(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 112074856 B
(45)授权公告日 2021.10.08

(21)申请号 202080002570.8

(22)申请日 2020.03.06

(65)同一申请的已公布的文献号
申请公布号 CN 112074856 A

(43)申请公布日 2020.12.11

(30)优先权数据
16/294,745 2019.03.06 US
16/579,697 2019.09.23 US
16/806,646 2020.03.02 US

(85)PCT国际申请进入国家阶段日
2020.10.30

(86)PCT国际申请的申请数据
PCT/US2020/021587 2020.03.06

(87)PCT国际申请的公布数据
WO2020/181271 EN 2020.09.10

(73)专利权人 阿梅里科普投资有限责任公司
地址 美国科罗拉多州

(72)发明人 J·西蒙斯

(74)专利代理机构 北京汇知杰知识产权代理有限公司 11587
代理人 李洁 董江虹

(51)Int.Cl.
G06Q 20/06(2006.01)
G06Q 20/38(2006.01)
G06Q 20/40(2006.01)
G06Q 30/06(2006.01)
G06Q 50/30(2006.01)
H04W 4/33(2006.01)
H04W 4/35(2006.01) (续)

(56)对比文件
CN 108922228 A,2018.11.30
CN 108563788 A,2018.09.21
CN 108922228 A,2018.11.30
CN 108563788 A,2018.09.21
CN 109299958 A,2019.02.01
US 2019036919 A1,2019.01.31
US 2018167198 A1,2018.06.14
US 2017244721 A1,2017.08.24
WO 2018163044 A1,2018.09.13
曹迪迪、陈伟.基于智能合约的以太坊可信存证机制.《计算机应用》.2018,第39卷(第04期),第1073-1080页.

审查员 鹿天然

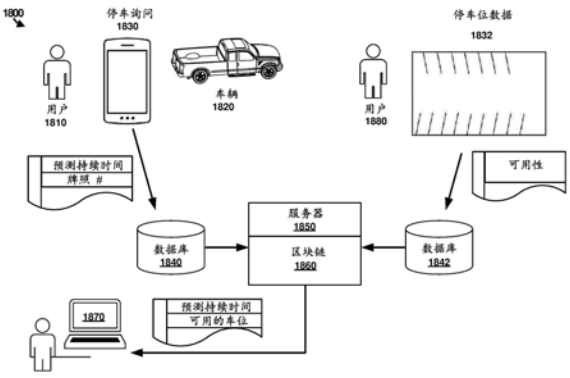
权利要求书3页 说明书40页 附图28页

(54)发明名称

基于区块链的商业库存系统和方法

(57)摘要

本文公开了用以生成区块链交易的定制视图的系统、方法和软件。在分布式节点网络中维护由多个用户从用户设备请求的区块条目的区块链。所述区块条目各自包括多个数据部分,所述多个数据部分各自与一个访问级别相关联。接收查看区块条目的一个或多个数据部分的请求,所述请求包括与至少一个访问级别相关联的访问代码。用区块条目的所述区块链评估所述请求中的所述访问代码以识别与所述访问级别相关联的一个或多个数据部分。生成包括与所述访问级别相关联的所述一个或多个数据部分的所述区块条目的定制视图。因此,在包括停车、酒店和自动驾驶车辆车队的行业中提供增强的操作效率和客户便利性。



CN 112074856 B

[转续页]

[接上页]

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/06(2006.01)

1.一种用于商业库存的跟踪、管理和实现的系统,包括:

节点网络,被可通信地耦合到分布式网络中的端点,

其中所述节点网络用来自一个或多个端点的条目维护分布式账本,

其中所述条目包括:来自客户的与库存提供者提供的商业库存相关的条目,以及来自该库存提供者的关于所述库存的可用性状态的条目,并且

其中存储在所述分布式账本中的一个或多个条目内的节段与核阅所述条目所需的至少一个访问级别相关联;

通信部件,用以接收查看存储在所述分布式账本中的所述一个或多个条目的至少一部分的请求,

其中所述请求包括与所述至少一个访问级别相关联的访问代码;

访问控制层,用以评估经由所述通信部件接收的所述请求中的所述访问代码,并且用以识别存储在所述分布式账本上的所述一个或多个条目内的所述节段,所述节段是通过所述请求中提供的所述至少一个访问级别可访问的;以及

访问平台或分散式应用程序,用以生成在所述分布式账本中维护的所述一个或多个条目内的由所述访问控制层识别为可访问的所述节段的定制视图。

2.根据权利要求1所述的系统,还包括抄本,所述抄本被配置为使发出查看所述一个或多个条目中的至少一部分的请求的用户的识别信息模糊。

3.根据权利要求1所述的系统,还包括人工智能引擎,用以核阅所述分布式账本内的条目并且指派核阅所述条目中的每个所需的访问级别。

4.根据权利要求3所述的系统,其中所述人工智能引擎将所述条目中的每个内的数据分类为一个或多个类别。

5.根据权利要求4所述的系统,其中所述访问控制层还为由所述人工智能引擎分类的数据的所述一个或多个类别中的每个设置不同的加密级别。

6.根据权利要求4所述的系统,其中所述一个或多个类别包括电子邮件地址、账户号码、余额、交易的各方、邮寄地址、车辆识别号码、牌照号码、生物统计、驾驶执照号码、照片或社会保障号码。

7.根据权利要求4所述的系统,其中所述商业库存包括停车设施中的停车位。

8.根据权利要求4所述的系统,其中所述商业库存包括指定区域中的停车位,并且其中所述指定区域包括城市的地区、街区、停车场和车库中的一个或多个。

9.根据权利要求1所述的系统,其中查看存储在所述分布式账本中的一个或多个条目的至少一部分的请求是采购订单、库存跟踪请求、租赁或出租请求、预留请求、财务审查请求、火器销售验证请求、零售销售请求或药物销售请求的一部分。

10.根据权利要求1所述的系统,其中与所述一个或多个条目内的节段相关联的所述至少一个访问级别包括私人访问级别、许可访问级别或公共访问级别中的至少一个。

11.一种用于生成用于库存跟踪、管理和实现的区块链交易的定制视图的方法,包括:

接收查看在区块链中维护的区块条目的一个或多个数据部分的请求,

其中所述区块条目包括:来自客户的与库存提供者提供的库存相关的条目,以及来自该库存提供者的关于所述库存的可用性状态的条目;

确定与和所述请求相关联的至少一个访问级别相关联的访问代码;

用区块条目的所述区块链评估所述请求中的所述访问代码以识别与所述访问级别相关联的一个或多个数据部分;以及

生成包括所识别的与所述访问级别相关联的所述一个或多个数据部分中的任何一个的所述区块条目中的至少一个的定制视图。

12.根据权利要求11所述的方法,其中用区块条目的所述区块链评估所述请求中的所述访问代码包括处理加密代码以验证查看与所述访问级别相关联的所述一个或多个数据部分的访问。

13.根据权利要求11所述的方法,还包括移除发出查看所述区块条目的一个或多个数据部分的请求的用户的识别信息或使所述识别信息模糊。

14.根据权利要求11所述的方法,还包括:

接收所述一个或多个数据部分的来自一个或多个端点的数据;

使用人工智能引擎将来自所述一个或多个端点的数据分成节段;以及

自动地为所述数据的每个节段指派至少一个访问级别。

15.根据权利要求14所述的方法,其中所述数据包括受限数据,并且自动地为所述数据的每个节段指派至少一个访问级别包括为所述受限数据指派安全调查级别。

16.根据权利要求15所述的方法,还包括:

监视所述受限数据的受限状态;以及

在确定所述受限数据的受限状态已经改变后,更新所述至少一个访问级别。

17.根据权利要求14所述的方法,其中所述库存包括停车设施中的停车位,并且其中所述一个或多个端点包括用于监视所述停车位的可用性状态的传感器。

18.根据权利要求11所述的方法,其中所述区块条目还包括关于私人交易的交易细节,并且所述至少一个访问级别最初被设置为私人的,并且所述方法还包括:

监视所述私人交易的状态;以及

在确定所述私人交易已经变成公共的后,将所述至少一个访问级别更新为公共的,允许用公共访问代码查看所述私人交易的公共部分。

19.根据权利要求11所述的方法,其中所述请求是采购订单、库存跟踪请求、租赁或出租请求、预留请求、财务审查请求、火器销售验证请求、零售销售请求或药物销售请求的一部分。

20.根据权利要求11所述的方法,其中与所述区块条目的所述一个或多个数据部分相关联的所述访问级别包括私人访问级别、许可访问级别和公共访问级别中的至少一个。

21.根据权利要求11所述的方法,其中与所述一个或多个数据部分相关联的所述访问级别包括安全调查级别。

22.根据权利要求21所述的方法,其中所述区块条目包括基于所述安全调查级别的编辑映射,并且其中生成所述区块条目中的至少一个的所述定制视图包括应用所述编辑映射来使所述区块条目的一部分所述一个或多个数据部分模糊。

23.根据权利要求11所述的方法,其中所述区块条目包括基于所述访问级别的多个编辑映射。

24.一种用于停车设施中的停车位交易的跟踪、管理和实现的系统,包括:

用于维护由多个用户从分布式节点网络中的用户设备请求的区块条目的区块链的装

置，

其中所述多个用户包括:所述停车设施的客户和所述停车设施的运营商，

其中所述区块条目包括:来自所述客户的与所述停车设施的该运营商提供的至少一个停车位相关的条目,以及来自所述停车设施的该运营商的关于所述至少一个停车位的可用性状态的条目,并且

其中所述区块条目各自包括多个数据部分,所述多个数据部分各自与一个访问级别相关联；

用于接收查看区块条目的一个或多个数据部分的请求的装置，

其中所述请求包括与至少一个访问级别相关联的访问代码；

用于用区块条目的所述区块链评估所述请求中的所述访问代码以识别与所述访问级别相关联的一个或多个数据部分的装置;以及

用于生成包括被识别为与所述访问级别相关联的所述一个或多个数据部分的所述区块条目的定制视图的装置。

25.根据权利要求24所述的系统,其中所述定制视图包括对数据部分进行编辑的应用程序。

26.一种用于生成用于停车设施交易的区块链数据的定制视图的方法,所述方法包括：

接收查看在区块链中维护的区块条目的一个或多个数据部分的请求，

其中所述区块条目的所述一个或多个数据部分包括受限信息;并且

其中所述区块条目的所述一个或多个数据部分各自与一个访问级别相关联,所述访问级别被指派给:所述停车设施的客户,以及与所述停车设施的运营商相关联的用户；

用区块条目的所述区块链评估所述请求中的访问代码以识别与所述访问级别相关联的一个或多个数据部分;以及

生成包括被识别为与所述访问级别相关联的所述一个或多个数据部分中的任何一个的所述区块条目的定制视图,同时对未经所述访问代码授权的所述受限信息中的任何一个应用编辑。

27.根据权利要求26所述的方法,其中与所述一个或多个数据部分相关联的所述访问级别包括安全调查级别。

28.根据权利要求27所述的方法,其中所述区块条目包括基于所述安全调查级别的编辑映射。

基于区块链的商业库存系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请是2020年3月2日提交的题为“Customized View Of Restricted Information Recorded Into A Blockchain”的第16/806,646号美国专利申请的部分继续;该美国专利申请是2019年9月23日提交的题为“Customized View Of Restricted Information Recorded Into A Blockchain”的第16/579,697号美国专利申请的继续;该美国专利申请是2019年3月6日提交的题为“Customized View Of Restricted Information Recorded Into A Blockchain”的第16/294,745号美国专利申请的继续;该美国专利申请要求享有2018年3月6日提交的题为“Customized View of Restricted Transactions Recorded into a Blockchain”的第62/639,393号美国临时专利申请和2018年7月23日提交的题为“Customized View of Restricted Information Recorded into a Blockchain”的第62/701,947号美国临时专利申请的优先权,出于所有的目的,所述美国临时专利申请中的每个的全部内容通过引用并入本文。

技术领域

[0003] 本技术的各实施方案总体上涉及库存交易(inventory transaction)系统。更具体地,一些实施方案涉及基于区块链的停车系统和其他库存跟踪系统。

背景技术

[0004] 区块链允许用户网络制作数据的数字账本(ledger)并且在该网络中的其他用户之间共享该数据。与先前的数据库结构不同,区块链数据库由散布在大型分布式网络上的众多独立节点维护。当交易被记录到区块链数据库中时,由于数据被存储在分布式网络中的不止一个节点中,因此改变该数据或从数据库移除该数据即使不是不可能的也是非常困难的。因此,数据由多个用户添加到区块链数据库中,并且改变记录的数据将要求这些用户中的每个(或大多数用户)同意改变。对添加、校订数据以及从区块链数据库移除数据的控制的此分布在网络中的用户之间建立信任,尤其是当用户彼此不熟悉时。

发明内容

[0005] 本技术的各实施方案总体上涉及库存交易系统。更具体地,一些实施方案涉及基于区块链的停车系统和其他库存跟踪系统。这些系统提供了本文所公开的用以生成区块链交易的定制视图的增强型系统、方法和软件应用程序。在一些实施方案中,在分布式节点网络中维护由多个用户从用户设备请求的区块条目的区块链。所述区块条目各自包括多个数据部分,所述多个数据部分各自与一个访问级别相关联。接收查看一个区块条目的一个或多个数据部分的请求,所述请求包括与至少一个访问级别相关联的访问代码。用区块条目的所述区块链评估所述请求中的所述访问代码以识别与所述访问级别相关联的一个或多个数据部分。生成包括与所述访问级别相关联的所述一个或多个数据部分的所述区块条目的定制视图。

[0006] 一些实施方案提供了一种用于停车设施中的停车位交易的跟踪、管理和实现的系统。所述系统可以维护由多个用户从分布式节点网络中的用户设备请求的区块条目的区块链(或分布式账本)。用户的示例可以包括所述停车设施的客户和/或所述停车设施的运营商。所述区块条目可以包括来自所述客户的与所述停车设施的该运营商提供的至少一个停车位相关的条目,以及来自所述停车设施的该运营商的关于所述至少一个停车位的可用性状态的条目。所述区块条目可以各自包括多个数据部分,所述多个数据部分各自与一个访问级别相关联。所述系统可以接收查看区块条目的一个或多个数据部分的请求。在一些实施方案中,所述请求可以包括与至少一个访问级别相关联的访问代码。然后,所述系统可以用区块条目的所述区块链来评估所述请求中的所述访问代码,以识别与所述访问级别相关联的一个或多个数据部分。可以生成包括与所述访问级别相关联的所述一个或多个数据部分的所述区块条目的定制视图。

[0007] 在一些实施方案中,可以生成用于停车设施交易的区块链数据的定制视图。所述方法可以包括接收查看在区块链中维护的区块条目的一个或多个数据部分的请求,其中所述区块条目的所述一个或多个数据部分包括受限信息。所述区块条目的所述一个或多个数据部分各自可以与一个访问级别相关联,所述访问级别被指派给:所述停车设施的客户,以及与所述停车设施的运营商相关联的用户。所述方法可以包括用区块条目的所述区块链评估所述请求中的访问代码以识别与所述访问级别相关联的一个或多个数据部分。所述方法可以包括生成包括与所述访问级别相关联的所述一个或多个数据部分中的任何一个的所述区块条目的定制视图,同时对未经所述访问代码授权的所述受限信息中的任何一个应用编辑。

[0008] 作为一个示例,在停车行业中,诸如车辆识别号码(VIN)、牌照号码、访问卡号码、订阅计划细节、使用历史和偏好、地址、已知的电子钱包、移动电话、电子钥匙、数字指纹、使用的信用/借记卡、使用的加密货币钱包等的客户和其车辆的识别信息都可以与其他客户信息一起保持在区块链上。客户将不希望任何此信息以公共格式可查看,并且公共访问可能导致停车设施的运营商和所有者承担法律责任。各实施方案使用各种加密和散列技术来将数据安全地存储在区块链上,并且仅允许授权用户查看该数据。作为一个示例,驾驶员可以进入停车库,并且可以使用他的车辆的年份、品牌和型号来在公共论坛中识别他,但是其他私人信息都将不可用于除了具有正确访问的用户之外的任何人察看,所述具有正确访问权的用户将包括该用户、正当的停车库工作人员、审查员、监管者等。

[0009] 在一些实施方案中,本技术适用的停车设施可以包括商业停车结构,诸如在限定的空间区域中具有许多停车位的停车场和车库,以及可以分布在指定区域的停车位,如城市或城镇的地区(sector)、社区、街区、或停车场、车库或其他停车结构的一部分。在一个示例中,一旦停车设施的客户和他们的车辆进入停车设施,就可能对停车设施的客户收费,并且该收费是基于区块链的。例如,一些人在他们进入车库或停车场时将被预先收取全天费用。一些人将基于在停车场或车库花费的时间被收取全天费用的一小部分。一些人能够不受限地24小时/365访问或每当停车设施开放时支付。在不适用日期或额外收费将适用时一些人将不能够用月票停车。本技术的实施方案使得基于区块链的停车交易管理和定制视图能够处理这些和其他按使用支付或基于订阅的停车使用实例,以提高停车业务操作中的便利性和效率。

[0010] 在停车示例中，供应链效率可以通过从客户交互到动态区块链的实时令牌化来提高。对消费者产品的纯净度的感知、如种子来自何处、喂给动物的谷物、天气和气候、从消费者角度的可追溯性对于停车是一样的。到消费者的供应链上的成本效率随着专门知识(know-how)和可采取行动的情报而改变大小，所有这些知识和情报以及更多的内容可以使用所公开的系统和方法更快速地和以更大的粒度收集和分析。经由客户和停车设施运营商端点上的用户界面共享的数据的实时令牌化不仅提供了数据的收集和定制查看，而且便于及时更新与停车场业务和其客户最相关的信息。

[0011] 在停车收益管理中，可以通过知道停车预留负载、信用卡处理、通过渠道捆绑包装销售(例如，在体育场处的停车位售完、显示未预留的停车位的百分比相比于没有预留就参加活动的人的百分比)来提高能力。停车的支付处理可以使用本公开内容的各实施方案通过支付或不支付进行预留或通过仅当相应的停车位由其车辆占用时实时地向用户收费来执行。

[0012] 人总是在最后一刻做出决定，并且将停车位交付给他们所需的技术将更快速地向客户收费、基于汽车的地理位置打开停车门(可以通过许多不同的方式进行认证，诸如VIN#、牌照、用信用卡支付的移动电话信息将汽车置于车位中/在车位中使用并且处理信用卡交易或支付方法，很像收费公路应答器)。设备可以是应答器或发射器。一个应用程序可以核实某人何时在其车辆内到达停车设施，并且如果GPS或其他地理定位技术在汽车/电话/用户上，当客户到达一个很像箭头地理位置的区域时，可以向所述客户收费。存在内置于应用程序的奖励、以及可以通过应用程序对其进行支付的违反行为、以及停车位价格的映射计算器。例如，一个停车场在下午2点到5点收取早到者$8、在下午6点收取$15，并且该同一停车场在一小时后收取$25，由于事件在下午7点开始。所有此信息都可以被记录到区块链中。另外，不同的停车场或一个停车设施内的某些车位可能有不同的价格。最靠近行人出口的车位最高可以在下午7点收取$50，最远的车位可能是$5。所有此信息可以显示在地图上，并且为寻找停车的应用程序的用户指明方向。所有此信息可以允许用户察看将来、实时或过去在一个区域中正在发生什么。

[0013] 物流提供了该技术的另一个直接应用。例如，对包裹或货物的跟踪、商品从一个地方到另一个地方的移动是重要的。所有信息都可以被包括在从货物所来自处和将去往处所传输的中。在各个地点，货物可以被扫描，因此在特定的时间知道货物的精确位置。这可以被输入到区块链记录中。另外，货物可以与特定的船、卡车、货车或其他递送机构(例如，递送无人机)相关联，并且可以实时地、根据请求或以特定的时间间隔跟踪递送机构的GPS位置。可以报告诸如买方、卖方、所有者保险信息等的附加信息，以及与记录在区块链上的GPS相关联的滞留费。公司和/或政府出于各种各样的原因不希望每个人都知道他们的业务，但是需要审查并且向检查员、控制者或监管者证明在某个时间/地方他们在做什么或做过什么的能力。将事物保持为私人的能力是强制的。这样，各实施方案可以使用私人、公共和混合区块链的组合来存储信息。此外，各种加密方案和访问级别可以与数据的单独的部分相关联，以在需要或希望的情况下确保隐私，而在必要时授予访问。

[0014] 在一些实施方案中，该技术可以为国防行业提供特定的应用。例如，美国政府需要审查和控制采购、物流、供应、部队移动等的能力。如果此信息落入坏人之手，则它可能导致致命的后果。在保持信息的某些方面为私人的中使信息的某些方面模糊对任务的成功是势

在必行的。具有将数据分类并且允许访问的能力是势在必行的，以确保仅所需的人具有访问(例如，察看、监视、影响或审查等)数据的能力，而不具有访问的任何人不能够察看数据部分。在一些实施方案中，系统可以自动地核阅与询问有关的文档，并且基于用户的调查(clearance)状态自动地应用一个或多个编辑(redaction)过滤器。

[0015] 该技术的再一个直接应用是停车设施的操作。例如，停车库或停车场的所有者或运营商可以根据需要(例如，每小时或每天)或作为订阅计划(例如，每月停车)的一部分为驾驶员提供停车位。除了收费停车位的此基本提供，停车设施所有者/运营商可以向司机提供各种辅助服务，以在使用该设施的过程期间增强便利性、安全性和舒适性。提供这样的辅助服务可以将特定的停车设施与位于附近的其他停车设施区分开来，以便为特定的设施的所有者或运营商提供在市场中的竞争优势，并且吸引和留住忠诚的停车客户。这样做时，停车设施可以经历增加的收入、减少的责任风险以及更有效率的业务操作。使用区块链和相关联的用户界面来获取、传输、记录和跟踪停车交易相关的数据促进对停车客户和设施所有者和运营商的前述益处，如下文通过示例的方式更详细地解释的。

[0016] 在一些实施方案中，可以使用本技术管理的物理结构中的库存单位包括除了停车设施之外的旅行相关的背景。例如，可以经由所公开的定制视图以与对于停车位而言相同的方式以及限定的库存的类似单元来管理用于一个或多个建筑物中的酒店房间以及甚至分布在连锁酒店品牌的许多位置的酒店房间的如预留、支付和核阅的交易。在一个示例中，一旦酒店的客户到达酒店或一旦在成功进行预留之后第一次进入他们的房间，所述酒店的客户就可能被收费。定制视图和区块链交易记录确保了享受其酒店停留的客户的隐私和安全以及运营商确信预留和支付之间的结合二者。酒店的收费和预留、以及相关服务的提供和业务操作都是基于区块链的，并且可以利用根据本公开内容的定制视图。根据本技术，在诸如旅行者的奖励积分的自动贷记或借记的使用实例中，实现了便利性和业务效率。由所公开的基于区块链的技术和定制视图提供的这样的自动化的益处在酒店背景下是明显的，而且也可能受航空公司和其他地面运输服务喜爱。

[0017] 自动驾驶车辆车队管理是该技术的又一个直接应用。例如，一个或多个自动驾驶车辆的所有者或运营商可能在工作日在特定时间范围(例如，高峰时间通勤时间)经历使用高峰，并且在非高峰时间期间和周末具有较少使用。自动驾驶车辆的某些乘客可以以特定的方式使用它们，像从特定位置和在特定时间呼叫自动驾驶车辆。乘客对自动驾驶车辆的跟踪使用模式可以使得车队的所有者或运营商能够实现经济效益并且增强用户体验。所有信息可以被包括在从何处运输谁以及到什么目的地、自动驾驶车辆在被呼叫时的位置以及自动驾驶车辆往返目的地所采用的路线中。这些和其他有用数据可以被输入到区块链记录中。另外，自动驾驶车辆的位置可以与特定的乘客相关联，并且其GPS位置可以被实时地、应请求或以特定的时间间隔被跟踪。区块链中记录的数据可以被用来便于自动计费和审查。

[0018] 附加信息，诸如电池能量使用、充电历史、车辆维护记录、责任保险信息等，可以与车辆和乘客识别符一起在区块链上报告、跟踪和记录。对于至少一些车队运营商和乘客，出于业务和/或个人原因，维护这些记录的隐私是重要的。然而，在诸如法院命令或执行令的一些情况下，记录在区块链中的这样的信息可能需要向检查员、控制者、警察或监管者公开。这样，各实施方案可以使用私人、公共和混合区块链的组合来存储信息。此外，各种加密方案和访问级别可以与数据的单独的部分相关联，以在需要或希望的情况下确保隐私，而

在必要时授予访问。

[0019] 作为另一个示例，在地面运输行业中，本技术可以被采用以跟踪自动驾驶或人类驾驶公共汽车、班车和出租车的位置，使得运营商和当前的或可能的乘客能够实时查看这些数据。例如，客户可能从机场外的停车设施呼叫在机场处的班车并且希望被接乘。使用本技术的定制视图，客户可以察看班车目前位于何处、确定到达时间的准确预计、并且察看他们是否在期望的车站处错过班车。例如，在客户希望最小化等待班车或其他地面交通工具的浪费时间的情况下，这可能对客户有很大益处。类似地，酒店班车和特定活动的班车运营商以及其客户可以以类似的方式受益以增加操作效率和便利性。

[0020] 在区块链中记录用于在各种各样的背景下对乘客进行地面运输的自动驾驶车辆或人类驾驶车辆的跟踪数据进一步使得能够实时更新和跟踪单个车队中或两个或更多个车辆车队中的公交车、班车和/或汽车状态。这些数据可以与区块链中记录的并且使用区块链跟踪的乘客接乘位置配对，其中运营商和乘客都可以利用所公开的定制视图来方便地评定操作状态，以及根据变化的需求或其他因素(诸如交通条件和天气)执行其他有用的功能，如变化接乘位置、提供状态更新和为车队车辆重新规划路线。

[0021] 从在地面运输中应用和使用本技术产生的其他技术效益包括为乘客提供一种为乘车进行支付的手段，并且还可能给使用私人和安全的基于区块链的交易的其驾驶员小费。所公开的定制视图可以被乘客有利地使用，不仅用于安排地面运输和察看他们的乘车将在何地以及在何时到达，他们还可以预付乘车费用、为稍后的日期和时间预定乘车，以及在一些实施方案中，更改他们的接乘点和目的地点以更好地满足他们的需要。本技术可以根据乘客的需要以及根据能够为乘客服务的车队资产的可用性无缝地调整人类驾驶或自动驾驶车辆的方向、导航和行程安排。随着乘客更新，以及为满足客户需要而对资产和/或驾驶员可用性做出的任何改变，乘车费用可以根据操作和环境条件的改变而被实时调整。通过使得乘客能够使用包括加密货币的任何形式的支付经由所公开的定制视图(例如，通过智能电话应用程序)进行支付，通过本技术在地面运输行业中的实践可以加强这些增值技术效益。对于地面运输车队和其他服务的运营商，他们的车辆和人员的性能和效率是容易量化的，以使用区块链中记录和不断更新的位置、定时和其他数据来定义和分析评定有意义的度量。

[0022] 作为又一个示例，在游戏行业中，客户社会保障号码、生物统计、地址、照片、驾驶执照、在先的游戏玩法、美国国税局(IRS)税务通知、获胜/失败、补偿、忠诚卡/玩家卡号码信息、出生日期、已知的伙伴、配偶/女朋友、喜爱的团队、喜欢/不喜欢的活动、小费数额、就财产而言时的ATM使用(ATM use while on property)、已知的电子钱包、使用的信用/借记卡、使用的加密货币钱包等都可以与其他客户信息一起保持在区块链上。客户将不希望此信息中的任何一个以公共格式可查看，并且公共访问可能导致娱乐场承担法律责任。各实施方案使用各种加密和散列技术来将数据安全地存储在区块链上，并且仅允许经授权的用户查看数据。作为一个示例，客户可以参加比赛，并且可以使用他的姓名或玩家号码可以被使用以在公共论坛中识别他，但是其他私人信息都将不可用于给除了具有正确访问的用户之外的任何人看到，所述具有正确访问的用户包括用户、恰当的娱乐场工作人员、审查员、监管者等。

[0023] 各实施方案提供了存储所有者意在保持为私人的但是在公共账本中可以由经授

权的实体或个人看到和审查的信息和提供对所述信息的访问的技术。世界各地都存在隐私法要求将信息保持为私人的。各实施方案可以通过确保数据以正确的格式存储并且仅以合规的方式可访问来确保遵守那些隐私法。作为另一个示例，企业和政府不希望它们的私人信息、知识或商业秘密变得为人所知。虽然这些团体没有什么要隐藏，但是使它们的所有信息处于任何人都具有人、企业、政府等如何操作的可查看性或知识的开放论坛中将引起损失、盗窃和增加的竞争。

[0024] 在一些实施方案中，可以使用用户的数字钱包中携带的任何加密货币(例如，以太币相对于比特币等)来执行投入交易或库存或停车以及其他旅行相关(例如，酒店房间)交易。在这样的示例中，本公开内容的实施方案可以使得能够基于由与区块链通信的外部数据源维护的兑换率在各种类型的加密货币之间或在加密货币和真实货币之间进行变换(shapeshift)或交换价值。例如，如果第一玩家仅具有比特币，并且对具有300个以太币的第二玩家投入2个比特币，并且第一玩家赢了投入，则适当数额的比特币将自动地从第二玩家的数字钱包中扣除，并且将按以太币的转换数额贷记到第一玩家的数字钱包。这样的用于支付处理的自动货币转换可以被应用于本文所描述的若干个示例，包括库存(例如，停车、零售等)交易跟踪、管理和实现场景。这样的分散式的并且自动的货币兑换可以连续操作并且不要求人为干预。在所公开的实施方案中，所述方法同样可以适用于人工智能系统和用户界面，用于进行投入和接受投入，以及在没有人为干预的情况下做出诸如游戏玩法、事件投入、投入类型和风险/赔率和支出的决策。

[0025] 在一些实施方案中，根据本技术的库存交易管理、处理和跟踪使得业务和其客户能够集成多种支付方法，并且无缝地计入可用于支付各种商品或服务的任何价值。例如，可用于库存交易的客户支付账户可能被预付费或它们可能链接到一个或多个其他账户。在一种使用实例中，由于账户被预付费(例如，由客户充钱)或账户已经收到类似的或不相关的交易的退款，账户可以用货币贷记或借记。例如，符合这样的库存的提供者的策略的已取消的停车或酒店预留(例如，在截止日期/时间之前取消)可以作为货币贷记到客户账户，以用于在另一个库存交易中使用，并且相关交易信息被记录在区块链中并且使其经由定制视图对客户和业务二者可得。

[0026] 一些实施方案允许数据平台连接到电子投票机器。这些机器可以直接报告关于投票人、选票的信息，并且将投票投到数据平台以用于存储在区块链中。数据平台可以加密和设置访问投票记录的访问级别。例如，投票机器可以收集人的信息、社会保障号码、地址、派别、生物统计、驾驶执照号码、照片等。这样，保持在选举中使用的此信息的大部分需要对公众保持为私人的，一些信息(例如，一个人确实在一个特定的选举中投票、他们的派别关系等)可能是公开的。此外，一些实施方案提供了用于识别和/或消除投票人欺诈的自动化技术的使用。例如，一些实施方案可以使用人工智能或机器学习引擎来核阅存储在区块链中的投票人数据，并且识别投票两次的投票人、非法投票人等。

[0027] 另外，在上文所提供的示例中，该技术可以在银行业务(banking)、陪审团投票、法庭审理、卫生保健、火器销售、零售销售、药物、退休金、财务交易、保险和需要审查、对数据的公共查看、对数据的私人查看等的许多其他应用中使用。

[0028] 本技术的一些实施方案可以在混合的格式下使用可选标志(marker)。例如，在一些实施方案中，系统可以具有将事物设置为私人的(不具有访问的人不可查看的)、公共的

(每个人可查看的)或二者的混合(一些信息是公共的并且一些信息是私人的)的能力。存在应使用公共区块链并且该公共区块链可以是完全透明的以让每个人看到的情形。还存在为了满足隐私法或仅仅因为人们不希望其他人知道他们是负责做某事的个人或组织的事实而要求一些信息的一些隐私的一些情况,这将是混合格式。使某些信息模糊或将其保持为私人的的能力对于以上行业是势在必行的。

[0029] 根据使用私人或混合格式的各实施方案,存在用于使数据安全的至少两个选项。例如,在一些实施方案中,可以通过将加密应用于解锁来完成信息的完全模糊。一些实施方案可以使用多层加密,以使得数据的部分可以被限制并且可以是不同的个人可访问的。在混合操作模式下,一些信息可以是公共的或可以被透明地看到,而其他信息将被保持为模糊的或私人的。在一些情况下,可以使用标志来指定数据访问级别。标志可以是向审查员、选举官员、控制者等示出用户是谁的某物,并且可以是如公民1或客户200的数字。在一些实施方案中,可以使用抄本(codex),该抄本可以由将扰乱用户的身份的系统控制,因此将没人知道用户是谁,因此使身份保持为私人的。仅负责审查或管理区块链的人将能够弄清责任方是谁。在一些实施方案中,除非需要审查和说明抄本,否则该抄本将永远不会提供此信息。

[0030] 在一些实施方案中,可以将审查功能集成到用户界面中,该用户界面将给予用户(例如,通过点击虚拟按钮)允许所有信息或一些信息(例如,列、格式、部段等)为私人的、公共的和限制访问的的能力。一些实施方案提供实时监视/审查功能,该监视/审查功能将示出并且允许用户双重或三重核查被保持为私人的的内容。在一些实施方案中,口令(password)或具有两方认证器、三方认证器、多重签名的口令等将是由区块链推动的分散式应用程序(DApp)的一部分,该分散式应用程序将使得用户能够提交、添加或附上将进入区块链的信息。在一些实施方案中,可以以分散式方式设立此信息,因此可以在分散式网络上实时自动地插入、测试和监视信息,以使得信息不被泄露或不被未经许可的各方非法入侵或看到。

[0031] 提供了此“发明内容”部分以便以简化形式介绍一系列概念,这一系列概念将在下文的“具体实施方式”部分中被进一步描述。此“发明内容”部分既不意在识别所要求保护的主题的关键特征或必要特征,也不意在用来限制所要求保护的主题的范围。将在下面的描述中在某种程度上阐述示例的附加方面、特征和/或优点,并且在某种程度上,根据所述描述示例的附加方面、特征和/或优点将是明显的,或可以通过实践本公开内容而获悉。

附图说明

[0032] 参考以下附图可以更好地理解本公开内容的许多方面。虽然结合这些附图描述了若干个实现,但是本公开内容不限于本文所公开的实现。相反,目的是涵盖所有替代方案、改型和等同物。

[0033] 图1例示了用于实现用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的操作架构。

[0034] 图2例示了在用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的实现中采用的视图定制过程。

[0035] 图3例示了用以生成记录到区块链中的受限交易的定制视图的一个实现中的分布

式账本架构的各种部件。

[0036] 图4例示了一个停车设施,对于该停车设施,可以至少部分地使用所公开的系统和方法来实现相关业务操作。

[0037] 图5例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0038] 图6例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0039] 图7例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0040] 图8例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0041] 图9例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0042] 图10例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0043] 图11例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0044] 图12例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0045] 图13例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0046] 图14例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0047] 图15例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图。

[0048] 图16例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的流程图。

[0049] 图17例示了用以生成记录到区块链中的受限交易的定制视图的财务审查场景的一个实现中的示例性操作架构。

[0050] 图18例示了用以生成记录到区块链中的受限交易的定制视图的停车设施业务操作跟踪场景的一个实现中的替代操作架构。

[0051] 图19例示了用以生成记录到区块链中的受限交易的定制视图的酒店业务操作跟踪场景的一个实现中的替代操作架构。

[0052] 图20例示了用以生成记录到区块链中的受限交易的定制视图的自动驾驶车辆车队业务操作跟踪场景的一个实现中的替代操作架构。

[0053] 图21例示了用以生成记录到区块链中的受限交易的定制视图的游戏监管场景的一个实现中的替代操作架构。

[0054] 图22例示了用以生成记录到区块链中的受限交易的定制视图的库存跟踪场景的一个实现中的替代操作架构。

[0055] 图23例示了记录到区块链中的受限交易的示例性定制视图。

[0056] 图24例示了记录到区块链中的受限交易的替代示例性定制视图。

[0057] 图25例示了记录到区块链中的受限交易的示例性定制视图。

[0058] 图26例示了记录到区块链中的受限交易的替代示例性定制视图。

[0059] 图27例示了能够提供记录到区块链中的受限或敏感数据的定制视图的数据访问系统的一个实现中的替代操作架构。

[0060] 图28例示了适合于实现本文所公开的技术的计算系统，该计算系统包括在附图中例示的和在下文的“具体实施方式”部分中讨论的架构、过程、操作场景和操作序列中的任何一个。

具体实施方式

[0061] 区块链已经在生成数据的区块链并且在分布式网络中的用户之间共享数据中变得司空见惯。与先前的数据库结构不同，区块链数据库由散布在大型分布式节点网络上的众多独立节点维护。公共区块链是向任何用户开放以将数据(在本文中也被称为交易或区块条目)输入和记录到区块链的区块中的数字账本。当交易被记录到区块链数据库中时，由于数据被存储在分布式网络中的不止一个节点中，因此改变交易数据或从数据库移除交易数据即使不是不可能的也是非常困难的。因此，数据由多个用户添加到区块链数据库中，并且通过添加、校订或移除数据来改变记录的数据将要求大多数用户或监督改变的主控制者和联署者(例如，经理和雇员、审查员和工头等)同意改变。

[0062] 另外，每个区块包含数据、当前区块的散列和先前区块的散列。区块链还可以在区块中存储关于交易的附加细节，诸如发起交易的用户名、与交易相关联的各方的其他用户名、时间戳、可执行代码以及与交易有关的其他信息。散列识别区块和存储在区块中的交易数据。散列相对于所有其他散列是独特的并且每当对区块进行改变时改变。由于每个区块包含前一区块的散列，因此区块形成所谓的区块链。任何对区块的篡改都将导致该区块的散列的改变。因此，由于区块链中的所有其他区块不再包含前一区块的有效散列，因此它们将变得无效。

[0063] 虽然改变区块链中的每个随后区块的散列可以是可能的，但是对于私人网络和公共网络二者，改变存储在分布式网络中的每个节点上的每个区块链几乎将是不可能的。存储先前散列以形成区块链和将区块链的完整副本分发到分布式网络(私人的、许可的和公共的)中的每个节点的此组合在用户以及网络中存储的交易之间建立信任系统，尤其是当用户彼此不熟悉时(即，公共网络)。

[0064] 本公开内容的示例描述了用于生成区块链交易的定制视图的系统、过程和应用程序。在分布式节点网络中维护由多个用户从用户设备请求的区块条目的区块链。所述区块条目各自包括多个数据部分，所述多个数据部分各自与一个访问级别相关联。接收查看一个区块条目的一个或多个数据部分的请求，所述请求包括与至少一个访问级别相关联的访问代码(例如，散列、私人密钥、生物统计、口令、个人识别码(PIN)等)。用区块条目的所述区块链评估所述请求中的所述访问代码以识别与所述访问级别相关联的一个或多个数据部分。生成包括与所述访问级别相关联的所述一个或多个数据部分的所述区块条目的定制视图。在一些实施方案中，存储在所述区块链中的数据的部分可以被单独地加密。这样，取决

于与所述访问代码相关联的访问级别，仅一部分数据的解密可以被授权或是可得的，而其他部分将保持安全。

[0065] 从本讨论可以领会的技术效果是识别用户被授权访问的条目数据(例如，银行业务机构中的财务记录、停车设施客户和相关联的交易数据、客户/供应者跟踪的库存、车辆车队乘客使用、路线和位置信息、用于游戏监管委员会的合规数据、来自政府或半政府机关的保密文档、用于医疗机构的健康记录、受保护的关键基础设施信息(PCII)、政府审查员/检查员所需的数据等)和提供记录在区块链交易中的数据的定制视图中增加效率。本文所描述的实施方案中的一些还通过仅在用户具有访问来自区块链条目的数据部分的授权的情况下才允许用户访问来提高安全。另外，一些实施方案可以提供示出何时和谁访问过各种数据的不可变的日志。另外，在一些实施方案中，可以发生自动核阅(例如，通过人工智能或机器学习引擎)以检测特定的事件(例如，盗窃用户账户访问证书或设施访问设备、内幕交易、洗钱、作弊、投票人欺诈等)。

[0066] 特别是对于PCII，本技术解决了影响客户信息以及客户的相应的信用卡或支付信息的保护的问题。本技术利用区块链来经由区块链进行支付交易，同时使用户信息模糊以维护交易的隐私。本技术的应用使得能够使相应的交易信息中的一些可用，可能以混合地私人的或甚至公共的形式可用，视情况而定，同时仍然允许经由所公开的定制视图发送关于用户的存储在区块链中的交易的一些信息。这使得客户能够将他们的信息保持为私人的，同时基于他们的使用或采购一个单位的商业库存获得透明的支付/定价的益处。在停车设施背景下，例如，作为额外的便利性和商业服务，使电动车辆充电站在一些停车位中可用。对于客户和运营商来说，提高了作为主库存交易的辅助的这样的服务的效率和便利性，其中在区块链上存储和更新与主库存(停车)和所有可用的辅助服务二者相关的所有信息(例如，定价、价格和可用性)并且可以经由定制视图而使所述所有信息对于所有感兴趣的各方是可得的。

[0067] 更具体地，一个实现可以提供生成银行业务交易的定制视图的非常规过程，该定制视图限制用户敏感信息(例如，反洗钱(AML)或了解你的客户(KYC)策略文档、(ADD)账户号码、账户余额、账户报表)，但是允许外部银行业务机构或用户核实账户具有用于交易的可用资金。另一个场景提供了审查区块链中的交易而不使得审查员能够查看交易的完整版本的非常规过程。例如，美国国税局(IRS)可能要求对在前一纳税年度内执行的所有货币交易进行审查。然而，可能不要求被审查的公司提供针对每个交易的客户姓名和地址的完整列表。通过提供交易的定制视图，IRS可以对交易数额的准确性有信心，并且公司可以维护其客户的匿名性。

[0068] 在游戏监管行业中可以领会本讨论的附加技术效果。例如，本文所描述的一个实现提供了查看游戏投入的结果而隐藏投入数额的非常规过程。当对于获利玩家监视游戏社区(例如，卡计数器(card counter)等)而允许玩家维护他们的钱罐的隐私时，这可能是有用的。在另一个示例中，游戏委员会可能要求交易的定制视图，以查看关于每个玩家的一些个人信息(例如，每个玩家都具有竞赛合法年龄的核实、每个玩家都没有被列入黑名单的核实、玩家句柄/昵称)，但是不使得其他个人信息(例如，用来买进游戏的信用卡号码、每个玩家的法定姓名等)是可查看的。

[0069] 在一些实施方案中，第三方可以查看游戏、游戏的相关联的统计和游戏的获胜者

或失败者。在一个示例中，用户可以从一系列可查看的游戏中选择要观看的游戏，并且然后基于他们正在观看的内容下他们的投入(例如，微小投入或派利分成法投入)。在另一个示例中，完全使用所公开的基于区块链的系统和方法托管和操作游戏引擎。例如，随机数生成器(RNG)可以用由外部验证源指定的投入获胜者指定机遇游戏而不是真实世界游戏的结果。包括RNG的游戏功能可以被保存在区块链上，或在区块链被分区以将用于运行游戏的计算和存储工作负荷散布开的情况下，所述游戏功能可以被保存在片断(shard)上。在另一个示例中，如果一个投入被取消，则所有投入都可能被无效。也可以与区块链一起利用所公开的系统和方法，以便于人们对将来可能发生的事件投入。在这样的情况下，考虑到事件可能发生的日期，如果该事件永远不会在包括玩家的投入的日期中的任何一个发生，则投入可以被取消，因为在投入中事件可能永远不会发生是先决条件。在该情况下，投入者将把他们的钱输给投入登记人、网上机器人或接受投入的人。

[0070] 另一个示例可以包括内华达州游戏委员会(Nevada Gaming Commission)要求来自寻求用于游戏机构(gaming establishment)的执照的申请人的先前的业务关系、雇用历史、犯罪记录和财务稳定性的公开文档。然而，可能不要求申请人提供删掉的犯罪行为记录。因此，文档的视图将被定制，以仅显示文档的被内华达州游戏委员会要求的那些部分，并且省略、编辑或以其他方式模糊被认为就寻求执照来说不相关的或不需要的数据。在一些实施方案中，可以基于投入者的位置，如由投入者的设备的IP地址或GPS位置所确定的，以适当的税率自动在线执行对投入交易和奖金的征税。在一个示例中，根据本公开内容的区块链为区块链提供了互操作性以在平台上或在投入之间通信。

[0071] 在一些实施方案中，系统可以摄取私人信息并且可以在不公开根本机密信息的情况下生成在做决定时可以使用的可公开查看的分数、品级(rating)或其他指标。在一些实施方案中，系统可以连接到附加的公共和私人数据源以收集附加信息。例如，如FBI报告、信用报告、背景报告等的公共信息。此附加信息可以存储在区块链中作为个人的记录或简档的一部分。这可以通过社会保障号码、驾驶执照、面部识别或指纹作为用于核实的第二因素来实现。这样，一旦一个人进入娱乐场并且注册一张卡来玩，就可能收集关于此人真正是谁的大数据，并且仅娱乐场、审查员和监管者可获得该信息，以查明此人就是他所说的那个人、是合法的并且在财产上是允许的或是能够玩的。如办公建筑物和机场的商业和政府建筑物可能能够具有摄像机系统，该摄像机系统读取进入停车设施的汽车的牌照或监视驾驶员和乘客的面部识别。可以对此信息进行比较和评分，以查看汽车或人进入设施是否安全。

[0072] 在一个示例中，娱乐场可以在分布式节点网络上托管或维护一个节点。这给予娱乐场他们可以访问和控制的他们自己的无可辩驳的事件的记录。如果网络出故障，娱乐场将仍然能够根据投入、游戏玩法、权益、奖励等管理其所有活动。一旦网络恢复在线，通过娱乐场的节点可以容易地对分布式节点网络进行任何必要的更新。此备份功能和独立节点场景为娱乐场提供了业务操作的连续性，并且可以在零售和停车位示例中以类似的方式享受这样的益处。

[0073] 在又一个实施方案中，对于跟踪包裹递送和库存转运的非常规过程可以认识到技术效果。例如，一个或多个包裹可以在原地被扫描，然后在包裹开始在一个货物单元中转运时被再次扫描。转运公司可能希望允许包裹中的一个的收件人查看与其盒子相关联的数据，但是不允许收件人查看交易中存储的与货物单元中的其他包裹相关联的所有其他数

据。因此，将使能针对收件人用户的交易的定制视图，该定制视图仅描述其包裹的位置、出发时间和预计到达时间。与产品相关联的附加信息也可以被收集并且被存储在区块链中，所述附加信息详述产品物流，诸如制造商、卖家、核查点位置、核查点雇员、质量控制经理、测试中心、以及整个装运过程中的保管链以及在货物单元的装运期间访问货物单元的个人。在任何时候或在接收时，可以使得接收方能够看到此信息的一部分，但不是全部，这取决于收件人的状态。例如，竞赛机构或监管者可能能够查看关于制造的骰子的选择性产品信息以及保管链，以核实在从受信任的骰子制造商处路由时，骰子没有受不良影响。此数据可以在定制视图中显示。

[0074] 另外，本文的示例描述了可以通过处理加密代码以验证查看与访问级别相关联的一个或多个数据部分的访问来用区块条目的区块链评估请求中的访问代码。在其他示例中，还维护用于区块条目中的多个数据部分中的每个的指针，所述指针指示用于区块条目中的多个数据部分中的每个的至少一个公布位置。另外，在此示例中，通过使用用于区块条目中的多个数据部分中的每个的指针来检索与访问级别相关联的一个或多个数据部分以生成定制视图。对数据部分的访问要求使用个人识别码代码、口令、指纹、条形码、视网膜扫描、令牌、调查表或包括两因素、多因素或附加安全认证器的任何其他类型的访问确定方法。

[0075] 在其他实施方案中，对于跟踪和记录停车设施中的活动、偏好和交易的非常规过程可以认识到附加技术效果。例如，进入和离开时间可以被收集并且被记录在区块链中，并且与车辆身份相关联。使用停车设施的车辆驾驶员或乘客的附加身份信息(例如，生物统计、面部识别或移动电话)可以与车辆身份同时被收集，并且被用来验证停车支付交易。电子钱包——包括用于真实或加密货币，以及在停车访问之前或在时间上接近停车访问经由用户界面接收的信用或借记卡账户信息可以安全地与停车客户相关联，并且被用于使用实时令牌化进行快速和安全的支付交易。与周期性的或反复出现的停车设施客户相关联的附加信息(例如，由特定的客户拥有或以其他方式使用的多个车辆识别符)也可以被收集并且被存储在区块链中，并且被利用以便于有效率的停车业务操作以及为客户增强的便利性。除了记录在区块链中的信息的手动数据输入以外，可以利用定位在停车设施中或附近的各种设备来便于提高的停车业务操作和客户体验，如下文通过示例的方式更详细地描述的。这些数据可以在定制视图中显示给停车设施工作人员和客户。

[0076] 在另一个示例中，通过维护用于与访问级别中的每个相关联的一个或多个数据部分的单独的区块条目来维护由多个用户从用户设备请求的区块条目的区块链。另外，在此场景中，验证请求中的访问代码以查看用于与访问级别中的每个相关联的多个或多个数据部分的一个或多个区块条目。在一些实现中，通过维护用于与访问级别中的每个相关联的一个或多个数据部分的单独的区块链来维护由多个用户从用户设备请求的区块条目的区块链。另外，在此实现中，验证请求中的访问代码以查看用于与访问级别中的每个相关联的多个或多个数据部分的一个或多个区块条目。

[0077] 在一些示例中，所接收的查看区块条目的一个或多个数据部分的请求包括与产品或包裹有关的或与在任何给定的时间在停车设施中的可用停车位有关的库存跟踪请求。在停车行业背景下，这样的请求可以由停车设施的所有者或运营商或由当前的或可能的停车客户接收。在其他示例中，所接收的查看区块条目的一个或多个数据部分的请求包括财务

审查请求。在一些场景中，所接收的查看区块条目的一个或多个数据部分的请求包括游戏监管请求或与涉及目前或在某个过去时间停放在停车设施中的车辆或该车辆进入或离开该设施的时间的调查有关的请求。在其他场景中，与区块条目的一个或多个数据部分相关联的访问级别包括私人访问级别、许可访问级别和公共访问级别中的至少一个。然而，在另一些示例中，与区块条目相关联的访问级别包括私人访问级别、许可访问级别和公共访问级别中的至少一个。

[0078] 虽然本公开内容描述了各实施方案，但是应领会为了附加行业中的技术改进可以包括附加示例。示例行业可以包括国防和安全、金融和保险、零售(例如，火器)、销售和执照发放、医疗记录、会计、装运和物流、药品和药物、大麻和大麻二酚(CBD)、石油和天然气、能量和商品、国家安全等。

[0079] 参考附图，图1例示了与处理用于管理示例性增强型系统的操作有关的示例性操作架构100，用该示例性增强型系统可以实践本公开内容的各方面。操作环境100包括区块链网络101。区块链网络101在基于用户的被批准的访问级别授权用户查看区块链条目中的数据部分的背景下采用视图定制过程200。区块链网络101可以在适合于执行视图定制过程200的支持架构中包括各种硬件和软件元素。在图28中关于控制器2800例示了一个这样的代表性架构。

[0080] 服务器节点110-112包括能够运行区块链应用程序的一个或多个服务器和设备。与服务器节点110-112交互的用户设备可以包括但不限于能够发射和接收编码用于访问用于停车的停车设施并且为其提供支付的信息的无线数据信号的个人计算机、移动电话、手持设备、平板计算机、台式计算机、膝上型计算机、可穿戴计算设备、投票机器、游戏机器、电子金融交易所、安全系统、应答器、摄像机或其他成像设备、钥匙坠(key fob)、传感器、访问卡等，或任何其他形式因素，包括计算机的任何组合或其变体。

[0081] 更具体地，图2例示了视图定制过程200，如所提及的，该视图定制过程可以由区块链网络101采用以生成记录到区块链中的受限交易的定制视图，如本文所描述的。视图定制过程200的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令来实现。程序指令指示区块链网络101操作如下，在图1的背景下附带说明地引用图2中的步骤。

[0082] 在操作中，区块链网络101维护由多个用户从用户设备请求的区块条目的区块链120，其中所述区块条目各自包括多个部分，所述多个部分各自与一个访问级别相关联(步骤201)。区块链数据库由散布在服务器节点110-112的区块链网络101上的众多独立用户维护。区块链120是对任何用户(例如，公共区块链)、特定的一组用户(例如，私人区块链)或私人和公共用户的组合(例如，混合区块链)开放以将数据输入和记录到区块链的区块130中的数字账本。区块链120可以由多个用户添加并且由分布式网络中的多个节点110-112记录。

[0083] 在停车行业背景下，停车设施运营商可以在区块链上维护某些记录，诸如公共可访问的停车设施入口的GPS位置、可用停车位的识别符(例如，字母数字的)、价格和停车销售、特价或促销。在一些实施方案中，这样的记录对于首次做以下动作之一的用户是公共可访问的：访问网站、订阅电子邮件列表、下载智能电话应用程序、首次在停车设施处停车等。其他记录，诸如客户的数字钱包、信用/借记卡账户信息、使用历史、车辆识别信息、肖像图

像等,可以作为仅由相应的客户和停车设施运营商可访问的私人记录在区块链上维护。在一些实施方案中,可以在有限的基础上——包括在订阅基础上——使车辆恢复或维修服务提供者可获得诸如目前的停车位置、车辆识别符和相关联的客户姓名的区块链记录。在此情况下,经历对车辆服务(例如,挡风玻璃更换、干洗、宠物寄宿)的需要的停车设施可以安排和接收提供者的服务,甚至在车辆所有者与车辆不在停车设施中的同一位置这样的时间期间。停车设施的客户可以可选地经由用户界面向停车设施授予许可,以使停车设施使用记录在区块链上的客户的支付账户信息处理对服务提供者的支付。在这种情况下,代替由车辆服务人员支付给设施运营商的订户费用或除了由车辆服务人员支付给设施运营商的订户费用之外,停车设施可以从车辆服务支付收取佣金,用于便于服务和支付处理。以相同的或类似的方式利用区块链的停车设施中的有关辅助服务可以包括,例如,汽车清洗或汽车美容、添加燃料、电动车辆充电、安排拼车或共乘、代客停车、自动售货机器、咖啡馆、报纸等。

[0084] 区块130包括区块条目140-142。区块条目140-142可以包括各种类型的数据,包括停车设施客户使用和交易记录、停车设施中可用的车位的数目和位置、自助停车或代客停车、游戏投入、库存记录、医疗记录、银行业务和财务记录、智能合同以及其任何其他类型的组合或变体。例如,用户(例如,停车客户)可以通过与另一个用户(例如,停车设施运营商)签订合同并且然后将该合同作为区块条目140存储在分布式网络环境中的节点110-112上的区块链120中来创建区块条目140。作为另一个示例,电子设备(例如,停车设施访问控制和支付处理设备和系统、传感器、用于检测停车设施中的停车位的可用性状态的信标或其他设备、电子投票机器、竞赛机器、在一个或多个服务器上运行的审查软件、终端用户设备等)可以自动地连接到区块链网络并且请求将数据添加到区块条目中。

[0085] 为了添加具有数据部分的新区块条目,区块链可以使用共识协议,如权益证明(PoS)或工作量证明(PoW)、委托权益证明(DPoS)等。例如,在PoW中,为了将服务器节点110-112选举为领导者以选择待被添加到区块链的下一个区块条目140,一个特定的服务器节点必须找到对一个特定的难题或数学问题的解决方案(通常是通过蛮力)。一旦找到解决方案,服务器节点就将该解决方案公布到其他节点用于验证。当节点的共识同意解决方案是正确的时,该新区块条目可以被添加到区块链。工作量证明的示例是SHA-256、Blake-256、CryptoNight、Quark、SHA-256、SHA-3、4crypt、scrypt-jane、HEFTY1或其他或其组合。相反,PoS基于服务器节点的参与和风险价值(例如,权益)。DPoS是PoS的有效率的变体,其通过将网络上的验证者的数目限制到一组委托代表(例如,投票人)以关于是否将条目添加到区块链进行投票来提供高级别的可扩展性。

[0086] 区块条目140-142各自还包括数据部分150-155。数据部分150-155包括组成区块条目140-142中的每个的部件,并且可以基于用户请求或交易格式(既是标准化的又是定制的)被分解成多个节段。例如,如果用户将来自交易的一部分数据标记为机密的,则该部分数据可以被分配为私人的。如果数据属于先前被分配为私人的类别,则该部分数据也可以被分配为私人的。例如,用户可以将所有信用卡号码归类为私人的。相反地,一部分数据也可以由用户分配为公共的或许可的。在一些实现中,如果始发或控制用户提供许可,则该部分数据可以仅被指定为接收用户可访问的(例如,交易的始发方将区块条目和所有数据部分分配为私人的,并且查看一部分数据的能力要求经由签名条款和条件表格进行准许)。此

用户准许特征可以包括在允许用户通过用户准许部段提供准许的访问平台中。

[0087] 本技术的一些实施方案修改用于将数据添加到区块链的传统协议和工作流程。例如，在一些实施方案中，要求服务器节点110-112将数据的部分识别或分类为一个或多个类别。例如，这可以使用人工智能或机器学习将数据分类为一个或多个类别(例如，电子邮件地址、车辆识别号码(VIN)、牌照号码、社会保障号码、用于面部识别算法的人脸的全部或部分图像、与解码射频识别(RFID)或近场通信(NFC)信号相关联的序列号码或客户账户号码等)来完成。在一些实施方案中，分散式应用程序(DApp)可能负责数据的初始排序和归类。当添加区块条目140-142时，通常包括先前区块的散列和时间戳的条目的起始行可以被修改为包括关于该条目内的数据类别、用于每个数据部分的访问级别、访问限制等的信息。例如，一些实施方案可以创建存储在区块条目内的索引和/或访问级别信息。这样，当稍后检索数据时，可以容易地识别该数据或使该数据与适当的访问级别相关联。再者，在一些实施方案中，负责添加数据的服务器节点可以组织数据并且为不同的数据部分150-155设置不同的加密级别。在其他实施方案中，可以使用中间件(例如，在位于区块链网络和连接设备之间的数据平台上)来对存储在区块链上的加密数据进行解密、将信息分类以及执行访问级别许可，从而创建定制视图。

[0088] 在一些场景中，用户可以设置将交易中的所有数据分配为公共的的默认设置，并且可以选择性地将数据的单独的节段分配为私人的，反之亦然。同样地，在数据对于一般公众是不可得的但是可能对于各种团体的用户(诸如，审查委员会成员、法律执行官员、政府监管人员、医务工作人员等)是可访问的的情况下，一部分数据也可以被分配为许可的。在其他示例中，区块链120可以包括用以将数据部分分配为私人的、许可的或公共的的默认规则。

[0089] 例如，区块链120可以确定任何驾驶执照号码、RFID、停放车辆的人的蓝牙®或NFC、停车设施预留停车位识别符、牌照号码、车辆识别号码或社会保障号码应被自动地设置为私人访问。虽然本文包括的若干个示例和实施方案描述了将被归类为私人的、许可的或公共的的主要访问级别，但是应理解，可以在本公开内容的范围内认识到任何数目的访问级别类别。此外，访问级别的状态可以基于对某些事件的检测而自动改变或更新。例如，关于一笔交易的所有数据可以在一段时间内保持为私人的，在该点处系统可以对于一些或所有相关数据将访问级别改变为公共的。

[0090] 在下一个操作中，区块链网络101接收来自用户的查看区块条目140的一个或多个数据部分150-155的请求，该请求包括与至少一个访问级别相关联的访问代码(步骤202)。查看请求可以由是区块条目140中存储的交易的一方的用户发起，该用户是诸如接收来自客户的数据请求的停车设施的运营商或游戏投入中的一个参与者。用户也可以是仅对业务操作或交易感兴趣但是不直接参与交易的用户，诸如，寻找方便的地方停车的驾驶员、核实收入数据的税务审查员、持有股票和债券的转让代理人或第三方财务保管人、代表贷方收集债务支付的催讨机构或查看最近公司股息交易的股票持有人。

[0091] 在下一个操作中，用区块条目的区块链评估访问代码以识别与访问级别相关联的一个或多个数据部分(步骤203)。可以基于诸如政府雇员、包裹递送雇员、银行经理、停车库客户和运营商等用户状态将访问代码指定给用户。可以基于给予用户的与访问级别或数据部分相关联的加密代码(例如，私人密钥或散列)确定访问代码。可以基于口令、签名、指纹、

条形码、处理芯片、调查表、生物统计、令牌以及可以使得用户能够核实授权以访问与访问级别相关联的数据部分150-155的任何其他方法进一步验证访问代码。在一些示例场景中，可以基于数据部分150-155的相关联的访问级别将数据部分150-155分成不同的区块链或区块条目。在此场景中，可能要求访问代码150来访问区块链或区块条目以查看与访问级别相关联的数据部分。

[0092] 在最后的操作中，生成包括与访问级别相关联的一个或多个数据部分150-155的区块条目的定制视图(步骤204)。该定制视图可以由数据访问平台生成。该定制视图可以被修改以仅并入与经验证的访问级别相关联的那些数据部分，或可以包括所有数据部分150-155，其中未授权的数据部分从记录视图用黑色涂掉。该定制视图可以被显现在用户设备上的区块链应用程序(例如，DApp)中、以记录消息的形式传送给用户、或以任何其他方式显示给用户或用户团体。

[0093] 根据各实施方案，将数据添加到区块链、安全级别筛选、数据归类、访问级别指派、审查和/或其他功能全都可以被自主地完成。例如，当车辆进入停车设施时，包括用于蓝牙®或其他无线信号的接收器的传感器、摄像机或其他成像设备以及诸如门和访问设备读取器的访问控制系统收集用于识别该车辆、其驾驶员并且可能还识别其乘客的数据。同时，诸如运动、重量、距离或接近感测设备的传感器收集用于监视停车设施中的停车位的可用性状态(例如，占用与未占用)的数据。

[0094] 作为另一个示例，当用户进入娱乐场时，可以从各种系统(例如，监控摄像机、停车库摄像机、忠诚卡系统、房间访问系统、娱乐数据库等)收集、添加数据到区块链。考虑到数据量，可以使用人工智能和/或机器学习引擎(例如，使用支持向量机、人工神经网络、贝叶斯网络、监督学习、无监督学习和/或其他技术)来识别、关联和分类可以被添加到区块链的相关数据。数据本身可以被加索引以用于搜索和/或将来摄取。在其他实施方案中，数据可以被分节段并且被添加到玩家的简档。由于各种数据部分可以被指派不同的访问级别，因此请求数据的人可以仅被自动地供应对于他们的访问级别适当的数据部分。类似地，数据可以被自动地核阅或审查以识别违反行为(例如，安保或安全考虑、不安全驾驶或停车设施中的其他不受欢迎的客户行为、竞赛规则违反行为、作弊、串通、禁止竞赛的人、不许可进入或以其他方式使用停车设施的车辆或人等)。

[0095] 类似于停车设施业务操作和娱乐场监视，本技术的各实施方案可以被应用于可以享受所公开的系统和方法的益处的垂直行业，所述所公开的系统和方法可以自动地记录、跟踪、分析以及核阅数据而无需人督管对于执行交易和聚集以及利用可采取行动的情报以提高业务操作和客户体验的核阅。例如，一些实施方案可以与安全数据集(可能存储在私人区块链上)接合以获得关于个人的生物统计或数据。这样，政府机关(例如，ICE或国土安全部)可以提供可以用来识别个人的数据并且可以确定是否应授予他们对特定的数据、活动和/或位置的访问。例如，系统的各实施方案可以用来为受信任旅行者计划(trusted traveler program)筛选个人。例如，当个人进入机场时，监控摄像机可以收集可以由人工智能或机器学习引擎摄取的视频数据。此数据可以与牌照、旅行记录、生物统计数据等相联系，以最初识别个人并且确定违反行为是否正在进行、对人进行预筛选(例如，为了更快速筛选)或确定是否可以拒绝用户进入飞机或其他旅行方式。在一些实施方案中，每个人可以使其驾驶执照被扫描，并且系统可以自动地将识别分类为合法的或欺诈的，并且在区块链

中搜索记录以帮助做出决定。

[0096] 图3例示了根据本技术的各实施方案的利用分布式账本架构的区块链数据平台的各种部件。如图3中所例示的，该区块链数据平台可以使用一个或多个服务器305A-305N。每个服务器可以包括区块链接口310、监视机构315、客户端接口320、规则引擎325、加密/解密模块330、分析模块335、事件模块340、多因素认证模块350、报告生成器355、和/或用于存储日志、订户策略、交易策略、位置策略等的数据库360和/或365。另外，区块链服务器305A-205N可以与区块链370、客户端375、受信任数据源380和/或记录385连接。

[0097] 这些模块、部件或数据库中的每个可以被体现为专用硬件(例如，一个或多个ASICS、PLD、FPGA等)，或被体现为用软件和/或固件适当地编程的可编程电路(例如，一个或多个微处理器、微控制器等)、或被体现为专用硬件和可编程电路的组合。本技术的其他实施方案可以包括这些模块和部件中的一些、全部或没有一个、以及其他模块、应用程序、数据库和/或部件。再者，一些实施方案可以将这些模块和部件中的两个或更多个并入到单个模块中，和/或将这些模块中的一个或多个的功能的一部分与不同的模块相关联。例如，在一个实施方案中，规则引擎325和事件模块340可以被组合成单个模块，用于在用户终端上识别和执行各种规则和事件策略。

[0098] 客户端375可以使用客户端接口320连接到区块链服务器305A-305N中的一个。客户端375可能能够从区块链服务器305A-305N下载(或已经预安装)固件或软件，该固件或软件允许客户端375输入并且查看区块条目(或其被选择的部分)。区块条目可以包括各种各样的交易(例如，财务交易、客户使用历史和停车库中的服务偏好、游戏投入、医疗记录、库存跟踪等)和各种各样的访问级别(私人的、许可的、公共的等)。在一些实施方案中，区块链服务器305A-305N处理加密代码以验证查看每个交易的一个或多个部分的访问。

[0099] 在一些实施方案中，区块链服务器305A-305N可以维护用于区块条目中的多个部分中的每个的指针，该指针指示用于区块条目中的多个部分中的每个的至少一个公布位置。然后可以通过使用用于区块条目中的部分中的每个的指针来检索与访问级别相关联的部分以生成区块条目的定制视图。在其他实施方案中，区块链服务器305A-305N可以维护用于与访问级别中的每个相关联的数据部分的单独的区块条目。区块链服务器305A-305N可以用区块链370的区块条目评估请求中的访问代码以识别与访问级别相关联的数据部分。在一些场景中，区块链服务器305A-305N可以维护用于与访问级别中的每个相关联的数据部分的单独的区块链。区块链服务器305A-305N然后可以用区块链370评估请求中的访问代码以识别与访问级别相关联的数据部分。

[0100] 在一些示例中，可以使用加密/解密模块330来加密存储在区块链370中的信息。在一些实施方案中，加密/解密模块330可以使用各种非同态加密和/或同态加密。虽然非同态加密可以提供更强的安全属性，但是同态加密的使用将允许对编码数据进行计算而无需解密。因此，停车设施和客户的车辆的各种部件或游戏系统的各种部件可以在数据部分上交互和操作而不暴露敏感数据。

[0101] 监视机构315可以监视交易和用户活动。这可以包括从外部源接收信息。在停车设施示例中，所述外部源包括人、设备或系统，诸如，使用用于停车设施的智能电话应用程序的客户、使用各种业务信息技术系统和客户端设备的设施管理人员和工作人员、用于蓝牙®或其他无线信号的接收器、摄像机或其他成像设备，以及收集用于识别该车辆、其

驾驶员并且可能还识别其驾驶员和乘客的数据的诸如门和访问设备读取器的访问控制系统。停车设施情况中的附加的外部数据源可以包括收集用于监视停车设施中的停车位的可用性状态(例如,占用与未占用)的数据的诸如运动、重量、距离或接近感测设备的传感器。在娱乐场示例中,所述外部源包括人、设备或系统,诸如但不限于客户端375、视频监控系统、忠诚卡系统、密钥引擎、生物统计传感器和其他外部系统。在一些实施方案中,可以在允许用户进入或访问货币交易、停车预留、用于停车的支付方法、停车历史、车辆、驾驶员和乘客个人识别信息、医疗记录、游戏投入、库存活动日志等之前使用多因素认证。

[0102] 例如,当停车设施客户经由智能电话应用程序访问其信用/借记卡的记录或核查用于停车支付的账户时,多因素认证模块350可以被用来要求两种不同类型的认证(例如,口令加上通过到与客户的账户注册数据相关联的电话号码的文本消息或电话呼叫传输到客户的字母数字代码)。作为另一个示例,当患者访问医疗记录时,多因素认证模块350可以被用来要求各种类型的认证(例如,个人个人识别码、生物统计、令牌等)。规则引擎325可以将规则叠加在正在呈现在客户端375上的交易界面上。这些规则可以基于存储在数据库365中的各种策略(例如,订户策略、交易策略、位置策略等)。分析模块335可以生成关于停车位使用趋势、层、客户端、游戏、医疗诊断、工资单、包裹递送、支出、账户和/或其他系统部件或活动的各种分析。此信息可以由报告生成器355使用以创建交易的定制视图。

[0103] 受限访问模块340可以被用来针对每个交易中的数据的不同的部分和针对不同的用户/用户类型创建定制访问要求。奖励可以存储在区块链370内、在记录385中。访问要求可以通过用户输入交易生成、基于先前指定的用户偏好确定、或通过其他方所要求的策略(例如,1996年的Health Insurance Portability and Accountability Act(HIPAA)所要求的针对医疗记录的许可访问、针对竞赛最低年龄的州法律等)确定,并且基于那些访问策略呈现记录的定制视图。数据库360和/或365可以被用于存储日志、订户策略、交易策略、位置策略等。这些可以是从与区块链370相关联的记录385检索的数据的本地存储器。另外,服务器305A-305N和区块链370可以与受信任数据源380连接,用于验证确定记录385内存储的数据所需的外部事件(例如,体育事件的结果、卖家/买方日记条目的对账等)或信息(例如,除了停车设施的注册用户以外的授权驾驶员,该注册用户已授权该授权驾驶员使用他们的停车账户、或安全调查的状态)。

[0104] 图4例示了停车设施400,对于该停车设施,可以至少部分地使用所公开的系统和方法来实现相关业务操作。停车设施400具有至少一个入口402和至少一个出口404。访问控制和支付门户控制台422定位在停车设施400的入口402和出口404处。在一些实施方案中,控制台422被划分为至少两个单独的并且不同的结构。例如,用于访问控制的第一控制台422定位在入口402处,并且用于支付处理的第二控制台422定位在出口404处。无论如何,控制台422的访问控制功能可以例如通过自动地可致动的进入门424和外出门426来实现。

[0105] 停车设施400包含位于道路表面406上的多个停车位408。停车位408中的每个可以用数字、字母或字母数字识别符标记,所述识别符诸如被描画在道路表面406上或被标志在位于车位408处或接近车位408的邻近的墙壁、栅栏或护栏上。在任何给定的时间,停车位408中的至少一部分可能被车辆(例如,第一车辆410)占用。其内未停放车辆的车位408自然可用于客户停放他们的车辆。在一个示例中,多个车位408中的每个车位408包括用于监视每个车位408的状态——如在停车设施400中目前被占用或目前可用——的传感器418或其

他设备。在一些实施方案中，多个这样的传感器418或其他设备中的一个定位在设施400中，并且被配置为监视至少两个车位408的可用性状态。

[0106] 传感器418可以包括接近传感器，所述接近传感器定位在道路表面406上、位于由相应的停车位408限定的区域内(例如，在其中心)。在一些实施方案中，接近传感器可以定位在斜坡、水平面、天花板、墙壁或邻近停车位408的其他结构上。无论如何，用于监视停车位408可用性状态的传感器418或其他设备被配置为连续地或周期性地传输表示相应的单个车位408或有限一组(例如，若干个)车位408是否被车辆占用的数据。这样，由传感器418传输的数据进一步表示特定的停车位408识别符和其可用性状态并且与之相关联。例如，第一车辆410目前停放在车位408中，并且至少若干个多个车辆也停放在被占用的车位416(图4中由“X”表示)。同时，至少若干个车位408当前未被车辆占用，如图4中由在道路表面406上可见的可用的车位414的相应的传感器418所示出的。在这些目前可用的车位414中有一个车位408，第二车辆412最近从该车位出发离开停车设施400。

[0107] 停车设施400的当前的或可能的客户可以在到达停车设施400之前查看可用的停车位414的库存。由传感器418提供的数据被记录在区块链中，并且可以被实时地或接近实时地传达到包括客户、工作人员和管理人员的用户，以使得可以及时地做出明智的决定。设施400中的停车位408的可用性状态的定制视图可以经由个人计算机、智能电话或其他合适的计算设备的显示器提供给客户。在一些实施方案中，停车位408可用性数据可以包括关于一个或多个停车位是否可以被保留以供客户在询问的同一天的稍后时间或在稍后某一天使用的所述一个或多个停车位的状态。因此，停车系统运营商以及其客户可以采用所公开的系统和方法，以便于每小时、每天或每月停车的相关交易和方便体验。

[0108] 例如，除了由传感器418提供的停车位可用性数据之外或代替由传感器418提供的停车位可用性数据，客户可以将他们的车辆或个人识别信息和他们的用于智能电话应用程序的账户注册数据包括在一起。车辆信息可以包括牌照440号码或车辆识别号码(VIN)，而生物统计或个人信息可以包括与停车账户注册相关联的驾驶员或乘客的肖像图像或用于获得进入停车设施400的访问设备(例如，钥匙卡或钥匙坠)的ID号码。

[0109] 访问控制和支付控制台422可以包括用于检测或以其他方式聚集车辆和个人识别信息中的一个或两个的一个或多个传感器或其他设备。例如，控制台422可以包括定位在车辆的一部分的视野中的射频接收器428，在该车辆上放置了对应的射频发射器或应答器432以用于在停车设施400中使用。发射器432被配置为发射无线信号，所述无线信号对唯一地识别车辆或其所有者或授权的用户的数据进行编码。发射器432也可以采用由停车客户携带的钥匙坠或钥匙卡的形式，并且在进入停车设施400时被手动地定位在接收器428的视野中。在任一种情况下，像前述传感器418一样，接收器428是记录在区块链中的停车业务操作相关的数据的外部源。接收器428可以在这些数据被记录在区块链中之前将这些数据中继到中间发射器或处理器，或接收器428可以将这些数据直接中继或以其他方式传输到执行将数据记录到区块链的计算和通信系统。

[0110] 在另一个示例中，控制台422包括摄像机420或其他成像设备，所述摄像机或其他成像设备在车辆接近控制台422定位时定位在车辆的挡风玻璃或侧窗的视野中。由摄像机420获取的静止图像或视频流可以被传输到本地或远程计算系统或服务器以用于进行图像处理分析。在停车客户已经先前提供了肖像图像作为记录在区块链上的账户注册数据的一

部分的情况下，图像处理分析可以被用来通过使用本领域技术人员已知的一个或多个面部识别技术来确定进入的车辆的驾驶员或乘客的身份。附加地或代替地，摄像机420可以定位在控制台422上，并且被配置为获取进入的车辆的牌照440和车辆识别号码中的至少一个的图像。这样的图像数据可以通过已知的字母和数字字符识别技术传输到本地或远程计算系统或服务器以用于进行图像处理分析，以确定车辆和与其相关联的停车客户的身份。在一些实施方案中，由摄像机420获取的图像或视频数据被使用，以使用肖像照片、生物统计、移动电话、牌照440号码和车辆识别号码中的两个或更多个来确定车辆和客户身份。例如在与注册肖像图像相比客户的面部外貌随时间改变的情况下，如由于自然老化、太阳晒黑或晒伤、戴着帽子、带妆、戴着假发、戴着眼镜、戴着有色隐形眼镜、戴着围巾或口罩以及生长面部毛发，使车辆和客户身份的确定基于不同于完整或部分面部图像的源或除了完整或部分面部图像以外的源可能对客户和停车设施400运营商是有利的。

[0111] 为了车辆进入停车设施400，对照区块链中记录的客户账户注册数据验证由接收器428和/或摄像机420获取的数据。在成功的用以核实客户和其车辆与声誉良好的停车账户相关联的验证过程后，进入门424被自动升起，并且任何其他访问控制设备(例如，能够刺穿轮胎的有尖的轨)被解除足够的时间，以许可车辆驾驶通过入口402并且到由道路表面406限定的主要停车区域上。在一个优选的实现中，当车辆驾驶员的车辆仍然静止在入口402处时(例如，恰好在进入门424被升起之前)，车辆驾驶员将接收到消息，所述消息通知他们最近的可用停车位414，或根据他们的预先记录的客户偏好确定的另一个可用停车位414。在一个示例中，定位在驾驶员的视野中的控制台420上的显示器或LED灯阵列显示可用的车位414的相应的识别符。在另一个示例中，以一音量级别从控制台420的扬声器大声读出可用的车位414识别符，所述音量级别足以使驾驶员透过关闭的玻璃窗听到并且考虑了停车设施400的典型背景噪声。

[0112] 包括车辆进入的一天中的时间和日期的时间戳可以与车辆和/或相应的客户的身份相关联地记录在区块链中。时间戳数据便于确定在客户从停车设施离开时要从客户索取和收取的停车费用。在包括停车设施400的订阅停车使用(例如，每周或每月)的使用实例中，将时间戳数据记录在区块链中便于客户和运营商根据需要对使用数据进行趋势预测和分析。

[0113] 所公开的系统和方法同样在车辆(例如，第二车辆412)离开设施400的过程期间便于提高的停车设施400业务操作和客户体验。接收器428、发射器432和摄像机420各自可以被单独地或以任何组合使用，如上文所描述的，以在到达出口404和离开停车设施400之前识别在控制台422处或接近控制台422的车辆或客户。在确定车辆或客户身份后，这些数据以及它们的相关联的时间戳被记录在区块链中。在预付订阅停车账户计划的情况下，在确定和验证车辆412或其相关联的客户后，外出门426被自动升起，并且任何其他访问控制设备(例如，能够刺穿轮胎的有尖的轨)被解除足够的时间，以许可车辆驾驶通过出口402并且自停车设施400离开。在该情况下，由于账户在预付停车订阅下，因此不需要执行支付处理。然而，在非订阅账户的情况下，必须在支付处理之前执行前述对车辆和客户身份的识别和验证。

[0114] 为了在要求支付处理(例如，每小时或每天停车)的情况下改进与离开停车设施400相关联的业务操作和客户体验，由接收器428和摄像机420中的至少一个获取的数据可

以被再次记录在区块链中，并且被用于根据停车费用、进入和外出时间戳和客户支付信息(例如，信用/借记卡账户、数字钱包或加密货币钱包)进行自动、快速和安全的支付处理，所述停车费用、进入和外出时间戳和客户支付信息中的每个也记录在区块链中。因此，在这样的情况下，在车辆和相关联的客户的识别和验证以及应付支付的成功完成后，外出门426被自动升起，并且任何其他访问控制设备被解除足够的时间，以许可车辆驾驶通过出口402并且自停车设施400离开。在一些实施方案中，控制台422可以包括如下设备和子系统：所述设备和子系统用于经由收入控制装备或移动电话(mobile)或应用程序或Dapp接受使用现金、信用/借记卡或用于真实或加密货币的数字钱包的手动支付。在一个示例中，控制台422包括定位成停在外出门426之前的车辆412的驾驶员够得着的支付接受设备430(诸如信用/借记读取器或现金/硬币计数器)和显示设备434。例如，不具有向停车设施400预先注册的账户的客户仍然可以交付停车支付以便离开设施400。即使对于这样的非注册客户，也可以通过利用区块链的所公开的系统和方法提高业务操作和客户体验，例如，通过使能驾驶员或车辆识别、基于由摄像机420获取的数据自动地计算用于费用确定的经过时间、以及在显示设备434上向驾驶员显示相关的支付指令和其他有用的信息。

[0115] 停车设施400中的收入控制装备可以包括前述的控制台422和诸如摄像机420、接收器428和传感器418的相关联的设备和子系统。附加地或代替地，停车设施400收入控制装备可以包括具有信用卡/账单接受器/移动支付能力的停车收费亭(kiosk)，以运行并且允许人进入/离开。停车收费亭可以集成到控制台422中，或它们可以是定位在设施400中的各种其他方便位置的独立运行的设备。收入控制控制售票、访问控制、访问卡、费用、税务、统计和分析、性能、停车控制(访问门，例如，424、426)、审查功能、网络和移动支付界面、打印机等。

[0116] 在一些实施方案中，以自动驾驶车辆体现的或包括自动驾驶车辆的停车设施400的客户可以由附加的设施400子系统导引，使得这些车辆在进入后可以安全停放它们自己，并且同样地在离开设施400之前或之后返回到指定位置。在图4的所例示的实施方案中，传感器418包括用于将归航信号发射到自动驾驶车辆中的对应的接收器的信标。信标信号与车辆中的接收器配对，并且在使得自动驾驶车辆能够进入设施400并且具有指派给它的可用的车位408的停车交易完成后生成。自动驾驶车辆还可以包括提供车辆识别的应答器或其他设备，所述车辆识别允许访问控制，并且对该汽车、公司、车辆的所有者等是唯一的。在自动驾驶车辆用户情况下，用于识别自动驾驶车辆的装置可以是发射器、应答器、牌照440识别、牌照440身份等中的一个或多个，使得能够在没有人参与的情况下进入和离开。在一个示例中，在非订阅停车账户的情况下，可以在支付处理之前执行车辆和客户身份的前述识别和验证。

[0117] 在一些实施方案中，停车设施400的一个或多个车位408包括电动车辆充电站436。充电站436可以被配置用于电动车辆的有线和无线充电的任一个或两个。充电站436可以包括用于识别利用在由相应的车辆占用的车位408中的充电站436的车辆或客户的设备和子系统。在一个示例中，在其车辆内或在其车辆上具有发射器432的注册客户可以被用来将充电使用统计(例如，接通/断开时间或递送到电动车辆的充电能量)与客户的关于停车设施400的账户相关联。这些充电站436相关数据可以被记录在区块链中，并且用于充电站436的使用的应付支付可以被自动地确定并且从记录在区块链中的客户的支付证书中扣除。用于

如电动车辆充电等的辅助服务的此支付过程可以在完成充电站436的使用后被发起和完成，或可以被添加到用于在离开停车设施400之前完成支付的上文描述的过程。根据所公开的系统和方法，本领域的普通技术人员可以容易地设想除了充电站436的使用之外的辅助服务(例如，挡风玻璃和其他车辆维护/维修服务、洗车、美容、干洗机、宠物寄宿等)在业务操作效率和客户体验改进方面如何可以类似地受益。

[0118] 通过所公开的系统和方法的应用，经由将车辆和其所有者与停车位和任何被选择的其他服务相关联并且将与交易数据相联系的信息存储在区块链上，进一步增强了停车操作以及这样的辅助服务的便利性和效率。客户和运营商经由定制视图可以容易地获得这些数据。如上文所描述的，通过在区块链上收集和存储诸如牌照440识别、牌照440身份的数据，以及使用摄像机420、传感器418、发射器432、信标、应答器、蓝牙、NFC等来便于身份管理。

[0119] 在一些实施方案中，根据所公开的系统和方法，停车设施400可以向其客户提供会员计划，以用于在进行停车预留、进行交易、订阅周期停车计划等时进行签约。本技术的区块链和定制视图可以被用来便于会员的奖励计划。在停车业务背景下，可以向达到某些里程碑如作为会员的时间或花费的美元的客户提供的奖励包括例如并且不限于免费洗车、免费停车日或其他特殊待遇。奖励还将与相应的客户相关联，并且在区块链上被记录和跟踪。奖励对于公司或个人可以是可得的。这样的奖励计划可以以类似于航空公司英里里程计划的方式为客户和停车设施运营商的利益而起作用。

[0120] 图5例示了用于停车设施业务操作和包括支付处理的交易的用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图500。块图500包括库存区块条目501、数据平台510、服务器520-522、区块链530-532和记录502。

[0121] 区块条目501表示将永久地记录到区块链中的任何数据交易，诸如从客户、连接的设备、停车设施400、运营商和工作人员以及外部源(例如，传感器418、接收器428和摄像机420)接收和记录的那些数据。区块条目501随后由矿工处理，并且通过数据平台510添加到区块链末尾的区块。区块条目501还包括本文已经由停车位、停车设施客户和停车费用表示的数据部分。停车位维护停车设施400中的停车位408的库存和可用性状态。停车设施客户包括与和客户相关联的车辆、驾驶员以及可能地还有乘客的识别符相关的数据，以及他们的账户和支付相关数据。停车费用包括指定在停车设施400中停车的费用的数据，包括按小时、按周或按月。应注意，虽然数据部分中的每个被单独地表示，但是数据部分是由区块条目501表示的一个交易的一部分。区块条目501可以包括出于进行停车设施400操作的目的已经在分布式账本平台环境中执行和记录的任何交易或合同。在此示例中，区块条目501可以包括客户的使用停车设施中的停车位的订单、预留或自发采购请求。在一些实施方案中，令牌可以替代地或代替地包括客户的使用停车设施中的停车位的订单、预留或自发采购请求中的一个或多个。

[0122] 数据平台510表示能够托管区块链应用程序的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。数据平台510提供了一种用于将停车交易和停车位可用性状态记录到区块链中的安全的分布式账本系统。数据平台510可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、监管当局、客户、公司雇员、停车设施400所有者、停车审查员、管理人员和工作人员、营销公司、广告商等的各种各

样的用户访问。

[0123] 数据平台510还可以包括服务器520-522。服务器520-522可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以使用包括例如并且不限于5G、WIFI、NFC、miracast等的通信协议向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。前述的传感器和访问控制或支付处理设备和系统可以自动地将交易或业务操作数据传送到网络节点，如上文参考图3和图4所描述的。在一些实施方案中，数据平台510可以动态地选择授权哪些服务器520-522存储数据。例如，公司或政府可能对其上存储区块链的服务器节点具有地理限制、加密标准、网络安全标准或其他限制。因此，数据平台510可以基于这些限制管理动态地被选择的服务器的物流。例如，如果一个特定的服务器被认为受到攻击或被非法入侵，则数据平台510可以从区块链网络动态地移除该服务器，并且如果需要，则考虑添加一个或多个附加服务器。这样，数据的每个所有者可以设置应将数据存储在哪里的选择准则和该服务器组所需的最低IT标准。

[0124] 块图500还包括区块链530-532。区块链530-532可以包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链530-532中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，每个数据部分(车位、客户和费用)已经被单独地记录到不同的区块中并且在单独的区块链530-532中。

[0125] 另外，区块链530-532中的每个与单独的访问级别相关联。例如，区块链530是公共访问区块链，该公共访问区块链允许与分布式账本交互的任何用户查看区块和存储在每个区块中的数据部分。公共用户可以是对查看区块链530中的可用于交易的一个或多个停车设施中的停车位感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，区块链531是数据部分仅可以由诸如内部公司人员的经授权的用户访问和查看的私人区块链。在此示例场景中，客户已经被单独地存储在区块链531上，并且对除了对数据具有独占访问的用户(诸如，发起交易的公司内的经理)之外的在区块链网络中交互的所有用户是私人的。区块链532是许可区块链，这意味着有限的一组各方但不是全部用户可以查看记录在区块中的数据部分。费用已经存储在区块链532内，并且可以由被允许访问数据的各方(诸如，审查员或控制者)查看。

[0126] 记录502例示了当请求查看存储在区块条目501中的交易数据时用户可以查看的内容。记录502可以包含最初输入在区块条目501中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0127] 图6例示了用于停车设施400业务操作和客户使用的用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程600的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0128] 在操作中，数据平台510接收待在区块链530-532的区块中维护的区块条目501(步骤601)。区块条目501在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台510然后授权条目(例如，矿工验证区块中的散列)(步骤602)。如果区块未被验证，则交

易(区块条目501)被拒绝(步骤603)。然而,如果区块被接受,则评估数据部分中的每个的访问级别,并且基于所识别的访问级别将数据部分中的每个添加到区块链530-532中的每个中的区块(步骤604)。

[0129] 在下一个操作中,数据平台510接收查看区块条目的一个或多个数据部分的请求,其中该请求包括与至少一个访问级别相关联的访问代码(步骤605)。访问代码可以与公共、许可或私人访问级别相关联。数据平台510然后用区块链530-532中的每个评估请求中的访问代码,区块链530-532中的每个维护用于每个数据部分的每个单独的区块记录(步骤606)。如果确定与请求用户相关联的访问代码是公共的,则将为请求用户生成仅指示来自区块条目501的车位的定制视图(例如,记录502)(步骤607)。如果确定与请求用户相关联的访问代码是许可的,则将为请求用户生成指示来自区块条目501的车位和费用的定制视图(步骤608)。如果确定与请求用户相关联的访问代码是私人的,则将为请求用户生成指示来自区块条目501的所有数据部分(即,车位、客户和费用)的定制视图(步骤609)。

[0130] 在一些实施方案中,区块条目501还记录与停车设施交易相关的附加数据,诸如客户从其发起交易的位置和所涉及的停车设施400、交易和车辆进入设施400和从设施400离开的时间和日期戳、以及车辆进入设施400、离开设施400和在设施400附近移动的照片和/或视频。在一个示例中,除了被存储在区块条目501中之外,这样的成像还可以包括到定位在停车设施400处或远离停车设施400定位的安全监视站的实时流媒体。附加地或代替地,在车库或停车设施/停车场中,作为安全措施,摄像机可以监视停车设施400中的车辆的运动,并且作为安全措施,摄像机可以将这些数据存储在区块条目501和/或其他地方。出于安全目的,这些成像系统可以被集成在传感器418中或与传感器418共同定位。例如,在停放的车辆在车辆的停车设施400停留的预期时间表之外表现出运动的情况下,可以发起运动监视和成像安全协议。

[0131] 图7例示了用于酒店业务操作和包括支付处理的交易的用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图700。块图700包括库存区块条目701、数据平台710、服务器720-722、区块链730-732和记录702。

[0132] 区块条目701表示将被永久地记录到区块链中的任何数据交易,诸如从酒店客人、连接的设备、酒店、运营商和工作人员以及外部源(例如,钥匙卡读卡器、忠诚卡等)接收和记录的那些数据。区块条目701随后由矿工处理,并且通过数据平台710添加到区块链末尾的区块。区块条目701还包括本文已经由酒店房间、酒店客人和房间费用表示的数据部分。酒店房间维护酒店中的酒店客房的库存和可用性状态。酒店客人包括与以其姓名注册酒店房间的客人以及还可能与和注册客人相关联的其他客人的识别符相关的数据,以及他们的账户和支付相关的数据。房间费用包括指定停留在酒店房间的费用的数据,包括按夜。应注意,虽然数据部分中的每个被单独地表示,但是数据部分是由区块条目701表示的一个交易的一部分。区块条目701可以包括出于进行酒店操作的目的已经在分布式账本平台环境中执行和记录的任何交易或合同。在此示例中,区块条目701可以包括客户的使用酒店中的酒店房间或相关商品和服务的订单、预留或自发采购请求。在一些实施方案中,令牌可以替代地或代替地包括客户的使用酒店中的酒店房间或相关商品或服务的订单、预留或自发采购请求中的一个或多个。

[0133] 数据平台710表示能够托管区块链应用程序的任何一个或多个计算系统,其中图

28中的控制器2800是代表性的。数据平台710提供了一种用于将酒店交易和房间可用性状态记录到区块链中的安全的分布式账本系统。数据平台710可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、监管当局、客人和其他酒店客户、酒店雇员、酒店所有者、酒店审查员、管理人员和工作人员、营销公司、广告商等的各种各样的用户访问。

[0134] 数据平台710还可以包括服务器720-722。服务器720-722可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以使用包括例如并且不限于5G、WIFI、NFC、miracast等的通信协议向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。酒店房间钥匙卡读取器、忠诚卡接收器和包括传感器和访问控制或支付处理设备和系统的其他有用的设备和子系统可以自动地将交易或业务操作数据传送到网络节点，如上文参考图3所描述的。在一些实施方案中，数据平台710可以动态地选择授权哪些服务器720-722存储数据。例如，公司或政府可能对其上存储区块链的服务器节点具有地理限制、加密标准、网络安全标准或其他限制。因此，数据平台710可以基于这些限制管理动态地被选择的服务器的物流。例如，如果一个特定的服务器被认为受到攻击或被非法入侵，则数据平台710可以从区块链网络动态地移除该服务器，并且如果需要，则考虑添加一个或多个附加服务器。这样，数据的每个所有者可以设置应将数据存储在哪里的选择准则和该服务器组所需的最低IT标准。

[0135] 块图700还包括区块链730-732。区块链730-732可以包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链730-732中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，每个数据部分(房间、客人和费用)已经被单独地记录到不同的区块中并且在单独的区块链730-732中。

[0136] 另外，区块链730-732中的每个与单独的访问级别相关联。例如，区块链730是公共访问区块链，该公共访问区块链允许与分布式账本交互的任何用户查看区块和存储在每个区块中的数据部分。公共用户可以是对查看区块链730中的可用于交易的一个或多个酒店中的酒店房间感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，区块链731是数据部分仅可以由诸如内部公司人员的经授权的用户访问和查看的私人区块链。在此示例场景中，客人已经被单独地存储在区块链731上，并且对除了对数据具有独占访问的用户(诸如，发起交易的公司内的经理)之外的在区块链网络中交互的所有用户是私人的。区块链732是许可区块链，这意味着有限的一组各方但不是全部用户可以查看记录在区块中的数据部分。费用已经存储在区块链732内，并且可以由被允许访问数据的各方(诸如，审查员或控制者)查看。

[0137] 记录702例示了当请求查看存储在区块条目701中的交易数据时用户可以查看的内容。记录702可以包含最初输入到区块条目701中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0138] 图8例示了用于酒店业务操作和客人使用的用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程800的步骤中的一些或全部可以在用来

执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0139] 在操作中，数据平台710接收待在区块链730-732的区块中维护的区块条目701(步骤801)。区块条目701在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台710然后授权条目(例如，矿工验证区块中的散列)(步骤802)。如果区块未被验证，则交易(区块条目701)被拒绝(步骤803)。然而，如果区块被接受，则评估数据部分中的每个的访问级别，并且基于所识别的访问级别将数据部分中的每个添加到区块链730-732中的每个中的区块(步骤804)。

[0140] 在下一个操作中，数据平台710接收查看区块条目的一个或多个数据部分的请求，其中该请求包括与至少一个访问级别相关联的访问代码(步骤805)。访问代码可以与公共、许可或私人访问级别相关联。数据平台710然后用区块链730-732中的每个评估请求中的访问代码，区块链730-732中的每个维护用于每个数据部分的每个单独的区块记录(步骤806)。如果确定与请求用户相关联的访问代码是公共的，则将为请求用户生成仅指示来自区块条目701的房间的定制视图(例如，记录702)(步骤807)。如果确定与请求用户相关联的访问代码是许可的，则将为请求用户生成指示来自区块条目701的房间和费用的定制视图(步骤808)。如果确定与请求用户相关联的访问代码是私人的，则将为请求用户生成指示来自区块条目701的所有数据部分(即，房间、客人和费用)的定制视图(步骤809)。

[0141] 在一些实施方案中，区块条目701还记录与酒店房间交易相关的附加数据，诸如客户从其发起交易的位置和所涉及的酒店建筑物、交易和客人和/或其车辆进入和离开酒店的时间和日期戳、以及客人和或其车辆进入酒店、离开酒店和在酒店附近移动的照片和/或视频。在一个示例中，除了被存储在区块条目701中之外，这样的成像还可以包括到定位在酒店建筑物处或远离酒店建筑物定位的安全监视站的实时流媒体。附加地或代替地，为了客人和酒店工作人员成员的利益，作为安全措施，摄像机可以监视在酒店中和周围的客人和/或其车辆的运动，并且作为安全措施，摄像机可以将这些数据存储在区块条目701和/或其他地方。出于安全目的，这些成像系统可以被集成在诸如房间钥匙读取器的设备以及停车、游泳池、健身中心、娱乐场和酒店的其他设施的进入和离开通道中或与所述设备以及所述进入和离开通道共同定位。例如，在除了注册客人之外的人试图获得进入意在仅由注册的酒店客人使用的客人房间或酒店的其他区域的情况下，可以发起运动监视和成像安全协议。

[0142] 图9例示了用于自动驾驶车辆车队业务操作和包括支付处理的交易的用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图900。块图900包括库存区块条目901、数据平台910、服务器920-922、区块链930-932和记录902。

[0143] 区块条目901表示将被永久地记录到区块链中的任何数据交易，诸如从请求乘车的乘客、连接的设备、自动驾驶车辆车队经理和工作人员以及外部源(例如，GPS收发器、钥匙坠、忠诚卡等)接收和记录的那些数据。区块条目901随后由矿工处理，并且通过数据平台910添加到区块链末尾的区块。区块条目901还包括本文已经由车辆ID、乘客和乘车价格或费用表示的数据部分。车辆ID维护一个地理区域中的自动驾驶车辆的库存和可用性状态。乘客包括与以其姓名请求所识别的自动驾驶车辆的乘客的识别符相关的数据，以及他们的账户和支付相关数据。在一些实施方案中，乘客还包括识别乘客的请求的目的地的数据。费用包括指定乘客利用自动驾驶车辆的费用的数据。在一些实施方案中，待收取的费用基于

从乘客的当前位置到请求的目的地的英里里程。应注意，虽然数据部分中的每个被单独地表示，但是数据部分是由区块条目901表示的一个交易的一部分。区块条目901可以包括出于进行自动驾驶车辆车队操作的目的已经在分布式账本平台环境中执行和记录的任何交易或合同。在此示例中，区块条目901可以包括乘客的使用自动驾驶车辆或自动驾驶车辆车队运营商的相关服务的订单、预留或自发打车(ride hailing)请求。在一些实施方案中，令牌可以替代地或代替地包括乘客的使用自动驾驶车辆或自动驾驶车辆车队运营商的相关服务的订单、预留或自发打车请求中的一个或多个。

[0144] 数据平台910表示能够托管区块链应用程序的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。数据平台910提供了一种用于将自动驾驶车辆车队交易以及自动驾驶车辆位置和可用性状态记录到区块链中的安全的分布式账本系统。数据平台910可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、监管当局、乘客和其他自动驾驶车辆车队客户或服务提供者、车队雇员、车队所有者、车队审查员、管理人员和工作人员、营销公司、广告商等的各种各样的用户访问。

[0145] 数据平台910还可以包括服务器920-922。服务器920-922可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以使用包括例如并且不限于5G、WIFI、NFC、miracast等的通信协议向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。车辆钥匙坠、钥匙卡读取器、忠诚卡接收器、以及包括位置(例如，GPS)传感器和访问控制或支付处理设备和系统的其他有用的设备和子系统可以自动地将交易或业务操作数据传送到网络节点，如上文参考图3所描述的。

[0146] 在一些实施方案中，数据平台910可以动态地选择授权哪些服务器920-922存储数据。例如，公司或政府可能对其上存储区块链的服务器节点具有地理限制、加密标准、网络安全标准或其他限制。因此，数据平台910可以基于这些限制管理动态地被选择的服务器的物流。例如，如果一个特定的服务器被认为受到攻击或被非法入侵，则数据平台910可以从区块链网络动态地移除该服务器，并且如果需要，则考虑添加一个或多个附加服务器。这样，数据的每个所有者可以设置应将数据存储在哪里的选择准则和该服务器组所需的最低IT标准。

[0147] 块图900还包括区块链930-932。区块链930-932可以包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链930-932中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，每个数据部分(车辆、乘客和费用)已经被单独地记录到不同的区块中并且在单独的区块链930-932中。

[0148] 另外，区块链930-932中的每个与单独的访问级别相关联。例如，区块链930是公共访问区块链，该公共访问区块链允许与分布式账本交互的任何用户查看区块和存储在每个区块中的数据部分。例如，公共用户可以是对查看区块链930中的可用于交易的当前可用于打车的车队中的自动驾驶车辆的当前位置，以及特定的车辆可能在任何时间点具有的任何使用限制感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，区块链931是数据

部分仅可以由诸如内部公司人员的经授权的用户访问和查看的私人区块链。在此示例场景中，乘客已经被单独地存储在区块链931上，并且对除了对数据具有独占访问的用户(诸如，发起交易的公司内的经理)之外的在区块链网络中交互的所有用户是私人的。区块链932是许可区块链，这意味着有限的一组各方但不是全部用户可以查看记录在区块中的数据部分。费用已经存储在区块链932内，并且可以由被允许访问数据的各方(诸如，审查员或控制者)查看。

[0149] 记录902例示了当请求查看存储在区块条目901中的交易数据时用户可以查看的内容。记录902可以包含最初输入到区块条目901中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0150] 图10例示了用于自动驾驶车辆车队业务操作和客人使用的用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程1000的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0151] 在操作中，数据平台910接收待在区块链930-932的区块中维护的区块条目901(步骤1001)。区块条目901在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台910然后授权条目(例如，矿工验证区块中的散列)(步骤1002)。如果区块未被验证，则交易(区块条目901)被拒绝(步骤1003)。然而，如果区块被接受，则评估数据部分中的每个的访问级别，并且基于所识别的访问级别将数据部分中的每个添加到区块链930-932中的每个中的区块(步骤1004)。

[0152] 在下一个操作中，数据平台910接收查看区块条目的一个或多个数据部分的请求，其中该请求包括与至少一个访问级别相关联的访问代码(步骤1005)。访问代码可以与公共、许可或私人访问级别相关联。数据平台910然后用区块链930-932中的每个评估请求中的访问代码，区块链930-932中的每个维护用于每个数据部分的每个单独的区块记录(步骤1006)。如果确定与请求用户相关联的访问代码是公共的，则将为请求用户生成仅指示来自区块条目901的车辆的定制视图(例如，记录902)(步骤1007)。如果确定与请求用户相关联的访问代码是许可的，则将为请求用户生成指示来自区块条目901的车辆和费用的定制视图(步骤1008)。如果确定与请求用户相关联的访问代码是私人的，则将为请求用户生成指示来自区块条目901的所有数据部分(即，车辆、乘客和费用)的定制视图(步骤1009)。

[0153] 在一些实施方案中，区块条目901还记录与自动驾驶车辆车队交易相关的附加数据，诸如乘客从其发起交易的位置和所涉及的车辆、交易和乘客和/或其被指派的车辆ID进入和离开相应的车辆的时间和日期戳、以及乘客进入被指派的自动驾驶车辆、离开被指派的自动驾驶车辆和由被指派的自动驾驶车辆运输的照片和/或视频。在一个示例中，除了被存储在区块条目901中之外，这样的成像还可以包括到定位在自动驾驶车辆车队的建筑物或设施处或远离自动驾驶车辆车队的建筑物或设施定位的安全监视站的实时流媒体。附加地或代替地，为了乘客和车队工作人员成员的利益，作为安全措施，摄像机可以监视载着乘客的自动驾驶车辆在到乘客的目的地途中的运动，并且作为安全措施，摄像机可以将这些数据存储在区块条目901和/或其他地方。出于安全目的，这些成像系统在车辆事故或涉及乘客或被指派的自动驾驶车辆的其他事件的情况下可能是有用的。在这种情况下，可以向警察或保险公司调查员提供定制视图，以为解决事件后问题提供有用的数据。

[0154] 图11例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个实现中的块图1100。块图1100包括库存区块条目1101、数据平台1110、服务器1120-1122、区块链1130-1132和记录1102。

[0155] 区块条目1101表示将被永久地记录到区块链中的任何数据交易。区块条目1101随后由矿工处理，并且通过数据平台1110添加到区块链末尾的区块。区块条目1101还包括本文已经由产品、买方和价格表示的数据部分。应注意，虽然数据部分中的每个被单独地表示，但是数据部分是由区块条目1101表示的一个交易的一部分。区块条目1101可以包括已经在分布式账本平台环境中执行和记录的任何交易或合同。在此示例中，区块条目1101可以包括用于库存的采购订单。

[0156] 数据平台1110表示能够托管区块链应用程序的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。数据平台1110提供了一种用于将交易记录到区块链中的安全的分布式账本系统。数据平台1110可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、游戏监管委员会、客户、公司雇员等的各种各样的用户访问。

[0157] 数据平台1110还可以包括服务器1120-1122。服务器1120-1122可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。在一些实施方案中，数据平台可以动态地选择授权哪些服务器1120-1122存储数据。例如，公司或政府可能对其上存储区块链的服务器节点具有地理限制、加密标准、网络安全标准或其他限制。因此，数据平台1110可以基于这些限制管理动态地被选择的服务器的物流。例如，如果一个特定的服务器被认为受到攻击或被非法入侵，则数据平台1110可以从区块链网络动态地移除该服务器，并且如果需要，则考虑添加一个或多个附加服务器。这样，数据的每个所有者可以设置应将数据存储在哪里的选择准则和该服务器组所需的最低IT标准。

[0158] 块图1100还包括区块链1130-1132。区块链1130-1132可以包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链1130-1132中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，每个数据部分(产品、买方和价格)已经被单独地记录到不同的区块中并且在单独的区块链1130-1132中。

[0159] 另外，区块链1130-1132中的每个与单独的访问级别相关联。例如，区块链1130是公共访问区块链，该公共访问区块链允许与分布式账本交互的任何用户查看区块和存储在每个区块中的数据部分。公共用户可以是对查看区块链1130中的交易感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，区块链1131是数据部分仅可以由诸如内部公司人员的经授权的用户访问和查看的私人区块链。在此示例场景中，买方已经被单独地存储在区块链1131上，并且对除了对数据具有独占访问的用户(诸如，发起交易的公司内的经理)之外的在区块链网络中交互的所有用户是私人的。区块链1132是许可区块链，这意味着有限的一组各方但不是全部用户可以查看记录在区块中的数据部分。价格已经存储在区块链1132内，并且可以由被允许访问数据的各方(诸如，审查员或控制者)查看。

[0160] 记录1102例示了当请求查看存储在区块条目1101中的交易数据时用户可以查看的内容。记录1102可以包含最初输入到区块条目1101中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0161] 图12例示了用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程1200的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0162] 在操作中，数据平台1110接收待在区块链1130-1132的区块中维护的区块条目1101(步骤1201)。区块条目1101在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台1110然后授权条目(例如，矿工验证区块中的散列)(步骤1202)。如果区块未被验证，则交易(区块条目1101)被拒绝(步骤1203)。然而，如果区块被接受，则评估数据部分中的每个的访问级别，并且基于所识别的访问级别将数据部分中的每个添加到区块链1130-1132中的每个中的区块(步骤1204)。

[0163] 在下一个操作中，数据平台1110接收查看区块条目的一个或多个数据部分的请求，其中该请求包括与至少一个访问级别相关联的访问代码(步骤1205)。访问代码可以与公共、许可或私人访问级别相关联。数据平台1110然后用区块链1130-1132中的每个评估请求中的访问代码，区块链1130-1132中的每个维护用于每个数据部分的每个单独的区块记录(步骤1206)。如果确定与请求用户相关联的访问代码是公共的，则将为请求用户生成仅指示来自区块条目1101的产品的定制视图(例如，记录1102)(步骤1207)。如果确定与请求用户相关联的访问代码是许可的，则将为请求用户生成指示来自区块条目1101的产品和价格的定制视图(步骤1208)。如果确定与请求用户相关联的访问代码是私人的，则将为请求用户生成指示来自区块条目1101的所有数据部分(即，产品、买方和价格)的定制视图(步骤1209)。

[0164] 用于流程图1200的另一个实现可以是在竞赛验证过程的背景下。例如，在大门槛获胜上下投入的用户可能要求来自娱乐场经理的批准。在此示例场景中，当投入的支出发生时，可能要求访问区块链中的用户的数据，以确保由娱乐场经理为用户批准投入。

[0165] 图13例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个替代实现中的块图。块图1300包括游戏投入区块条目1301、数据平台1310、服务器1320-1322、区块链1330、访问平台1340和记录1302。

[0166] 区块条目1301表示将被永久地记录到区块链中的任何数据交易。区块条目1301随后由矿工处理，并且通过数据平台1310添加到区块链末尾的区块。区块条目1301还包括本文已经由投入数额、信用卡号码和年龄表示的数据部分。应注意，虽然数据部分中的每个被单独地表示，但是数据部分是由区块条目1301表示的一个交易的一部分。区块条目1301可以包括已经在分布式账本平台环境中执行和记录的任何交易或合同。然而，在此示例中，区块条目1301包括竞赛投入。还应注意，虽然请求用户(诸如，不是投入的直接参与者的第三方观察者)可能能够查看区块链1330的一些数据，但是查看区块条目1301可能要求访问代码。访问代码可以呈生物统计验证的形式。

[0167] 数据平台1310表示能够托管区块链应用程序的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。数据平台1310提供了一种用于将交易记录到区块链中的安全的分布式账本系统。数据平台1310可以在众多分布式网络节点上实现，所述分布式网络

节点可以由诸如审查员、财务机构、游戏监管委员会、客户、公司雇员等的各种各样的用户访问。

[0168] 数据平台1310还包括服务器1320-1322。服务器1320-1322可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。

[0169] 块图1300还包括区块链1330。区块链1330包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链1330中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，每个数据部分(投入数额、信用卡号码和年龄)已经用单独的加密代码记录到区块链1330中。

[0170] 另外，与区块链1330中的每个数据部分相关联的每个加密代码与单独的访问级别相关联。例如，投入数额与公共访问加密代码相关联，该公共访问加密代码允许与分布式账本交互的任何用户查看区块中的数据部分。公共用户可以是对查看投入数额感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，信用卡号码与私人加密代码相关联，该私人加密代码仅可以由诸如内部会计部门的经授权的用户访问和查看。年龄与许可加密代码相关联，该许可加密代码可以由有限的一组各方但不是全部用户查看。例如，游戏委员会可以要求查看年龄，以确保所有玩家具有下竞赛投入的合法年龄。然而，其他玩家或投入的观察者可能不能够查看每个玩家的年龄。

[0171] 访问平台1340表示能够验证访问区块链条目数据的用户请求的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。访问平台1340在区块链1330中记录的数据部分与为请求用户生成记录1302之间提供安全的加密中介物。访问平台1340可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、游戏监管委员会、客户、公司雇员等的各种各样的用户访问。记录1302例示了当请求查看存储在区块条目1301中的交易数据时用户可以查看的内容。记录1302可以包含最初输入到区块条目1301中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0172] 图14例示了用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程1400的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0173] 在操作中，数据平台1310接收待在区块链1330的区块中维护的区块条目1301(步骤1401)。区块条目1301在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台1310然后授权条目(例如，矿工验证区块中的散列)(步骤1402)。如果区块未被验证，则交易(区块条目1301)被拒绝(步骤1403)。然而，如果区块被接受，则评估数据部分中的每个的访问级别，并且基于所识别的访问级别将数据部分中的每个添加到区块链1330(步骤1404)连同将加密代码添加到区块链1330(步骤1405)。

[0174] 在下一个操作中，数据平台1340接收查看区块条目的一个或多个数据部分的请求，其中该请求包括与至少一个访问级别相关联的加密代码(步骤1406)。加密代码可以与

公共、许可或私人访问级别相关联。数据平台1340然后用区块链1330中的数据部分中的每个评估请求中的加密代码(步骤1407)。如果确定与请求用户相关联的加密代码是公共的，则将为请求用户生成仅指示来自区块条目1301的投入数额的定制视图(例如，记录1302)(步骤1408)。如果确定与请求用户相关联的加密代码是许可的，则将为请求用户生成指示来自区块条目1301的投入数额和年龄的定制视图(步骤1409)。如果确定与请求用户相关联的加密代码是私人的，则将为请求用户生成指示来自区块条目1301的所有数据部分(即，投入数额、信用卡号码和年龄)的定制视图(步骤1410)。

[0175] 图15例示了用以生成记录到区块链中的受限交易的定制视图的增强型应用程序的一个替代实现中的块图。块图1500包括货币转移区块条目1501、数据平台1500、服务器1520-1522、区块链1530、访问平台1540和记录1502。

[0176] 区块条目1501表示将被永久地记录到区块链中的任何数据交易。区块条目1501随后由矿工处理，并且通过数据平台1510添加到区块链末尾的区块。区块条目1501还包括本文已经由交易各方、银行账户号码和可用资金表示的数据部分。应注意，虽然数据部分中的每个被单独地表示，但是数据部分是由区块条目1501表示的一个交易的一部分。区块条目1501可以包括已经在分布式账本平台环境中执行和记录的任何交易或合同。然而，在此示例中，区块条目1501包括将钱从一个用户的银行账户转移到另一个用户的银行账户的银行业务交易。

[0177] 数据平台1510表示能够托管区块链应用程序的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。数据平台1510提供了一种用于将交易记录到区块链中的安全的分布式账本系统。数据平台1510可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、游戏监管委员会、客户、公司雇员等的各种各样的用户访问。

[0178] 数据平台1510还包括服务器1520-1522。服务器1520-1522可以表示分布式网络节点可以与其通信的任何一个或多个计算系统。示例包括其上安装有对应的应用程序或服务的其他设备，使得用户设备的操作用户可能能够传送待被添加到区块链并且被分布在分布式网络的网络节点之间的交易。示例包括媒体服务器、网络服务器和可以向用户设备和网络节点传输交易数据或从用户设备和网络节点接收交易数据的其他类型的端点。

[0179] 块图1500还包括区块链1530。区块链1530包含连续不断地增长的一列记录——被称为区块，所述记录使用密码学被链接和保护。区块链1530中的区块中的每个包含时间戳和散列。散列包括当前区块的密码散列和区块链中的前一区块的密码散列二者。每个区块还包含与区块条目相关联的数据。在此示例场景中，已经用单独的访问级别标记将每个数据部分(各方、账户号码和可用资金)记录到区块链1530中。

[0180] 另外，与区块链1530中的每个数据部分相关联的每个访问级别标记与单独的访问级别相关联。例如，各方与公共访问标记相关联，该公共访问标记允许与分布式账本交互的任何用户查看区块中的数据部分。公共用户可以是对查看交易各方感兴趣的任何用户，并且对于此数据部分不存在隐私。相反地，账户号码与私人访问标记相关联，该私人访问标记可以仅由诸如用于每一方的转移银行的经授权的用户访问和查看。可用资金与许可访问标记相关联，该许可访问标记可以由有限的一组各方但不是全部用户查看。例如，收款银行可能要求查看可用资金，以确保转移账户中有可用资金来完成货币交易。

[0181] 访问平台1540表示能够验证访问区块链条目数据的用户请求的任何一个或多个计算系统，其中图28中的控制器2800是代表性的。访问平台1540在区块链1530中记录的数据部分与为请求用户生成记录1502之间提供安全的访问标记中介物。访问平台1540可以在众多分布式网络节点上实现，所述分布式网络节点可以由诸如税务审查员、财务机构、游戏监管委员会、客户、公司雇员等的各种各样的用户访问。记录1502例示了当请求查看存储在区块条目1501中的交易数据时用户可以查看的内容。记录1502可以包含最初输入到区块条目1501中的数据部分的全部或不包含所述数据部分，并且基于由请求用户提供的授权和与每个数据部分相关联的访问级别生成。

[0182] 图16例示了用以生成记录到区块链中的受限交易的定制视图的一个实现中的流程图。视图定制过程1600的步骤中的一些或全部可以在用来执行定制视图特征的应用程序的一个或多个部件的背景下以程序指令实现。

[0183] 在操作中，数据平台1510接收待在区块链1530的区块中维护的区块条目1501(步骤1601)。区块条目1501在分布式节点网络中由用户从用户设备请求并且包含数据部分。数据平台1510然后授权条目(例如，矿工验证区块中的散列)(步骤1602)。如果区块未被验证，则交易(区块条目1501)被拒绝(步骤1603)。然而，如果区块被接受，则评估数据部分中的每个的访问级别，并且基于所识别的访问级别将数据部分中的每个添加到区块链1530(步骤1604)连同将访问标记添加到区块链1530(步骤1605)。

[0184] 在下一个操作中，访问平台1540接收查看区块条目的一个或多个数据部分的请求，其中该请求包括与至少一个访问级别相关联的访问代码(步骤1606)。该访问代码可以与公共、许可或私人访问级别相关联。访问平台1540然后用区块链1530中的数据部分中的每个评估请求中的访问代码(步骤1607)。如果确定与请求用户相关联的访问代码是公共的，则将为请求用户生成仅指示来自区块条目1501的各方的定制视图(例如，记录1502)(步骤1608)。如果确定与请求用户相关联的访问代码是许可的，则将为请求用户生成指示来自区块条目1501的各方和可用资金的定制视图(步骤1609)。如果确定与请求用户相关联的访问代码是私人的，则将为请求用户生成指示来自区块条目1501的所有数据部分(即，各方、账户号码和可用资金)的定制视图(步骤1610)。

[0185] 图17例示了用以生成记录到区块链中的受限交易的定制视图的财务审查场景的一个实现中的示例性操作架构1700。在操作中，用户1710将薪金1730转移到用户1720以换取服务。交易记录从用户1710传送到数据库1740，该交易记录指示服务名称和费用成本。该记录然后经由服务器1750被维护在区块链1760中。应注意，在此场景中，交易还由用户1720记录在接收端上，其中指示利润和服务的交易记录被传送到数据库1742并且经由服务器1750被维护在区块链1760中。

[0186] 在下一个操作中，政府税务审查员1770请求查看对于用户1720记录的利润。用户1770可能未被授权查看记录中记录的服务或来自用户1710的费用。服务器1750可以接收请求，并且处理指示在此时间点用户1770仅被授权查看用户1720的利润的访问代码。服务器1750然后为用户1770生成该记录的定制视图，该定制视图仅指示用户1720的利润。尽管用户1770不能够看到交易的完整记录，但是用户1770能够相信该记录的指示用户1720的利润的部分是有效的，因为它已经被维护在区块链1760中。

[0187] 图18例示了用以生成记录到区块链中的受限交易的定制视图的停车客户账户和

交易跟踪场景的一个实现中的替代操作架构1800。在操作中，在智能电话应用程序上登录他们的账户的用户1810提交关于在图4的停车设施400中是否有车位可用于停放车辆1820的询问1830。用户1810输入其到达停车设施400入口402处的预计时间以及其将需要停放其车辆1820的预计时间。根据客户的账户数据，例如，应用程序将车辆1820与牌照号码相关联。预计进入时间和出去时间以及车辆1820的牌照号码的记录从用户1810传送到数据库1840，该记录指示停车交易的预测持续时间。该记录然后经由服务器1850被维护在区块链1860中。应注意，在此场景中，车辆1820的到达时间交易还由用户1880记录在接收端上，其中指示车辆1820的预计和实际到达时间的交易记录被传送到数据库1842并且经由服务器1850被维护在区块链1860中。在一些实施方案中，在实际车辆1820到达时间在预计车辆1820到达时间之后一预定阈值时间量(例如，5分钟)发生的情况下，用户1810必须重新发起询问以被指派停车设施400中的任何可用的停车位。

[0188] 在下一个操作中，另一个停车客户，例如用户1870，请求查看停放在用户1870偏爱的车位的车辆1820的出发时间和到达时间。用户1870可能未被授权查看车辆1820的牌照号码。服务器1850可以接收该请求并且处理指示在此时间点用户1870仅被授权查看分别为车辆1820和停车设施400记录的预测持续时间和可用的车位的访问代码。然后，服务器1850为用户1870生成记录的定制视图，该视图仅指示预测的持续时间和可用的车位。

[0189] 图19例示了用以生成记录到区块链中的受限交易的定制视图的酒店客人账户和交易跟踪场景的一个实现中的替代操作架构1900。在操作中，在智能电话应用程序上登录他们的账户的客人1910提交关于在酒店1920处是否有房间可用于停留的询问1930。客人1910输入其入住酒店1920的期望的入住日期以及其需要停留在酒店1920的夜晚数目。根据客户的账户数据，例如，应用程序将停留长度数据与进行询问1930的客人的姓名相关联。在酒店1920处的入住时间和停留的夜晚数目的记录从客人1910传送到数据库1940。该记录然后经由服务器1950被维护在区块链1960中。应注意，在此场景中，酒店1920的入住时间交易还由用户1980记录在接收端上，其中指示客人1910到达酒店1920的预计和实际到达时间的交易记录被传送到数据库1942并且经由服务器1950被维护在区块链1960中。在一些实施方案中，在实际酒店1920入住时间在预计酒店1920到达时间之后一预定阈值时间量(例如，18小时)发生的情况下，客人1910必须重新发起询问1930以被指派酒店1920中的任何可用的酒店房间。

[0190] 在下一个操作中，另一个酒店1920客户，例如客人1970，请求查看目前由客人1910占用但是客人1970偏爱的酒店1920房间的出发日期和时间。客人1970可能未被授权查看客人1910的姓名。服务器1950可以接收该请求并且处理指示在此时间点客人1970仅被授权查看预测退房日期和时间以及在酒店1920处的其他可用的房间的访问代码。然后，服务器1950为客人1970生成记录的定制视图，该视图仅指示这些数据，而不指示客人1910的姓名。图20例示了用以生成记录到区块链中的受限交易的定制视图的自动驾驶车辆车队乘客账户和交易跟踪场景的一个实现中的替代操作架构2000。在操作中，在智能电话应用程序上登录他们的账户的乘客2010提交关于车队2032是否有自动驾驶车辆2020可供在某一时间乘车并且到期望的目的地的询问2030。乘客2010输入其在由自动驾驶车辆车队2032供应的指定位置处的期望的接乘日期和时间以及其请求的乘车目的地。根据客户的账户数据，例如，应用程序将乘车请求相关数据与进行询问2030的乘客的姓名相关联。此乘车请求数据

的记录从乘客2010传送到数据库2040。该记录然后经由服务器2050被维护在区块链2060中。应注意，在此场景中，自动驾驶车辆2020的乘车请求数据还由用户2080记录在车队2032接收端上，其中指示请求的车辆2020、接乘时间和位置、以及乘客2010目的地的交易记录被传送到数据库2042并且经由服务器2050被维护在区块链2060中。在一些实施方案中，在乘客2010未出现在预先安排的接乘位置并且经过预定的时间段(例如，在预先安排的接乘时间之后10分钟)，乘客2010必须重新发起询问2030以被指派来自车队2032的任何可用的自动驾驶车辆2020。

[0191] 在下一个操作中，另一个车队2032客户，例如乘客2070，请求查看目前为乘客2010服务但是乘客2070偏爱的自动驾驶车辆2020将再次可用于租用的时间和日期。乘客2070可能未被授权查看乘客2010的姓名。服务器2050可以接收该请求并且处理指示在此时间点乘客2070仅被授权查看预测的车辆2020可用性日期和时间以及车队2032的其他可用的车辆的访问代码。然后，服务器2050为乘客2070生成记录的定制视图，该定制视图仅指示这些数据，而不指示乘客2010的姓名。

[0192] 图21例示了用以生成记录到区块链中的受限交易的定制视图的游戏监管场景的一个实现中的替代操作架构2100。在操作中，用户2110与用户2120签署体育投入2130。体育投入2130的记录从用户传送到数据库2140，该记录指示预测团队和用户2110至2120的驾驶执照号码。该记录然后经由服务器2150被维护在区块链2160中。应注意，在此场景中，交易还发起从体育计分委员会2132到数据库2142的传送，该交易指示游戏的官方分数。游戏的官方分数被传送到数据库2142并且经由服务器2150被维护在区块链2160中。

[0193] 在下一个操作中，体育投入管理用户2170可以请求查看来自区块链2160的预测结果以及游戏的官方分数。用户2170可能未被授权查看用户2110-2120中的每个的驾驶执照。服务器2150可以接收请求，并且处理指示在此时间点用户2170仅被授权查看用户2110-2120中的每个的预测结果和官方分数的访问代码。服务器2150然后生成记录的定制视图，该定制视图仅为用户2170指示预测结果和官方分数。尽管用户2170不能够看到交易的完整记录，但是用户2170能够相信该记录的指示用户2110-2120的部分具有存档的有效驾驶执照，因为此数据已经被维护在区块链2160中。

[0194] 图22例示了用以生成记录到区块链中的受限交易的定制视图的库存跟踪场景的一个实现中的替代操作架构2200。在操作中，用户2210将包裹2230的货物转移到用户2220以将其递送到各个用户——包括跟踪包裹A的用户2270。用于包裹2230的货物的出发时间交易的记录从用户2210转移到数据库2240，该记录指示包裹A和包裹B的出发时间。该记录然后经由服务器2250被维护在区块链2260中。应注意，在此场景中，用于包裹2230的货物的到达时间交易也由用户2220记录在接收端上，其中指示包裹A和包裹B的到达时间的交易的记录被传送到数据库2242，并且经由服务器2250被维护在区块链2260中。

[0195] 在下一个操作中，跟踪包裹A的用户2270请求查看对于包裹A记录的出发时间和到达时间。用户2270可能未被授权查看对于包裹B记录的出发时间和到达时间。服务器2250可以接收请求并且处理指示在此时间点用户2270仅被授权查看对于包裹A记录的出发时间和到达时间的访问代码。服务器2250然后为用户2270生成该记录的定制视图，该定制视图仅指示对于包裹A记录的出发时间和到达时间。

[0196] 再次参考图18，图22的库存跟踪场景以与停车设施情况类似的方式实现或以其他

方式利用区块链和所公开的系统和方法。在后一种情况下,产品是停车设施中的停车位,并且被跟踪的库存是可用的停车位的数目和位置。在产品或服务的交付时间对产品或服务的客户和提供者重要的情况下,可以根据所公开的系统和方法利用区块链来提高业务操作的效率和客户体验。例如,在图18中所呈现的停车情况下,基于客户的预期进入到停车设施400的时间和从停车设施400离开的时间来获得客户的停车请求的预测持续时间使得运营商能够满足其客户的需要,同时有效地充分利用停车位库存以最大化收入。例如,在一个运营商在一个城市具有不止一个停车设施的情况下,所述设施的库存可以被利用以达到相同的目的。类似地,对于图22的库存跟踪场景(例如,在一个区域中具有多个存储位置的零售存储操作),所公开的系统和方法、运营商以及其客户可以访问关于特定产品的目前的位置和可用数量的实时数据(包括它们在转运中时),从而享受由此提高的便利性和增加的销售流量。

[0197] 图23例示了记录到区块链中的受限交易的示例性定制视图。图23包括计算系统2301,该计算系统包括能够本机地(natively)或在网络浏览器的背景下运行区块链应用程序、流传输应用程序或以任何其他方式执行应用程序的一个或多个设备。计算系统2301可以包括适合于生成停车交易记录的定制视图的支持架构中的各种硬件和软件元素。在图28中关于控制器2800例示了一种这样的代表性架构。

[0198] 计算系统2301还包括根据本文所描述的过程的能够维护区块链交易的完全记录的区块链应用程序部件2302。用户界面2303包括可以由区块链应用程序部件产生的定制视图2310。用户界面2303可以在定制视图2310中显示来自区块条目的、用户被授权查看的数据部分。用户最初可能仅具有查看区块条目的公共部分(诸如,停放在或计划停放在停车设施400处的车辆的一个子集的牌照号码)的访问。

[0199] 然后可以在请求中传送加密代码以查看许可的数据部分。一旦计算系统2301核实该加密代码,就可以将许可的数据部分添加到定制视图2310。许可的数据部分包括与所述子集中的车辆相关联的每个客户的姓名和肖像图像。然而,当前由所述子集中的客户中的每个占用的停车位可能保持为私人的,并且因此用户将不能够在定制视图2310中查看到停车位数据。

[0200] 图24例示了记录到区块链中的受限交易的替代示例性定制视图2400。图24包括存储区块链2402的副本的服务器节点2401。区块链2402存储已经使用散列代码链接的区块,诸如区块2410和2412。每个区块包含可以被进一步分解成数据部分的交易。例如,区块2412存储在图4的停车设施400处的最新的、实时的停车交易记账(tally)2420。记账2420包括每个客户的姓名、每个客户的车辆的牌照号码、每个客户在停车上花费的月累计的钱的数额(或保持的停车订阅计划的指示)和客户的车辆目前停放在其中的停车设施400中的停车位的识别符。应注意,也可以在区块2412中包括附加数据,诸如使用的月累计辅助服务和在停车设施400处的这样的服务上花费的钱的数额。

[0201] 在与图24中所例示的示例对应的使用实例中,记账2420中的客户中的一个(例如,Mary)是停车账户所有者,并且记账2420中所示出的剩余客户是Mary的账户的授权用户。在该使用实例中,Mary和Ed是离婚的前配偶,并且Mary负责支付Ed的在停车设施400处的所有停车费用,无论出于任何原因。Mary为女儿Jess支付停车费用,出于在停车设施400附近上大学课程的目的。对于每个用户访问受限停车记录,包括复选标志以指示可以由每个用户

(例如,Mary、Ed和Jess)查看哪些数据部分。例如,Mary正在使用移动设备2430访问月累计停车交易历史。在此示例场景中,Mary被授权查看授权用户的姓名(Ed和Jess)和使用美元数额中的每个,因为Mary负责将那些数额支付给停车设施400。Mary还被允许对她自己的和Jess的牌照号码、使用数额和占用的停车位ID的私人访问。然而,根据Mary和Ed的离婚协议,Mary可能不具有跟踪Ed的行踪的任何能力。因此,Mary无法访问Ed的牌照号码或在停车设施400中目前占用的停车位。如可以在移动设备2430上显示的定制视图中看出的,Mary查看授权的数据部分2440,并且被阻止查看未授权的数据部分2441。

[0202] 图25例示了记录到区块链中的受限交易的示例性定制视图。图25包括计算系统2501,该计算系统包括能够本机地或在网络浏览器的背景下运行区块链应用程序、流传输应用程序或以任何其他方式执行应用程序的一个或多个设备。计算系统2501可以包括适合于生成工资单交易记录的定制视图的支持架构中的各种硬件和软件元素。在图28中关于控制器2800例示了一种这样的代表性架构。

[0203] 计算系统2501还包括根据本文所描述的过程的能够维护区块链交易的完全记录的区块链应用程序部件2502。用户界面2503包括可以由区块链应用程序部件产生的定制视图2510。用户界面2503可以在定制视图2510中显示来自区块条目的、用户被授权查看的数据部分。用户最初可能仅具有查看区块条目的公共部分(诸如,工资单上的每个雇员的姓名)的访问。

[0204] 然后可以在请求中传送加密代码以查看许可的数据部分。一旦计算系统2501核实该加密代码,就可以将许可的数据部分添加到定制视图2510。许可的数据部分包括工资单交易上的每个雇员的工资和出生日期。然而,每个雇员的社会保障号码可能保持为私人的,并且因此用户将不能够在定制视图2510中查看到社会保障数据。

[0205] 图26例示了记录到区块链中的受限交易的替代示例性定制视图。图26包括存储区块链2602的副本的服务器节点2601。区块链2602存储已经使用散列代码链接的区块,诸如区块2610和2612。每个区块包含可以被进一步分解成数据部分的交易。例如,区块2612存储在线扑克游戏投入条目2620。投入条目2620包括每个玩家的姓名、用于每个玩家的投入数额、每个玩家可用于进行投入的资金数额和玩家排名索引。应注意,也可以在区块2612中包括附加数据,诸如游戏统计、获胜/失败百分比等。

[0206] 对于每个用户访问投入条目,包括复选标志以指示可以由每个用户查看哪些数据部分。例如,Sue正在使用移动设备2630访问扑克游戏投入条目。在此示例场景中,Sue被授权查看玩家的姓名和投入数额中的每个,因为姓名和投入数额是公众可访问的。Sue还被允许对她自己的资金数额和排名的私人访问。然而,Sue不具有对其他玩家的可用资金和排名的访问。如可以在移动设备2630上显示的定制视图中看出的,Sue查看授权的数据部分2640,并且被阻止查看未授权的数据部分2641。

[0207] 图27例示了能够提供记录到区块链中的受限或敏感数据的定制视图的数据访问系统的一个实现中的替代操作架构。如图27中所例示的,用户2710A-2710N可以使用各种电子设备来请求访问文档、电子记录、物理位置(例如,保险箱、房间、建筑物、区域等)或信息。例如,根据各实施方案,用户2710A-2710N可以具有不同的访问级别,诸如授予用户对保密信息(例如,国家或组织秘密)或对受限区域的访问的安全调查。通常,安全调查(例如,保密的、秘密的、最高秘密的等)不足以得到对所有文档和/或数据的访问。代替地,个人还必须

有必要知道特定信息。

[0208] 请求可以被提交给访问控制框架2720，该访问控制框架可以翻译和验证来自不同系统(例如，应用程序、钥匙卡系统、指纹读取器、生物统计设备、口令、多因素认证等)的请求。一经验证，该访问控制框架可以将请求提交给安全施加器2730，该安全施加器可以使用各种安全协议来处理请求。例如，请求文档或位置的安全级别可能要求附加的多次验证(例如，口令和硬件设备、生物统计、位置核实、PIN、口令等)。在一些实施方案中，安全应用程序可以从与数据相关联的区块链上的区块中的字段或元数据提取此信息。

[0209] 存储在区块链2740中的文档或数据2750A-2750B可以具有不同的字段或部分，所述字段或部分可以由具有相异的“需要知道”或访问级别的不同的个人访问(例如，合规的官员与较低级别的公司雇员、具有较高安全调查级别的个人与具有较低安全调查级别的个人等)。例如，在一些实施方案中，各种编辑映射可以被存储在区块链中并且在向用户2710A-2710N呈现之前由文档生成器2760应用。这样，可以向请求同一文档或数据的两个用户呈现不同的结果。

[0210] 作为一个示例，信息自由访问请求可以产生已经被认为公众可用的经编辑的文档，而具有安全调查和“需要知道”的个人将被呈现不同的访问级别。根据各实施方案，可以接收来自用户的初始请求。系统可以识别符合该请求的信息，并且根据FOIA请求设置用于响应于该请求的计时器时段(例如，30天)。系统然后可以确定符合该请求的每条信息是否具有任何分类限制。如果确定任何信息是不受限制的(例如，没有分类级别)，则系统可以用包括无需检查的信息的响应来响应于做出该请求的用户。此类型的特征减少了政府雇员的工作负荷，并且确保满足用于响应的时间段(例如，通过在雇员之间优先处理并且重新指派核阅)。在一些实施方案中，如果剩余足够的时间，则系统可以在发送之前请求人工核阅并且批准包括的信息。

[0211] 当系统识别机密信息时，系统接下来将评估访问和调查。例如，如果请求数据的人具有比管理员高的访问/调查，则该信息将被自动地发送。如果需要做出编辑以符合安全调查，则文档生成器2760可以应用所需的任何编辑和/或移除不应包括在响应中的文档。虽然在图27中未例示，但是一些实施方案可以包括机器学习/人工智能部件，以核阅数据和/或元数据并且识别不应包括的部分。

[0212] 其他实施方案可以具有寻求变化信息的其他类型的个人(例如，寻求关于竞赛者、银行业务客户、执行审查的监管者等的信息的人)。存在许多这样的使用实例。此外，一些实施方案可以使用具有在分散式对等网络上运行的后端代码的分散式应用程序(Dapp)来提交请求、从区块链检索信息以及与其他应用程序(例如，其他Dapp)通信。

[0213] 安全施加器2730还可以核阅用户的证书状态或安全级别。用户的记录可以存储在区块链2745上。例如，关于背景核查的信息、银行账户信息、旅行信息、用户与其相关联的项目(过去的和现在的)、家族历史、医疗历史、证书、生物统计、口令、签名等可以存储在用户的记录上。安全施加器2730可以检索该信息并且在生成数据或文档的定制视图中利用该信息。

[0214] 图28例示了示出了表示主机计算机系统的计算机系统化的示例机器的块图。控制器2800可以与实体通信，所述实体包括一个或多个用户2825客户端/终端设备2820、用户输入设备2805、外围设备2810、可选的协同处理器设备(例如，密码处理器设备)2815和网络

2830。用户可以经由终端设备2820通过网络2830与控制器2800建立关系。在一些实施方案中，终端设备2820与控制器2800之间的通信的全部或一部分可以被加密。各种法律、标准或最佳实践可能要求密码学以用于存储、传输和/或利用各种类型的数据、信息、代码、信令等。

[0215] 计算机可以采用中央处理单元(CPU)或处理器来处理信息。处理器可以包括可编程通用或专用微处理器、可编程控制器、专用集成电路(ASIC)、可编程逻辑设备(PLD)、嵌入式部件、这样的设备的组合等。处理器响应于用户和/或系统生成的请求执行程序部件。这些部件中的一个或多个可以用软件、硬件或硬件和软件二者实现。处理器传递指令(例如，操作和数据指令)以使能各种操作。

[0216] 控制器2800可以包括时钟2865、CPU 2870、存储器(诸如只读存储器(ROM)2885和随机存取存储器(RAM)2880)和协同处理器2875等。这些控制器部件可以连接到系统总线2860，并且通过系统总线2860连接到接口总线2835。另外，用户输入设备2805、外围设备2810、协同处理器设备2815等可以通过接口总线2835连接到系统总线2860。接口总线2835可以连接到许多接口适配器，诸如处理器接口2840、输入输出接口(I/O)2845、网络接口2850、存储接口2855等。

[0217] 处理器接口2840可以便于协同处理器设备2815与协同处理器2875之间的通信。在一个实现中，处理器接口2840可以加快请求或数据的加密和解密。输入输出接口(I/O)2845使用协议诸如用于处理音频、数据、视频接口、无线收发器等的协议(例如，Bluetooth®、IEEE894a-b、串行、通用串行总线(USB)、数字视频接口(DVI)、802.11a/b/g/n/x、蜂窝等)来便于用户输入设备2805、外围设备2810、协同处理器设备2815等与控制器2800的部件之间的通信。网络接口2850可以与网络2830通信。通过网络2830，控制器2800可以是对远程终端设备2820可访问的。网络接口2850可以使用各种有线和无线连接协议，诸如，直接连接、以太网、无线连接，诸如，IEEE 802.11a-x、miracast等。交互游戏系统的一些部件可以包括各种协议或符合由不同协会或监管机关提出的各种标准或证明。例如，一些实施方案可以使用时隙会计系统(SAS)协议或符合游戏到系统(G2S)标准。

[0218] 网络2830的示例包括因特网、局域网(LAN)、城域网(MAN)、广域网(WAN)、无线网络(例如，使用无线应用协议WAP)、安全的自定义连接等。网络接口2850可以包括防火墙，该防火墙在一些方面可以支配和/或管理在计算机网络中访问/代理数据的许可，并且跟踪不同的机器和/或应用程序之间的变化的信任级别。防火墙可以是具有硬件和/或软件部件的任何组合的任何数目的模块，所述硬件和/或软件部件能够例如在特定的一组机器与应用程序之间、在机器与机器之间、和/或在应用程序与应用程序之间执行预定的一组访问权，以监管这些变化的实体之间的通信量流和资源共享。

[0219] 防火墙可以附加地管理访问控制列表和/或具有对访问控制列表的访问，该访问控制列表详述了许可，包括例如个人、机器和/或应用程序对对象的访问和操作权以及许可权所处的情形。在不偏离本公开内容的新颖技术的前提下，在防火墙的功能中执行或包括的其他网络安全功能可以是例如但不限于入侵防御、入侵检测、下一代防火墙、个人防火墙等。应领会，控制器2800可能能够使用网络接口2850来传送和接收支付数额。支付可以通过由控制器2800执行的应用程序(诸如，使用Bluetooth®的国家搏击俱乐部(National Fighting Club，NFC)应用程序点击)来驱动。2855可以与诸如存储设备2890、可移动磁盘设

备等的许多存储设备通信。存储接口2855可以使用各种连接协议，诸如串行高级技术附件(SATA)、IEEE 894、以太网、光纤、通用串行总线(USB)等。

[0220] 用户输入设备2805和外围设备2810可以连接到I/O接口2845并且可能地连接到其他接口、总线和/或部件。用户输入设备2805可以包括卡读取器、指纹读取器、操纵杆、键盘、麦克风、鼠标、遥控器、视网膜读取器、触摸屏、传感器等。外围设备2810可以包括天线、音频设备(例如，麦克风、扬声器等)、摄像机、外部处理器、通信设备、射频识别器(RFID)、扫描仪、打印机、存储设备、收发器等。协同处理器设备2815可以通过接口总线2835连接到控制器2800，并且可以包括微控制器、处理器、接口或其他设备。

[0221] 计算机可执行指令和数据可以存储在处理器可访问的存储器(例如，寄存器、高速缓存存储器、随机存取存储器、闪存等)中。这些存储的指令代码(例如，程序)可以使处理器部件、母板和/或其他系统部件建立关系以执行期望的操作。控制器2800可以采用各种形式的存储器，所述存储器包括片上CPU存储器(例如，寄存器)、RAM 2880、ROM 2885和存储设备2890。存储设备2890可以采用任何数目的有形、非暂时性存储设备或系统，诸如固定或可移动磁盘驱动器、光学驱动器、固态存储器设备和其他处理器可读存储介质。存储在存储器中的计算机可执行指令可以包括交互游戏平台，该交互游戏平台具有执行特定任务或实现特定抽象数据类型的一个或多个程序模块，诸如例程、程序、对象、部件、数据结构等。例如，存储器可以包含操作系统(OS)部件2895、模块和其他部件、数据库表等。这些模块/部件可以从存储设备——包括从通过接口总线2835可访问的外部存储设备——存储和访问。

[0222] 数据库部件可以存储由处理器执行以处理存储的数据的程序。数据库部件可以以关系数据库、可扩展数据库和安全数据库的形式实现。这样的数据库的示例包括DB2、MySQL、Oracle、Sybase等。替代地，可以使用诸如阵列、散列、列表、堆栈、结构化文本文件(例如，XML)、表等的各种标准数据结构来实现数据库。这样的数据结构可以存储在存储器和/或结构化文件中。

[0223] 控制器2800可以在分布式计算环境中实现，在分布式计算环境中任务或模块由远程处理设备执行，所述远程处理设备通过诸如局域网(“LAN”)、广域网(“WAN”)、因特网等的通信网络链接。在分布式计算环境中，程序模块或子例程可以位于本地和远程存储设备二者中。可以采用分布式计算来负载平衡和/或聚合用于处理的资源。替代地，控制器2800的各方面可以通过因特网或通过其他网络(包括无线网络)以电子方式分布。相关领域的技术人员将认识到，交互游戏系统的部分可以驻留在服务器计算机上，同时对应的部分可以驻留在客户端计算机上。控制器2800的各方面特定的数据结构和数据传输也包含在本公开内容的范围内。

[0224] 从前述公开内容可以领会某些发明方面，其中下面是多个示例。

[0225] 附图中提供的功能块图、操作场景和序列以及流程图表示用于执行本公开内容的新颖方面的示例性系统、环境和方法学。虽然出于简化解释的目的，本文所包括的方法可以是功能图、操作场景或序列或流程图的形式并且可以被描述为一系列动作，但是应理解和领会，所述方法不受动作的顺序限制，因为一些动作可能据此以不同的顺序发生和/或与本文所示出和所描述的其他动作同时发生。本领域技术人员将理解和领会，方法可以替代地被表示为一系列互相联系的状态或事件，诸如在状态图中。此外，一个新颖的实现可能不要求在一种方法学中所例示的所有动作。

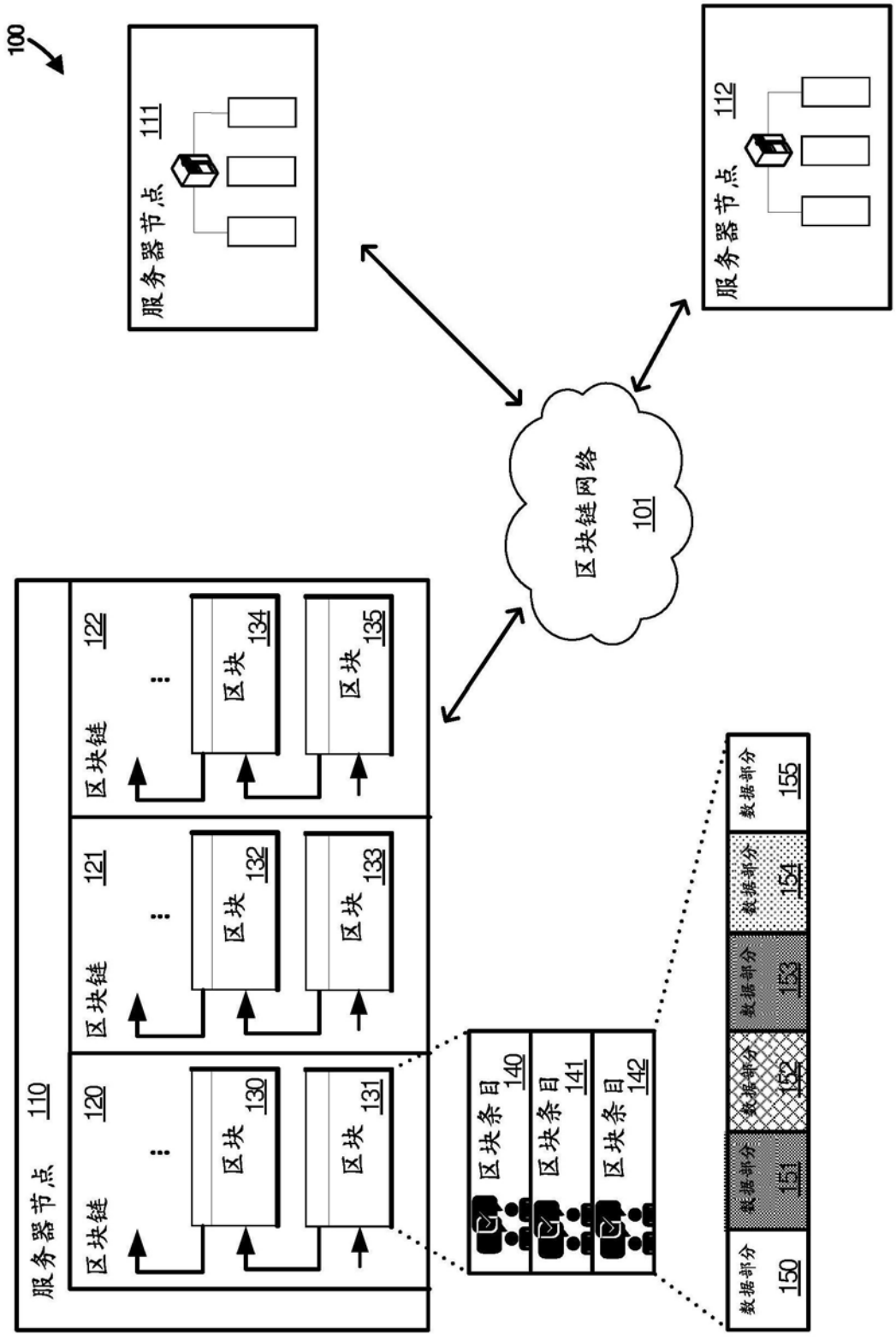

100
服务器节点 111
服务器节点 112
区块链网络 101
服务器节点 110
区块链 120
区块链 121
区块链 122
区块 130
区块 131
区块 132
区块 133
区块 134
区块 135
区块条目 140
区块条目 141
区块条目 142
数据部分 150
数据部分 151
数据部分 152
数据部分 153
数据部分 154
数据部分 155

图1

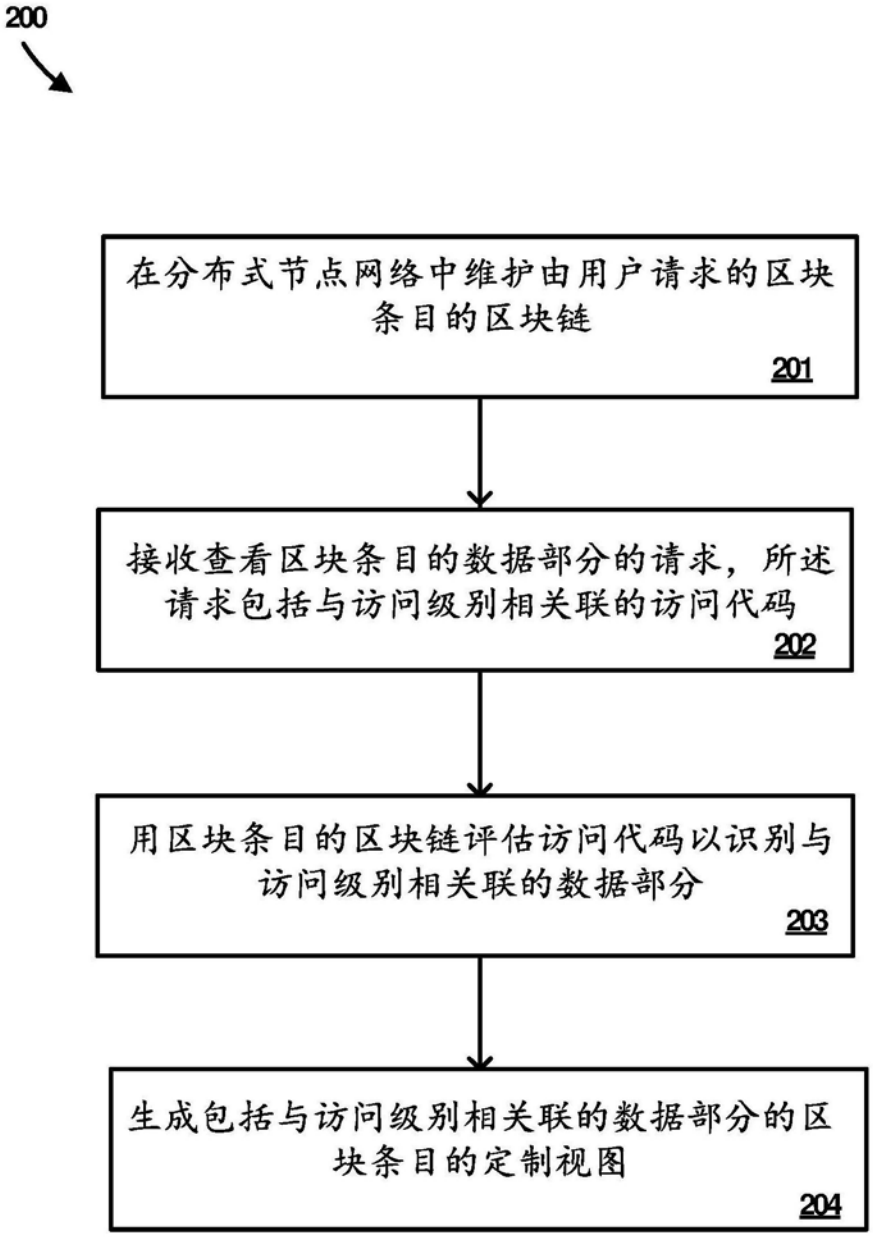

200
在分布式节点网络中维护由用户请求的区块条目的区块链
201
接收查看区块条目的数据部分的请求，所述请求包括与访问级别相关联的访问代码
202
用区块条目的区块链评估访问代码以识别与访问级别相关联的数据部分
203
生成包括与访问级别相关联的数据部分的区块条目的定制视图
204

图2

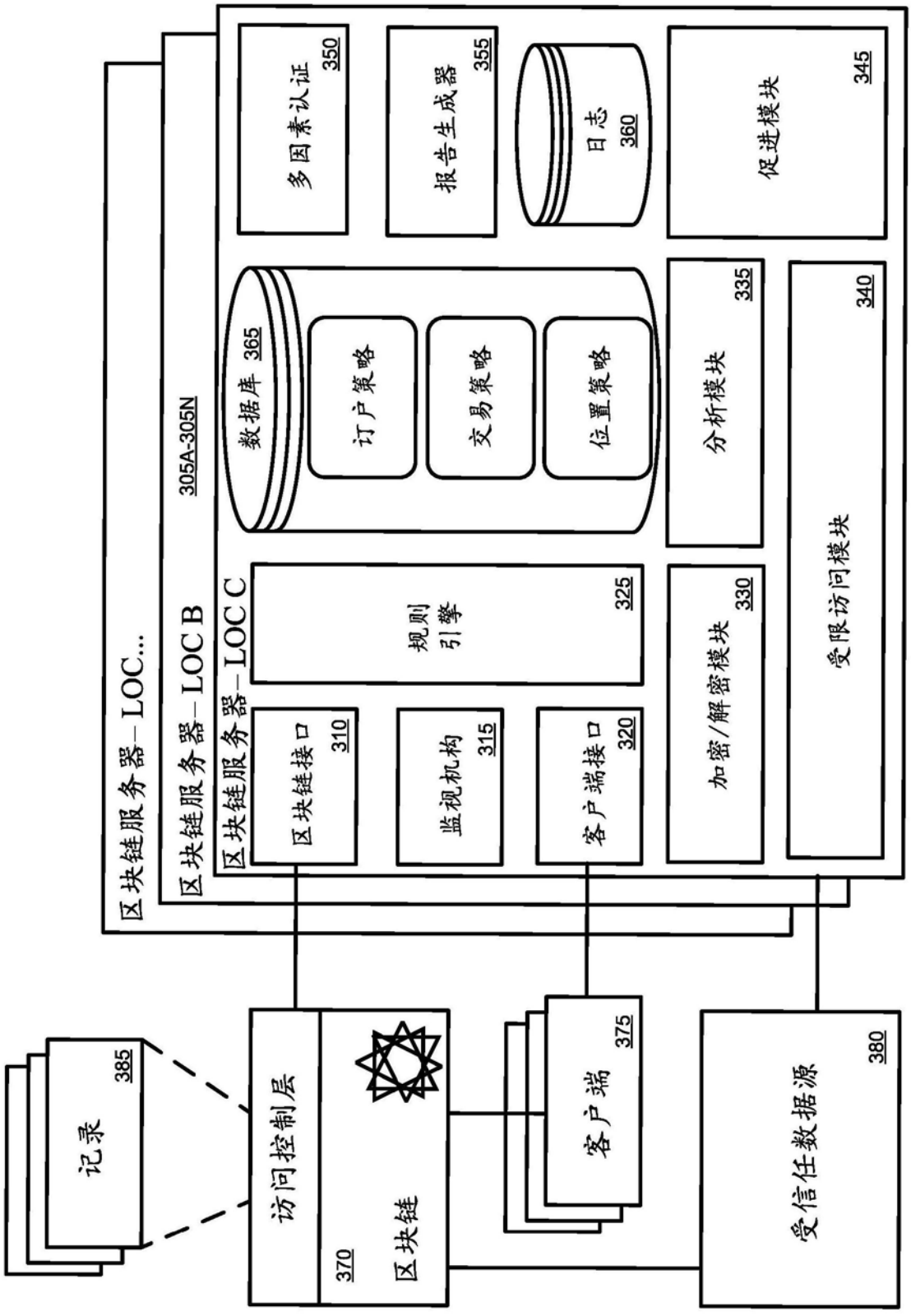

区块链服务器– LOC...
区块链服务器– LOC B
305A-305N
区块链服务器– LOC C
多因素认证 350
报告生成器 355
日志 360
促进模块 345
数据库 365
订户策略
交易策略
位置策略
分析模块 335
受限访问模块 340
规则引擎 325
区块链接口 310
监视机构 315
客户端接口 320
加密/解密模块 330
记录 385
访问控制层
370
区块链
客户端 375
受信任数据源 380

图3

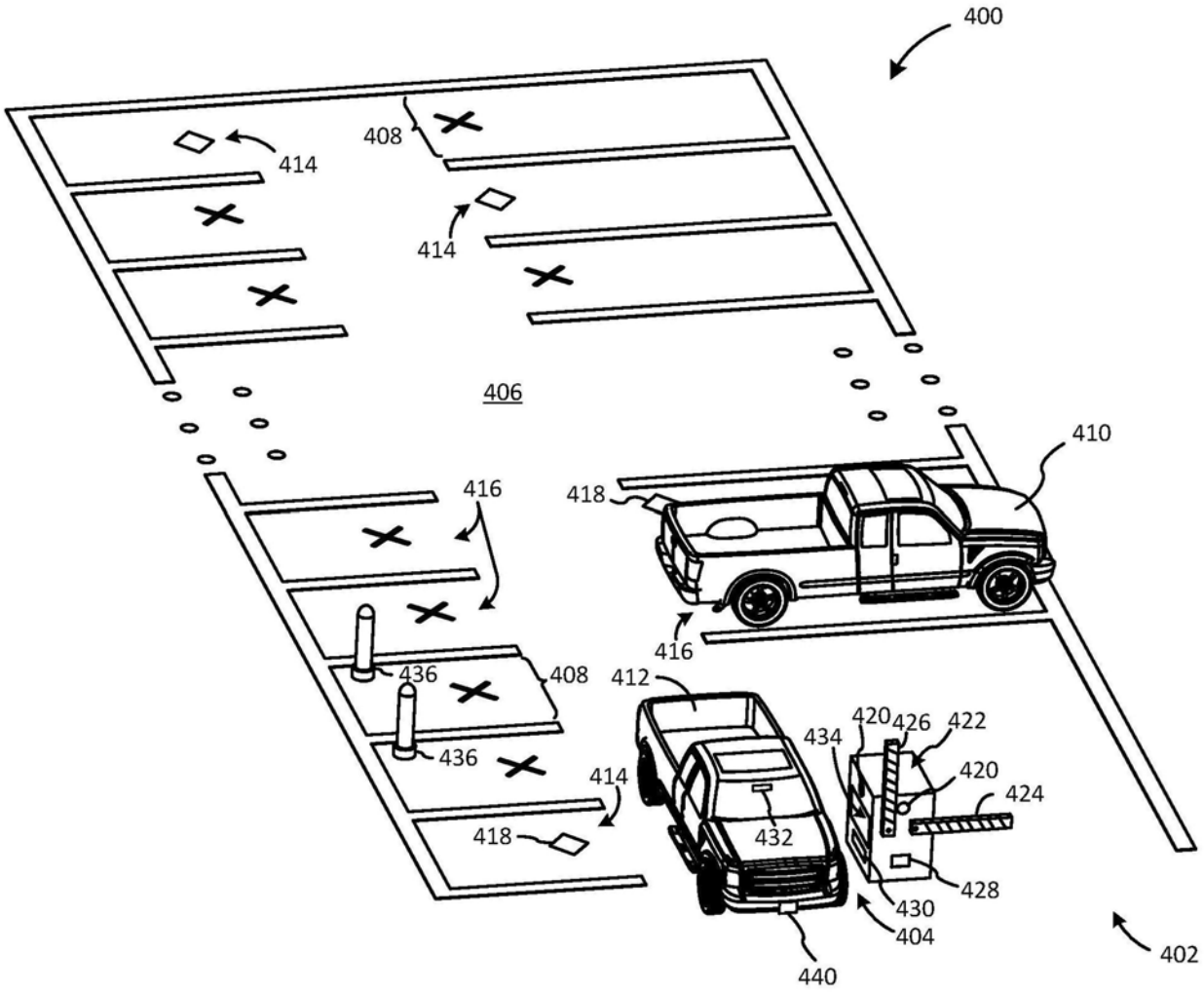

400
408
414
414
406
410
418
416
416
436
408
412
436
420
426
422
434
420
424
414
418
432
428
430
404
440
402

图4

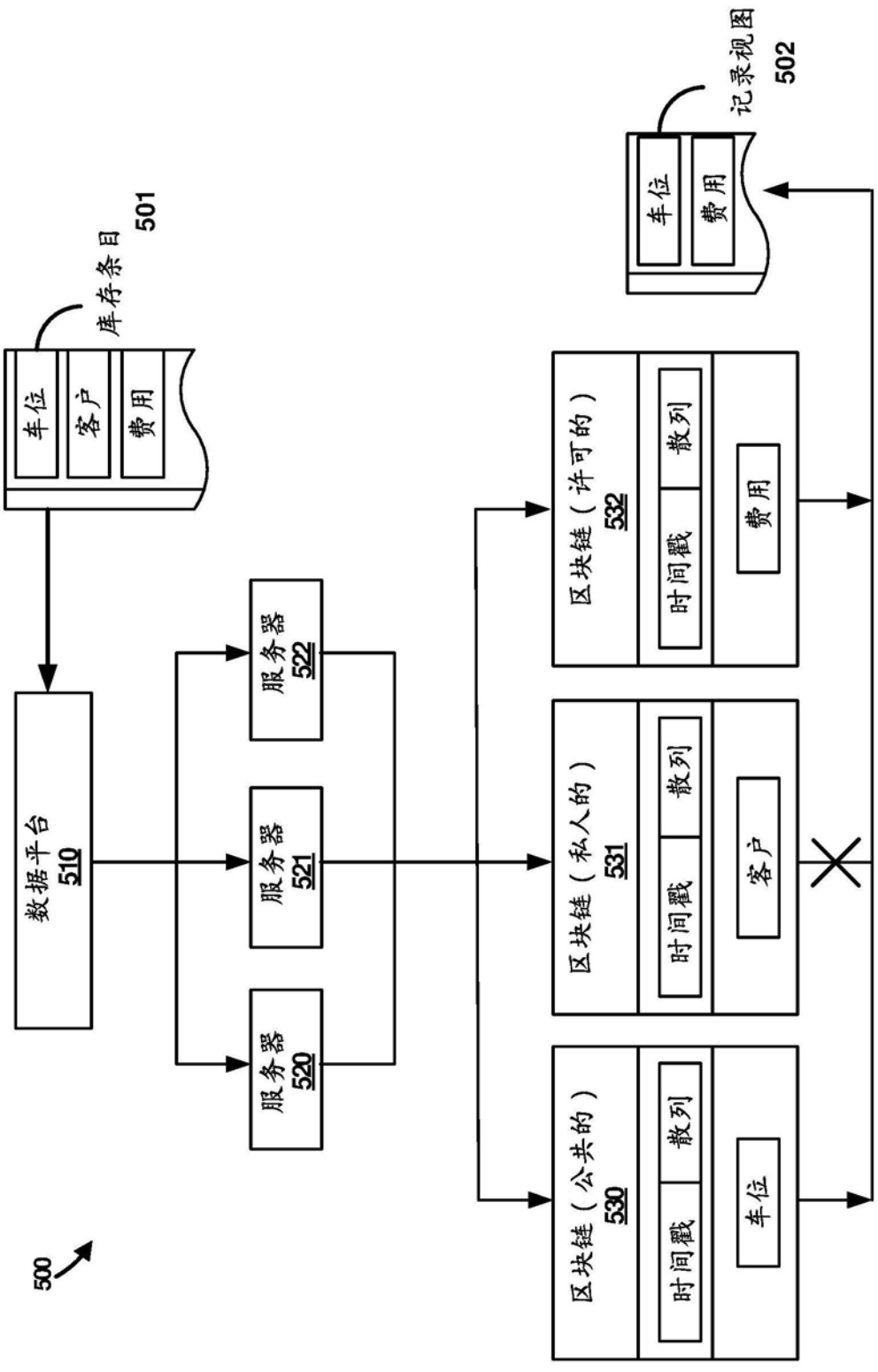

500
数据平台
510
服务器
520
服务器
521
服务器
522
库存条目
501
车位
客户
费用
记录视图
502
车位
费用
区块链（公共的）
530
时间戳
散列
车位
区块链（私人的）
531
时间戳
散列
客户
区块链（许可的）
532
时间戳
散列
费用

图5

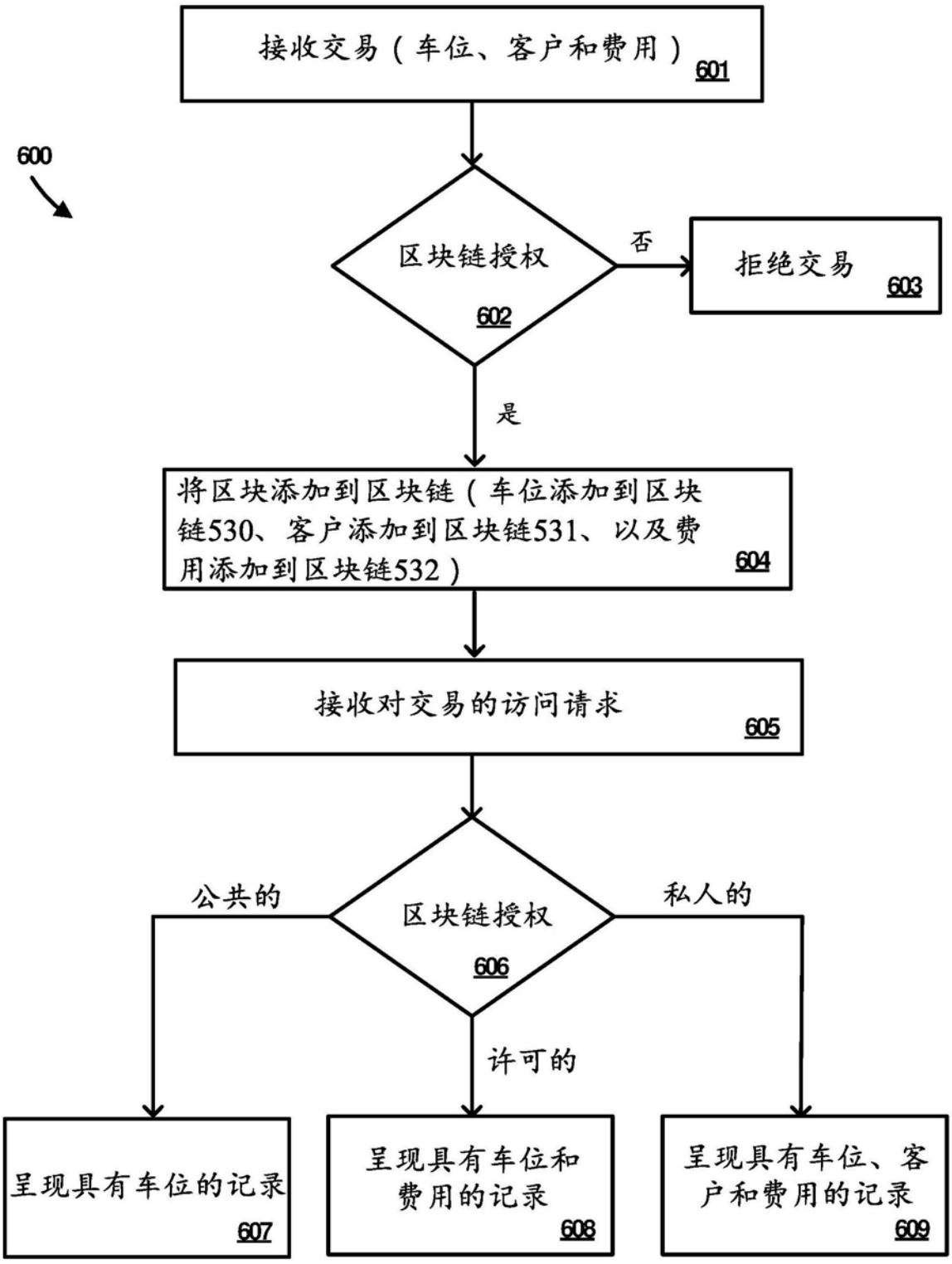

600
接收交易（车位、客户和费用）
601
区块链授权
602
否
拒绝交易
603
是
将区块添加到区块链（车位添加到区块链530、客户添加到区块链531、以及费用添加到区块链532）
604
接收对交易的访问请求
605
区块链授权
606
公共的
私人的
许可的
呈现具有车位的记录
607
呈现具有车位和费用的记录
608
呈现具有车位、客户和费用的记录
609

图6

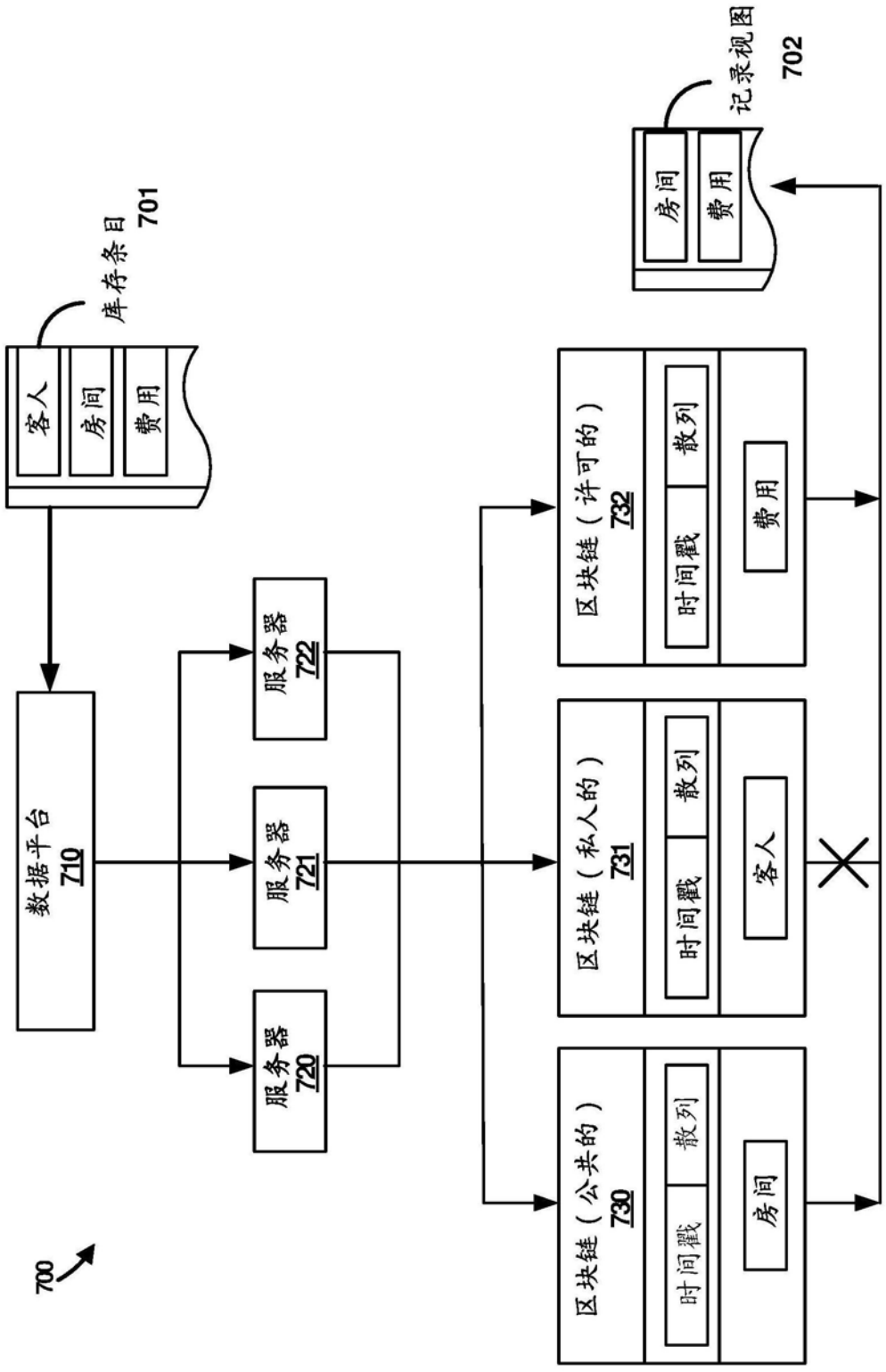

700
数据平台
710
服务器
720
服务器
721
服务器
722
库存条目
701
客人
房间
费用
记录视图
702
房间
费用
区块链（公共的）
730
时间戳
散列
房间
区块链（私人的）
731
时间戳
散列
客人
区块链（许可的）
732
时间戳
散列
费用

图7

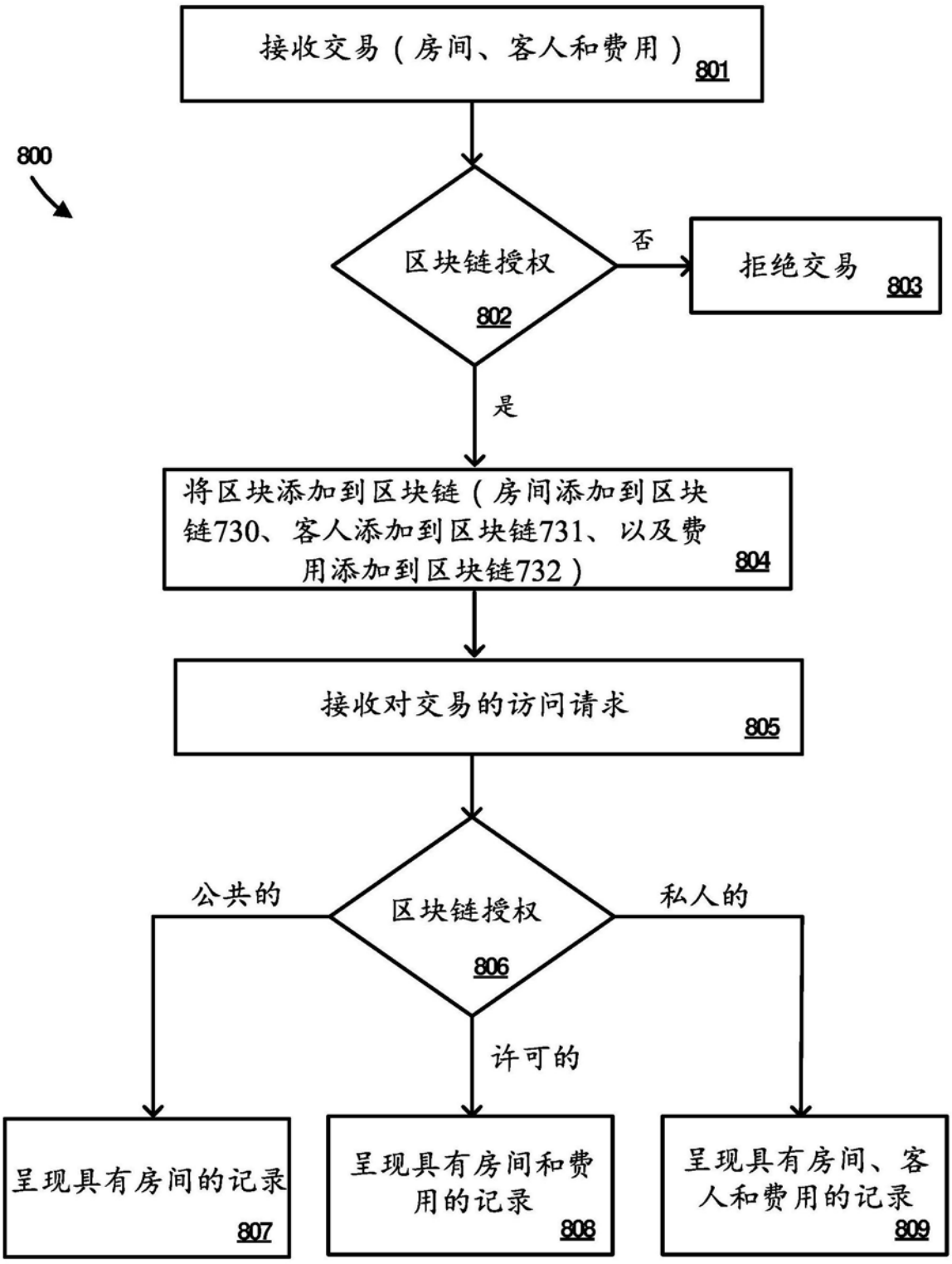

800
接收交易（房间、客人和费用）
801
区块链授权
802
否
拒绝交易
803
是
将区块添加到区块链（房间添加到区块链730、客人添加到区块链731、以及费用添加到区块链732）
804
接收对交易的访问请求
805
区块链授权
806
公共的
私人的
许可的
呈现具有房间的记录
807
呈现具有房间和费用的记录
808
呈现具有房间、客人和费用的记录
809

图8

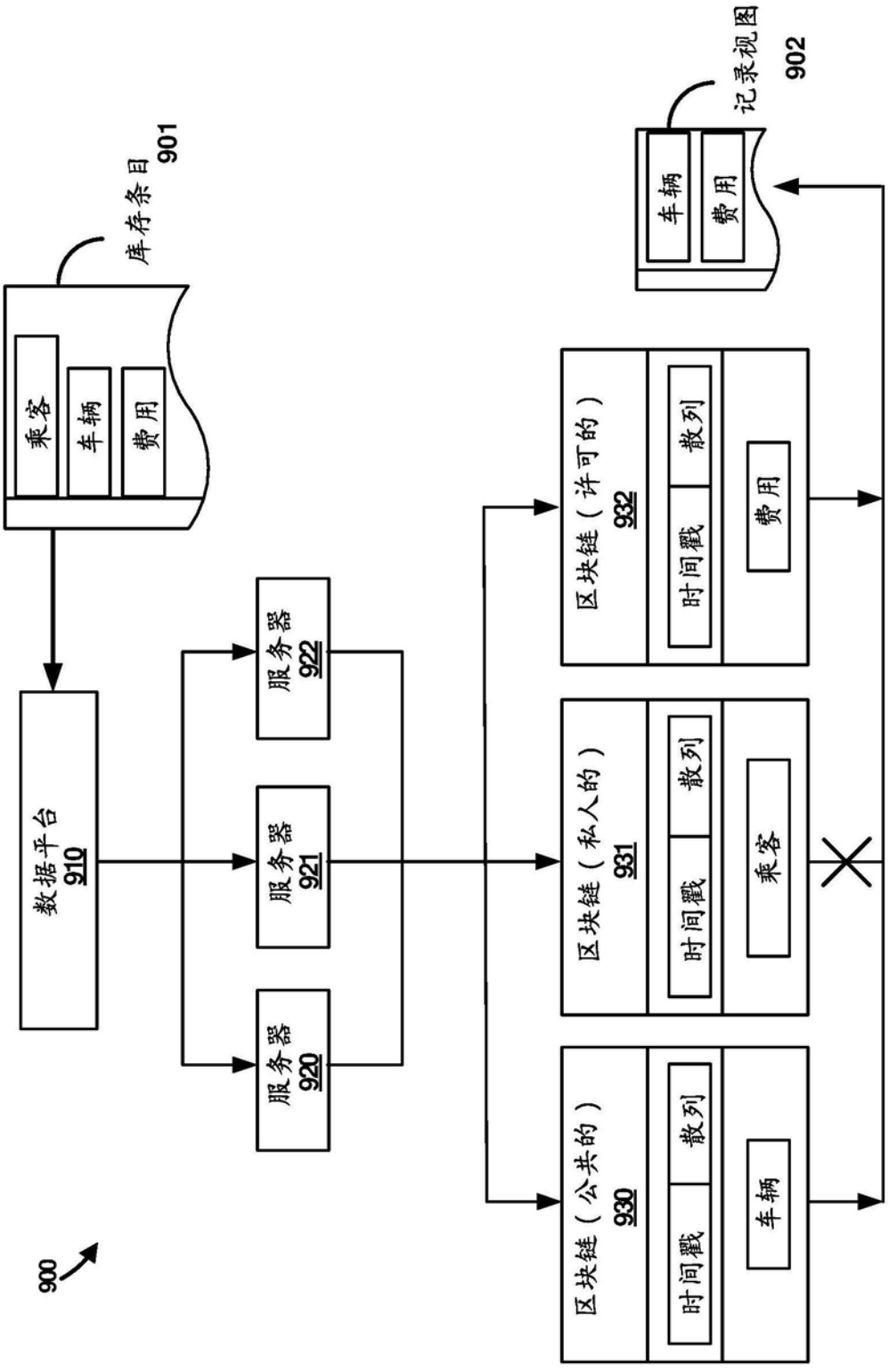

900
数据平台
910
服务器
920
服务器
921
服务器
922
乘客
车辆
费用
库存条目
901
区块链（公共的）
930
时间戳
散列
车辆
区块链（私人的）
931
时间戳
散列
乘客
区块链（许可的）
932
时间戳
散列
费用
记录视图
902
车辆
费用

图9

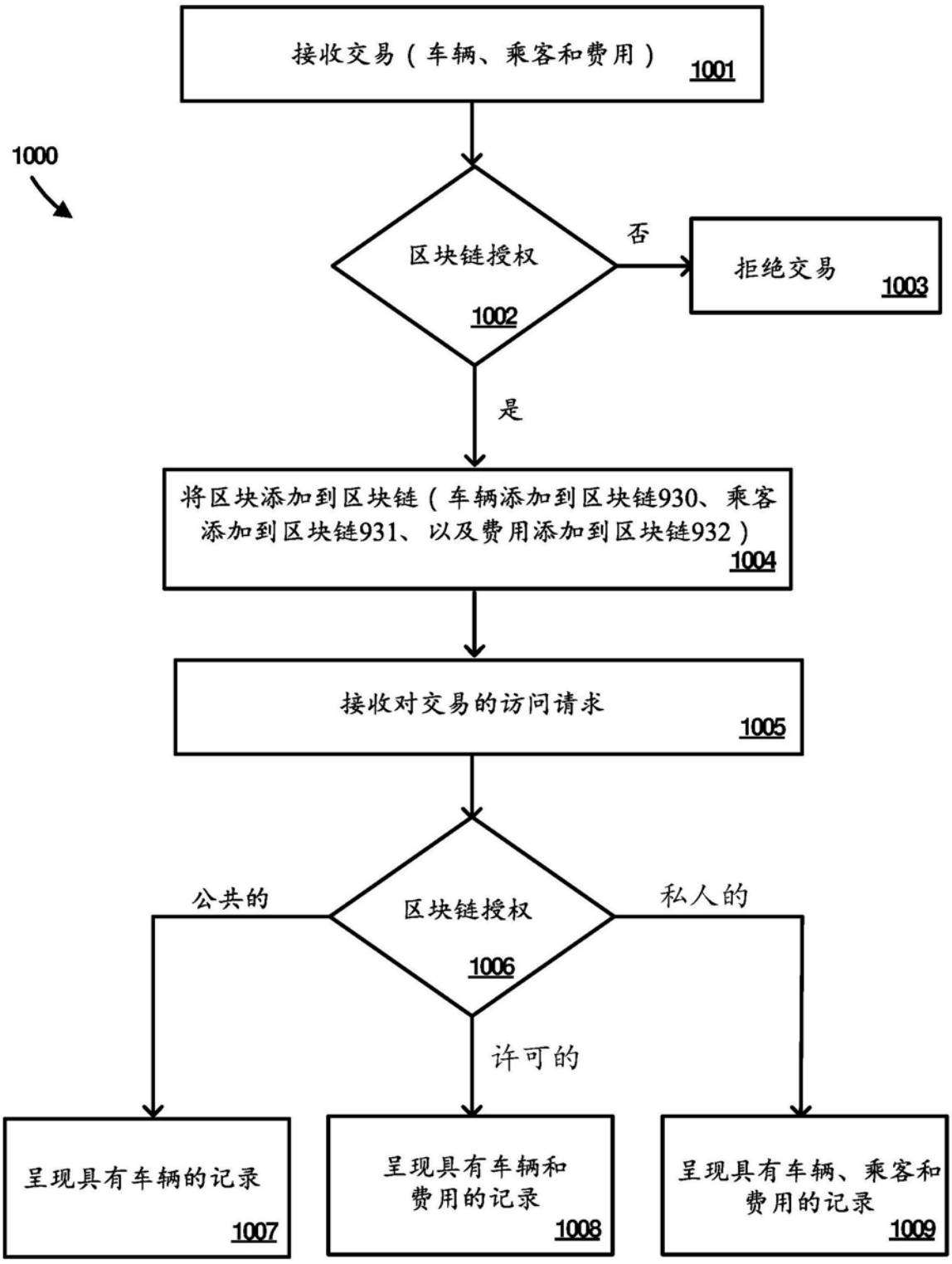

1000
接收交易（车辆、乘客和费用）
1001
区块链授权
1002
否
拒绝交易
1003
是
将区块添加到区块链（车辆添加到区块链930、乘客添加到区块链931、以及费用添加到区块链932）
1004
接收对交易的访问请求
1005
区块链授权
1006
公共的
私人的
许可的
呈现具有车辆的记录
1007
呈现具有车辆和费用的记录
1008
呈现具有车辆、乘客和费用的记录
1009

图10

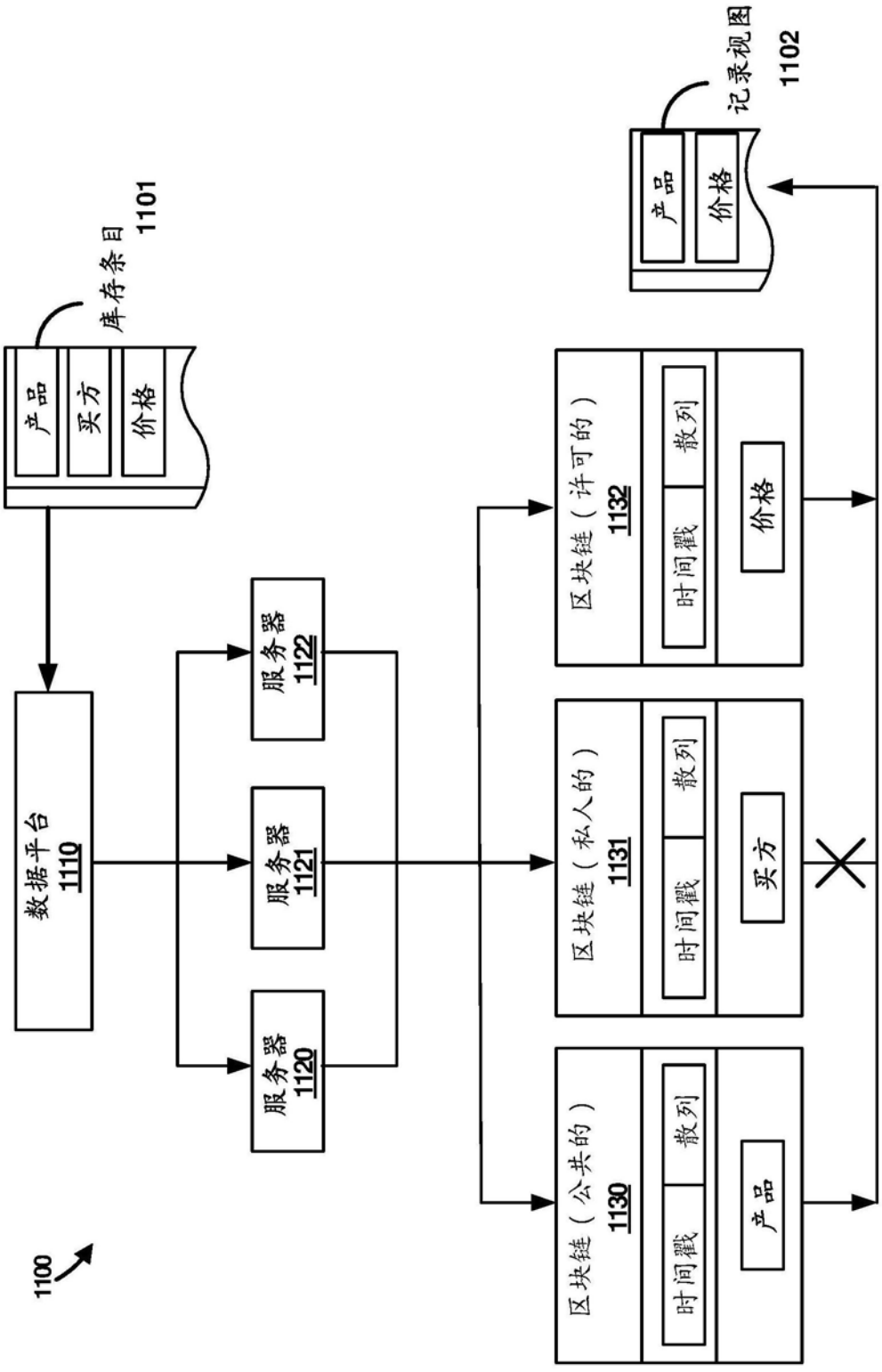

1100
数据平台
1110
服务器
1120
服务器
1121
服务器
1122
库存条目
1101
产品
买方
价格
记录视图
1102
产品
价格
区块链（公共的）
1130
时间戳
散列
产品
区块链（私人的）
1131
时间戳
散列
买方
区块链（许可的）
1132
时间戳
散列
价格

图11

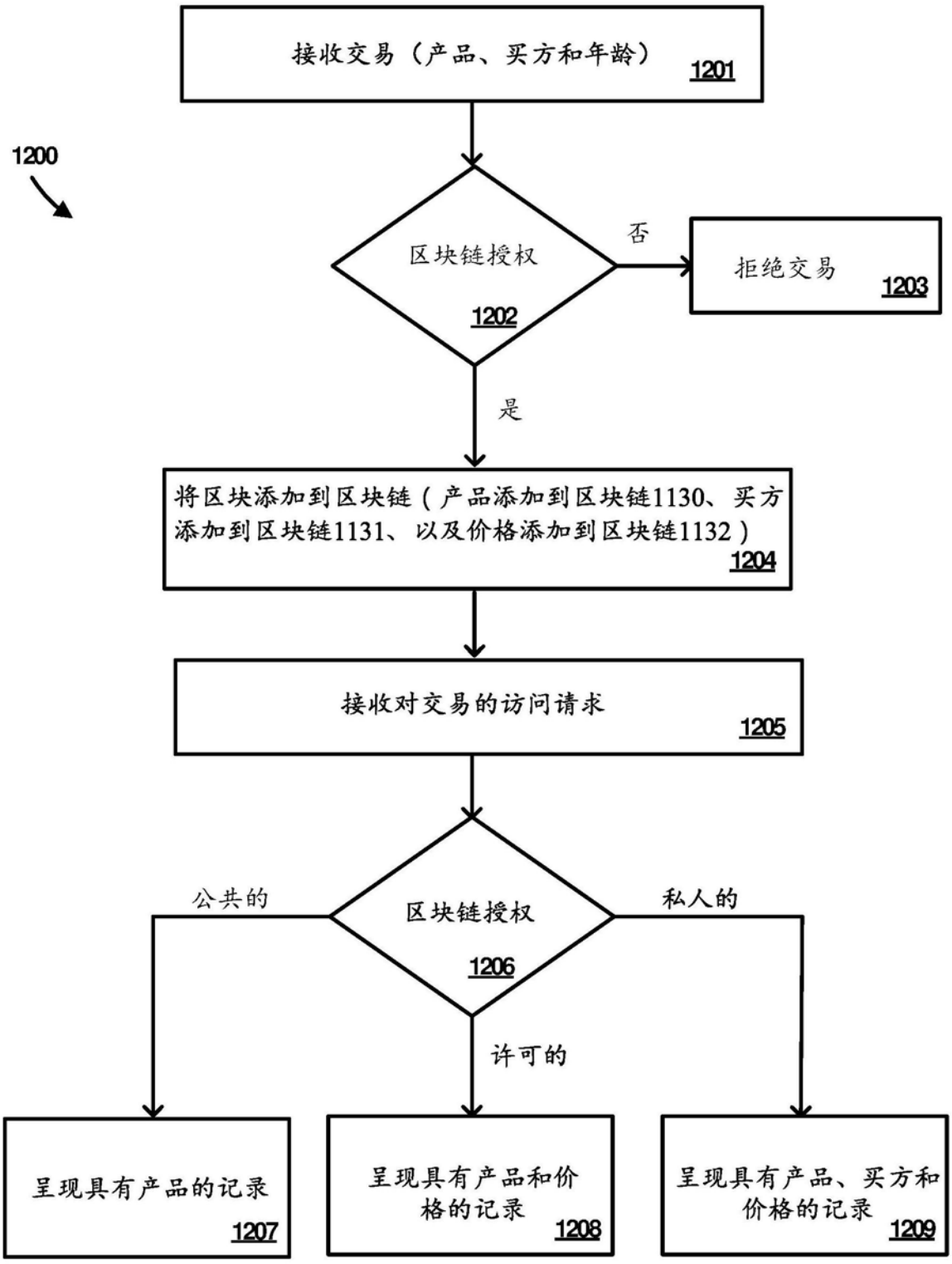

1200
接收交易（产品、买方和年龄）
1201
区块链授权
1202
否
拒绝交易
1203
是
将区块添加到区块链（产品添加到区块链1130、买方添加到区块链1131、以及价格添加到区块链1132）
1204
接收对交易的访问请求
1205
区块链授权
1206
公共的
私人的
许可的
呈现具有产品的记录
1207
呈现具有产品和价格的记录
1208
呈现具有产品、买方和价格的记录
1209

图12

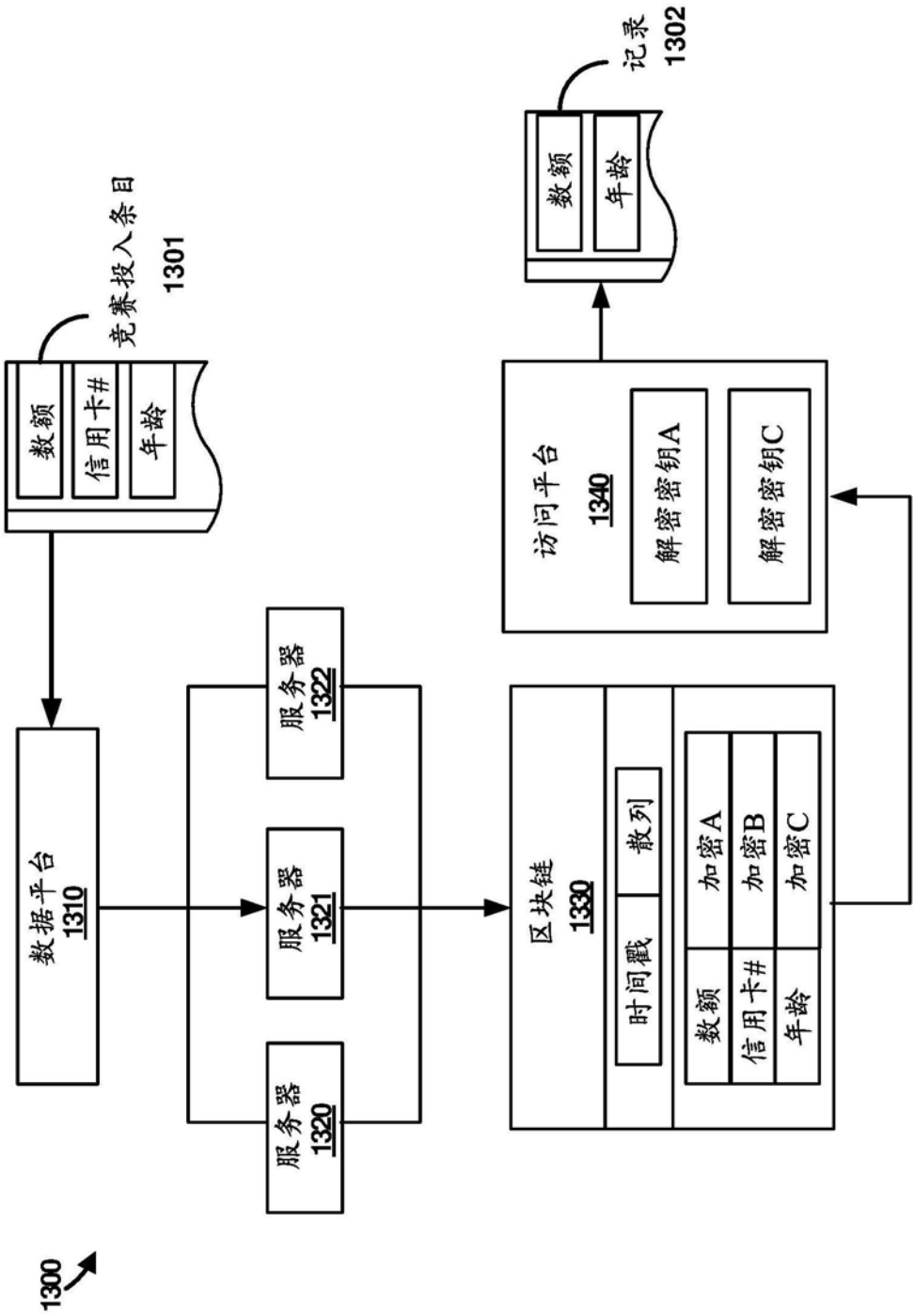

竞赛投入条目
1301
数额
信用卡#
年龄
记录
1302
数额
年龄
访问平台
1340
解密密钥A
解密密钥C
数据平台
1310
服务器
1322
服务器
1321
服务器
1320
区块链
1330
时间戳
散列
数额
信用卡#
年龄
加密A
加密B
加密C
1300

图13

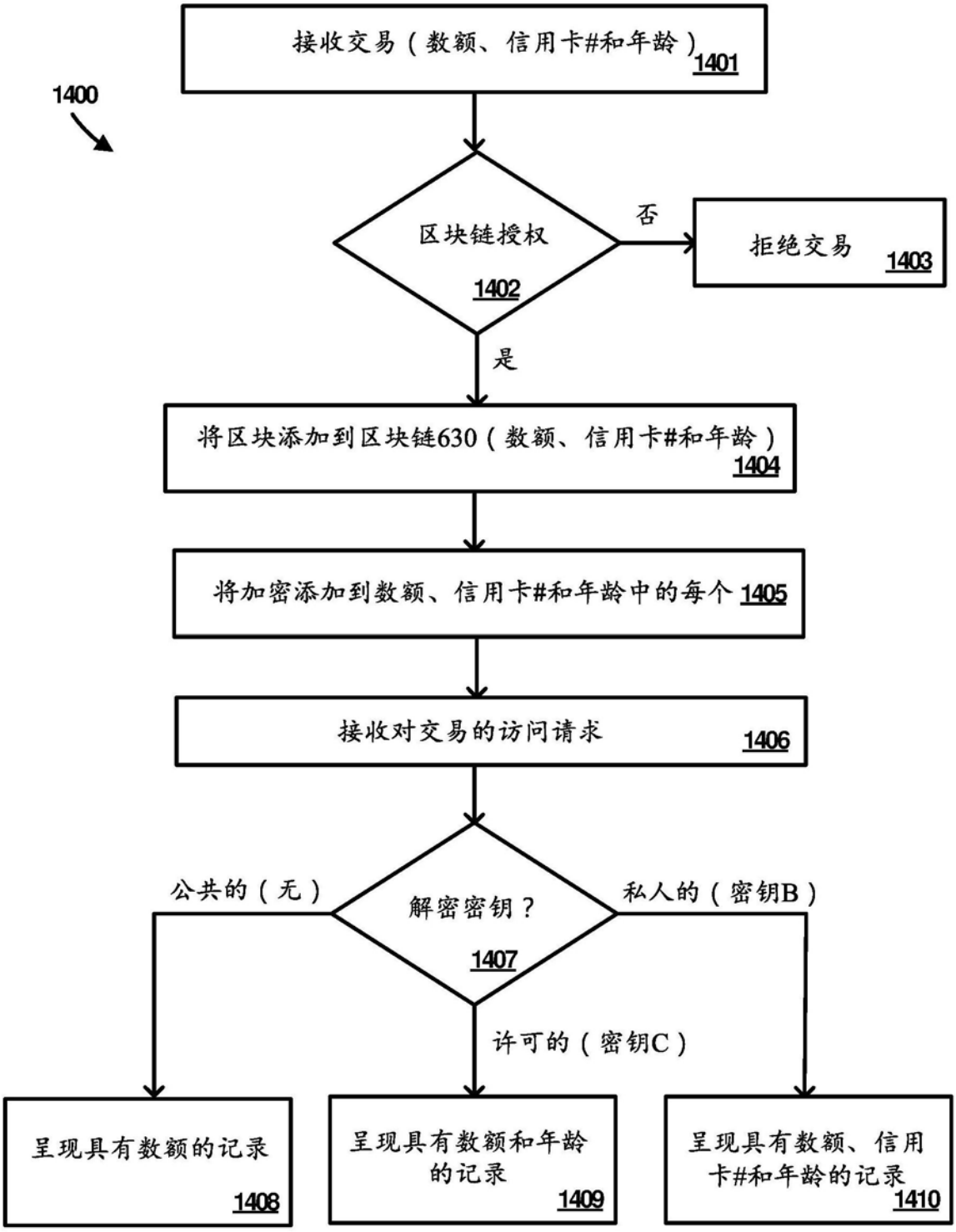

1400
接收交易（数额、信用卡#和年龄）
1401
区块链授权
1402
否
拒绝交易
1403
是
将区块添加到区块链630（数额、信用卡#和年龄）
1404
将加密添加到数额、信用卡#和年龄中的每个 1405
接收对交易的访问请求
1406
公共的（无）
解密密钥？
1407
私人的（密钥B）
许可的（密钥C）
呈现具有数额的记录
1408
呈现具有数额和年龄的记录
1409
呈现具有数额、信用卡#和年龄的记录
1410

图14

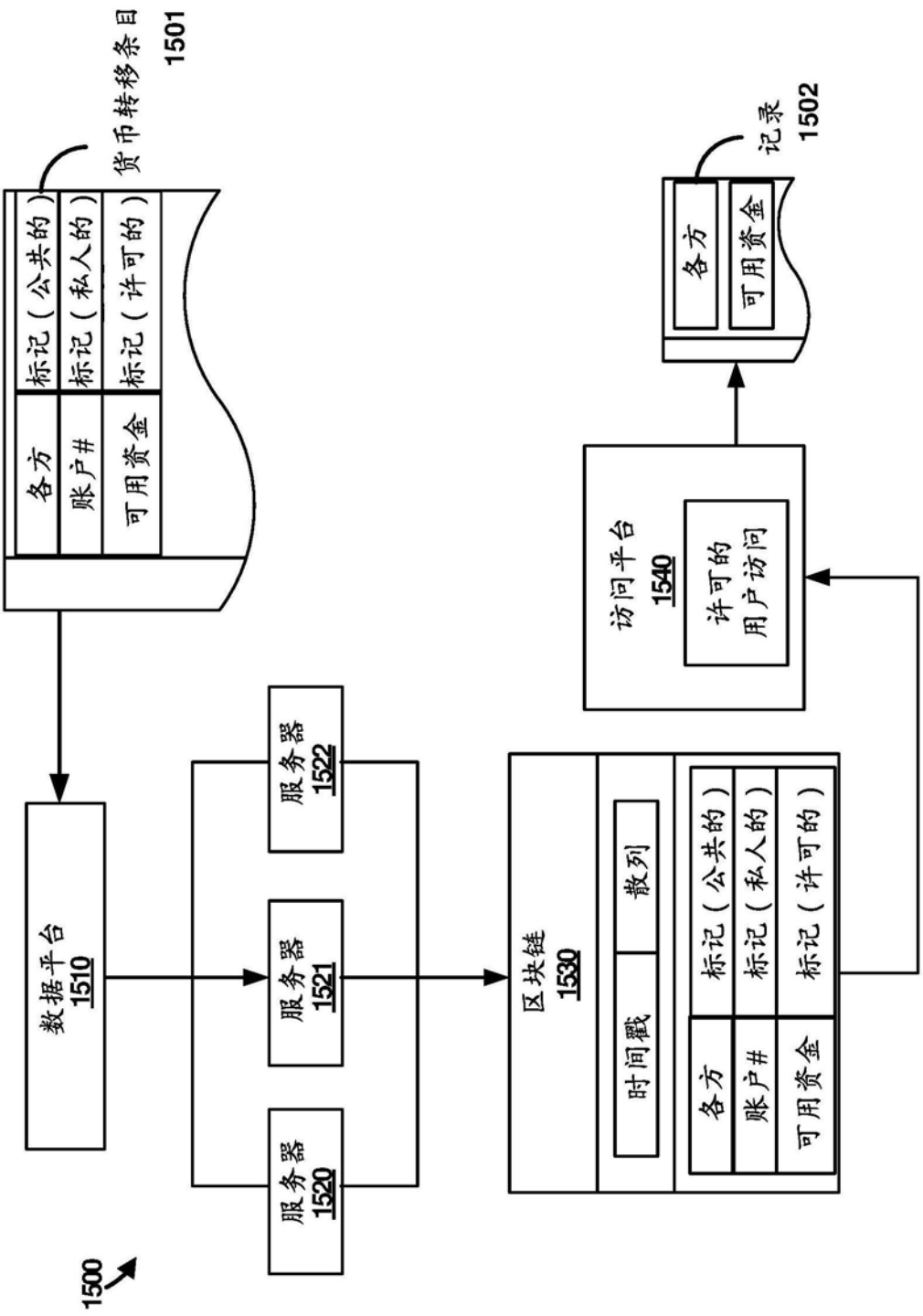

货币转移条目
1501
各方
账户#
可用资金
标记（公共的）
标记（私人的）
标记（许可的）
记录
1502
各方
可用资金
访问平台
1540
许可的
用户访问
数据平台
1510
服务器
1520
服务器
1521
服务器
1522
区块链
1530
时间戳
散列
各方
账户#
可用资金
标记（公共的）
标记（私人的）
标记（许可的）
1500

图15

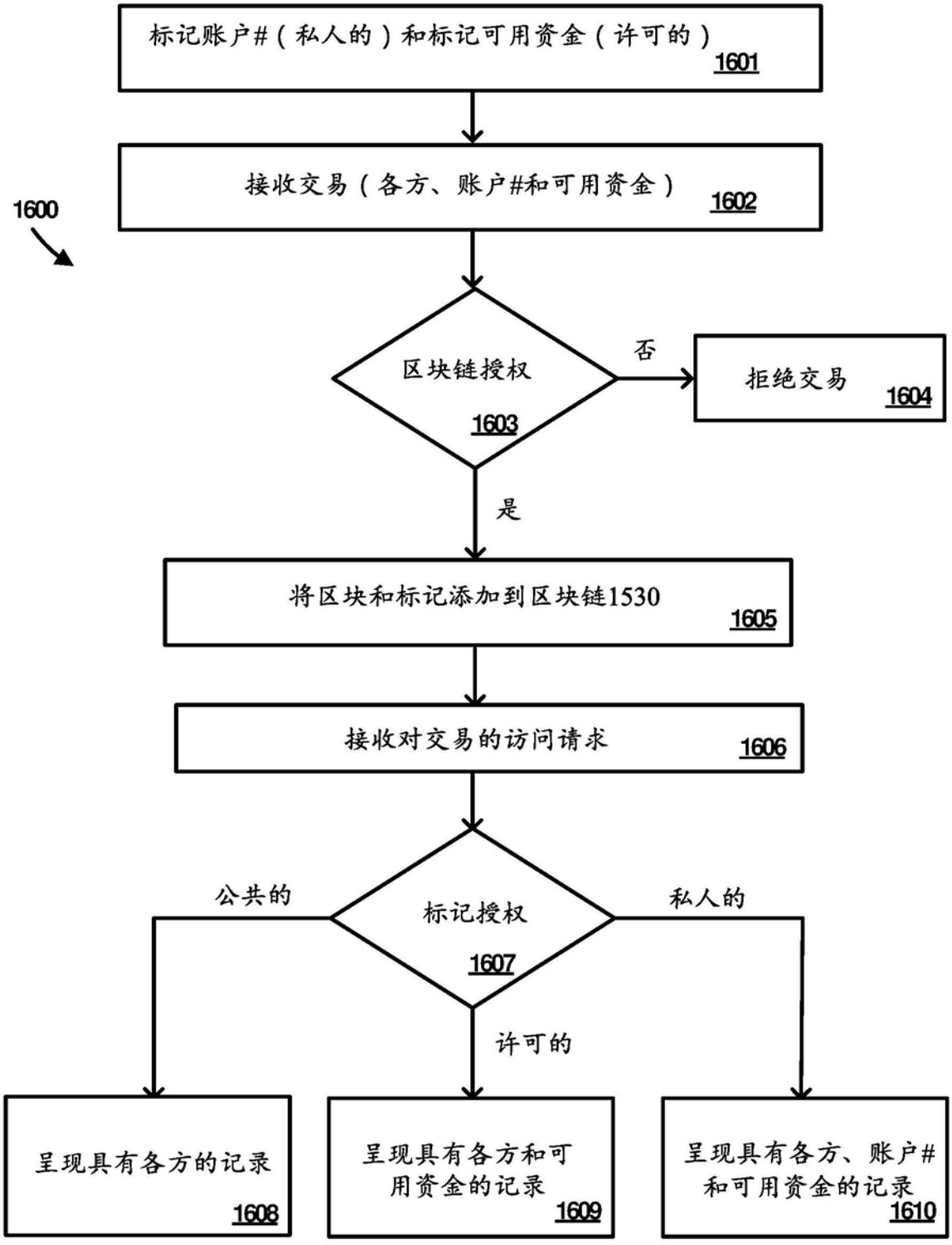

标记账户#（私人的）和标记可用资金（许可的）
1601
接收交易（各方、账户#和可用资金）
1602
1600
区块链授权
1603
否
拒绝交易
1604
是
将区块和标记添加到区块链1530
1605
接收对交易的访问请求
1606
公共的
标记授权
1607
私人的
许可的
呈现具有各方的记录
1608
呈现具有各方和可用资金的记录
1609
呈现具有各方、账户#和可用资金的记录
1610

图16

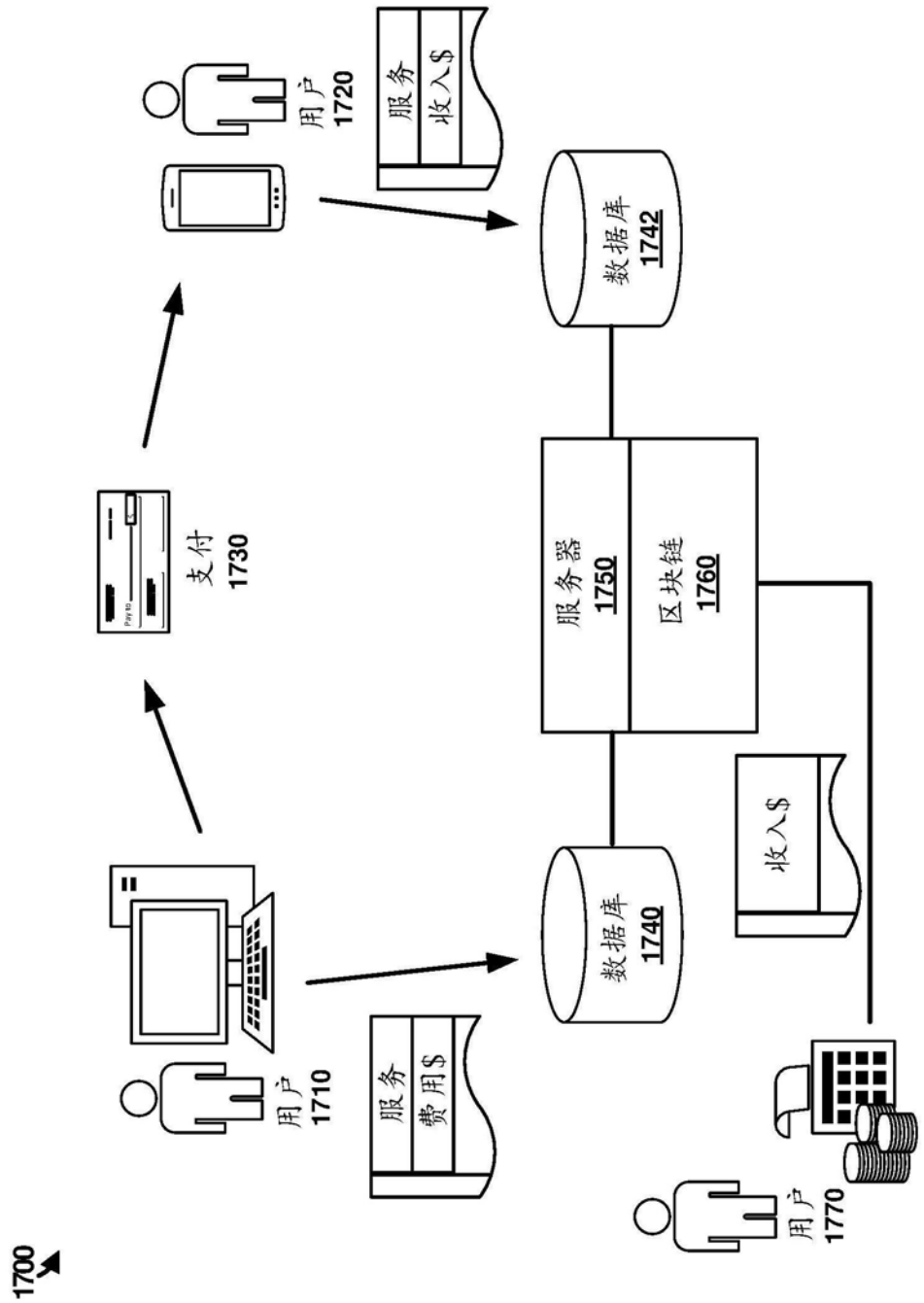

1700
用户
1710
服务
费用$
支付
1730
用户
1720
服务
收入$
数据库
1742
服务器
1750
区块链
1760
数据库
1740
收入$
用户
1770

图17

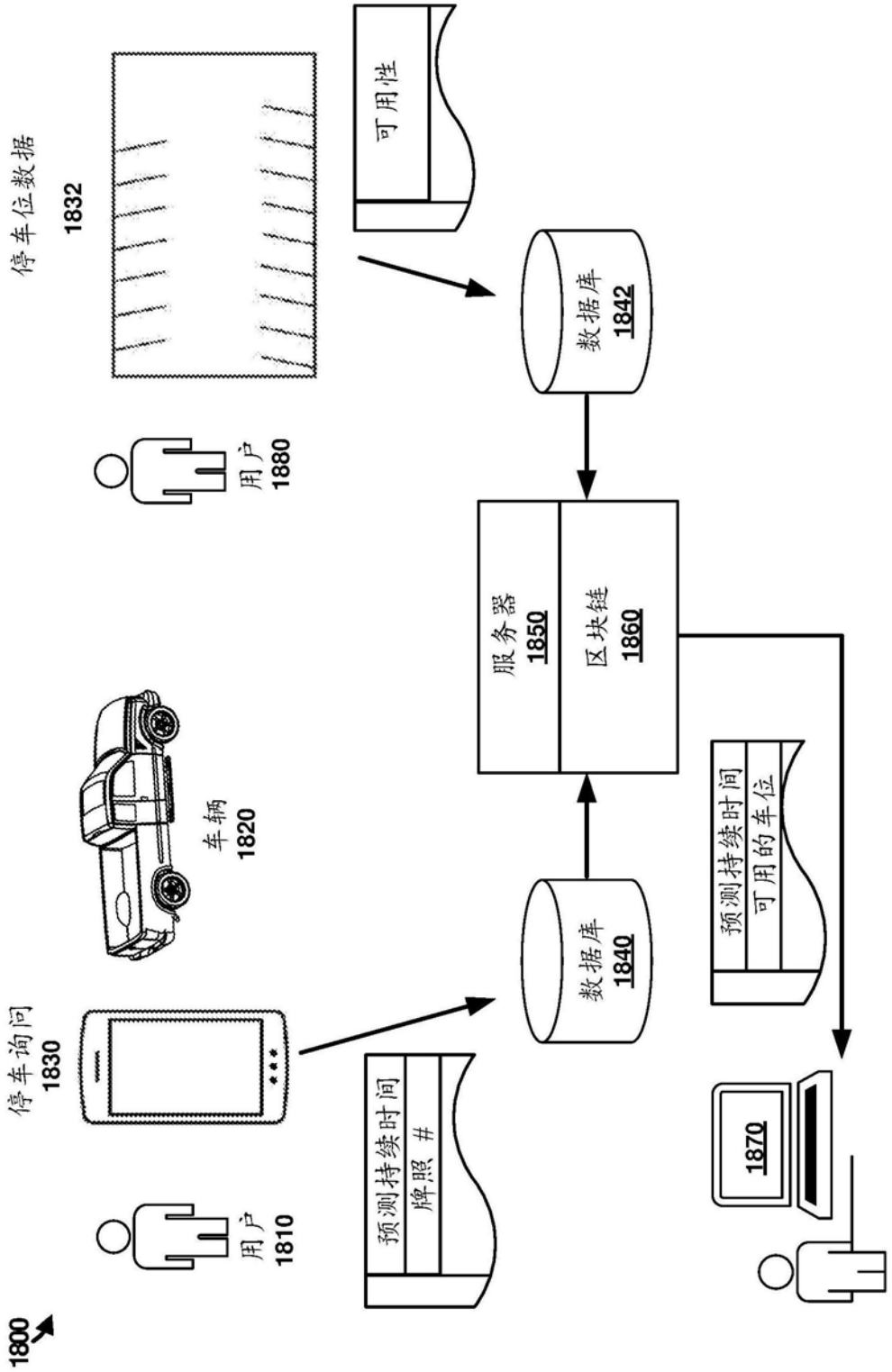

1800
停车询问
1830
用户
1810
预测持续时间
牌照 #
车辆
1820
停车位数据
1832
用户
1880
可用性
数据库
1842
服务器
1850
区块链
1860
数据库
1840
预测持续时间
可用的车位
1870

图18

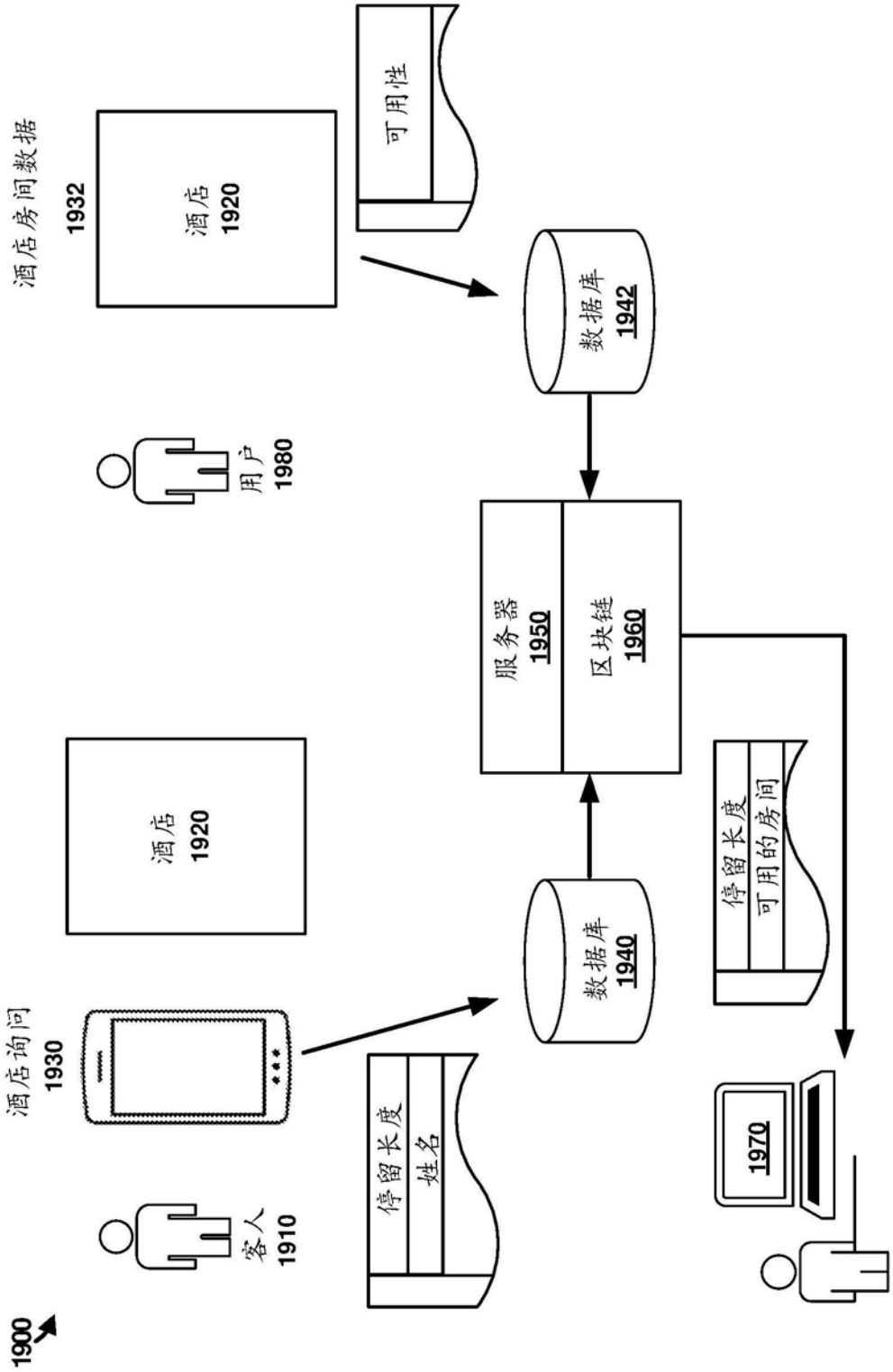

1900
客人
1910
酒店询问
1930
酒店房间数据
1932
酒店
1920
酒店
1920
用户
1980
停留长度
姓名
可用性
数据库
1940
数据库
1942
服务器
1950
区块链
1960
停留长度
可用的房间
1970

图19

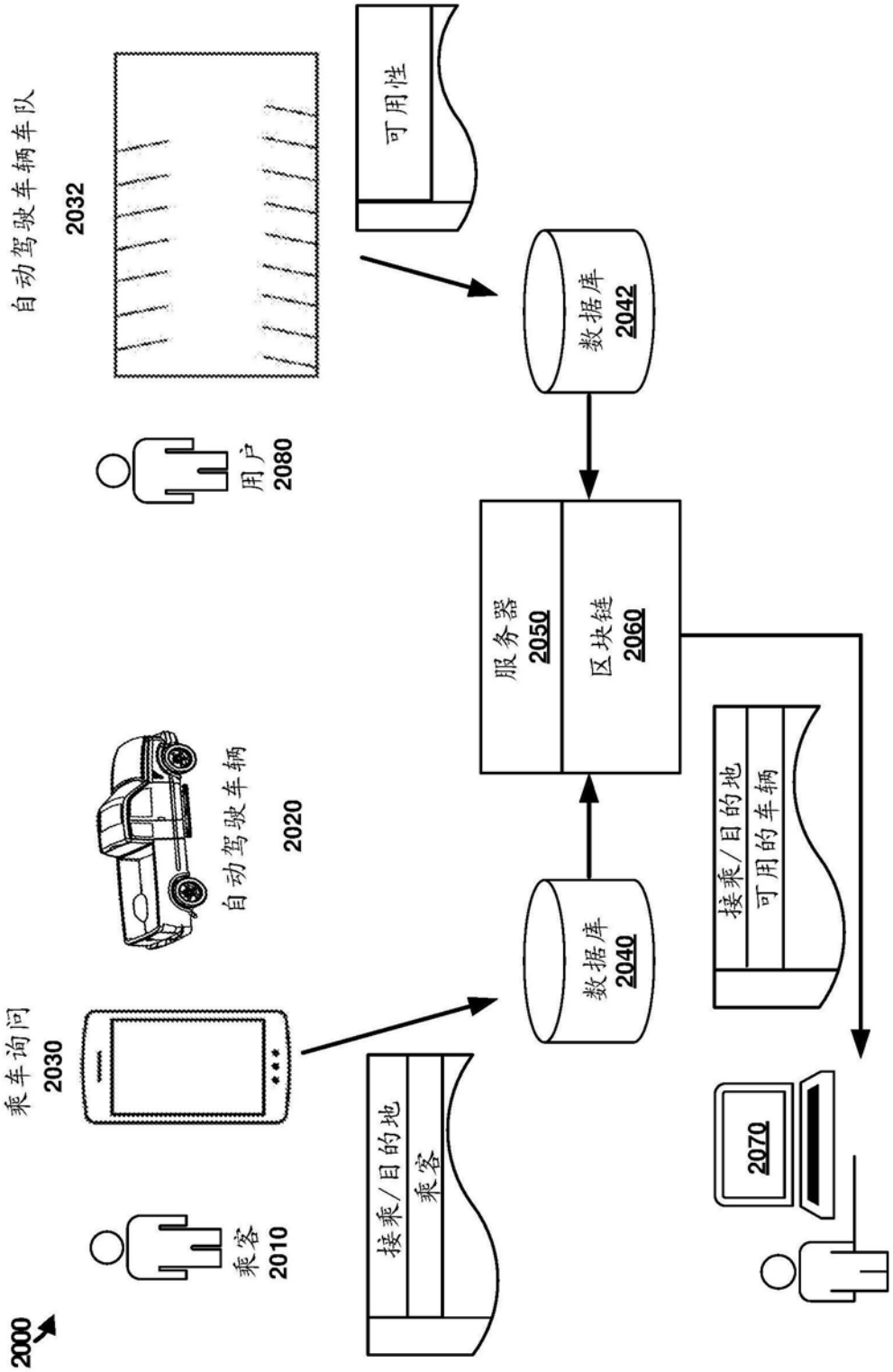

2000
乘客
2010
乘车询问
2030
自动驾驶车辆
2020
自动驾驶车辆车队
2032
用户
2080
接乘/目的地
乘客
数据库
2040
服务器
2050
区块链
2060
可用性
数据库
2042
接乘/目的地
可用的车辆
2070

图20

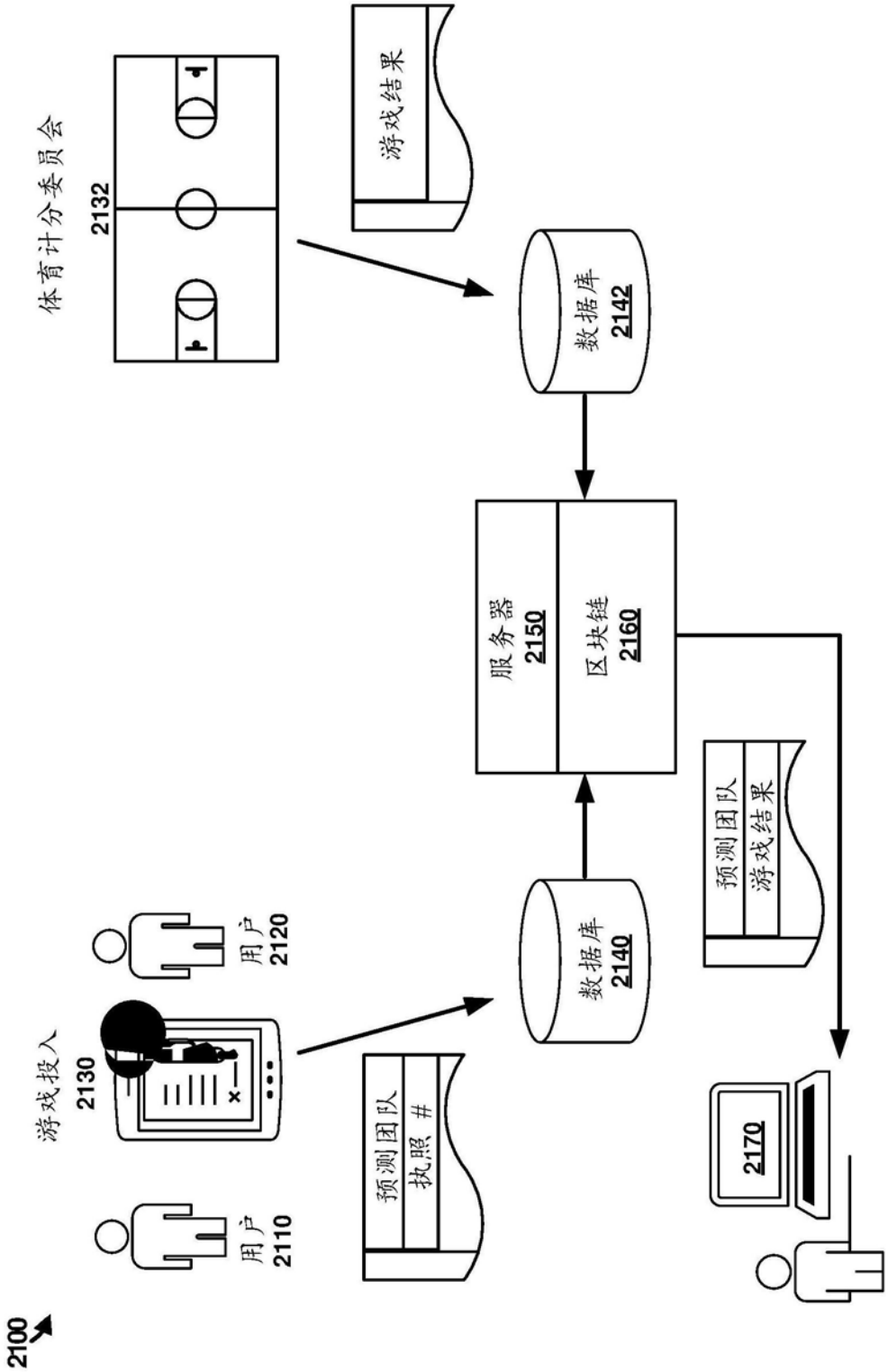

2100
游戏投入
2130
用户
2110
用户
2120
预测团队
执照 #
数据库
2140
服务器
2150
区块链
2160
预测团队
游戏结果
2170
体育计分委员会
2132
游戏结果
数据库
2142

图21

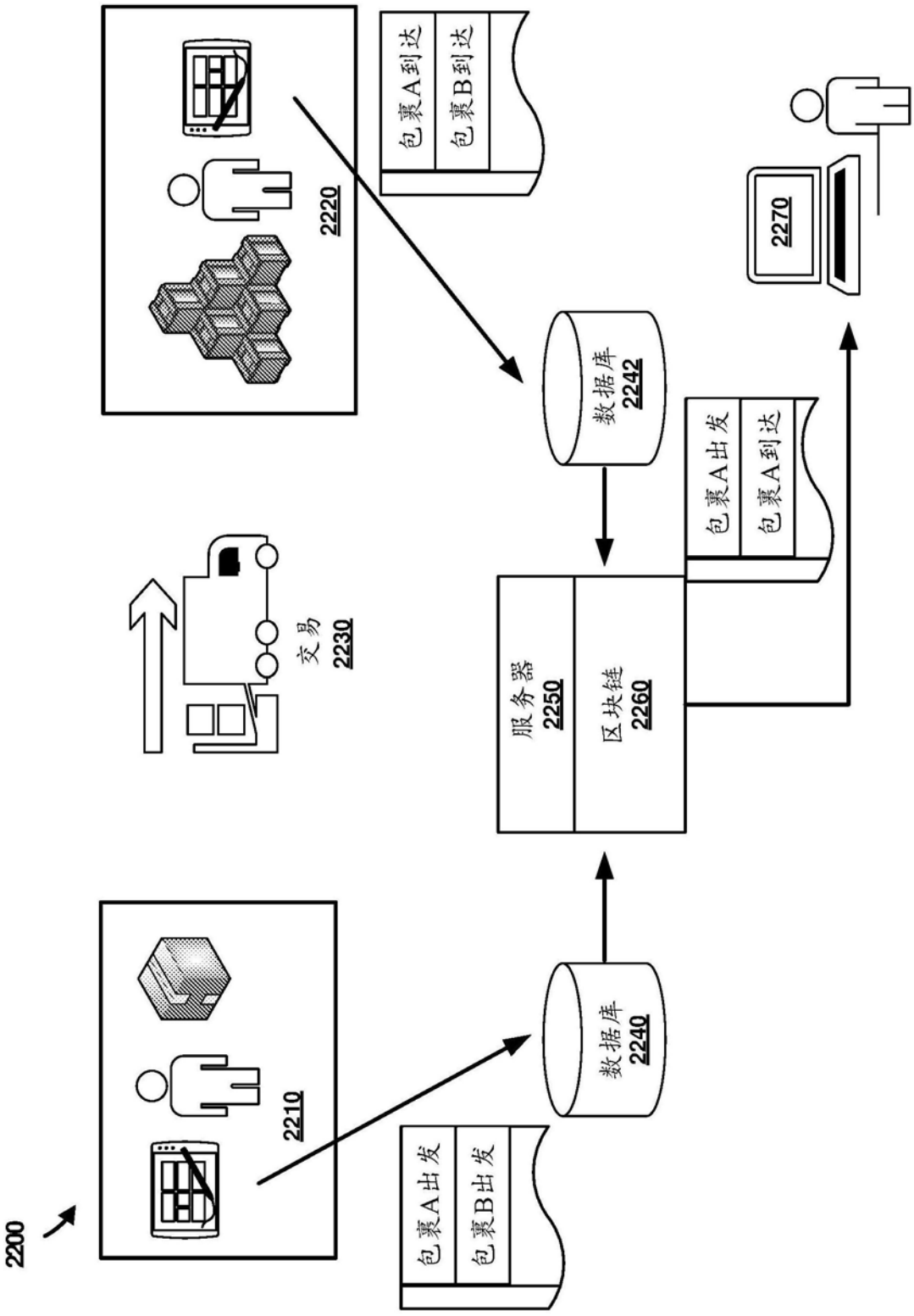

2200
2210
包裹A出发
包裹B出发
数据库
2240
服务器
2250
区块链
2260
交易
2230
2220
包裹A到达
包裹B到达
数据库
2242
包裹A出发
包裹A到达
2270

图22

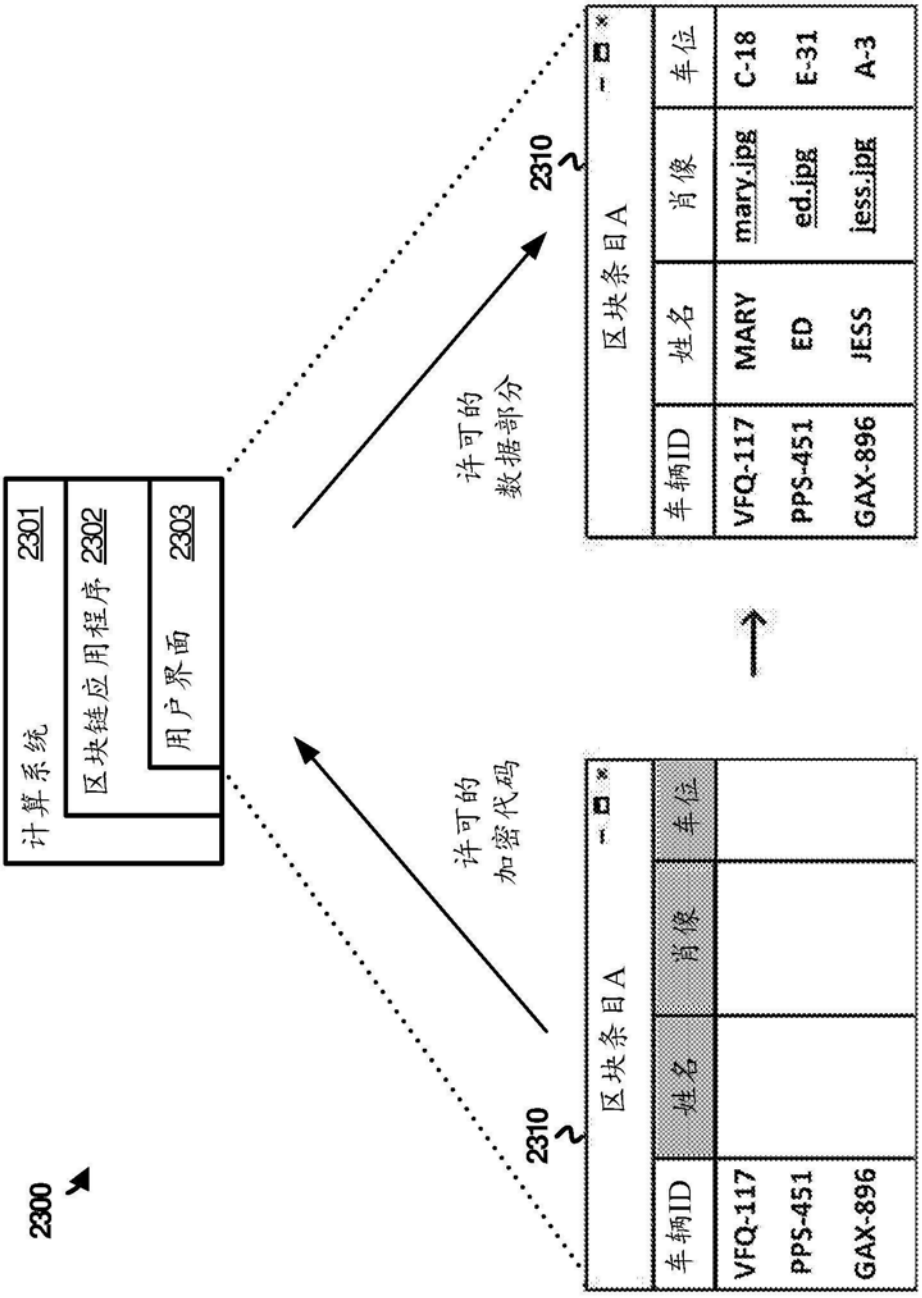

2300
计算系统 2301
区块链应用程序 2302
用户界面 2303
许可的
加密代码
许可的
数据部分
2310
区块条目A
车辆ID
姓名
肖像
车位
VFQ-117
PPS-451
GAX-896
MARY
ED
JESS
mary.jpg
ed.jpg
jess.jpg
C-18
E-31
A-3

图23

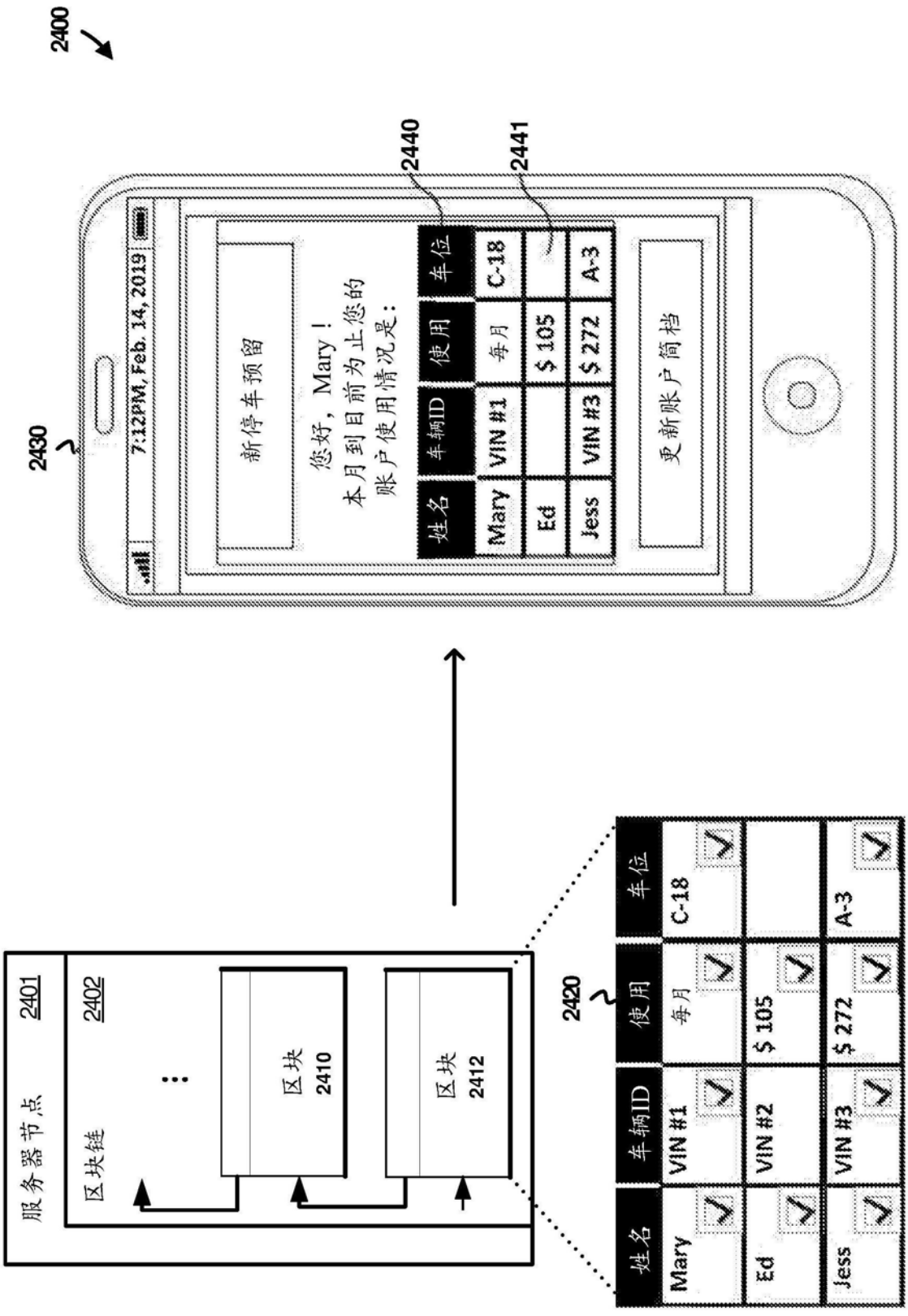

2400
2430
7:12PM, Feb. 14, 2019
新停车预留
您好，Mary！
本月到目前为止您的
账户使用情况是：
2440
2441
姓名 车辆ID 使用 车位
Mary VIN #1 每月 C-18
Ed $ 105
Jess VIN #3 $ 272 A-3
更新账户简档
服务器节点 2401
区块链 2402
区块 2410
区块 2412
2420
姓名 车辆ID 使用 车位
Mary VIN #1 每月 C-18
Ed VIN #2 $ 105
Jess VIN #3 $ 272 A-3

图24

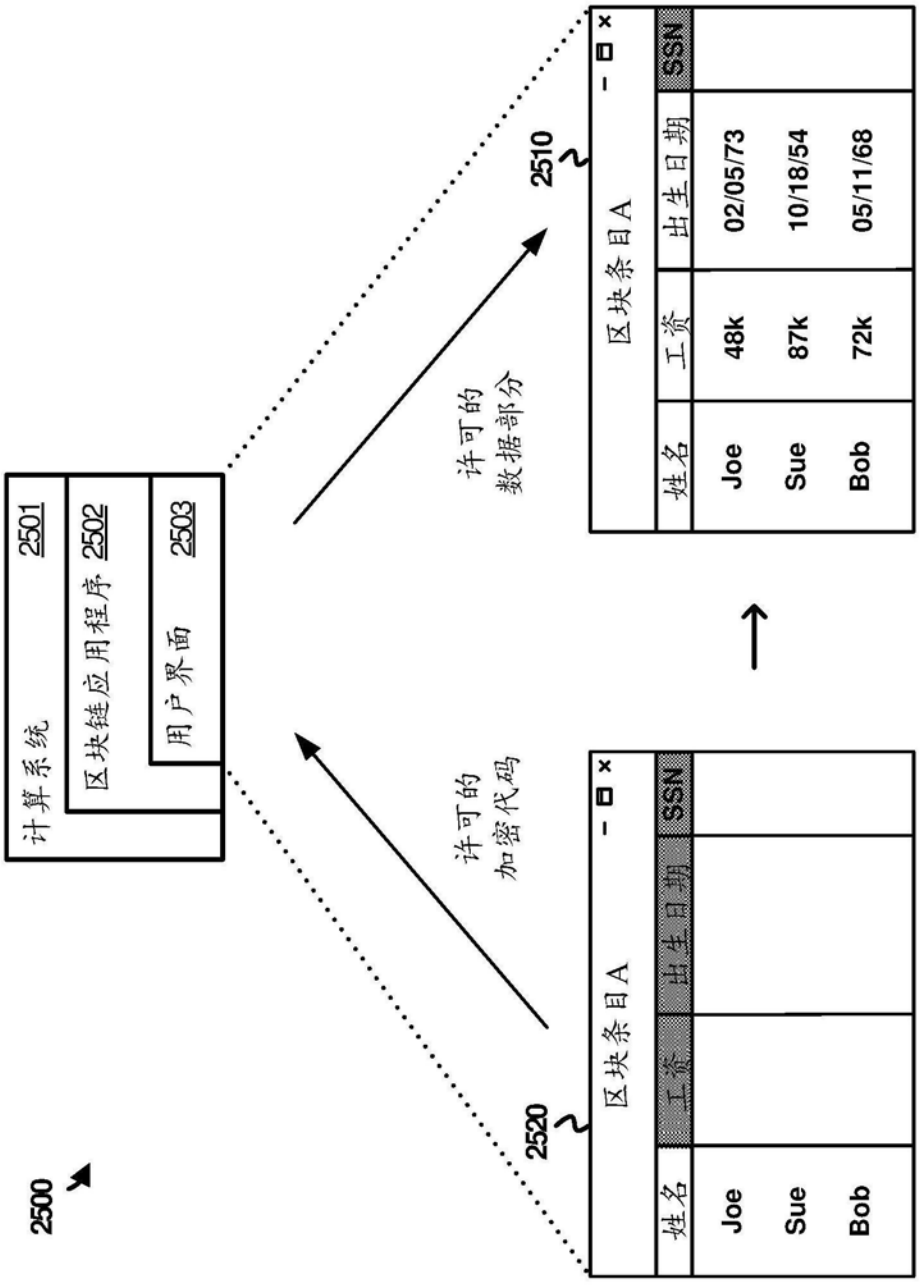

2500
计算系统 2501
区块链应用程序 2502
用户界面 2503
许可的
加密代码
许可的
数据部分
2520
2510
区块条目A
区块条目A
姓名
工资
出生日期
SSN
Joe
Sue
Bob
48k
87k
72k
02/05/73
10/18/54
05/11/68

图25

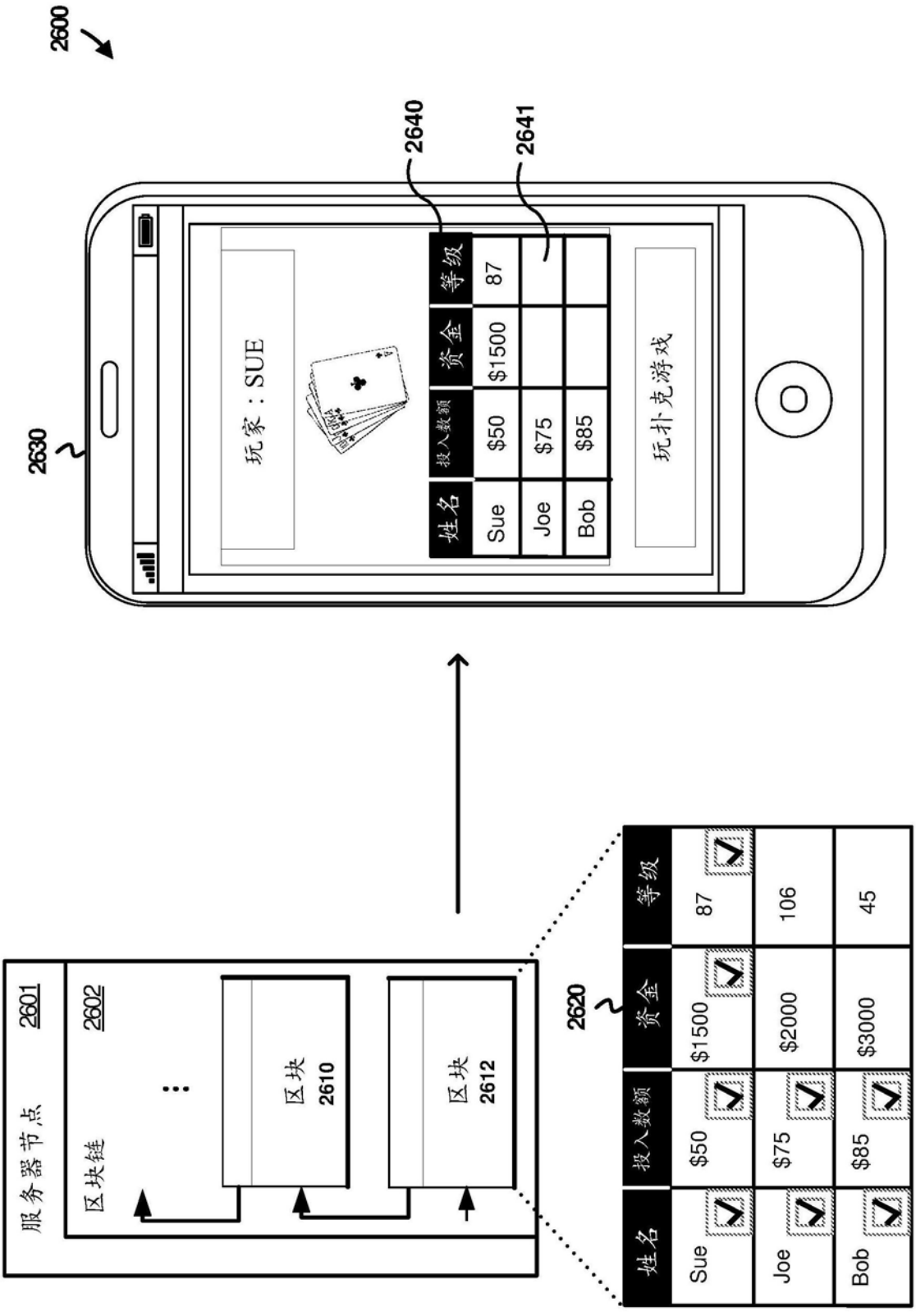

2600
2640
2641
2630
玩家：SUE
姓名
投入数额
资金
等级
Sue
$50
$1500
87
Joe
$75
Bob
$85
玩扑克游戏
服务器节点
2601
区块链
2602
区块
2610
区块
2612
2620
姓名
投入数额
资金
等级
Sue
$50
$1500
87
Joe
$75
$2000
106
Bob
$85
$3000
45

图26

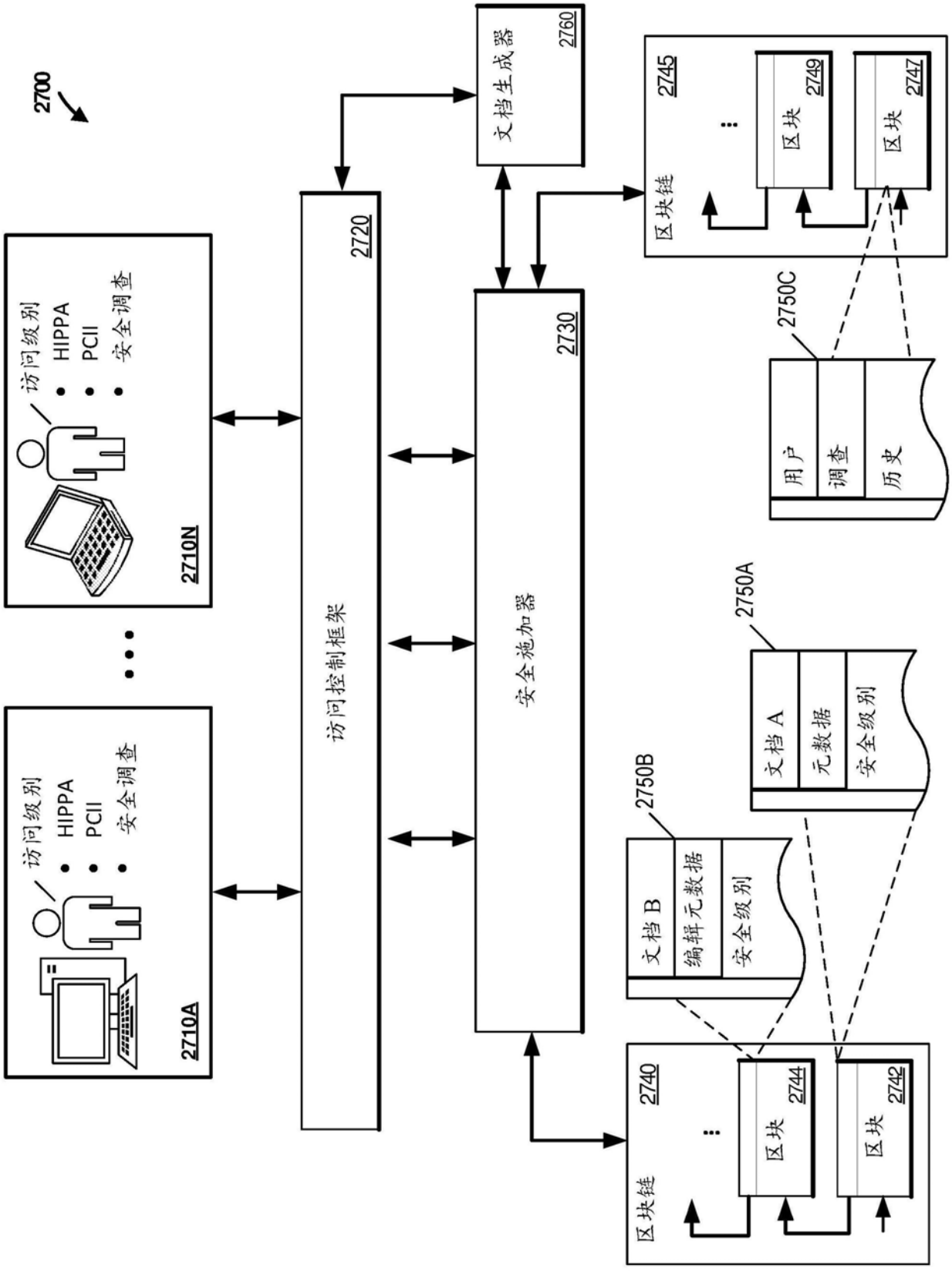

2700
访问级别
• HIPPA
• PCII
• 安全调查
2710A
2710N
访问控制框架
2720
安全施加器
2730
文档生成器
2760
区块链
2745
区块
2749
区块
2747
2750C
用户
调查
历史
2750A
文档 A
元数据
安全级别
2750B
文档 B
编辑元数据
安全级别
区块链
2740
区块
2744
区块
2742

图27

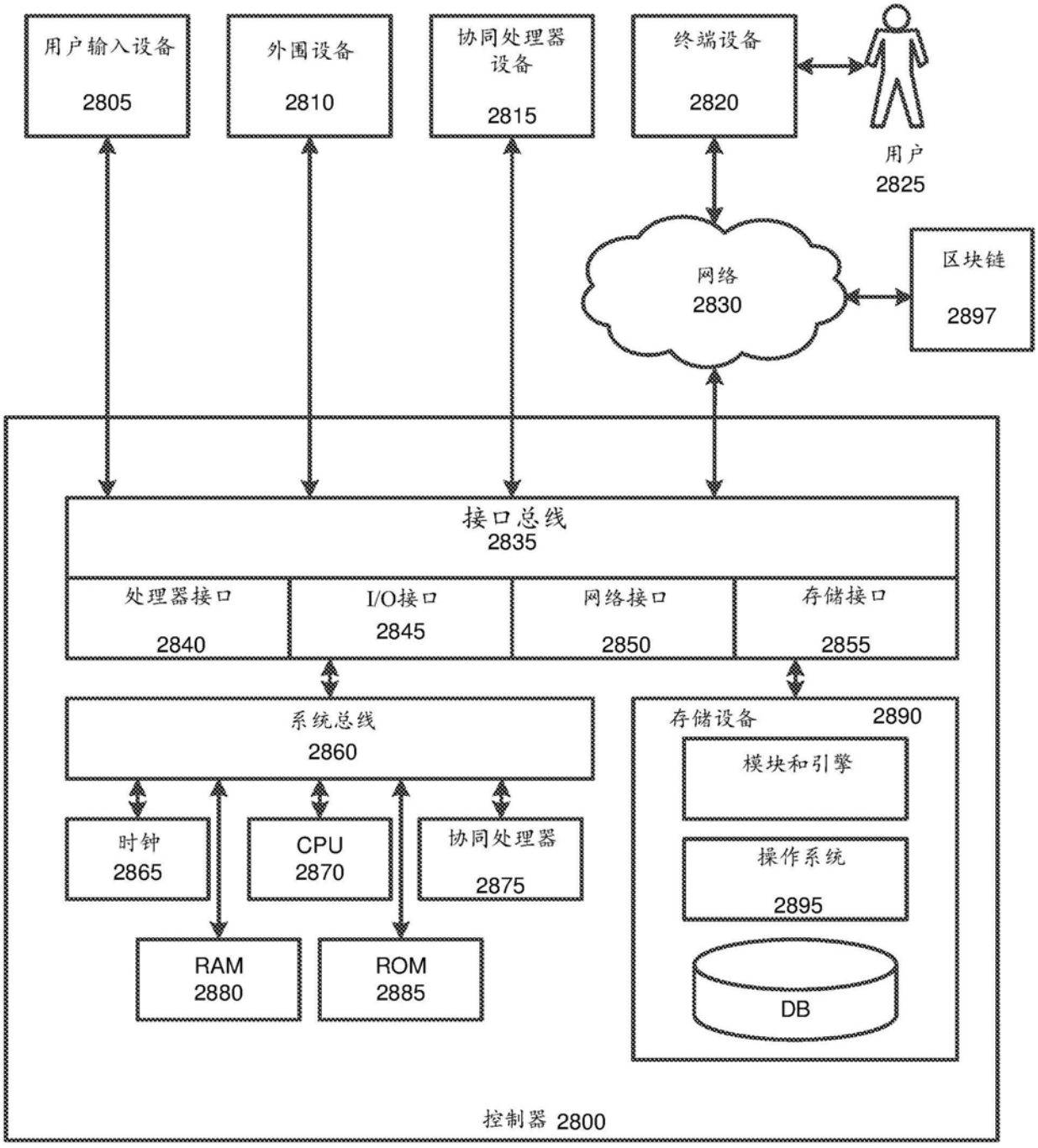

用户输入设备
2805
外围设备
2810
协同处理器设备
2815
终端设备
2820
用户
2825
网络
2830
区块链
2897
接口总线
2835
处理器接口
2840
I/O接口
2845
网络接口
2850
存储接口
2855
系统总线
2860
存储设备
2890
模块和引擎
时钟
2865
CPU
2870
协同处理器
2875
操作系统
2895
RAM
2880
ROM
2885
DB
控制器 2800

图28