间)实施智能合约的执行和对车辆的控制,而不涉及车辆管理系统。因此,对车辆的控制可以不依赖于车辆管理系统的可用性或车辆与车辆管理系统之间的无线连接的质量,从而导致根据智能合约对车辆的更稳健和独立的控制。

[0006] 应理解,提供以上发明内容是为了以简化的形式介绍在具体实施方式中进一步描述的一系列概念。这并不意味着识别所要求保护的主题的关键或必要特征,所述主题的范围由具体实施方式之后的权利要求唯一地限定。此外,所要求保护的主题不限于解决上文或本公开的任何部分中提及的任何缺点的实施方式。

附图说明

[0007] 图1是根据一个实施例的示例性车辆管理系统的示意性框图;

[0008] 图2A是根据一个实施例的包括车辆管理系统中所包括的车辆的数据的第一非同质化令牌(NFT)的示意性框图;

[0009] 图2B是根据一个实施例的包括车辆管理系统中所包括的人的数据的第二NFT的示意性框图;

[0010] 图3是根据一个实施例的车辆的数字密钥系统的示意性框图;

[0011] 图4是根据一个实施例的示出用于在区块链上管理车辆管理系统的数据的示例性

方法的流程图;

[0012] 图5是根据一个实施例的示出用于创建车辆的数字密钥的示例性方法的流程图;

[0013] 图6是根据一个实施例的示出供车辆管理系统认证车辆的操作者的示例性方法的流程图;以及

[0014] 图7是根据一个实施例的示出供车辆基于智能合约来控制车辆的功能性的示例性方法的流程图。

具体实施方式

[0015] 以下描述涉及用于基于将车辆、车辆操作者和车辆拥有者数据存储在诸如区块链上的分布式账本系统中来使用定制的数字密钥控制对车辆的访问和操作的系统和方法。在各种实施例中,车辆、车辆操作者和车辆拥有者数据可以存储在区块链上的非同质化令牌(NFT)中。

[0016] 分布式账本是在分散式对等(P2P)网络的每个节点处维护的交易记录。通常,分布式账本由捆绑在一起形成“区块”的区块链交易分组组成。当对分布式账本进行更改时(例如,当创建新的区块链交易和/或区块时),每个节点必须就如何将更改整合到分布式账本中形成共识。在达成共识之后,将达成一致的更改推送到每个节点,使得每个节点维护更新后的分布式账本的相同副本。未达成共识的任何更改会被忽略。因此,与传统的集中式账本不同,单方不能单方面地更改分布式账本。

[0017] 在分布式账本的一个应用中,每个新的区块可以密码地链接到前一个区块,以便形成链(例如,区块链)。更具体地,为了创建新区块,可以向区块内的每个区块链交易指派哈希值(例如,加密哈希函数的输出,诸如SHA-2或MD5)。然后,可以利用密码技术(例如,默克尔树)将这些哈希值组合在一起以生成表示整个新区块的哈希值。然后,可以将此哈希值与前一个区块的哈希值组合以形成包括在新区块的标头中的哈希值,从而将新区块密码地链接到区块链。为此,在新区块的标头中使用的精确值取决于新区块中的每个区块链交易的哈希值,以及每个先前区块中的每个区块链交易的哈希值。

[0018] 在一些实施例中,针对新区块生成的哈希值可以用作操纵随机数值的密码谜题的输入。当找到密码谜题的解决方案时,解决的节点发布解决方案,并且其他节点然后验证所述解决方案是正确的解决方案。由于所述解决方案还可能取决于区块链内的每个区块链交易的特定哈希值,因此如果解决的节点试图修改任何区块链交易,则所述解决方案将不会被其他节点验证。更具体地,如果单个节点试图修改区块链内的先前区块链交易,则针对密码组合技术的每一层生成不同哈希值的级联。这导致一个或多个区块的标头不同于未进行完全相同修改的每个其他节点中的对应标头。因此,由修改的节点生成的解决方案将解决不了呈现给没有相同修改的任何节点的密码谜题。因此,由修改的节点生成的新区块的版本被容易辨识为包括不正确的修改并且受到共识排斥。这种无法修改过去的区块链交易导致区块链一般被描述为可信的、安全的和/或不可变的。

[0019] 对于基于分布式账本的车辆管理系统,可以将车辆、车辆拥有者和车辆操作者的数据(包括建立访问和操作车辆的权限的数字密钥数据)写入到区块链的区块,如上所述。通过这种方式,可以以不可变的方式存储数字密钥数据。

[0020] 智能合约是使得能够在不同方之间自动执行和/或实行协议或交易的计算机协

议。具体地,智能合约可以是位于区块链上的特定地址处的计算机代码。智能合约可以包括一个或多个触发条件,所述一个或多个触发条件在满足时对应于一个或多个动作。对于一些智能合约,基于一个或多个决策条件来确定执行一个或多个动作中的哪个(些)动作。执行智能合约的合约执行VM可以订阅包括与触发条件和/或决策条件相关的数据的一个或多个数据流。因此,合约执行VM可以将数据流路由到智能合约,使得智能合约可以检测到触发条件已经出现和/或分析决策条件以引导实行实体执行一个或多个动作。

[0021] 通过在分布式账本中记录智能合约,存在智能合约的公开且可信的记录以及由智能合约引导执行的动作背后的推理。因此,生成智能合约的各方可以以透明且客观的方式依赖于它们的合约的自动实行。分布式账本可以是公共账本(每个节点可以容易地查看每个区块链交易的基础数据)或私人账本(基础数据需要加密密钥才能查看),或者公共账本和私人账本的组合。

[0022] 另外,本文公开了用于为车辆管理系统的车辆的不同拥有者和/或操作者生成定制的可撤销数字密钥的系统和方法,其中数字密钥可以允许每个操作者/拥有者对车辆和/或车辆的各种功能性的使用条款的不同级别的访问。可以在车辆管理系统上创建和/或更新数字密钥(例如,经由互联网浏览器中的车辆管理系统的网络应用程序),或者可以经由在车辆的拥有者的电子装置上运行的车辆管理系统的计算机应用程序(在本文中还称为应用程序)创建和/或更新数字密钥。如本文所述,对车辆和/或车辆的各种功能性的使用条款的不同访问级别可以在存储在区块链上的一个或多个NFT中的一个或多个智能合约中限定。智能合约可以由嵌入区块链的副本中的合约执行VM来执行,其中区块链的副本可以包括在数字密钥中并且被传递和安装在车辆处,或者区块链的副本可以是存储在车辆管理系统处的区块链的主副本。通过使用独立创建并存储在区块链上的智能合约来管理使用条款,可以实现为不同车辆和个体创建不同使用条款的更大灵活性。此外,区块链的不变性提供了数字密钥历史的永久记录。

[0023] 可以基于在嵌入区块链中的合约执行VM处接收到的实时事件数据来自动执行智能合约。所述实时事件数据可以从在车辆处运行的流服务传输,并且可以包括例如使用数字密钥的操作者的识别信息;数字密钥的到期数据;操作者访问车辆的时间;操作者使用车辆的功能性的时间;和/或其他数据。数字密钥可以参考NFT以获得车辆、拥有者和/或操作者数据以输入到智能合约中,或者智能合约可以参考NFT以获得用于合约执行的车辆、拥有者和/或操作者数据。

[0024] 由于各种原因,在车辆而不是车辆管理系统处执行智能合约可以是有利的。可以在车辆处更快地执行合约,其中可以不依赖于车辆与车辆管理系统之间的通信。例如,由于网络或技术问题,通信可能会延迟或不可用。可以减少车辆管理系统对处理和存储器资源的使用,从而提高车辆管理系统的总体效率。

[0025] 图1示出了包括车辆管理系统的车辆生态系统。所述车辆管理系统包括区块链,各种NFT可以存储在所述区块链上。所述NFT可以包括如图2A中所示的一辆或多辆车辆的NFT-VID,以及可以是如图2B中所示的分布式账本中的参与者的车辆管理系统的各个用户的NFT-DID。车辆管理系统可以生成数字密钥,所述数字密钥可以存储在用户的电子装置(诸如图3中所示的电子装置)中,并且用于访问和/或操作一辆或多辆车辆中的车辆。车辆的新的NFT可以由车辆管理系统通过遵循图4中所示的方法来创建。可以通过遵循图5中所示的

方法来生成数字密钥。当使用数字密钥来访问或操作车辆时,可以经由图6中所示的方法来认证数字密钥的用户。基于与数字密钥相关联的权限,车辆的ECU可以通过遵循图7中所示的方法来控制车辆的访问和操作。

[0026] 图1示出了包括车辆管理系统102的车辆生态系统100。车辆管理系统102可以用于控制车辆130的访问和/或使用,其中车辆130可以是车辆车队142的成员。在一些实施例中,车辆车队142可以包括相同或类似的车辆。例如,车辆130可以是租赁汽车,并且车辆车队142可以是车辆租赁公司拥有的租赁汽车车队;或者车辆130可以是递送车辆,并且车辆车队142可以是用于递送由公司出售的产品的各种大小的车辆车队。在其他实施例中,车辆车队142可以包括各种类型的多个车辆。例如,道路施工公司可以管理车辆车队,包括卡车、挖掘机、起重机、反铲挖掘机、管理车辆等。每个车辆130可以由相同的驾驶员或由不同的驾驶员操作(例如,驾驶)。在一些实施例中,不同的驾驶员可以各自具有不同的分派车辆(例如,与出租汽车一样)。在其他实施例中,一个或多个驾驶员可以驾驶和/或共享车辆车队142的一辆或多辆车辆。例如,道路施工公司可以雇用第一驾驶员来操作公司拥有的第一车辆;雇用第二驾驶员来操作所述第一车辆和第二车辆中的任一者;雇用第三驾驶员来操作第三车辆,但不操作所述第一车辆或所述第二车辆;雇用第四驾驶员来操作所述第二车辆和第四车辆;等等。换句话说,各种操作者可具有访问和使用车队142的某些车辆130的权限,而没有访问和使用车队142的其他车辆130的权限。公司可以基于各种标准,诸如培训、责任水平、资历、信任程度、技能水平或其他,向各种操作者授予访问和使用车辆130的权限。如下面更详细描述的,可以经由数字密钥向各种操作者授予权限,所述数字密钥可以相对于操作者、访问类型和/或每个车辆130的功能性进行定制。

[0027] 车辆130可以是汽车、大巴、卡车或由操作者操作的不同类型的机械或车辆。车辆130可以由内燃发动机提供动力,或者车辆130可以是由电源提供动力的电动车辆,或者车辆130可以是由内燃发动机和电源两者提供动力的混合动力车辆。车辆130还可以是在特定环境中使用的专用车辆,诸如在私人设施(诸如室内设施)的某些区域中使用的高尔夫球车或运输车辆。车辆130可以在公共和/或私人道路和高速公路上操作,或者在一组轨道或导轨(例如,火车)上操作。通常,车辆130可以是由操作者操作的任何类型的车辆。

[0028] 可以经由远程无钥匙进入(RKE)系统来控制对车辆130的访问,所述RKE系统使用(例如,具有固定频率的)射频(RF)信号在操作者与车辆130之间传输和接收车辆控制功能性。RKE系统可以依赖于操作者选择操作者装置(诸如遥控钥匙或智能电话)上的控制元件(例如,物理或虚拟按钮)来获得对车辆130的访问,或者RKE系统可以是被动无钥匙进入(PKE)系统,其中当操作者装置进入车辆130的阈值接近度时自动地控制对车辆130的进入。RKE系统可以另外提供附加的功能性,诸如起动发动机、打开和关闭防盗警报器、发起车厢内热控制或操作在车辆130中提供的某些特征。例如,车辆130可以包括提升和降低的液压底座,或者用于犁地、拖曳、平地、收割等的特征,可以由RKE或PKE系统控制其使用。此外,RKE/PKE系统可不使用特定的电子装置(例如,遥控钥匙),并且可依赖于可以存储在各种装置(诸如智能电话)上的数字密钥。

[0029] 车辆130可以包括电子控制单元(ECU)132,诸如数字驾驶舱ECU,所述电子控制单元可以控制无钥匙进入系统的操作。ECU 132可以包括处理器,所述处理器可以执行存储在ECU 132的存储器中的指令以实施无钥匙进入系统的若干部分。在一些实施例中,ECU 132

可以由车辆130的电力存储装置(诸如电池)供电。电池可以是专用ECU电池,或者电池可以是例如用于ECU 132的输入-输出控制器的指定电池,由此在经由车辆130的其他电源得不到电力的情况下,执行指令的电力可以是可用的。在各种实施例中,当车辆130的马达或发动机未操作并且车辆130的主电池未充电时,电池可以向无钥匙进入系统供应足够的电力进行操作。

[0030] 车辆130可以包括通信模块133,所述通信模块可以支持车辆130与包括数字密钥和/或车辆管理系统102的电子装置之间的无线通信。无线通信可以依赖于各种无线技术(例如,射频、红外、近场通信(NFC)等)中的一种或多种。例如,可以经由支持双向通信的RF链路建立无线连接,由此RF信号可以从包括数字密钥的电子装置传输到车辆130,和/或RF信号可以从车辆130传输到电子装置。通信模块133可以使用任何过去、现在或未来的通信协议(例如,BLUETOOTH™、USB 2.0、USB 3.0等)经由无线局域网(LAN)或广域网(WAN)进行通信。

[0031] 车辆管理系统102包括被配置为执行存储在非暂时性存储器104中的机器可读指令的一个或多个处理器106。存储器104可以包括用于存储由处理器106执行以实施本文公开的各种功能性的程序和例程的一个或多个数据存储结构,诸如光学存储器装置、磁存储器装置或固态存储器装置。存储器104可以包括任何期望类型的易失性和/或非易失性存储器,诸如静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、快闪存储器、只读存储器(ROM)等。

[0032] 例如,处理器106可以是任何合适的处理器、处理单元或微处理器。处理器106可以是多处理器系统,并且因此可以包括彼此相同或类似并且经由互连总线通信地耦合的一个或多个附加处理器。处理器106可以是单核的或多核的,并且在其上执行的程序可被配置用于并行或分布式处理。在一些实施例中,处理器106可任选地包括分布在两个或更多个装置中的单独部件,所述单独部件可远程定位和/或被配置用于协调处理。在一些实施例中,处理器106的一个或多个方面可以由在云计算配置中配置的可远程访问的联网计算装置虚拟化和执行。

[0033] 车辆管理系统102可以包括通信模块107,所述通信模块可以管理车辆管理系统102与车辆130的类似通信模块(例如,通信模块133)和/或包括数字密钥的操作者装置之间的无线通信。

[0034] 车辆管理系统102可以包括区块链108,所述区块链可以由车辆管理系统102用作分布式账本,以存储用于访问、操作和/或使用车辆130的各种功能性的许可。在各种实施例中,区块链108可以存储一个或多个非同质化令牌(NFT),包括车辆130的权限和其他数据,在本文称为NFT-VID。区块链108还可存储包括与车辆130有联系或相关联的各种人员的权限和其他数据的一个或多个NFT,在本文称为NFT-DID。与车辆130有联系或相关联的各种人员可以包括车辆130的一个或多个车辆拥有者137以及车辆130的一个或多个车辆操作者138。NFT-VID和NFT-DID可以被写入到区块链108并随着新区块被添加到区块链108而更新。区块链108还可以(例如,在NFT-VID和NFT-DID中)存储发送到各个监管机构140、由监管机构使用或从监管机构接收的数据。

[0035] 暂时参考图2A,示出了示例性NFT-VID 200。NFT-VID 200可以包括NFT-VID标识符201,可使用所述NFT-VID标识符来参考NFT-VID 200。NFT-VID 200可以包括各种可修改和/

或不可变的数据字段。不可变的数据字段可以包括车辆字段202,所述车辆字段可以包括NFT-VID 200所对应的车辆(例如,车辆130)的识别信息。在各种实施例中,单个NFT-VID 200可以1:1关系对应于单个车辆,其中没有其他NFT-VID对应于所述车辆,并且没有其他车辆对应于NFT-VID 200。车辆字段202可以包括例如不可变的车辆ID 204,诸如车辆识别号码(VIN)。车辆字段202还可以包括车辆的其他识别信息(例如,品牌、型号、颜色、年份等)。所述识别信息可以包括文本数据和/或其他类型的数据,诸如图像数据(例如,车辆的一个或多个图像、车辆的识别数据的图像等)。在其他实施例中,车辆字段202可以包括其他可修改和/或不可变的数据字段。例如,可修改字段可以包括标题状态字段、注册状态字段、保险信息字段、金融数据字段等。

[0036] NFT-VID 200的其他可修改数据字段可以包括车辆拥有者字段206,所述车辆拥有者字段可以存储车辆的一个或多个拥有者的识别信息。所述识别信息可以包括一个或多个拥有者ID 208(例如,每个车辆拥有者的拥有者ID 208)。例如,在一些实施例中,拥有者ID 208可以是相应车辆拥有者206的驾驶执照,或不同类型的标识。在其他实施例中,拥有者ID 208可以例如经由NFT-DID的标识符来参考车辆202的拥有者的NFT-DID,而不是直接参考拥有者。所参考的NFT-DID可以包括拥有者识别信息,如下文参考图2B所述。

[0037] 另外,车辆拥有者字段206可以包括一个或多个智能合约210,所述一个或多个智能合约可以在满足与相关拥有者206有关的车辆202的某些条件时自动执行。一个或多个智能合约可以存储为计算机代码,以响应于满足某些条件基于嵌入区块链(诸如图1的区块链108)中的合约执行虚拟机(VM)可用的实时事件数据在所述合约执行VM上执行。在各种实施例中,实时事件数据可以从例如在车辆202处运行的流服务流式传输到合约执行VM。下文参考图7更详细地描述智能合约的执行。

[0038] NFT-VID 200的可修改数据字段可以包括车辆操作者字段212,所述车辆操作者字段可以存储车辆的一个或多个操作者的识别信息。所述识别信息可以包括一个或多个操作者ID 214(例如,每个车辆操作者的操作者ID 214)。操作者ID 214可以是相应车辆操作者的驾驶执照或其他识别号码或代码,或者操作者ID 214可以参考操作者的NFT-DID,其中操作者的NFT-DID可以包括操作者的识别信息。车辆操作者字段212还可以包括操作者智能合约字段216,所述操作者智能合约字段可以存储一个或多个智能合约,所述一个或多个智能合约可以在满足与相关车辆202有关的操作者212的某些条件时自动执行。例如,智能合约可以确立车辆只能在工作时间由操作者操作。当操作者访问车辆时,在车辆处运行的流服务可以向嵌入安装在车辆管理系统处或车辆处或不同装置上的区块链中的合约执行VM通知访问时间。如果操作者试图在工作时间之外访问车辆,则合约执行VM可以接收访问时间,并且在工作时间之外的访问时间可以导致执行智能合约。当执行智能合约时,可以生成用于对操作者禁用车辆访问的指令,合约执行VM将所述指令发送到车辆进行实施。例如,所述指令可以包括在被执行时启用或禁用访问的计算机代码,或者所述指令可以在车辆ECU处被转换为计算机代码。当在车辆处执行代码时,可以阻止操作者访问车辆。

[0039] NFT-VID 200的可修改数据字段可以包括所指派的数字密钥字段218,所述数字密钥字段可以包括关于与车辆202相关联的一个或多个数字密钥的信息。例如,可将所述一个或多个数字密钥中的第一数字密钥指派给车辆拥有者206中的第一拥有者。第一数字密钥可以确立第一拥有者始终有权访问车辆202的所有功能性。可将所述一个或多个数字密钥

中的第二数字密钥指派给车辆操作者212中的第一操作者。所述第二数字密钥可确立第一操作者始终有权访问车辆202,并且有权访问车辆202的第一组功能性。可将所述一个或多个数字密钥中的第三数字密钥指派给车辆操作者212中的第二操作者。所述第三数字密钥可确立第二操作者始终有权访问车辆202,并且有权访问车辆202的第二组功能性。可将所述一个或多个数字密钥中的第四数字密钥指派给车辆操作者212中的第三操作者。所述第四数字密钥可确立第三操作者在特定时间期间有权访问车辆202,并且有权访问车辆202的第三组功能性,等等。例如,车辆202可以是由合作农场共享的拖拉机,其中不同的数字密钥由合作组织的不同成员使用。第一操作者可以是将拖拉机用于第一目的的成员;第二操作者可以是将拖拉机用于第二目的的成员;以及第三操作者可以是被允许在日间时间期间使用拖拉机的成员;等等。

[0040] 图2B示出了示例性NFT-DID 250。NFT-DID 250可以包括各种可修改和/或不可变的数据字段。NFT-DID 250可以包括不可变的NFT-DID标识符251,可使用所述NFT-DID标识符来参考NFT-VID 250。不可变的数据字段还可包括人员字段252,所述人员字段可以包括NFT-DID 250所对应的人员的识别信息。所述人员可以是车辆的拥有者或操作者,或者是以不同方式链接到车辆或车辆管理系统的人员。例如,所述人员可以是车辆的前拥有者,或者是租赁、管理车辆或与车辆一起工作的某人。在各种实施例中,单个NFT-DID 250可以1:1关系对应于单个人员,其中没有其他NFT-DID对应于所述人员,并且没有其他人员对应于NFT-DID 250。人员字段252可以包括存储在例如人员的可修改ID号字段254中的人员的识别信息(例如,驾驶执照)。人员字段252还可以包括人员的其他识别信息(例如,性别、年龄、证书、资格、培训数据等)。所述识别信息可以包括文本数据和/或其他类型的数据,诸如图像数据(例如,人员的图像)。

[0041] NFT-DID 250的可修改数据字段可以包括拥有车辆字段256,所述拥有车辆字段可以存储人员252所拥有的一辆或多辆车辆(例如,车辆202)的识别信息。识别信息可以存储在可修改的车辆ID字段258中,所述可修改的车辆ID字段可以包括多个车辆ID(例如,所拥有的每个车辆一个车辆ID 258)。例如,车辆ID 258可以是VIN号码。在一些实施例中,车辆ID 258可以例如经由NFT-VID的标识符来参考所拥有的车辆的NFT-VID,而不是经由车辆ID(例如,VIN号码)直接参考车辆。所参考的NFT-VID可以包括车辆识别信息,如上文参考图2A所述。

[0042] 另外,对于一辆或多辆所拥有的车辆256,拥有车辆字段256可以包括存储在拥有者智能合约字段260中的一个或多个拥有者智能合约,所述一个或多个拥有者智能合约可以在满足与对应的所拥有的车辆256有关的人员252的某些条件时自动执行。一个或多个智能合约可以存储为计算机代码,所述计算机代码可响应于满足某些条件在嵌入区块链(诸如图1的区块链108)中的虚拟机上执行。在一些实施例中,拥有者智能合约可以与NFT-VID 200的拥有者智能合约字段210的拥有者智能合约相同。在此类情况下,由人员252参考车辆202创建的智能合约的第一副本可以存储在NFT-DID 250的拥有者智能合约字段260中,并且智能合约的第二副本可以存储在NFT-VID 200的拥有者智能合约字段210中。替代地,对NFT-DID 250的一个或多个拥有者智能合约260的参考可以存储在拥有者智能合约210中(例如,而不是存储智能合约的两个副本),或者对NFT-VID 200的一个或多个拥有者智能合约210的参考可以存储在NFT-DID 250的拥有者智能合约260中。

[0043] NFT-DID 250的可修改数据字段可以包括操作车辆字段262,所述操作车辆字段可以存储人员252所操作的一辆或多辆车辆的识别信息。由人员252操作的一个或多个车辆可以是或包括人员252所拥有的一辆或多辆拥有的车辆256,和/或由人员252操作的一辆或多辆车辆可以不为人员252所拥有。识别信息可以包括一个或多个车辆ID 264(例如,每个操作的车辆262一个车辆ID 264)。车辆ID 264可以是相应车辆202的驾驶执照或其他识别号码或代码,或者车辆ID 264可以参考由人员252操作的车辆202的NFT-VID 200,其中NFT-VID 200可以包括车辆202的识别信息(例如,车辆ID 204)。操作车辆字段262还可以包括操作者智能合约字段266,所述操作者智能合约字段可以存储一个或多个智能合约,所述一个或多个智能合约可以在满足人员252和相关的车辆202的某些条件时自动执行。在一些实施例中,操作者智能合约266可以与NFT-VID 200的操作者智能合约216相同,其中操作者智能合约266可以包括对操作者智能合约216的参考,或者操作者智能合约216可以包括对操作者智能合约266的参考,或者同一智能合约的副本可以存储在操作者智能合约266和操作者智能合约216两者中。

[0044] NFT-DID 250的可修改数据字段可以包括所指派的数字密钥字段268,所述数字密钥字段可以包括关于与人员252相关联的一个或多个数字密钥的信息。例如,可针对人员252针对所拥有的车辆256中的第一拥有的车辆创建一个或多个数字密钥中的第一数字密钥。所述第一数字密钥可确立人员252始终有权访问第一拥有的车辆的所有功能性。可将一个或多个数字密钥中的第二数字密钥指派给人员252以操作操作车辆262中的第一操作车辆。所述第二数字密钥可确立人员252始终有权访问第一操作车辆,并且有权访问第一操作车辆的第一组功能性。可将一个或多个数字密钥中的第三数字密钥指派给人员252以操作操作车辆262中的第二操作车辆。所述第二数字密钥可确立人员252始终有权访问第二操作车辆,并且有权访问第二操作车辆的第二组功能性,且依此类推。例如,人员252可以是公司车辆的拥有者,并且可以依据经验和培训将各种数字密钥指派给公司的不同员工以使用公司车辆的不同功能性。

[0045] 返回到图1,区块链108可包括合约执行虚拟机(VM)109,所述合约执行虚拟机可执行在NFT-VID或NFT-DID中包括的一个或多个智能合约,如上文描述。在各种实施例中,车辆130可以包括流服务134的一种实现方式(例如,oracle),所述流服务可以将来自车辆130的实时事件数据流式传输到合约执行VM 109。合约执行VM 109可以基于从流服务134接收到的实时事件数据来执行一个或多个智能合约。

[0046] 在一些实施例中,区块链135可以包括在车辆130中,其中区块链135是区块链108的副本。在此类实施例中,区块链135的合约执行VM 136可以被配置为从流服务134接收实时数据,并且基于所述实时数据执行存储在区块链135上的一个或多个智能合约。通过在车辆130中包括区块链135,不依赖于与车辆管理系统102的通信来执行智能合约,由此车辆管理系统102的可用性的缺乏(例如,由于意外停机时间或缺乏与车辆130的连接性)可能不影响一个或多个智能合约对车辆130的控制。在其他实施例中,区块链108的副本可替代地或另外安装在车辆130的操作者的装置中,并且区块链108的副本的合约执行VM可以被配置为从流服务134接收实时数据,并且基于所述实时数据执行存储在区块链108的所述副本上的一个或多个智能合约。

[0047] 通过在车辆130和/或操作者的装置处包括区块链108的副本,可以创建分布式账

本,其中数字密钥和/或智能合约的有效性可以通过各种装置和/或车辆130处的区块链108的多个副本来验证,因此增加了车辆130的安全性。另外,可以增加车辆管理系统102对外部因素的稳健性。例如,在其中在车辆管理系统102的区块链108处执行智能合约的第一状况下,电力中断可能使车辆管理系统102对于车辆130不可用,由此车辆130可能无法访问或执行智能合约,从而限制对车辆130的访问或使用。在其中在车辆130的区块链135处执行智能合约的第二状况下,对存储在区块链135上的智能合约的访问或执行可不受电力中断影响。

[0048] 在其他实施例中,区块链108的副本可替代地或另外安装在车辆130的操作者的装置中,并且区块链108的副本的合约执行VM可以被配置为从流服务134接收实时数据,并且基于实时数据执行存储在区块链108的副本上的一个或多个智能合约。

[0049] 在其他实施例中,区块链108的拥有者副本可替代地或另外安装在车辆拥有者137中的一者或多者的装置中,其中区块链108的拥有者副本可用于满足分布式账本的要求。可查阅区块链108的拥有者副本以认证操作者和/或验证智能合约。然而,区块链108的拥有者副本可以包括或可以不包括被配置为监听由流服务134流式传输的实时事件数据并基于所述实时事件数据执行智能合约的合约执行VM。例如,车辆130可不包括区块链135,并且可由合约执行VM 109接收由流服务134流式传输的实时事件数据,所述合约执行VM可基于所述实时事件数据执行一个或多个智能合约。在执行一个或多个智能合约之前,车辆管理系统102可以通过将所述一个或多个智能合约与在拥有者装置处存储的区块链108的其他副本上存储的一个或多个智能合约的副本进行比较来验证所述一个或多个智能合约。在验证之后,当执行一个或多个智能合约时,合约执行VM 109可以向车辆130传输指令。所述指令可以在ECU 132处执行,所述ECU可以启用或禁用对车辆130的一个或多个功能性的访问和/或使用。在一些实施例中,所述指令可以包括将在车辆处执行以启用或禁用访问的计算机代码。在其他实施例中,可以在ECU 132处将所述指令转换成计算机代码。使用区块链108的拥有者副本进行验证并且使用车辆管理系统102处的区块链108(的主副本)进行合约执行的优点在于,区块链135可以不包括在数字密钥中并且安装在车辆130和/或操作者装置处,这可以减小由车辆管理系统102无线传输的数字密钥的大小,并且减少操作者装置和/或ECU 132消耗的资源量。

[0050] 车辆管理系统102的非暂时性存储器104可以包括NFT-VID管理模块112,所述NFT-VID管理模块可以包括用于管理存储在区块链108上的NFT-VID的指令。类似地,非暂时性存储器104可包括NFT-DID管理模块114,所述NFT-DID管理模块可包括用于管理存储在区块链108上的NFT-DID的指令。在各种实施例中,NFT-VID管理模块112和NFT-DID管理模块114可以包括指令,所述指令在由处理器106执行时致使车辆管理系统102进行下文参考图4更详细地讨论的方法400的分别用于创建、存储和更新NFT-VID和NFT-DID的步骤中的一者或多者。

[0051] 车辆管理系统102可包括数字密钥管理模块116,所述数字密钥管理模块可包括用于管理存储在NFT-VID和/或NFT-DID中的可撤销数字密钥的指令,所述NFT-VID和/或NFT-DID存储在区块链108上。数字密钥管理模块116可包括指令,所述指令在由处理器106执行时致使车辆管理系统102进行在下文参考图5更详细地讨论的方法500的用于创建和更新存储在区块链108上的NFT-VID和/或NFT-DID中的数字密钥的步骤中的一者或多者。

[0052] 车辆管理系统102可以可操作地/通信地耦合到用户输入装置120和显示装置124。

用户输入装置120可以包括以下各项中的一者或多者:触摸屏、键盘、鼠标、触控板、运动感测相机,或被配置为使得用户能够与车辆管理系统102交互并操纵所述车辆管理系统内的数据的其他装置。在一个示例中,用户输入装置120可以使得用户能够执行与管理车辆130的访问和/或操作权限相关的各种动作,包括但不限于在区块链108上记录车辆130的购买/销售或新拥有者,以及管理车辆130的一个或多个数字密钥的颁发和使用。显示装置124可包括利用几乎任何类型的技术的一个或多个显示装置。在一些实施例中,显示装置124可以包括计算机监视器,可在所述计算机监视器上显示车辆130、车辆拥有者136和/或车辆操作者138的数据。显示装置124可以与处理器106、非暂时性存储器104和/或用户输入装置120组合在共享外壳中,或者可以是外围显示装置,并且可以包括监视器、触摸屏、投影仪或本领域已知的其他显示装置,其可以使得用户能够使用存储在非暂时性存储器104中的各种数据和/或与所述各种数据交互。

[0053] 现在参考图3,示出了数字密钥系统300,所述数字密钥系统包括其上已经安装有车辆管理系统(VMS)应用程序304的电子装置302,其中VMS应用程序304包括数字密钥306。在一些实施例中,数字密钥306可以不包括在VMS应用程序304中,并且可以存储在VMS应用程序304之外的电子装置302的存储器中。VMS应用程序304可以是从图1的车辆管理系统102的网站下载和安装的应用程序(或用于PC的应用程序)。VMS应用程序304可以允许电子装置302的用户(例如,车辆的操作者或拥有者)与车辆管理系统102交互和/或使用车辆管理系统102的各种功能性。例如,车辆的拥有者可以使用VMS应用程序304来创建或更新数字密钥306;将数字密钥306传送给车辆的操作者;访问存储在一个或多个NFT中的车辆和/或操作者数据,所述一个或多个NFT存储在车辆管理系统102的区块链上或存储在数字密钥306中所存储的区块链的副本上;以及其他功能性。

[0054] 数字密钥306可以由操作者350结合车辆管理系统102使用以获得对图1的车辆130的访问。具体地,电子装置302包括无线通信模块303,所述无线通信模块可以管理与车辆130的通信模块133和/或上述车辆管理系统102的数字密钥管理模块116的无线通信。在各种实施例中,电子装置302是操作者350的智能电话。

[0055] 在各种实施例中,车辆130可以具有RKE系统,其中当电子装置302在阈值接近度内时,操作者350可以请求访问车辆130。例如,当电子装置302在阈值接近度内时,可以启动VMS应用程序304,由此可以在电子装置302上显示VMS应用程序304的GUI 305以请求访问车辆130。在一些实施例中,操作者350可以在阈值接近度内时在GUI 305中选择应用程序的控制元件以请求访问。在其他实施例中,RKE是PKE系统,并且VMS应用程序304可以在阈值接近度内时自动请求访问。当请求访问时,可以将数字密钥306传输到通信模块133。当在通信模块133处接收到数字密钥306时,可以认证数字密钥306和/或操作者350。

[0056] 在一个实施例中,对数字密钥306和操作者350中的一者或两者的认证可以由车辆管理系统102实施。例如,可将操作者350和/或数字密钥306的信息从通信模块133无线地传输到车辆管理系统102的通信模块107。操作者350和/或数字密钥306的信息可以由车辆管理系统102处理(例如,通过执行数字密钥管理模块116的代码)以认证操作者350和/或数字密钥306。如果操作者350和/或数字密钥306经过认证,则车辆管理系统102可以将成功认证从通信模块107传输到车辆130的通信模块133,并且车辆130的ECU 132可以解锁车辆130的一个或多个门以允许操作者350对车辆130的访问。下文参考图6更详细地描述在车辆管理

系统102处认证操作者350和/或数字密钥306的信息。

[0057] 在其他实施例中,可将在通信模块133处接收到的操作者350和/或数字密钥306的信息发送到车辆130的ECU 132进行认证,或者可将操作者350和/或数字密钥306的信息从电子装置302的无线通信模块303传输到车辆管理系统102的通信模块107以进行认证,之后将数字密钥306传输到ECU 132以访问车辆130。

[0058] 参考图6,示出了用于认证车辆的操作者(例如,车辆130的操作者350)和/或操作者的数字密钥(例如,数字密钥306)的示例性方法600。方法600可以由车辆管理系统的处理器(诸如车辆管理系统102的处理器106)执行。

[0059] 方法600开始于602,其中方法600包括确定操作者是否已经请求访问车辆。如上所述,当操作者进入车辆的阈值接近度时,可以请求访问车辆。当请求访问车辆时,车辆可以将访问请求的细节传输到车辆管理系统(例如,传输到车辆管理系统102的通信模块107)。访问请求的细节可以包括操作者的识别信息、数字密钥和/或数字密钥的具体细节。如果在602处确定尚未请求访问车辆,则方法600前进到604。在604处,方法600包括一直等到请求访问,并且方法600回到602。

[0060] 在606处,方法600包括接收操作者识别信息和/或数字密钥的信息。在一些实施例中,可以从车辆(例如,车辆130的通信模块133)或操作者的电子装置(例如,电子装置302的无线通信模块303)接收操作者识别信息和/或数字密钥的信息。在一些实施例中,操作者识别信息可以与数字密钥分开发送,而在其他实施例中,可以从数字密钥中提取操作者识别信息。

[0061] 在608处,方法600包括认证操作者和/或数字密钥信息。认证操作者和/或数字密钥信息可以包括将操作者的识别信息与存储在车辆管理系统处的操作者的识别信息进行比较。在各种实施例中,操作者的识别信息和/或数字密钥信息可以在区块链(例如,区块链108)上存储在操作者的NFT(例如,NFT-DID 250)和车辆的NFT(例如,NFT-VID 200)中的一者或多者中。例如,存储在车辆管理系统的非暂时性存储器中(例如,在数字密钥管理模块116中)的认证码可以从区块链中提取操作者的NFT,并且确定操作者识别信息是否与存储在操作者的NFT中的操作者的识别信息匹配。如果信息匹配,则可以认证操作者。类似地,认证码可以从区块链中提取车辆的NFT,并且确定数字密钥(或数字密钥信息)是否与记录在车辆NFT中(例如,在所指派的数字密钥字段218中)的车辆的数字密钥匹配。在一些实施例中,可使用面部辨识软件将由操作者智能电话的相机生成的操作者的图像与存储在操作者的NFT中的操作者的图像进行比较。应理解,可以使用各种不同的技术和技艺来认证操作者,并且本文提供的示例是用于说明而非限制。

[0062] 在610处,方法600包括确定对操作者和/或数字密钥的认证是否成功。如果在610处确定对操作者和/或数字密钥的认证是成功的,则方法600前进到614。在614处,方法600包括将认证和/或数字密钥的细节发送到车辆。认证的细节可以包括认证成功的指示。认证的细节还可以包括车辆授予操作者访问权的指令。

[0063] 替代地,如果在610处确定认证不成功,则方法600前进到612。在612处,方法600包括将不成功的认证记录在存储在车辆管理系统处的区块链上的操作者的NFT和/或车辆的NFT中。例如,不成功的认证可以存储在对指派给操作者的数字密钥的参考中(例如,在所指派的数字密钥字段218/268中)。通过这种方式,车辆的拥有者可以查阅NFT(例如,经由车辆

管理系统的GUI)以查看关于拥有者已经为车辆指派或向车辆的操作者指派的数字密钥的成功和不成功的认证尝试。方法600结束。

[0064] 返回到图3,数字密钥306包括操作者和车辆的各种信息。所述信息可以包括例如操作者数据308(例如,操作者的识别信息)、车辆数据310(例如,车辆的标识信息)和数字密钥的到期数据312,诸如数字密钥有效的时段的指示,和/或数字密钥终止有效并且不能再用于访问车辆的时间的指示。在一些实施例中,到期数据312可以另外或替代地包括建立数字密钥306可以到期或被撤销的条件的规则。所述规则可以建立在一个或多个智能合约中,例如,存储在与车辆130相关联的NFT-VID的操作者智能合约216中,或存储在与操作者相关联的NFT-DID的操作者智能合约266中,如上所述,所述NFT-VID和NFT-DID可存储在区块链中。例如,车辆130的拥有者可以为车辆130的操作者编写智能合约,所述智能合约指定数字密钥306在操作者的驾驶执照的到期日期到期,或者数字密钥306在操作者牵涉事故的情况下或在一种或多种其他状况下到期。一般来说,可以建立在不再满足时使数字密钥306到期的条款和条件。当数字密钥到期或被撤销时,可以从车辆的NFT-VID和/或操作者的NFT-DID中移除与数字密钥306相关联的车辆的访问和/或使用权限。在此类情况下,VMS应用程序304可以向车辆的操作者和/或拥有者发送通知。

[0065] 数字密钥306还可以包括流服务应用程序313,所述流服务应用程序可以被传输到车辆并在车辆的ECU处启动,以发起流服务(例如,用于在区块链上执行智能合约的oracle)。流服务可以将车辆的实时事件数据流式传输到嵌入车辆管理系统的区块链(例如,区块链108)的主副本中的合约执行VM。合约执行VM可以基于所接收的事件数据来执行与操作者和/或车辆有关的一个或多个智能合约,如下文参考图7更详细地描述。

[0066] 在一些实施例中,数字密钥306可以另外包括区块链314,所述区块链可以是车辆管理系统的区块链的主副本的版本或副本。区块链314可以包括合约执行VM 316,所述合约执行VM可以与嵌入主副本中的合约执行VM相同。区块链314还可以包括车辆的NFT-VID 320和操作者的NFT-DID 318的所存储的副本,所述副本分别可以是图2A和图2B的NFT-VID 200和NFT-DID 250的副本。区块链314可以在成功认证之后被传输到车辆130并安装在ECU 132中,其中合约执行VM 316可以被配置为接收由在车辆处发起的流服务流式传输的实时事件数据。当区块链314安装在ECU 132中时,ECU 132可以在不依赖于车辆管理系统102的情况下管理对车辆130的访问。例如,车辆130的通信模块133可能例如由于车辆管理系统102处的互联网连接性问题或技术问题而无法与车辆管理系统102的通信模块107建立联系。因此,在此类问题或难题的情况下,可以根据存储在区块链314的NFT-DID 318和/或NFT-VID 320中的一个或多个智能合约来维持对车辆130的控制,包括对车辆130的访问和对车辆130的一个或多个功能性的使用,从而导致与在依赖于与车辆管理系统102的通信时可以实现的控制相比更稳健的控制实现方式。另外,通过减少与车辆管理系统102的通信量,可以减少车辆管理系统的存储器和处理资源的消耗并将所述存储器和处理资源卸载到车辆130,从而降低操作车辆管理系统102的成本以及在车辆管理系统102处出现延迟和技术问题的可能性。

[0067] 图4示出了用于管理在安装在车辆管理系统(诸如图1的车辆管理系统102)中的区块链上存储车辆的数据、车辆的拥有者的数据和车辆的操作者的数据的示例性方法400。方法400可以由车辆管理系统的处理器(例如,处理器106)基于存储在车辆管理系统的存储器

(例如,存储器104)中的指令来执行。例如,指令可以存储在存储器的数字密钥管理模块(例如,数字密钥管理模块116)中,或存储器的NFT-VID管理模块(例如,NFT-VID管理模块112)中,或者存储在存储器的NFT-DID管理模块(例如,NFT-DID管理模块114)中。车辆数据、拥有者数据和/或操作者数据可以由车辆管理系统在生成向车辆的一个或多个操作者和/或拥有者授予对车辆的访问权的数字密钥期间使用,如本文所述。

[0068] 方法400开始于401,其中方法400包括接收更新存储在车辆管理系统的区块链中的数据的请求。

[0069] 在402处,方法400包括确定所述请求是否指示车辆管理系统将管理新的车辆。如果在402处确定所述请求未指示车辆管理系统将管理新的车辆,则方法400前进到406。如果在402处确定所述请求指示将管理新的车辆,则方法400前进到404。在404处,方法400包括在区块链上创建车辆的NFT-VID(例如,图2A的NFT-VID 200),以及车辆的一个或多个拥有者和一个或多个操作者的一个或多个NFT-DID。可以基于从请求中提取的信息来创建NFT-VID和NFT-DID。例如,所述信息可以包括车辆的信息、车辆的一个或多个拥有者的信息以及车辆的一个或多个操作者的信息,所述一个或多个操作者可以包括一个或多个拥有者。可以将所述信息写入到NFT-VID的字段中,如上文参考图2A所述,并且写入到NFT-DID的字段中,如上文参考图2B所述。当已经创建了车辆的NFT-VID和车辆的拥有者和操作者的一个或多个NFT-DID时,NFT-VID和一个或多个NFT-DID可以存储在区块链中。具体地,可以将NFT-VID和一个或多个NFT-DID写入到当前数据区块,其中当前数据区块经由本领域已知的一个或多个程序并入到区块链中。然后,方法400可前进到406。

[0070] 在406处,方法400包括确定所述请求是否指示已经购买由车辆管理系统管理的车辆,其中所述车辆具有一个或多个新拥有者。如果在406处确定所述请求未指示已经购买由车辆管理系统管理的车辆并且所述车辆具有新拥有者,则方法400前进到410。如果在406处确定所述请求指示车辆具有一个或多个新拥有者,则方法400前进到408。在408处,方法400包括用所述一个或多个新拥有者更新存储在区块链上的车辆的NFT-VID,并且更新所述一个或多个新拥有者的一个或多个NFT-DID。可基于从所述请求提取的信息来更新NFT-VID和一个或多个NFT-DID。例如,在一些实施例中,当更新NFT-VID时,可以删除在车辆拥有者字段中列出的一个或多个先前拥有者(例如,车辆拥有者206)的识别信息,并且用一个或多个新拥有者取代。在其他实施例中,在车辆拥有者字段中列出的一个或多个先前拥有者的识别信息可以不从NFT-VID中移除,而是可以被标记为先前拥有者,或者存储在车辆的先前拥有者的单独字段中。

[0071] 如果新拥有者已经记录在存储在车辆管理系统的区块链中的NFT-DID中,则可以更新新拥有者的NFT-DID以反映新拥有者对车辆的所有权。例如,可以将车辆添加到新拥有者的NFT-DID的拥有车辆字段(例如,拥有车辆256)。如果新拥有者操作车辆,则可将所述车辆添加到NFT-DID的操作车辆字段(例如,操作车辆262)。如果新拥有者尚未记录在存储在车辆管理系统的区块链中的NFT-DID中,则可以利用请求中包括的信息来创建新拥有者的新NFT-DID,如上所述。

[0072] 类似地,当更新新拥有者的一个或多个NFT-DID时,可以更新先前拥有者的一个或多个NFT-DID以从拥有车辆字段中移除车辆。在一些实施例中,可不从一个或多个先前拥有者的NFT-DID中移除车辆,而是可将车辆标记为先前拥有车辆,或存储在先前拥有车辆的

NFT-DID的单独字段中。

[0073] 当已经更新了车辆的NFT-VID和车辆的拥有者的一个或多个NFT-DID时,NFT-VID和一个或多个NFT-DID可以存储在区块链中。然后,方法400可前进到410。

[0074] 在410处,方法400包括确定所述请求是否指示已经向一个或多个新操作者授予对由车辆管理系统管理的车辆的访问权,所述一个或多个新操作者可以包括一个或多个新拥有者。如果在410处确定所述请求未指示已经向一个或多个新操作者授予对由车辆管理系统管理的车辆的访问权,则方法400前进到414。如果在410处确定所述请求指示已经向一个或多个新操作者授予对由车辆管理系统管理的车辆的访问权,则方法400前进到412。在412处,方法400包括生成将授予一个或多个新操作者的车辆的一个或多个数字密钥。下文关于图5更详细地描述生成数字密钥。在生成数字密钥之后,可以用一个或多个数字密钥更新存储在区块链上的车辆的NFT-VID,并且可以用一个或多个数字密钥更新一个或多个新操作者的一个或多个NFT-DID。例如,所生成的数字密钥可以存储在车辆的NFT-VID的所指派的数字密钥字段(例如,所指派的数字密钥字段218)和/或一个或多个新操作者的NFT-DID的所指派的数字密钥字段(例如,所指派的数字密钥字段268)中。

[0075] 另外,例如,如果车辆具有新拥有者,则所述请求可以提供删除指派给车辆的先前操作者的车辆的一个或多个先前数字密钥的指令。替代地,在一些情况下,指派给车辆的先前操作者的车辆的一个或多个先前数字密钥可以不被删除并且可以保持有效。例如,车辆可能没有所有权变化,并且可以在不更改指派给其他当前操作者的数字密钥的情况下向新操作者授予对车辆的访问权。

[0076] 当已经更新了车辆的NFT-VID和车辆的新操作者的一个或多个NFT-DID时,NFT-VID和一个或多个NFT-DID可以存储在区块链中。然后,方法400可前进到414。

[0077] 作为示例,与其他数字密钥系统相比,本文描述的车辆管理系统基于在分布式账本中使用NFT来存储车辆和车辆拥有者/操作者数据可以允许在车辆的使用期过程中灵活地跟踪车辆与各个拥有者和/或操作者之间的各种变化的潜在复杂的关系。例如,第一方对车辆的所有权的记录可以经由一个或多个NFT存储在分布式账本(例如,区块链)的第一条目中。一个或多个NFT可以包括车辆的NFT-VID和/或拥有者的NFT-DID。第一方向第二方出租车辆的记录可以存储在分布式账本的第二条目中,其中NFT-VID和NFT-DID可以在分布式账本中更新。使用车辆的权限的记录可以存储在分布式账本的第三条目中,所述第三条目更新车辆的NFT-VID和拥有者的NFT-DID,并且添加操作者的新NFT-DID。随着时间的推移,拥有者和/或操作者可能会变化并且例如由拥有者更新。由于分布式账本系统的已知性质和优点,车辆、拥有者和操作者的当前和历史信息可以在任何时间安全地存储和访问,其中与不使用分布式账本的不同种类的车辆管理系统相比,未授权的个体入侵和/或篡改的概率更低。通过这种方式,可以有效地管理车辆和与车辆相关联的实体的可靠且可信的记录集,而不依赖于车辆管理系统的集中式规范。

[0078] 在414处,方法400包括向车辆的相关的新拥有者和新操作者发送创建或更新NFT-VID和NFT-DID的通知,并且方法400结束。

[0079] 现在参考图5,示出了用于创建车辆管理系统(诸如图1的车辆管理系统102)的车辆的数字密钥以传输到车辆的操作者来使用车辆的示例性方法500。方法500可以由车辆管理系统的处理器(例如,处理器106)基于存储在车辆管理系统的存储器(例如,存储器104)

中的指令来执行。例如,指令可以存储在以下各项中的一者或多者中:存储器的数字密钥管理模块(例如,数字密钥管理模块116)、存储器的NFT-VID管理模块(例如,NFT-VID管理模块112),以及存储器的NFT-DID管理模块(例如,NFT-DID管理模块114)。

[0080] 方法500开始于502,其中方法500包括确定是否已经接收到对新数字密钥的请求。在一些实施例中,可以由车辆管理系统响应于例如由于新拥有者购买车辆而注册车辆的新操作者的请求而生成对新数字密钥的请求。在一些实施例中,当购买被记录在车辆管理系统中时,可以由车辆管理系统自动发起请求。在此类情况下,关于车辆的访问和使用的默认使用条款(例如,权限)可以包括在所述请求中。例如,默认使用条款可以指定新操作者具有对车辆的完全访问权,并且可以不针对新操作者禁用车辆的任何功能性。

[0081] 在其他实施例中,所述请求可以由新拥有者使用车辆管理系统的应用程序的GUI(例如,VMS应用程序304的GUI 305)发起。例如,新拥有者可以通过在计算机的浏览器或新拥有者的计算装置(例如,电子装置302)的应用程序上登录到车辆管理系统来访问GUI。新拥有者可以将用于访问和/或使用车辆的使用条款输入到GUI中,并且GUI可以基于由新拥有者输入的数据来生成请求。在一些情况下,新拥有者可以在GUI中打开车辆的现有数字密钥,并且修改现有数字密钥的数据。例如,可以由车辆管理系统使用默认使用条款自动生成数字密钥,并且新拥有者可以打开自动生成的数字密钥,并且使用针对新操作者的不同期望的使用条款替换所述默认使用条款。

[0082] 如果在502处确定尚未接收到对新数字密钥的请求,则方法500前进到504。在504处,方法500包括一直等到接收到请求,并且方法500回到502。

[0083] 如果在502处确定已经接收到对新数字密钥的请求,则方法500前进到506。在506处,方法500包括针对操作者创建新数字密钥。在各种实施例中,可以基于在请求中包括的信息(例如,默认包括的或由新拥有者指定的信息)来创建新数字密钥。所述数字密钥可以是图3的数字密钥306的非限制性版本,并且可以包括用于操作者的数据(例如,操作者数据308)和车辆的数据(例如,车辆数据310)的字段,所述字段可以从请求中提取。所述数字密钥可以包括用于数字密钥的到期数据(例如,到期数据312)的字段,所述字段可以包括可以使数字密钥无效的到期日期和/或期限。如果过了到期日期,则在一些实施例中,可以从在请求中包括的一个或多个NFT中提取信息。例如,所述请求可以包括车辆的NFT-VID(例如,图2A的NFT-VID 200)和操作者的NFT-DID,其中NFT-VID和NFT-DID可以存储在车辆管理系统的区块链中,如上文参考图4所述。

[0084] 在508处,方法500包括在一个或多个智能合约中嵌入或更新使用条款。在各种实施例中,可以将用于操作车辆的期望的使用条款写入到一个或多个智能合约中,所述一个或多个智能合约在满足某些条件时自动执行。一个或多个智能合约可以由嵌入安装在车辆管理系统处或车辆处的区块链(例如,区块链108或区块链314)中的合约执行VM(例如,合约执行VM 109或合约执行VM 316)执行。确定是否已经满足某些条件可以基于由安装在车辆处并在车辆处实施的流服务(例如,流服务134)流式传输到合约执行VM的实时事件数据。例如,流服务可以由车辆的ECU(例如,车辆130的ECU 132)实施。

[0085] 在510处,方法500包括更新区块链上的一个或多个NFT以包括新操作者和一个或多个智能合约的数据。如上文参考图2A和图2B所描述的,分别将车辆的细节存储在与车辆相关联的NFT-VID中,并且将拥有者或操作者的细节存储在与拥有者或操作者相关联的

NFT-DID中。

[0086] 在512处,方法500包括将流服务应用程序(例如,流服务应用程序313)复制到数字密钥。当使用数字密钥获得对车辆的访问时,流服务应用程序可以被传递到车辆,并且例如由车辆的ECU启动以发起流服务,如上所述。所述流服务可以将实时事件数据传输到嵌入区块链中的合约执行VM,其中实时事件数据可以使合约执行VM执行一个或多个智能合约中的一者或多者。

[0087] 在各种实施例中,可以将存储在车辆管理系统处的区块链(例如,区块链108)的版本复制到数字密钥。当使用数字密钥获得对车辆的访问时,可以将区块链(例如,区块链314)的版本传递到车辆并存储在例如ECU的存储器中。通过将区块链的版本存储在车辆处,由流服务流式传输的实时事件数据可以由嵌入存储在车辆处的区块链的版本中的合约执行VM的版本接收,并且智能合约可以由合约执行VM基于所述实时事件数据来执行,而不是依赖于车辆管理系统来执行智能合约并将执行的结果传输到所述车辆。由于不依赖于车辆管理系统来执行智能合约,例如,甚至当车辆失去与车辆管理系统的连接性时,也可以更快且更可靠地执行合约执行。

[0088] 在514处,方法500包括将数字密钥的副本以电子方式(例如,无线地)传递到新操作者。在各种实施例中,可以将数字密钥的副本传递到新操作者的电子装置,诸如智能电话。在一些实施例中,数字密钥的副本可以安装在由新操作者使用的专用物理装置(诸如遥控钥匙)中。

[0089] 作为示例,公司可以是车辆的拥有者,并且可以雇用新操作者来操作车辆。公司的管理者可经由车辆管理系统的GUI针对新操作者创建数字密钥。当管理者创建数字密钥时,管理者可以创建智能合约,所述智能合约确立新操作者具有在公司的工作时间期间访问和使用车辆的权限,但在工作时间之外没有访问和操作车辆的权限。可以基于由管理者输入到例如在GUI中显示的合约创建向导的一个或多个字段中的数据来生成智能合约。车辆管理系统可以从区块链中检索车辆的NFT-VID,并且针对新操作者创建(或从区块链中检索)NFT-DID。新操作者可以保存在NFT-VID中,例如,保存在车辆操作者字段212中。智能合约可以保存在NFT-VID中,例如保存在操作者智能合约字段216中。车辆可以保存在新操作者的NFT-DID中,例如,保存在操作车辆262中。智能合约可以保存在NFT-DID中,例如保存在操作者智能合约字段266中。另外,数字密钥的标识符可以保存在NFT-VID和NFT-DID中,例如分别保存在所指派的数字密钥字段218和所指派的数字密钥字段268中。在已经更新NFT-VID和NFT-DID之后,可以将更新后的NFT-VID和更新后的NFT-DID保存在区块链上。

[0090] 管理者可以选择控制元件,诸如复选框,以将区块链的版本包括在车辆中,使得在车辆处而不是在车辆管理系统处实施用于实行使用条款的合约执行。如果管理者选择控制元件以将区块链的版本包括在车辆中,则可以将存储在车辆管理系统处的区块链的副本存储在数字密钥中。如果管理者未选择控制元件以将区块链的版本包括在车辆中,则可以不将存储在车辆管理系统处的区块链的副本存储在数字密钥中,由此可在车辆管理系统处实施智能合约的实行。当执行合约时,合约可以生成可以由车辆的ECU实施以控制对车辆的一个或多个功能性的访问和/或使用的指令和/或计算机代码。

[0091] 在管理者在智能合约中指定车辆的期望的使用条款之后,管理者可以在GUI中选择控制元件以生成数字密钥。车辆管理系统可以基于管理员输入来生成数字密钥。车辆管

理系统可以将用于在车辆处实施流服务的应用程序复制到数字密钥,并且可以将数字密钥无线地传输到新操作者。

[0092] 现在参考图7,示出了用于基于操作者的数字密钥来控制操作者对车辆的访问和对车辆功能性的使用的示例性方法700。所述访问和使用可以由一个或多个智能合约控制,如上文参考图5所述。方法700可以由车辆的ECU根据存储在ECU的存储器中的指令来执行。

[0093] 方法700开始于702,其中方法700包括确定是否已经接收到使用车辆的功能性的请求。出于方法700的目的,所述功能性可以包括打开车辆的门以获得对车辆的访问。使用功能性的请求可以由操作者生成。可以由于操作者例如经由车辆的一个或多个控件命令发起对功能性的使用的动作而生成使用所述功能性的请求。例如,当存储数字密钥的操作者的电子装置进入车辆的阈值接近度时,可以生成访问车辆的请求,或者当操作者选择车辆的仪表板上的按钮或类似控件时,可生成以特定操作模式操作车辆的请求。

[0094] 如果在702处确定尚未接收到使用车辆的功能性的请求,则方法700前进到704。在704处,方法700包括一直等到接收到请求,并且方法700回到702。

[0095] 如果在702处确定已经接收到使用车辆的功能性的请求,则方法700前进到706。在706处,方法700包括从操作者的电子装置接收数字密钥。所述数字密钥可确立适用于操作者的车辆使用条款,如上文参考图5所述。在一些实施例中,当操作者进入车辆的阈值接近度内时,可以将数字密钥自动传递到车辆。

[0096] 在708处,方法700包括启动存储在数字密钥中的流服务应用程序以发起流服务(例如,流服务134)。流服务134可以将车辆的实时事件数据流式传输到嵌入区块链中的合约执行VM,其中适用于操作者和车辆的智能合约包括在存储在区块链上的一个或多个NFT中。在一些实施例中,区块链可以存储在车辆管理系统(例如,车辆管理系统102)处,其中适用于操作者和车辆的智能合约基于从车辆流式传输的实时事件数据在车辆管理系统处自动执行。在其他实施例中,存储在车辆管理系统处的区块链的副本可包括在数字密钥中,由此可将区块链的所述副本传递到车辆并存储在车辆处。在此类实施例中,适用于操作者和车辆的智能合约可以在车辆处自动执行,而不依赖于车辆管理系统。

[0097] 在710处,方法700包括确定所请求的功能性是否被智能合约中确立的使用条款允许。如果智能合约中确立的使用条款允许所请求的功能,则智能合约可不基于实时事件数据自动执行。如果智能合约不基于实时事件数据自动执行,则可假设所述使用条款允许操作者使用所请求的功能性。替代地,如果基于实时事件数据自动执行智能合约,则可以将包括限制、禁用或启用所请求的功能性的操作代码的指令从合约执行VM传输到车辆的ECU。车辆的ECU可以执行操作代码以对操作者实行所述使用条款。

[0098] 如果在710处确定智能合约不允许所请求的功能性(例如,执行智能合约并且将包括操作代码的指令传输到车辆),则方法700前进到712。在712处,方法700包括通过实施操作代码来限制或禁用所请求的功能性,并且向操作者通知所请求的功能性不为适用于操作者的使用条款所允许。

[0099] 如果在710处确定智能合约允许所请求的功能性(例如,不执行智能合约并且不将数据传输到车辆),则方法700前进到714。在714处,方法700包括执行所命令的动作以实施所请求的功能性。

[0100] 在716处,方法700包括确定是否已经接收到限制或禁用功能性的请求,其中所述

请求是根据智能合约中限定的使用条款生成的。可以基于已经到时间或基于在合约执行VM处接收到的新事件来撤销使用车辆的功能性的权限。例如,使用条款可以允许操作者在第一时间执行所命令的动作,但不允许操作者在第二时间执行所命令的动作。替代地或另外,使用条款可基于第一组事件数据允许操作者执行所命令的动作,但基于新的第二组事件数据不允许操作者执行所命令的动作。所述请求可以由嵌入区块链中的合约执行VM基于智能合约的执行来生成。例如,在其中在合约执行VM处接收的事件数据不会导致执行智能合约的第一状况下,可不将限制或禁用功能性的请求从合约执行VM发送到车辆ECU。在其中在合约执行VM处接收到的事件数据导致执行智能合约的第二状况下,可将限制或禁用功能性的请求从合约执行VM发送到车辆ECU。所述请求可以包括在由车辆ECU执行时可以终止或阻止所命令的动作的计算机代码。

[0101] 如果在716处确定尚未接收到限制或禁用功能性的请求,则方法700前进到718。在718处,方法700包括继续车辆的操作,并且方法700回到716。替代地,如果在716处确定已经接收到限制或禁用功能性的请求,则方法700前进到720。在720处,方法700包括终止和/或阻止所命令的动作,并且根据在智能合约中确立的使用条款向操作者通知不再允许功能性。在一些实施例中,终止和/或阻止所命令的动作可以包括执行通过执行智能合约生成的计算机代码。

[0102] 作为示例,例如由车辆的拥有者确立或在生成数字密钥时默认确立的智能合约可以指定车辆的操作者的驾驶执照必须是有效的且是最新的,以让操作者操作车辆。在第一时间,操作者的驾驶执照可以是有效的且最新的。当操作者使用数字密钥来操作车辆时,操作者使用数字密钥来操作车辆的事件可以由在车辆处运行的流服务发送到存储在区块链中的合约执行VM,所述区块链安装或存储在例如车辆管理系统处或车辆处。当合约执行VM接收到所述事件时,合约执行VM可以从事件的数据中识别车辆。合约执行VM可以从区块链检索与车辆相对应的NFT-VID。合约执行VM可以从NFT-VID(例如,分别从操作者智能合约216和操作者ID 214)检索操作者的智能合约和操作者ID,并且将事件数据输入到智能合约中。所述智能合约可以从操作者ID(例如,驾驶执照)确定操作者的驾驶执照是有效的,并且在智能合约中确立的使用条款允许操作者在第一时间操作车辆,由此智能合约可不执行。由于智能合约未执行,因此可以允许操作者在第一时间操作车辆。

[0103] 在稍后的第二时间,操作者的驾驶执照可能不是有效的和最新的(例如,过期、暂停等)。当操作者使用数字密钥来操作车辆时,操作者使用数字密钥来操作车辆的事件可以由在车辆处运行的流服务发送到存储在区块链中的合约执行VM。所述合约执行VM可从事件数据中识别车辆。合约执行VM可从区块链中检索与车辆相对应的NFT-VID,并且从NFT-VID中检索操作者的智能合约和操作者ID,并且将事件数据和/或操作者ID输入到智能合约中。所述智能合约可以从操作者ID确定操作者的驾驶执照不是有效的,并且在智能合约中确立的使用条款不允许操作者在第二时间操作车辆,由此智能合约可执行。当所述智能合约执行时,可生成指令和/或代码,合约执行VM可将所述指令和/或代码发送到车辆。当所述指令和/或代码被传输到车辆时,车辆的ECU可以执行所述指令和/或代码,这可以禁用对车辆的访问和/或车辆的操作。由于被禁用的访问,可不允许操作者在第二时间操作车辆。

[0104] 因此,公开了用于生成车辆的数字密钥以供车辆的一个或多个操作者使用的方法和系统,所述一个或多个操作者可以包括车辆的一个或多个拥有者,其中所述数字密钥可

以针对不同的操作者和/或拥有者确立不同的使用条款(包括访问)。为了实行不同的使用条款,可以将使用条款编写为保存在区块链上的智能合约,其中基于从在车辆处运行的流服务传输到嵌入区块链中的合约执行VM的实时事件数据而自动执行所述智能合约。所述智能合约可以存储在区块链上的NFT中,其中NFT可以与车辆、车辆的拥有者或车辆的操作者中的至少一者相关联。包括NFT的区块链的主副本可以存储在车辆管理系统中,并且区块链的副本可以包括在用于安装在车辆中的数字密钥中,其中接收事件数据的区块链可以安装在车辆管理系统处或车辆处。用于在车辆处运行流服务的应用程序也可以包括在数字密钥中。

[0105] 所述数字密钥可以包括车辆、车辆的一个或多个拥有者以及车辆的一个或多个操作者的识别信息。可以经由车辆管理系统(例如,经由互联网浏览器)创建和/或更新数字密钥,或者可以使用在车辆的拥有者的电子装置上运行的车辆管理系统的应用程序创建和/或更新数字密钥。还可以经由车辆管理系统来创建和/或更新由数字密钥用来参考车辆、拥有者和/或操作者数据并存储智能合约的NFT。

[0106] 所述智能合约可以由嵌入区块链的副本中的合约执行VM来执行,所述区块链的副本包括在数字密钥中并存储在车辆处,或者所述智能合约可以由存储在车辆管理系统处的区块链的主副本的第二合约执行VM执行。通过在车辆处而不是在车辆管理系统处执行智能合约,可以增加执行合约的速度,并且可以减少车辆管理系统对处理和存储器资源的使用,从而增加车辆管理系统的整体效率。另外,当在车辆处执行智能合约时,合约执行可不依赖于往返车辆管理系统的通信,所述通信可能会由于网络或技术问题而延迟或不可用。当智能合约在车辆和操作者的计算装置处或之间执行并且不涉及在无线网络上与车辆管理系统通信时,数字密钥数据和其中确立的权限的安全性也可由于网络上的减少的通信量而得以增加。因此,车辆处的合约执行可以导致使用条款的更稳健和更可靠的实行。

[0107] 一般来说,就针对不同的车辆和个体创建不同的使用条款而言,在存储在区块链上的智能合约中确立使用条款可允许更大的灵活性。拥有者可以通过与用于管理车辆管理系统或管理车辆操作的规范分开的方式自由地创建覆盖不同复杂程度的广泛多种不同权限的各种智能合约。相比之下,用车辆管理系统的操作规范支持可适用于车辆和/或操作者的广泛多种可能的使用条款可能是昂贵的,并且由于有限的可用的开发人员时间,广泛多种可能的使用条款可能是缓慢的。通过利用智能合约的灵活性,可以减少车辆管理系统消耗的资源量,并且可以提高维护车辆管理系统的总体效率。车辆拥有者可以经由车辆管理系统的GUI以易于使用的方式独立地创建新的或不同的使用条款,而无需编写任何计算机代码。另外,由于区块链作为分布式账本操作,其中区块链的各种副本可能存在于不同的车辆或拥有者装置处,因此可以确保存储在区块链的NFT中的车辆、拥有者和操作者数据的有效性,并且可以增加智能合约的安全性。当出现存储在区块链上的数据(诸如智能合约)可能已被未经授权的人员更改的可能性时,可以比较区块链的副本以确定区块链的一个或多个副本的数据是否与区块链的其他副本不一致,且因此是无效的。

[0108] 此外,出于其他原因,对车辆使用的分布式控制可为有利的。例如,公司可能更喜欢分布式系统,因为车辆管理系统和收入流的技术方面可以更有效地分开。例如,公司可能希望在不影响已经建立的车辆控制的机能的情况下出售车辆管理系统。在本文提出的分布式系统下,购买者可以简单地通过维护区块链来支持传统客户,并且可不必维护用于执行

多种不同的车辆控制例程的代码,所述代码在所提出的区块链实现方式中将由拥有者创建的智能合约处置。另外,分布式系统可以更容易缩放,其中可以在不影响车辆管理系统的性能的情况下实现包括更多定制和复杂的使用条款。

[0109] 通过由车辆管理系统维护的区块链的副本上的智能合约来控制对车辆的访问和对车辆的功能性的使用的技术效果是,可以确保智能合约的有效性,可提高车辆管理系统的效率,并且可以增加可以针对车辆的不同操作者限定不同使用条款的灵活性。

[0110] 本公开还提供对一种车辆管理系统的支持,所述车辆管理系统包括:区块链;流服务,所述流服务被配置为向嵌入所述区块链中的合约执行虚拟机(VM)实时提供事件数据;以及非暂时性存储器,所述非暂时性存储器存储指令,所述指令在由所述车辆管理系统的处理器执行时致使所述车辆管理系统进行以下操作:基于来自车辆的拥有者的输入针对所述车辆管理系统的车辆的操作者生成数字密钥,所述数字密钥基于一个或多个智能合约来控制所述操作者对所述车辆的访问和对所述车辆的一个或多个功能性的使用;将所述车辆、所述拥有者和所述操作者的数据存储在所述区块链中,所述数据包括所述一个或多个智能合约;以及将所述数字密钥无线地传输到所述操作者的计算装置。在所述系统的第一示例中,经由数字密钥控制对车辆的访问和/或对车辆的一个或多个功能性的使用还包括:将用于实施流服务的版本的计算机应用程序包括在数字密钥中;响应于在车辆处执行所述应用程序,经由所述流服务的所述版本在所述车辆管理系统处实时地接收所述车辆的事件数据;将所述车辆的所述事件数据转发到嵌入所述区块链中的合约执行VM;响应于所述合约执行VM执行所述一个或多个智能合约中的至少一个智能合约,从所述合约执行VM接收控制对车辆的访问和/或对车辆的一个或多个功能性的使用的指令;以及将所述接收到的指令发送到所述车辆以由所述车辆的电子控制单元(ECU)执行。在任选地包括所述第一示例的所述系统的第二示例中,经由数字密钥控制对车辆的访问和/或对车辆的一个或多个功能性的使用还包括:将区块链的副本包括在数字密钥中,并且包括在第一次使用所述数字密钥时将所述副本安装在所述车辆处的指令;将用于在所述车辆处实施所述流服务的版本的计算机应用程序包括在所述数字密钥中,所述版本向嵌入所述车辆处的所述区块链的所述副本中的合约执行VM提供实时事件数据,所述合约执行VM被配置为基于所述实时事件数据自动执行存储在所述区块链的所述副本中的一个或多个智能合约,所述一个或多个智能合约在被执行时向所述车辆的ECU提供控制对所述车辆的所述访问和/或对所述车辆的所述一个或多个功能性的所述使用的代码以供执行,并且其中包括所述数字密钥的所述计算装置和所述车辆都不与所述车辆管理系统通信以控制对所述车辆的所述访问和/或对所述车辆的所述一个或多个功能性的所述使用,并且嵌入所述车辆管理系统的所述区块链中的所述合约执行VM不执行智能合约。在任选地包括所述第一示例和所述第二示例中的一者或两者的所述系统的第三示例中,由所述车辆管理系统在所述车辆处周期性地更新所述区块链。在任选地包括所述第一示例到所述第三示例中的一者或多者或每一者的所述系统的第四示例中,将所述车辆、所述拥有者和所述操作者的所述数据存储在所述区块链上还包括:将所述车辆的所述数据写入到存储在所述区块链上的所述车辆的非同质化令牌(NFT);将所述拥有者的所述数据写入到存储在所述区块链上的所述拥有者的NFT;以及将所述操作者的所述数据写入到存储在所述区块链上的所述操作者的NFT。在任选地包括所述第一示例到第四示例中的一者或多者或每一者的所述系统的第五示例中,所述车辆的所述NFT包

括以下各项中的至少一者:所述车辆的识别信息、关于指派给所述车辆的数字密钥的信息、所述车辆的一个或多个拥有者的标识信息、所述车辆的一个或多个操作者的标识信息。在任选地包括所述第一示例到第五示例中的一者或多者或每一者的所述系统的第六示例中,所述拥有者的所述NFT包括以下各项中的至少一者:所述拥有者的识别信息、关于指派给所述拥有者的数字密钥的信息、所述拥有者所拥有的一辆或多辆车辆的标识信息、所述拥有者所操作的一辆或多辆车辆的标识信息。在任选地包括所述第一示例到第六示例中的一者或多者或每一者的所述系统的第七示例中,所述操作者的所述NFT包括以下各项中的至少一者:所述操作者的识别信息、关于指派给所述操作者的数字密钥的信息、所述操作者所拥有的一辆或多辆车辆的标识信息、所述操作者所操作的一辆或多辆车辆的标识信息。在任选地包括所述第一示例到所述第七示例中的一者或多者或每一者的所述系统的第八示例中,所述一个或多个智能合约存储在以下各项中的至少一者中:所述操作者的所述NFT、所述车辆的所述NFT和所述拥有者的所述NFT。在任选地包括所述第一示例到所述第八示例中的一者或多者或每一者的所述系统的第九示例中,所述一个或多个智能合约存储在所述操作者的所述NFT和所述车辆的所述NFT中,并且所述智能合约在所述操作者的所述计算装置和所述车辆的ECU中的至少一者处执行,而不在所述车辆管理系统处执行。在任选地包括所述第一示例到所述第九示例中的一者或多者或每一者的所述系统的第十示例中,由所述车辆的所述拥有者经由所述车辆管理系统的图形用户界面(GUI)创建所述数字密钥。在任选地包括所述第一示例到所述第十示例中的一者或多者或每一者的所述系统的第十一示例中,由所述车辆管理系统经由所述数字密钥对所述操作者进行认证,之后授予访问权。

[0111] 本公开还提供对一种用于通过车辆管理系统管理对车辆的使用的方法的支持,所述方法包括:在制造所述车辆时针对所述车辆创建包括所述车辆的数据的非同质化令牌(NFT),并且将所述车辆的所述NFT存储在所述车辆管理系统的区块链上;在购买所述车辆之后,针对所述车辆的拥有者创建包括所述拥有者的数据的NFT,并且将所述拥有者的所述NFT存储在所述区块链上;针对所述车辆的操作者创建包括所述操作者的数据的NFT,所述操作者是由所述车辆的所述拥有者指派,并且将所述操作者的所述NFT存储在所述区块链上;以及响应于由所述拥有者输入到所述车辆管理系统的应用程序中的数据,创建一个或多个智能合约,所述一个或多个智能合约控制对所述车辆的访问和对所述车辆的功能性的使用中的至少一者,所述一个或多个智能合约能够在包括所述区块链的副本的一个或多个计算装置处执行。在所述方法的第一示例中,所述方法还包括:针对所述操作者生成数字密钥,所述数字密钥包括所述一个或多个智能合约,并且将所述数字密钥传输到所述操作者的计算装置;在嵌入安装在所述车辆处的所述区块链的副本中的合约执行虚拟机(VM)处从所述车辆的流服务接收事件数据,所述合约执行VM被配置为基于所述事件数据执行所述一个或多个智能合约;以及响应于由所述合约执行VM执行所述一个或多个智能合约中的智能合约,将所述合约执行VM的输出传输到所述车辆的电子控制单元(ECU)以供执行。在任选地包括所述第一示例的所述方法的第二示例中,所述方法还包括:将用于在所述车辆处实施所述流服务的应用程序包括在所述数字密钥中。在任选地包括所述第一示例和所述第二示例中的一者或两者的所述方法的第三示例中,所述方法还包括:将所述区块链的所述副本安装在所述数字密钥中,所述区块链的所述副本包括所述合约执行VM的版本,所述合约执行VM的所述版本被配置为从在所述车辆处实施的所述流服务接收事件数据,并且使用所述

数字密钥基于所述操作者的计算装置处的接收到的事件数据执行所述一个或多个智能合约。在任选地包括所述第一示例到所述第三示例中的一者或多者或每一者的所述方法的第四示例中,所述方法还包括:使用从所述车辆管理系统接收到的所述区块链的更新后的版本来更新安装在所述数字密钥中的所述区块链的所述版本和安装在所述车辆的所述ECU中的所述区块链的所述版本中的至少一者。

[0112] 本公开还提供对一种用于控制车辆的操作者对所述车辆的访问和对所述车辆的功能性的使用中的至少一者的方法的支持,所述方法包括:在所述车辆处接收由所述车辆的操作者的计算装置传输的数字密钥;执行存储在所述数字密钥中的应用程序以在所述车辆处安装车辆管理系统的区块链的副本和流服务,所述流服务被配置为将所述车辆的实时事件数据流式传输到嵌入所述区块链的所述副本中的合约执行虚拟机(VM);响应于智能合约基于所述实时事件数据在所述合约执行VM处执行,从所述合约执行VM接收用于控制所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的至少一者的指令,所述智能合约存储在所述操作者的非同质化令牌(NFT)和所述车辆的NFT中的至少一者上;以及在所述车辆的电子控制单元(ECU)处执行所述指令。在所述方法的第一示例中,包括所述合约执行VM的所述区块链的副本安装在所述数字密钥处,并且所述智能合约在存储所述数字密钥的所述操作者的所述计算装置处执行。在任选地包括所述第一示例的所述方法的第二示例中,在其中所述智能合约基于实时事件数据执行的第一状况下,导致所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的至少一者被限制或禁用,并且在其中所述智能合约不基于实时事件数据执行的第二状况下,所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的所述至少一者不被限制或禁用。

[0113] 本公开还提供对一种用于在去中心化对等(P2P)网络上的分布式账本中跟踪与实物资产相关联的至少一个非同质化令牌(NFT)的方法的支持,所述方法包括:将第一方对所述实物资产的所有权的记录存储在所述分布式账本的第一条目中,所述第一条目包括所述NFT;将所述第一方向第二方出租所述实物资产的记录存储在所述分布式账本的第二条目中,所述第二条目包括所述NFT;将使用所述实物资产的权限的记录存储在所述分布式账本的第三条目中,所述第三条目包括所述NFT,所述权限被指派给所述实物资产的操作者。在所述方法的第一示例中,所述实物资产是车辆。在任选地包括所述第一示例的所述方法的第二示例中,所述权限是访问所述车辆的权限。在任选地包括所述第一示例和所述第二示例中的一者或两者的所述方法的第三示例中,所述权限是使用所述车辆的功能性的权限。在任选地包括所述第一示例到所述第三示例中的一者或多者或每一者的所述方法的第四示例中,所述分布式账本中的与所述实物资产相关联的所述至少一个NFT包括以下各项中的至少一者:所述车辆的第一NFT,所述第一NFT包括所述车辆的识别信息和适用于所述车辆的一个或多个智能合约;所述车辆的拥有者的第二NFT,所述第二NFT包括所述拥有者的识别信息和适用于所述拥有者的关于所述车辆的一个或多个智能合约;以及所述车辆的操作者的第三NFT,所述第三NFT包括所述操作者的识别信息和适用于所述操作者的关于所述车辆的一个或多个智能合约。在任选地包括所述第一示例到第四示例中的一者或多者或每一者的所述方法的第五示例中,所述方法还包括:响应于满足与车辆相关联的智能合约的条件,所述智能合约的由此的执行生成指令,所述指令在被传输到所述车辆时禁用所述车

辆的功能性。

[0114] 应注意,本文所包括的示例控制和估计程序可与各种发动机和/或车辆系统配置一起使用。本文公开的控制方法和程序可作为可执行指令存储在非暂时性存储器中,并且可以由包括控制器的控制系统结合各种传感器、致动器和其他发动机硬件来实施。本文所述的具体程序可表示任何数量的处理策略(诸如事件驱动的、中断驱动的、多任务、多线程等)中的一个或多个。因而,所示出的各种动作、操作和/或功能可按示出的顺序执行、并行执行,或者在一些情况下被省略。同样,处理顺序不一定是实现本文描述的示例性实施例的特征和优点所必需的,而是为了便于说明和描述而提供。可以根据所使用的特定策略而重复地执行所示出的动作、操作和/或功能中的一者或多者。此外,所描述的动作、操作和/或功能可图形地表示将被编程到发动机控制系统中的计算机可读存储介质的非暂时性存储器中的代码,其中所描述的动作通过结合电子控制器在包括各种发动机硬件部件的系统中执行指令来实施。

[0115] 应理解,本文公开的配置和程序本质上是示例性的,并且这些具体实施例不应被视为具有限制意义,因为许多变型是可能的。例如,以上技术可应用于V-6、I-4、I-6、V-12、对置4缸以及其他发动机类型。此外,除非明确地相反指出,否则术语“第一”、“第二”、“第三”等不意图表示任何顺序、位置、数量或重要性,而是仅用作标记以区分一个要素与另一个要素。本公开的主题包括本文公开的各种系统和配置以及其他特征、功能和/或性质的所有新颖且非显而易见的组合和子组合。

[0116] 如本文所使用,除非另有指定,否则术语“约”被解释为表示所述范围的±5%。

[0117] 所附权利要求特别地指出被视为新颖且非显而易见的某些组合和子组合。这些权利要求可指“一个”要素或“第一”要素或其等同物。此类权利要求应理解为包括一个或多个此类要素的并入,既不要求也不排除两个或更多个此类要素。所公开的特征、功能、要素和/或性质的其他组合和子组合可通过修正本权利要求或通过在此申请或相关申请中提出新的权利要求来要求保护。此类权利要求,无论与原始权利要求相比在范围上更广、更窄、等同或不同,也都被视为包括在本公开的主题内。

[0118] 根据本发明,提供一种车辆管理系统,所述车辆管理系统具有:区块链;流服务,所述流服务被配置为向嵌入所述区块链中的合约执行虚拟机(VM)实时提供事件数据;以及非暂时性存储器,所述非暂时性存储器存储指令,所述指令在由所述车辆管理系统的处理器执行时致使所述车辆管理系统进行以下操作:基于来自车辆的拥有者的输入针对所述车辆管理系统的车辆的操作者生成数字密钥,所述数字密钥基于一个或多个智能合约来控制所述操作者对所述车辆的访问和对所述车辆的一个或多个功能性的使用;将所述车辆、所述拥有者和所述操作者的数据存储在所述区块链中,所述数据包括所述一个或多个智能合约;以及将所述数字密钥无线地传输到所述操作者的计算装置。

[0119] 根据一个实施例,经由数字密钥控制对车辆的访问和/或对车辆的一个或多个功能性的使用还包括:将用于实施流服务的版本的计算机应用程序包括在数字密钥中;响应于在车辆处执行所述应用程序,经由所述流服务的所述版本在所述车辆管理系统处实时地接收所述车辆的事件数据;将所述车辆的所述事件数据转发到嵌入所述区块链中的合约执行VM;响应于所述合约执行VM执行所述一个或多个智能合约中的至少一个智能合约,从所述合约执行VM接收控制对车辆的访问和/或对车辆的一个或多个功能性的使用的指令;以

及将所述接收到的指令发送到所述车辆以由所述车辆的电子控制单元(ECU)执行。

[0120] 根据一个实施例,经由数字密钥控制对车辆的访问和/或对车辆的一个或多个功能性的使用还包括:将区块链的副本包括在数字密钥中,并且包括在第一次使用所述数字密钥时将所述副本安装在所述车辆处的指令;将用于在所述车辆处实施所述流服务的版本的计算机应用程序包括在所述数字密钥中,所述版本向嵌入所述车辆处的所述区块链的所述副本中的合约执行VM提供实时事件数据,所述合约执行VM被配置为基于所述实时事件数据自动执行存储在所述区块链的所述副本中的一个或多个智能合约,所述一个或多个智能合约在被执行时向所述车辆的ECU提供控制对所述车辆的所述访问和/或对所述车辆的所述一个或多个功能性的所述使用的代码以供执行;并且其中包括所述数字密钥的操作者的所述计算装置和所述车辆都不与所述车辆管理系统通信以控制对所述车辆的所述访问和/或对所述车辆的所述一个或多个功能性的所述使用,并且嵌入所述车辆管理系统的所述区块链中的所述合约执行VM不执行智能合约。

[0121] 根据一个实施例,由所述车辆管理系统在所述车辆处周期性地更新所述区块链。

[0122] 根据一个实施例,将所述车辆、所述拥有者和所述操作者的所述数据存储在所述区块链上还包括:将所述车辆的所述数据写入到存储在所述区块链上的所述车辆的非同质化令牌(NFT);将所述拥有者的所述数据写入到存储在所述区块链上的所述拥有者的NFT;以及将所述操作者的所述数据写入到存储在所述区块链上的所述操作者的NFT。

[0123] 根据一个实施例,所述车辆的所述NFT包括以下各项中的至少一者:所述车辆的识别信息;关于指派给所述车辆的数字密钥的信息;所述车辆的一个或多个拥有者的标识信息;所述车辆的一个或多个操作者的标识信息。

[0124] 根据一个实施例,所述拥有者的所述NFT包括以下各项中的至少一者:所述拥有者的识别信息;关于指派给所述拥有者的数字密钥的信息;所述拥有者所拥有的一辆或多辆车辆的标识信息;所述拥有者所操作的一辆或多辆车辆的标识信息。

[0125] 根据一个实施例,所述操作者的所述NFT包括以下各项中的至少一者:所述操作者的识别信息;关于指派给所述操作者的数字密钥的信息;所述操作者所拥有的一辆或多辆车辆的标识信息;所述操作者所操作的一辆或多辆车辆的标识信息。

[0126] 根据一个实施例,所述一个或多个智能合约存储在以下各项中的至少一者中:所述操作者的所述NFT、所述车辆的所述NFT和所述拥有者的所述NFT。

[0127] 根据一个实施例,所述一个或多个智能合约存储在所述操作者的所述NFT和所述车辆的所述NFT中,并且所述一个或多个智能合约在所述操作者的所述计算装置和所述车辆的ECU中的至少一者处执行,而不在所述车辆管理系统处执行。

[0128] 根据一个实施例,由所述车辆的所述拥有者经由所述车辆管理系统的图形用户界面(GUI)创建所述数字密钥。

[0129] 根据一个实施例,由所述车辆管理系统经由所述数字密钥对所述操作者进行认证,之后授予访问权。

[0130] 根据本发明,一种用于通过车辆管理系统管理对车辆的使用的方法,包括:在制造所述车辆时针对所述车辆创建包括所述车辆的数据的非同质化令牌(NFT),并且将所述车辆的所述NFT存储在所述车辆管理系统的区块链上;在购买所述车辆之后,针对所述车辆的拥有者创建包括所述拥有者的数据的NFT,并且将所述拥有者的所述NFT存储在所述区块链

上;针对所述车辆的操作者创建包括所述操作者的数据的NFT,所述操作者是由所述车辆的所述拥有者指派,并且将所述操作者的所述NFT存储在所述区块链上;以及响应于由所述拥有者输入到所述车辆管理系统的应用程序中的数据,创建一个或多个智能合约,所述一个或多个智能合约控制对所述车辆的访问和对所述车辆的功能性的使用中的至少一者,所述一个或多个智能合约能够在包括所述区块链的副本的一个或多个计算装置处执行。

[0131] 在本发明的一个方面,所述方法包括:针对所述操作者生成数字密钥,所述数字密钥包括所述一个或多个智能合约,并且将所述数字密钥传输到所述操作者的计算装置;在嵌入安装在所述车辆处的所述区块链的副本中的合约执行虚拟机(VM)处从所述车辆的流服务接收事件数据,所述合约执行VM被配置为基于所述事件数据执行所述一个或多个智能合约;以及响应于由所述合约执行VM执行所述一个或多个智能合约中的智能合约,将所述合约执行VM的输出传输到所述车辆的电子控制单元(ECU)以供执行。

[0132] 在本发明的一个方面,所述方法包括:将用于在所述车辆处实施所述流服务的应用程序包括在所述数字密钥中。

[0133] 在本发明的一个方面,所述方法包括:将所述区块链的所述副本安装在所述数字密钥中,所述区块链的所述副本包括所述合约执行VM的版本,所述合约执行VM的所述版本被配置为从在所述车辆处实施的所述流服务接收事件数据,并且使用所述数字密钥基于所述操作者的计算装置处的接收到的事件数据执行所述一个或多个智能合约。

[0134] 在本发明的一个方面,所述方法包括:使用从所述车辆管理系统接收到的所述区块链的更新后的版本来更新安装在所述数字密钥中的所述区块链的所述版本和安装在所述车辆的所述ECU中的所述区块链的所述版本中的至少一者。

[0135] 根据本发明,一种用于控制车辆的操作者对所述车辆的访问和对所述车辆的功能性的使用中的至少一者的方法,包括:在所述车辆处接收由所述车辆的操作者的计算装置传输的数字密钥;执行存储在所述数字密钥中的应用程序以在所述车辆处安装车辆管理系统的区块链的副本和流服务,所述流服务被配置为将所述车辆的实时事件数据流式传输到嵌入所述区块链的所述副本中的合约执行虚拟机(VM);响应于智能合约基于所述实时事件数据在所述合约执行VM处执行,从所述合约执行VM接收用于控制所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的至少一者的指令,所述智能合约存储在所述操作者的非同质化令牌(NFT)和所述车辆的NFT中的至少一者上;以及在所述车辆的电子控制单元(ECU)处执行所述指令。

[0136] 在本发明的一个方面,包括所述合约执行VM的所述区块链的副本安装在所述数字密钥处;并且所述智能合约在存储所述数字密钥的所述操作者的所述计算装置处执行。

[0137] 在本发明的一个方面,在其中所述智能合约基于实时事件数据执行的第一状况下,导致所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的至少一者被限制或禁用;并且在其中所述智能合约不基于实时事件数据执行的第二状况下,所述操作者对所述车辆的所述访问和对所述车辆的所述功能性的所述使用中的所述至少一者不被限制或禁用。

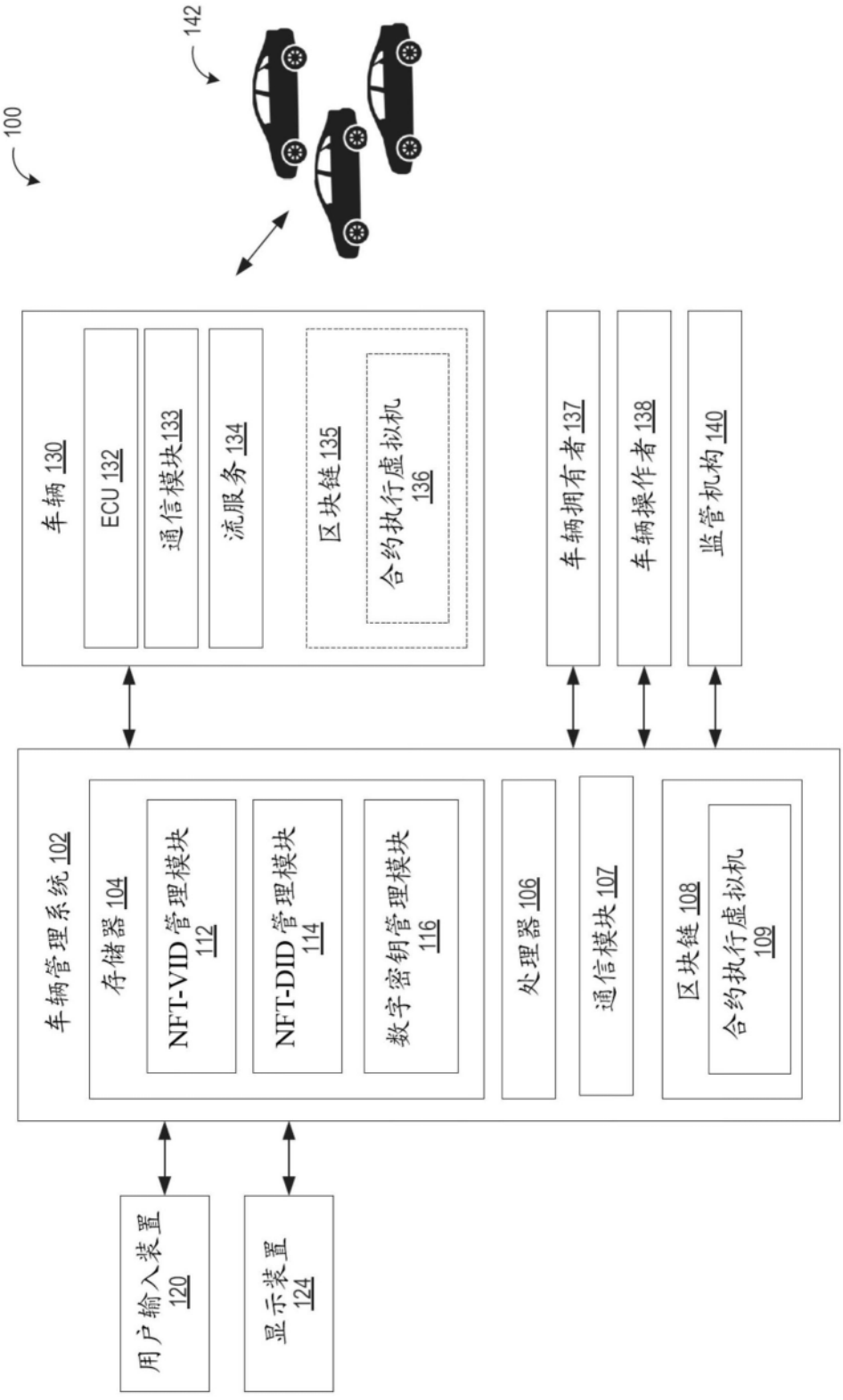

100
142
车辆 130
ECU 132
通信模块133
流服务 134
区块链 135
合约执行虚拟机 136
车辆拥有者 137
车辆操作者 138
监管机构 140
车辆管理系统 102
存储器 104
NFT-VID 管理模块 112
NFT-DID 管理模块 114
数字密钥管理模块 116
处理器 106
通信模块 107
区块链 108
合约执行虚拟机 109
用户输入装置 120
显示装置 124

图1

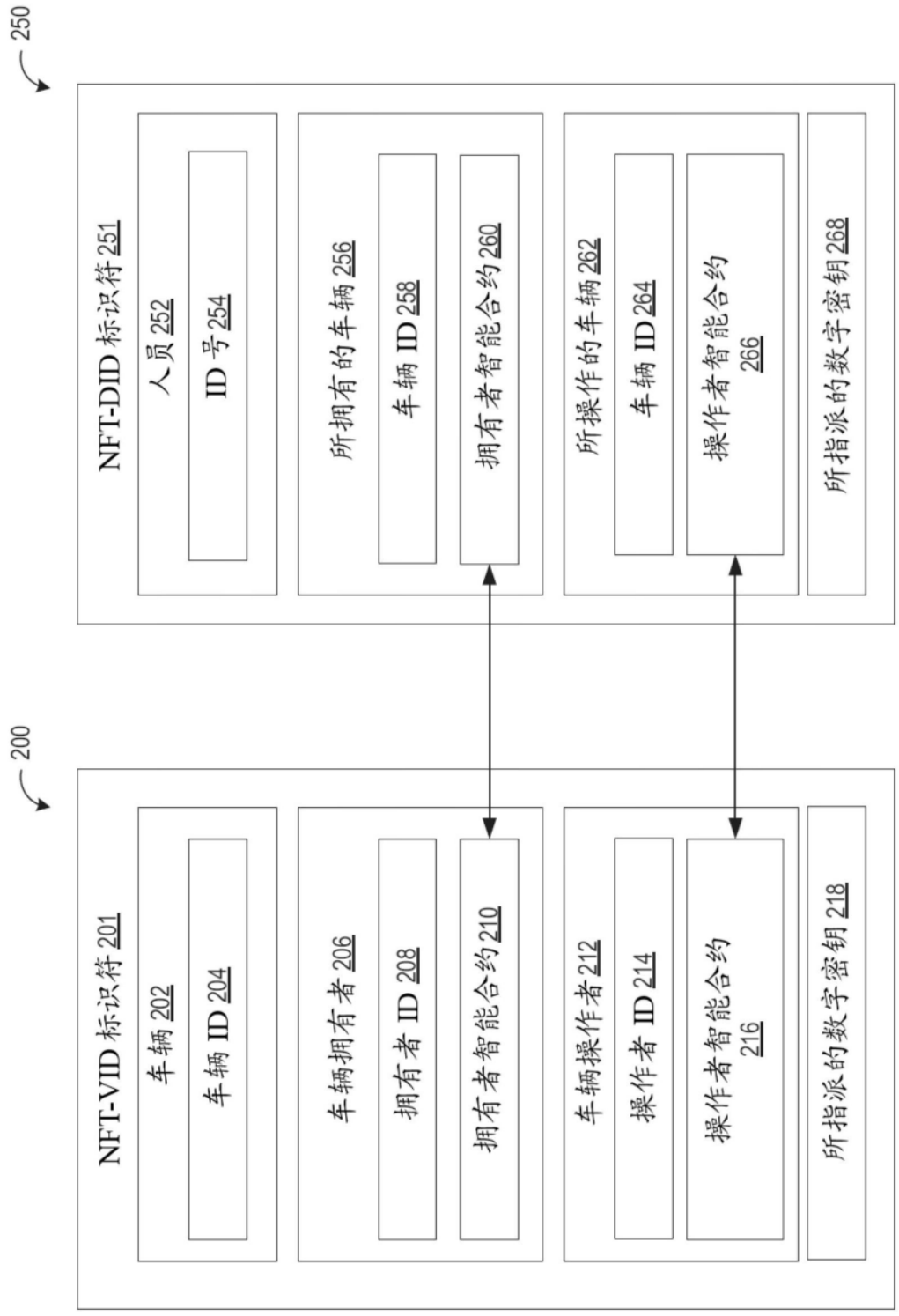

250
NFT-DID 标识符 251
人员 252
ID 号 254
所拥有的车辆 256
车辆 ID 258
拥有者智能合约 260
所操作的车辆 262
车辆 ID 264
操作者智能合约 266
所指派的数字密钥 268
200
NFT-VID 标识符 201
车辆 202
车辆 ID 204
车辆拥有者 206
拥有者 ID 208
拥有者智能合约 210
车辆操作者 212
操作者 ID 214
操作者智能合约 216
所指派的数字密钥 218

图 2A

图 2B

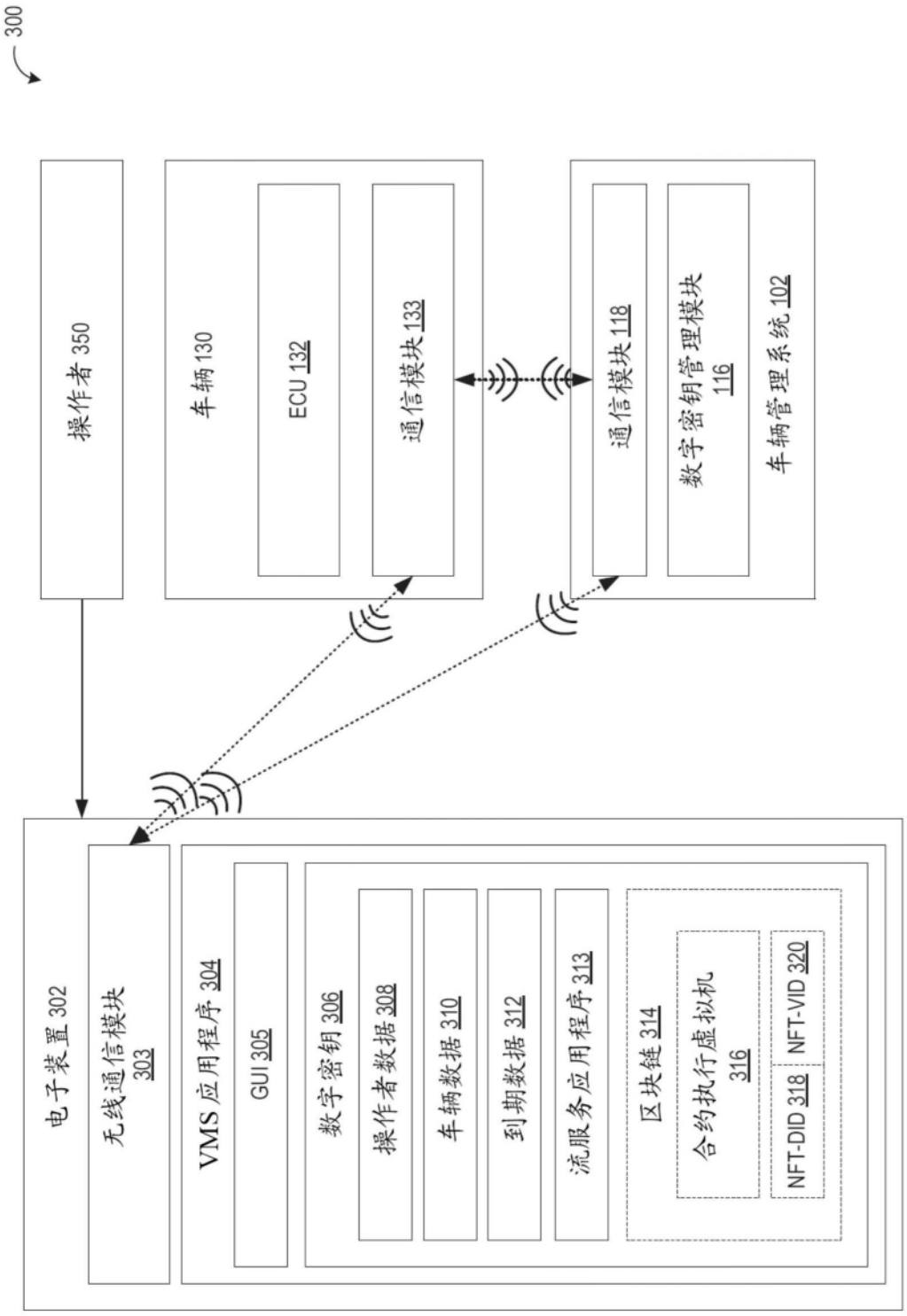

300
操作者 350
车辆 130
ECU 132
通信模块 133
通信模块 118
数字密钥管理模块 116
车辆管理系统 102
电子装置 302
无线通信模块 303
VMS 应用程序 304
GUI 305
数字密钥 306
操作者数据 308
车辆数据 310
到期数据 312
流服务应用程序 313
区块链 314
合约执行虚拟机 316
NFT-DID 318
NFT-VID 320

图3

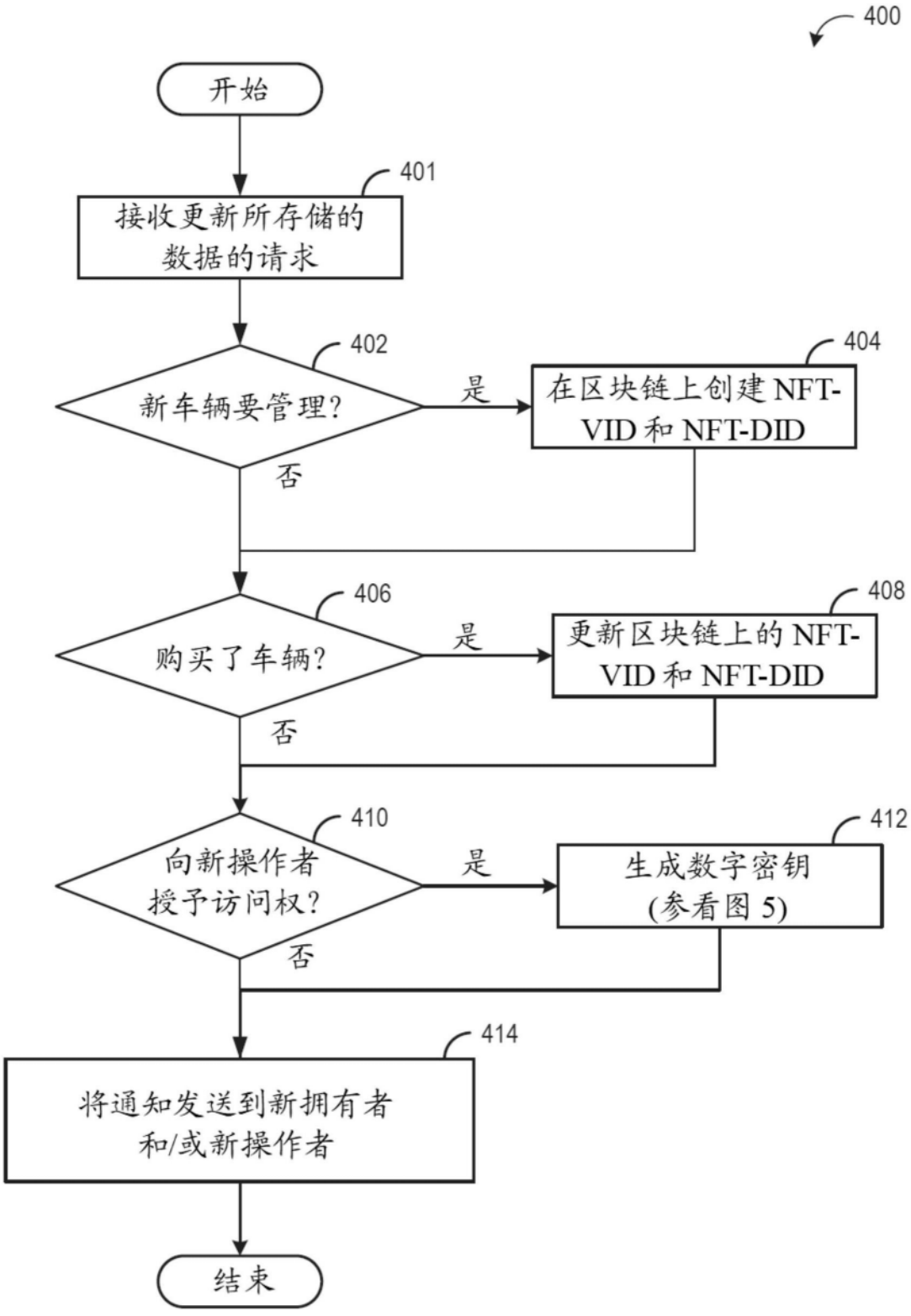

400
开始
401
接收更新所存储的数据的请求
402
新车辆要管理?
是
404
在区块链上创建 NFT-VID 和 NFT-DID
否
406
购买了车辆?
是
408
更新区块链上的 NFT-VID 和 NFT-DID
否
410
向新操作者授予访问权?
是
412
生成数字密钥(参看图 5)
否
414
将通知发送到新拥有者和/或新操作者
结束

图4

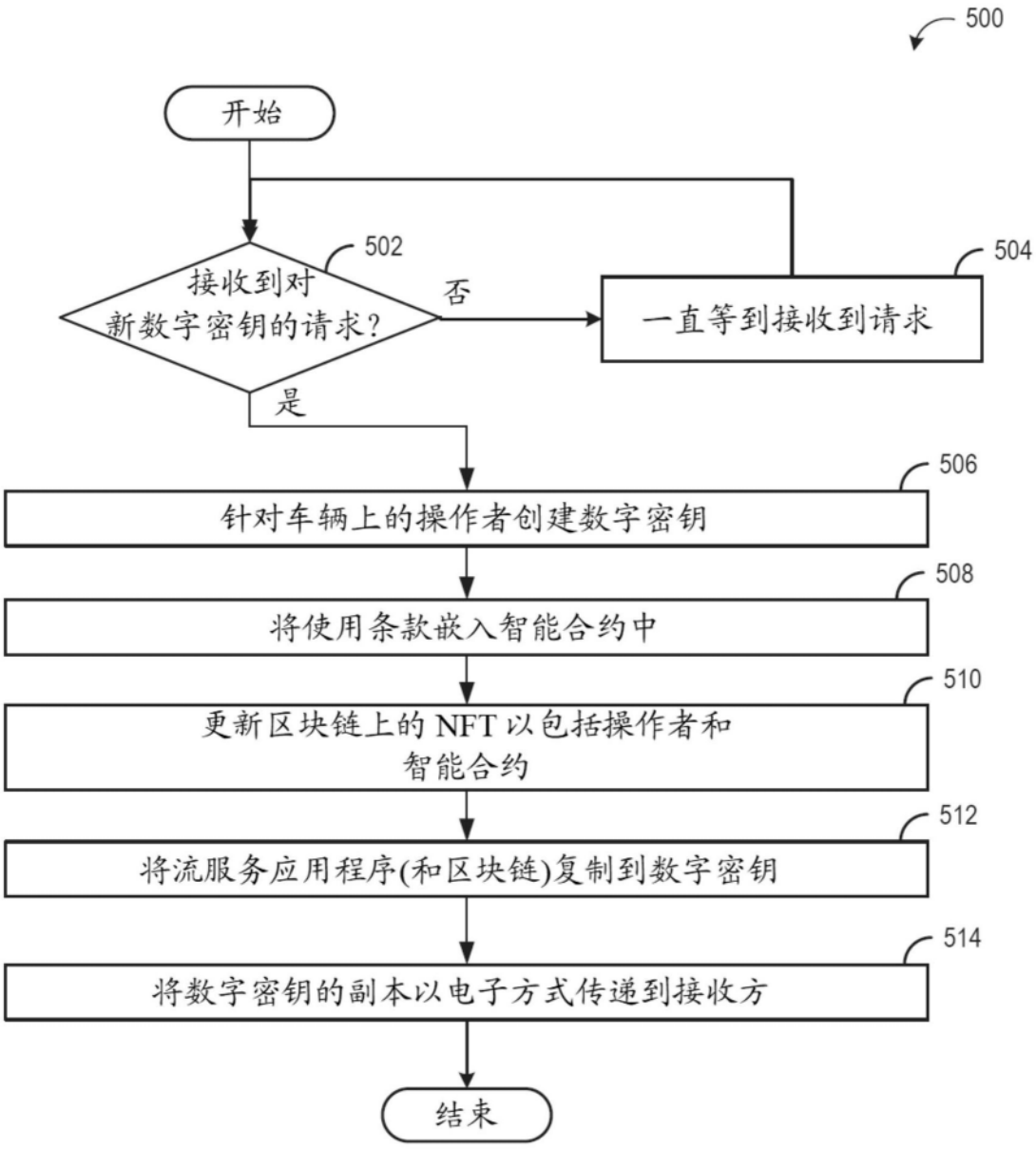

500
开始
502
接收到对新数字密钥的请求?
否
504
一直等到接收到请求
是
506
针对车辆上的操作者创建数字密钥
508
将使用条款嵌入智能合约中
510
更新区块链上的 NFT 以包括操作者和智能合约
512
将流服务应用程序(和区块链)复制到数字密钥
514
将数字密钥的副本以电子方式传递到接收方
结束

图5

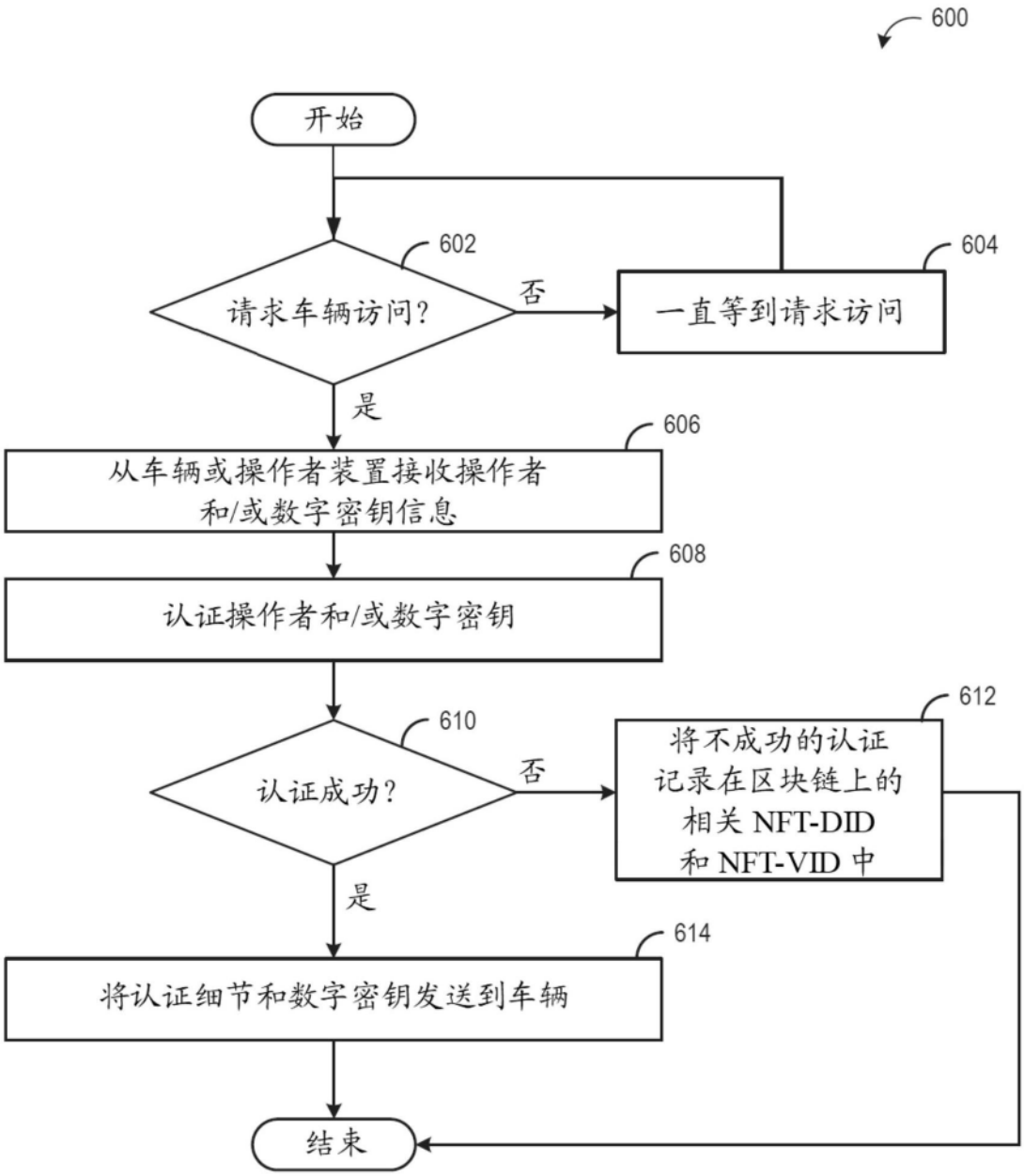

600
开始
602
请求车辆访问?
否
604
一直等到请求访问
是
606
从车辆或操作者装置接收操作者和/或数字密钥信息
608
认证操作者和/或数字密钥
610
认证成功?
否
612
将不成功的认证记录在区块链上的相关 NFT-DID 和 NFT-VID 中
是
614
将认证细节和数字密钥发送到车辆
结束

图6

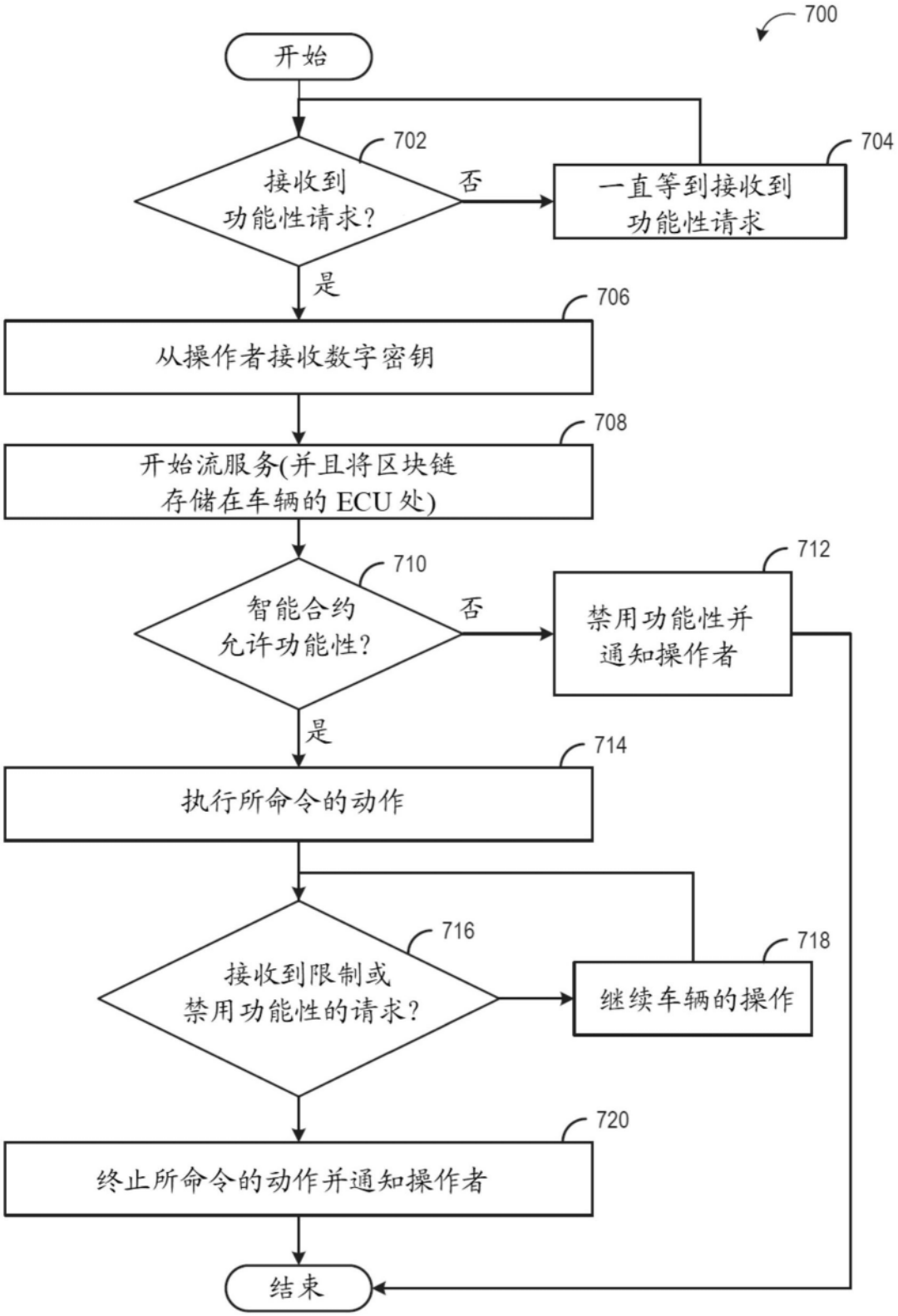

700
开始
702
接收到
功能性请求?
否
704
一直等到接收到
功能性请求
是
706
从操作者接收数字密钥
708
开始流服务(并且将区块链
存储在车辆的 ECU 处)
710
智能合约
允许功能性?
否
712
禁用功能性并
通知操作者
是
714
执行所命令的动作
716
接收到限制或
禁用功能性的请求?
718
继续车辆的操作
720
终止所命令的动作并通知操作者
结束

图7