



(12) 发明专利

(10) 授权公告号 CN 113168622 B

(45) 授权公告日 2022.03.18

(21) 申请号 201980076006.8

(22) 申请日 2019.09.18

(65) 同一申请的已公布的文献号
申请公布号 CN 113168622 A

(43) 申请公布日 2021.07.23

(30) 优先权数据
62/733,535 2018.09.19 US
16/228,555 2018.12.20 US(85) PCT国际申请进入国家阶段日
2021.05.18(86) PCT国际申请的申请数据
PCT/US2019/051783 2019.09.18(87) PCT国际申请的公布数据
WO2020/061226 EN 2020.03.26(73) 专利权人 易享信息技术有限公司
地址 美国加利福尼亚州

(72) 发明人 P·K·帕德玛纳伯翰

(74) 专利代理机构 北京市联德律师事务所
11361

代理人 黄大正 张来光

(51) Int.Cl.
G06Q 20/02 (2006.01)
G06Q 20/40 (2006.01)
G06Q 20/38 (2006.01)
G06F 16/27 (2006.01)
G06F 21/62 (2006.01)(56) 对比文件
CN 106537346 A, 2017.03.22
CN 107169371 A, 2017.09.15
US 8326876 B1, 2012.12.04
US 8271641 B2, 2012.09.18
WO 2017003974 A1, 2017.01.05
QI XIA 等. MedShare: Trust-less
Medical Data Sharing Among Cloud Service
Providers via Blockchain.《IEEE ACCESS》
.2017,第5卷第14757-14767页.

审查员 赵伟华

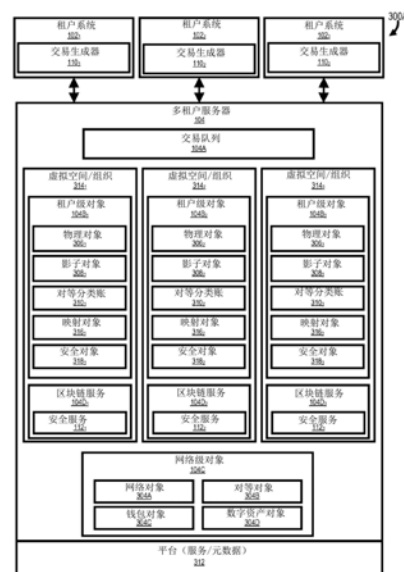
权利要求书3页 说明书16页 附图11页

(54) 发明名称

区块链网络中的基于字段的对等许可

(57) 摘要

描述了一种用于多租户服务器管理区块链网络中的数据的方法。方法包括生成用于网络的交换对象，其中交换对象包括成组的交换字段以及交换字段的集合中的每个交换字段和与网络中的每个对等方相关联的对象的字段之间的映射；确定网络中每个交换字段和每个对等方的许可；使用交换对象代表网络中的第一对等方生成交易对象，其中，交易对象包括用于成组的交换字段的成组的字段值，并且基于许可对成组的值中的一个或多个字段值进行加密；以及使交易对象对网络中的第二对等方可用，以尝试获得用于改变第一对等方的对象的共识。



1. 一种用于多租户服务器管理对等区块链网络中的数据的方法,所述方法包括:

由所述多租户服务器生成用于所述对等区块链网络的交换对象,其中所述交换对象包括一个或多个交换字段以及所述一个或多个交换字段中的每个交换字段与和所述对等区块链网络中的每个对等方相关联的物理对象的字段之间的映射;

由所述多租户服务器确定针对所述一个或多个交换字段中的交换字段和所述对等区块链网络中的对等方的每个组合的许可;

基于所述交换对象,由所述多租户服务器代表所述对等区块链网络中的第一对等方生成交易对象,其中所述交易对象包括所述一个或多个交换字段的成组的字段值,并且基于确定的许可对所述成组的字段值中的一个或多个字段值进行加密;和

由所述多租户服务器代表所述第一对等方使得所述交易对象对所述对等区块链网络中的第二对等方可用,以尝试获得改变对应于所述第一对等方的物理对象的共识。

2. 根据权利要求1所述的方法,还包括:

由所述多租户服务器生成对应于所述第一对等方的第一组许可钥;和

由所述多租户服务器生成对应于所述第二对等方的第二组许可钥。

3. 根据权利要求2所述的方法,其中所述第一组许可钥中的每个许可钥对应于所述第一对等方的关于所述一个或多个交换字段中的第一交换字段的许可,并且

其中所述第二组许可钥中的每个许可钥对应于所述第二对等方的关于所述一个或多个交换字段中的第二交换字段的许可。

4. 根据权利要求3所述的方法,其中生成所述交易对象包括使用所述第一组许可钥对所述一个或多个字段值进行加密。

5. 根据权利要求4所述的方法,其中所述第一组许可钥包括针对所述一个或多个交换字段中对应的交换字段读取、更新和插入访问许可。

6. 根据权利要求5所述的方法,还包括:

响应于从所述对等区块链网络中的第二对等方接收共识,由所述多租户服务器将所述交易对象添加到所述第一对等方的第一分类账和所述第二对等方的第二分类账;和

由所述多租户服务器代表所述第二对等方使用所述第二组许可钥读取所述一个或多个字段值。

7. 根据权利要求6所述的方法,其中读取所述一个或多个字段值包括:使用所述第二组许可钥中的第一钥对所述一个或多个字段值中的第一值进行解密,并且使用所述第二组许可钥中的第二钥对所述一个或多个字段值中的第二值进行解密。

8. 根据权利要求1所述的方法,其中所述多租户服务器包括用于所述对等区块链网络中的第一对等方的虚拟空间,

其中所述虚拟空间包括对所述第一对等方可用而所述对等区块链网络中的第二对等方不可访问的数据和服务。

9. 一种非暂态机器可读存储介质,其包含指令,所述指令当由多租户服务器的处理器执行时致使所述处理器:

生成用于对等区块链网络的交换对象,其中所述交换对象包括一个或多个交换字段以及所述一个或多个交换字段中的每个交换字段与和所述对等区块链网络中的每个对等方相关联的物理对象的字段之间的映射;

确定针对所述一个或多个交换字段中的交换字段和所述对等区块链网络中的对等方的每个组合的许可；

基于所述交换对象，代表所述对等区块链网络中的第一对等方生成交易对象，其中所述交易对象包括所述一个或多个交换字段的成组的字段值，并且基于确定的许可对所述成组的字段值中的一个或多个字段值进行加密；和

代表所述第一对等方使得所述交易对象对所述对等区块链网络中的第二对等方可用，以尝试获得改变对应于所述第一对等方的物理对象的共识。

10. 根据权利要求9所述的非暂态机器可读存储介质，其中所述指令还致使所述处理器：

生成对应于所述第一对等方的第一组许可钥；和

生成对应于所述第二对等方的第二组许可钥。

11. 根据权利要求10所述的非暂态机器可读存储介质，其中所述第一组许可钥中的每个许可钥对应于所述第一对等方的关于所述一个或多个交换字段中的第一交换字段的许可，并且

其中所述第二组许可钥中的每个许可钥对应于所述第二对等方的关于所述一个或多个交换字段中的第二交换字段的许可。

12. 根据权利要求11所述的非暂态机器可读存储介质，其中生成所述交易对象包括使用所述第一组许可钥对所述一个或多个字段值进行加密。

13. 根据权利要求12所述的非暂态机器可读存储介质，其中所述第一组许可钥包括针对所述一个或多个交换字段中对应的交换字段读取、更新和插入访问许可。

14. 根据权利要求13所述的非暂态机器可读存储介质，其中所述指令还致使所述处理器：

响应于从所述对等区块链网络中的第二对等方接收共识，由所述多租户服务器将所述交易对象添加到所述第一对等方的第一分类账和所述第二对等方的第二分类账；和

由所述多租户服务器，代表所述第二对等方使用所述第二组许可钥读取所述一个或多个字段值。

15. 根据权利要求14所述的非暂态机器可读存储介质，其中读取所述一个或多个字段值包括：使用所述第二组许可钥中的第一钥对所述一个或多个字段值中的第一值进行解密，并且使用所述第二组许可钥中的第二钥对所述一个或多个字段值中的第二值进行解密。

16. 根据权利要求9所述的非暂态机器可读存储介质，其中所述多租户服务器包括用于所述对等区块链网络中的第一对等方的虚拟空间，

其中所述虚拟空间包括对所述第一对等方可用而所述对等区块链网络中的第二对等方不可访问的数据和服务。

17. 一种管理对等区块链网络中的数据的多租户服务器，所述多租户服务器包括：
处理器；

存储器，所述存储器存储指令，所述指令当由所述处理器执行时致使所述处理器：

生成用于所述对等区块链网络的交换对象，其中所述交换对象包括一个或多个交换字段以及所述一个或多个交换字段中的每个交换字段与和所述对等区块链网络中的每个对

等方相关联的物理对象的字段之间的映射；

确定针对所述一个或多个交换字段中的交换字段和所述对等区块链网络中的对等方的每个组合的许可；

基于所述交换对象，代表所述对等区块链网络中的第一对等方生成交易对象，其中所述交易对象包括所述一个或多个交换字段的成组的字段值，并且基于确定的许可对所述成组的字段值中的一个或多个字段值进行加密；和

代表所述第一对等方使得所述交易对象对所述对等区块链网络中的第二对等方可用，以尝试获得改变对应于所述第一对等方的物理对象的共识。

18. 根据权利要求17所述的多租户服务器，其中所述指令还致使所述处理器：

生成对应于所述第一对等方的第一组许可钥；和

生成对应于所述第二对等方的第二组许可钥。

19. 根据权利要求18所述的多租户服务器，其中所述第一组许可钥中的每个许可钥对应于所述第一对等方的关于所述一个或多个交换字段中的第一交换字段的许可，并且

其中所述第二组许可钥中的每个许可钥对应于所述第二对等方的关于所述一个或多个交换字段中的第二交换字段的许可。

20. 根据权利要求19所述的多租户服务器，其中生成所述交易对象包括使用所述第一组许可钥加密所述一个或多个字段值。

区块链网络中的基于字段的对等许可

[0001] 相关申请的交叉引用

[0002] 本申请要求于2018年12月20日提交的美国专利申请第16/228,555号和于2018年9月19日提交的美国临时申请第62/733,535号的权益,其通过引用并入本文。

技术领域

[0003] 一个或多个实施方案涉及数据管理领域;更具体地,向存储在对等(peer-to-peer)区块链网络中的数据的字段分配和实施基于对等方(peer)的许可。

背景技术

[0004] 区块链是使用加密技术链接和保护的记录/区块的连续扩展列表。具体地,区块链中的每个区块可以包括紧接在前的区块的密码散列、当前区块的时间戳,以及交易数据(例如与区块链网络中的对等方相关联的信息的添加/修改)。此外,区块链可以经由验证/确认将被添加到链的新区块的系统通过对等网络来共享和管理,使得区块链中的区块在不改变所有后续区块的情况下不能被改变,这需要网络共识。该架构允许通过使用加密技术来保护存储在区块内的信息;通过使用对等网络来共享/分配信息;通过区块添加的共识来信任;以及通过使用加密技术、区块的链式处理/链接和对等分配(例如区块链网络中的每个对等方可以维护网络中的所有已验证/确认的交易的分类账)来使存储在区块内的信息不可变。

[0005] 与区块链架构相比,多租户云架构依赖于将信息集中在公共数据库或其他数据结构中。虽然与区块链架构相比,基于云的架构提供了许多益处,包括从租户移除许多管理功能并且相反将这些功能集中在集中式系统上的能力,但是这些架构在租户间通信期间不提供相同级别的安全性、信任和信息不变性。此外,尽管区块链架构提供许多益处,包括上文所描述的益处,但这些架构不允许对等方之间的保密或其他访问许可/权限的实施。即,对等分类账的块中的每条信息对区块链网络中的所有对等方可见,并且每个对等方在区块链网络中具有相同的权限/权限。

附图说明

[0006] 以下附图使用相同的附图标记来表示相同的元件。尽管以下附图示出了各种示例性实施方案,但是可替代实施方案也在所附权利要求的精神和范围内。在附图中:

[0007] 图1示出了说明根据一个示例性实施方案的包括多租户服务器的计算环境的框图。

[0008] 图2示出了根据一个示例性实施方案的多租户服务器在对等区块链网络中管理数据的方法。

[0009] 图3A示出了根据一个示例性实施方案的包括每个租户系统的成组的单独的区块链服务的计算环境。

[0010] 图3B示出了根据另一个示例性实施方案的包括成组的共享区块链服务的计算环

境。

[0011] 图4示出了根据一个示例性实施方案的对应于成组的租户系统的物理对象。

[0012] 图5示出了根据一个示例性实施方案的包括交换字段与物理对象的字段之间的成组的映射的交换对象。

[0013] 图6示出了根据一个示例性实施方案的租户系统中的每一个的安全对象。

[0014] 图7示出了根据一个示例性实施方案的对应于租户系统的影子对象的示例。

[0015] 图8示出了根据一个示例性实施方案的交易对象的示例。

[0016] 图9示出了根据一个示例性实施方案的包括成组的条目/块的区块链的示例。

[0017] 图10A示出了根据一个示例性实施方案的电子装置。

[0018] 图10B示出了可以根据一个示例性实施方案来实施计算环境和服务器的环境的框图。

具体实施方式

[0019] 图1是示出根据一个示例性实施方案的计算环境100的框图。计算环境100包括租户系统102₁-102₃、多租户服务器104和成组的通信网络106。在该示例性计算环境100中,租户系统102₁-102₃可以是对等区块链网络108的一部分,并且多租户服务器104提供云环境以经由交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D来管理对等区块链网络108中的租户系统102₁-102₃的数据和交易,包括安全服务112。例如,区块链服务104D可以生成将租户系统102的物理对象的字段映射到用于处理对等区块链网络108中的交易的交换字段的映射数据。另外,区块链服务104D可以为区块链网络108中的每个租户系统102生成公钥和私钥,并且使用这些钥来分配/实施与交换字段有关的许可/权限。即,可以使用被允许访问这些字段的租户系统102的私钥和/或公钥对交换字段进行加密,并且可以针对不同的许可/权限级别向对应的租户系统102提供单独的密钥的组。

[0020] 例如,如下面将更详细描述,租户系统102₁的交易生成器110₁可以生成请求以(1)将新记录添加/插入到与租户系统102₁相关联的物理对象,或者(2)修改/更新与租户系统102₁相关联的物理对象的现有记录。物理对象可以包括用于每个记录的成组的字段,并且被存储在与租户系统102₁相关联的多租户服务器104的租户级对象104B的一部分/分区中,使得物理对象仅可由租户系统102₁访问(例如租户系统102₂和租户系统102₃不被允许读或写到租户系统102₁的物理对象)。该请求可以导致在与租户系统102₁相关联的租户级对象104B的部分/分区中的影子对象中添加记录。影子对象表示到物理对象的未委托的数据(即,对等区块链网络108中的对等方/租户之间尚未达成共识的数据)。交易队列104A可以使用影子对象来生成交易对象,该交易对象将被分配到其他租户系统102₁/使得其他租户系统102₂和102₃可用于接收对于所提出的对租户系统102₁的物理对象的添加/修改的共识。

[0021] 在一个实施方案中,交易对象的字段的集合是物理对象的字段的子集,并且交易对象的字段的集合由包括在网络级对象104C中的交换对象来定义。在该实施方案中,交换对象可以包括将被包括在交易对象中的成组的交换字段,并且交换对象的每个交换字段可以被映射到租户系统102₁-102₃的物理对象中的字段。例如租户系统102₁的物理对象可以包括字段A-D,租户系统102₂的物理对象可以包括字段E-H,并且租户系统102₃的物理对象可以包括字段I-K。在该示例中,对等区块链网络108的交换对象的第一交换字段可以被映射到

租户系统102₁的字段B、租户系统102₂的字段F和租户系统102₃的字段I。类似地,对等区块链网络108的交换对象的第二交换字段可以被映射到租户系统102₁的字段C、租户系统102₂的字段E和租户系统102₃的字段J。因此,当接收到用于添加/修改租户系统102₁的物理对象的记录的提议时,对应的交易对象包括具有来自所提议的物理/影子对象的字段B的值的的第一交换字段和具有来自所提议的物理/影子对象的字段C的值的第二交换字段。交换对象经由用于对等区块链网络108中的验证/确认目的的映射元数据提供统一交易对象,同时允许租户系统102₁仅向对等区块链网络108中的其他租户/对等方揭示信息的特定部分(例如,物理对象中的敏感信息/字段可能不包括在交易对象中,该交易对象分布在对应区块链网络108中的租户系统102₁-102₃之间,并随后包括在分布式分类账中)。

[0022] 如本文所描述的,多租户服务器104可以代表租户系统102₁-102₃执行对等区块链网络108的许多功能。具体地,多租户服务器104可以包括用于每个租户系统102₁-102₃的虚拟空间/组织。每个虚拟空间/组织可以包括对应的租户系统102₁-102₃的数据和应用/服务,并且在逻辑上与其他租户系统102₁-102₃的所有其他虚拟空间/组织分离。例如每个虚拟空间/组织可以包括对应于对应的租户/租户系统102₁-102₃和区块链服务104D的单独实例化或访问的租户级对象104B。在该配置/架构中,每个租户系统102₁-102₃的虚拟空间/组织可以代表对应的租户系统102₁-102₃执行一个或多个区块链功能/操作。例如响应于接收到来自租户系统102₁的向租户系统102₁的物理对象的现有记录添加/插入新记录或者修改/更新现有记录的请求,多租户服务器104可以在多租户服务器104内的租户系统102₁的虚拟空间/组织中生成影子对象记录。作为响应,交易队列104A可以使用对等区块链网络108的交换对象来生成与影子对象中的记录相对应的交易对象,使得交易对象包括具有来自影子对象的数据的交换字段,和使用租户系统102₁的成组的密码密钥来生成与影子对象中的记录相对应的交易对象,使得该交易对象可以被分配或者以其他方式对其他租户系统102₂和102₃的虚拟空间/组织可用。

[0023] 具体地,区块链服务104D的安全服务112可以基于每个租户系统102的许可/权限级别对交易对象的每个交换字段进行加密。例如,安全服务112可以确定租户系统102₁已经读取、更新和插入用于第一和第二交换字段的许可/权限。相反,租户系统102₂可以仅具有对第一交换字段的读取许可以及对第二交换字段的读取和更新许可。最后,租户系统102₃可以不具有与第一交换字段相关的许可/权限,并且可以具有用于第二交换字段的读取、更新和插入权限。在该示例情形中,安全服务112可以基于租户系统102₁-102₃的私钥和公钥以及所分配的许可/权限级别来生成用于租户系统102₁的第一组密钥、用于租户系统102₂的第二组密钥以及用于租户系统102₃的第三组密钥。第一组密钥允许租户系统102₁读取、更新和插入与第一和第二交换字段相关的数据;第二组密钥允许租户系统102₂读取第一交换字段并读取和更新第二交换字段;以及第三组密钥允许租户系统102₃读取、更新和插入与第二交换字段相关的数据。因此,如上所述以及如下面将更详细描述,多租户服务器104的安全服务112提供对区块链网络108中的数据的许可/权限级别控制。

[0024] 在分配交易对象之后,其他租户系统102₂和102₃的虚拟空间/组织此后可以分析交易对象以确定验证/确认是否适当。交易队列104A可以等待来自租户系统102₂和102₃的虚拟空间/组织的验证/确认,从而实现对租户系统102₁的物理对象的所提出的改变的共识。响应于共识,领导租户系统102₁-102₃的虚拟空间/组织可以 (1) 在对应物理对象中添加记录或

修改记录(适当时),以及(2)将对应的条目/块添加到领导租户系统 102_1-102_3 的分布式分类账中。此后,领导租户系统 102_1-102_3 的虚拟空间/组织可以向其他/剩余租户系统 102_1-102_3 的虚拟空间/组织发送请求以将改变委托给它们的物理对象(基于在交换对象中定义的映射)和/或将对应的条目/块添加到这些租户系统 102_1-102_3 的分类账。如上所述并且如下面将更详细描述,由多租户服务器104提供的云环境(例如由多租户服务器104提供的虚拟空间/组织)可以用于管理租户系统 102_1-102_3 之间的区块链交易。具体地,安全服务112对交换字段加密,使得可以对每个对等方/租户系统102和每个交换字段实施许可/权限(例如读取、更新和插入许可/权限)。

[0025] 下面将通过示例更详细地描述图1的计算环境100的每个元件。在一些实施方案中,计算环境100可以包括比图1所示的更多元件。因此,图1的计算环境100仅仅是为了说明的目的。

[0026] 如图1所示和如上所述,租户系统 102_1-102_3 和多租户服务器104可以通过成组的一个或多个通信网络106连接。该组一个或多个通信网络106可以例如是局域网(LAN)、广域网(WAN),诸如因特网的全局区域网络(GAN),或这些网络的组合。在另一个实施方案中,租户系统 102_1-102_3 和多租户服务器104可以经由有线或无线介质维持彼此的直接连接。

[0027] 每个租户系统 102_1-102_3 可以是可由一个或多个用户操作的计算系统。例如租户系统 102_1-102_3 中的每一者可以是个人计算机(PC)、工作站、膝上型计算机、平板计算机、移动电话、智能电话、个人数字助理(PDA等)。如下面将更详细描述,租户系统 102_1-102_3 可以与多租户服务器104通信以修改/添加/存储和获取数据。

[0028] 租户系统 102_1-102_3 (有时称为客户端、对等或用户系统)可各自包括用于向用户呈现界面(例如图形用户界面(GUI))的屏幕/显示器(例如液晶(LCD)显示器),包括在网页中呈现的界面。如下面将更详细描述,租户系统 102_1-102_3 中的每一者可以包括对应的交易生成器 110_1-110_3 ,用于从用户接收输入以更与租户系统 102_1-102_3 相关联的改物理对象(例如在物理对象中添加新记录或修改物理对象中的现有记录),并且触发从对等区块链网络108中的其他租户系统 102_1-102_3 获得共识(例如验证/确认)以进行更改的过程。

[0029] 租户系统 102_1-102_3 可以各自与一个或多个组织/租户相关联。例如租户系统 102_1 的用户可以是第成组的组织/租户的客户,并且租户系统 102_3 的用户可以是第二组织/租户的客户。组织/租户可以是已经与多租户服务器104的管理员签订合同以经由租户系统 102_1-102_3 向用户提供对存储在其中的数据的访问的任何公司、企业、机构、协会或社会。

[0030] 在一个实施方案中,多租户服务器104可以是向用户提供经由租户系统 102_1-102_3 和通信网络106对资源的访问的任何计算装置。例如多租户服务器104可以向租户系统 102_1-102_3 的用户提供对一个或多个物理对象和/或描述对物理对象的改变的一个或多个对应的分布式对等分类账中的数据的访问。例如租户系统 102_1 的物理对象可以对应于医学实验室报告。在该示例性实施方案中,物理对象中的记录可以包括实验室报告标识符字段、患者姓名字段、实验室网络标识符字段、实验室测试标识符字段、患者标识符字段和社会保障号码字段。当期望对租户系统 102_1-102_3 的物理对象进行更改/改变(例如向物理对象添加新记录或修改物理对象中的现有记录)时,多租户服务器104使用交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D来尝试在对等区块链网络108中做出这些更改(例如在物理对象和与租户系统 102_1-102_3 相关联的分布式分类账中反映的更改)。

[0031] 多租户服务器104可以包括多租户系统的硬件和软件的各种元件。如本文所使用的,术语“多租户系统”指的是其中硬件和软件的各种元件可以由一个或多个租户共享的那些系统。例如多租户服务器104可以同时处理对大量租户的请求,并且给定数据库表可以存储对可能大得多的租户数量的记录。多租户服务器104可以包括应用平台,该应用平台包括允许应用执行的架构(例如服务和元数据),诸如系统的硬件或软件基础设施。在一个实施方案中,多租户服务器104包括用于每个租户系统102₁-102₃的数据/对象以及服务的分开的虚拟空间/组织(有时称为部分或分区)。例如每个租户系统102₁-102₃可以被分配单独的虚拟空间/组织。每个虚拟空间/组织是多租户服务器104内的逻辑分区,并且除了由多租户服务器104代表对应的租户系统102₁-102₃使用的服务(例如区块链服务104D)之外,还包括仅对该租户系统102₁-102₃可访问而对其他租户系统102₁-102₃不可访问的单独的租户级对象104B(例如租户系统102₁-102₃不能读取和/或写入另一租户系统102的租户级对象104B)。

[0032] 如图1所示,对等区块链网络108可以包括各自表示租户/对等方的租户系统102₁-102₃。图1所示的对等区块链网络108是区块链网络108内的对等方/租户的表示。在一些实施例中,对等区块链网络108可以被视为由多租户服务器104利用来自租户系统102₁-102₃的输入/请求来控制的分布式网络。如上所述并且如下面将更详细描述,多租户服务器104可以代表租户系统102₁-102₃执行各种功能/操作。例如,多租户服务器104可以使用区块链服务104D代表租户系统102₁-102₃执行区块链功能/操作。如上所述,在一些实施方案中,区块链功能/操作可以在与对应租户系统102₁-102₃相关联的单独的虚拟空间/组织中执行。

[0033] 尽管以三个租户/对等方(例如租户系统102₁-102₃)示出,但是在其他实施方式中,对等区块链网络108可以包括更多或更少的租户/对等方。例如,对等区块链网络108可以包括具有对应租户系统102的两个、四个、五个或更多个租户/对等方。因此,使用三个租户/对等方是为了说明的目的。

[0034] 现在参照图2A和图2B,将描述根据一些实施方案的用于多租户服务器104管理对等区块链网络108中的数据的方法200。具体地,多租户服务器104提供的多租户云环境可以用于管理针对所述对等区块链网络108中的数据的租户系统102₁-102₃的许可/权限。

[0035] 将结合图1所示的示例性计算环境100,图3A所示的示例性计算环境300A和/或图3B所示的示例性计算环境300B来描述方法200。然而,在其他实施方案中,方法200可以在其他环境中操作,包括多租户服务器104的不同实施方案。

[0036] 如上所述,将参照其他图的示例性实施方案来描述图2A和图2B的流程图中的操作。然而,应当理解,可以由不同于参考其他附图所讨论的那些实施方案来执行流程图的操作,并且参考这些其他附图所讨论的实施方案可以执行不同于参考流程图所讨论的那些操作。

[0037] 虽然以特定顺序在图2A和图2B中描述和显示,但是方法200的操作不限于该顺序。例如可以以不同的顺序或在部分或完全重叠的时间段中执行方法200的一个或多个操作。因此,方法200的描述和描绘是出于说明性目的,而并非旨在限制于特定实施方案。

[0038] 如图2A所示,方法200可以在操作202开始,其中区块链服务104D的成员资格服务302A确定和/或向对等区块链网络108添加成组的租户(有时也称作对等方)。在一些实施方案中,在网络对象304A中标识对等区块链网络108,并且在对象304B中标识用于对等区块链网络108的租户(例如由租户系统102₁-102₃的标识符所代表的租户)。例如成员资格服

务302A可以通过在操作202处检查对等对象304B来确定对等区块链网络108中的成组的租户。在一些实施方案中,向对等区块链网络108添加租户/租户系统 102_1-102_3 可能需要通过来自对等区块链网络108中的当前租户/租户系统 102_1-102_3 的验证/确认过程达成共识。在图1的示例性计算环境100、图3A的示例性计算环境300A和图3B的示例性计算环境300B中,下面用于阐述方法200,成员资格服务302A在操作202处确定对等区块链网络108包括租户系统 102_1-102_3 ,它们表示租户/对等方。

[0039] 如上所述,每个租户系统 102_1-102_3 可以包括多租户服务器104内的单独的虚拟空间/组织。每个虚拟空间/组织包括单独的租户级对象104B,除了由代表对应的租户系统 102_1-102_3 的多租户服务器104所使用的服务(例如区块链服务104D)之外,该租户级对象104B仅对该租户系统 102_1-102_3 是可访问的,而对其他租户系统 102_1-102_3 是不可访问的(例如租户系统 102_1-102_3 不能读取和/或写入另一租户系统 102_1-102_3 的租户级对象104B)。例如如图3A所示,每个租户系统 102_1-102_3 可以与具有对应的租户级对象 $104B_1-104B_3$ (例如物理对象 306_1-306_3 、影子对象 308_1-308_3 、对等分类账 310_1-310_3 ,以及映射对象 316_1-316_3)和、区块链服务 $104D_1-104D_3$ 的单独的虚拟空间/组织 314_1-314_3 相关联。虽然在图3A中示出为针对每个虚拟空间/组织 314_1-314_3 的区块链服务 $104D_1-104D_3$ 的单独实例化,但是每个虚拟空间/组织 314_1-314_3 可以改为具有对如图3B所示的区块链服务104D的单个实例化的单独访问。

[0040] 在操作204,成员资格服务302A可以为对等区块链网络108中的每个租户/租户系统 102_1-102_3 生成成组的公钥(PK)和私钥/密钥(SK)。在一个实施方案中,基于所确定的私钥来生成公钥。例如可以使用单向密码散列函数(例如SHA256)来基于对应的私钥生成租户系统 102_1-102_3 的公钥。在一个实施方案中,在操作204处生成之后,公钥和私钥/密钥可由成员资格服务302A存储在钱包对象304C中。如下面将更详细地描述的,交易队列104A可以利用钱包对象304C中存储的私钥/密钥来为租户系统 102_1-102_3 中的每个生成交易对象和成组的许可匙。具体地,交易队列104A可以使用公钥和私钥/密钥来实施对等区块链网络108所使用的交易的密码元件,安全服务112可以使用许可钥来实施租户系统 102_1-102_3 的许可/权限。

[0041] 在操作206,成员资格服务302A可以确定用于对等区块链网络108的交换对象。在一个实施方案中,交换对象由成组的交换字段和映射元数据来定义,映射元数据定义了每个交换字段与租户系统 102_1-102_3 的物理对象中的字段之间的映射。例如图4分别示出了租户系统 102_1-102_3 的物理对象 306_1-306_3 。在该示例中,对应于租户系统 102_1 的物理对象 306_1 包括记录 404_1-404_M ,该记录 404_1-404_M 由字段 406_1-406_N 组成,并且每个记录 404_1-404_M 包括用于每个字段 406_1-406_N 的值 $408_{1,1-M,N}$ 。类似地,对应于租户系统 102_2 的物理对象 306_2 包括由字段 412_1-412_H 组成的记录 410_1-410_G ,并且每个记录 410_1-410_G 包括用于每个字段 412_1-412_H 的值 $414_{1,1-G,H}$ 。类似地,对应于租户系统 102_3 的物理对象 306_3 包括由字段 418_1-418_S 组成的记录 416_1-416_Q ,并且每个记录 416_1-416_Q 包括用于每个字段 418_1-418_S 的值 $420_{1,1-Q,S}$ 。物理对象 306_1-306_3 中的每一者可以表示任何类型的数据。例如租户系统 102_1 可以在医学实验室中操作或者以其他方式对应于医学实验室。在该示例中,物理对象 306_1 可表示医学实验室报告(例如记录 404_1-404_2 中的每一者可对应于单独的医学实验室报告)。租户系统 102_2 可以在医生的办公室中操作或者以其他方式对应于医生的办公室。在该示例中,物理对象 306_2 可以

表示患者文件(例如每个记录410₁-410_G可以对应于单独的患者文件)。

[0042] 对于图4所示的示例性物理对象306₁-306₃,成员资格服务302A可确定如图5所示的可存储在数字资产对象304D中的交换对象502。如图5所示,交换对象502由交换字段504₁-504₃和将交换字段504映射到物理对象306的字段的映射元数据来定义。在此配置中,交换字段504₁映射到物理对象306₁的字段406₂、物理对象306₂的字段412_H和物理对象306₃的字段418₂。交换字段504₂映射到物理对象306₁的字段406_N和物理对象306₂的字段412₁和物理对象306₃的字段418₁。交换字段504₃映射到物理对象306₁的字段406₁和物理对象306₂的字段412₂。因此,交换对象502的映射元数据将交换字段504映射/链接到物理对象306的字段。在一些实施方案中,交换字段504₁-504₃的数目(即三)小于(1)物理对象306₁中的字段406₁-406_N的数目(即,N)、(2)物理对象306₂中的字段412₁-412_H的数目(即,H)和/或(3)物理对象306₃中的字段418₁-418_S的数目(即,S)。因此,将在租户系统102₁-102₃之间分布的所生成的交易对象以及包括在分布式对等分类账310中的对应数据/信息可以不包括敏感数据。

[0043] 交换字段504到物理对象306₁-306₃的字段406、412和418的映射指示物理对象306₁-306₃的字段406、412和418之间的关系。例如使用物理对象306₁表示医疗实验室报告并且物理对象306₂表示患者文件的上述示例,物理对象306₁的字段406₂可以对应于针对其生成对应的医疗实验室报告的患者标识符并且物理对象306₂的字段412_H可以对应于针对其表示对应的患者文件的患者标识符。如图5所示并且如上所述,这些字段406₂和412_H被映射到相同的交换字段504₁,指示这些字段406₂和412_H表示相似的数据(例如字段406₂和412_H都表示患者标识符)。

[0044] 在一些实施方案中,每个租户/租户系统102₁-102₃可以是包括区块链网络108的多个区块链网络的一部分。这些区块链网络中的每一者可包括与区块链网络108的重叠成员资格和/或可包括附加的对等方/租户系统102。在一些实施方案中,网络对象304A可以包括由多租户服务器104管理的每个区块链网络的标识符,对等对象304B可以包括用于由多租户服务器104管理的区块链网络中的每个对等方/租户系统102的标识符,钱包对象304C可以包括用于由多租户服务器104管理的区块链网络中的每个对等方/租户系统102的钥,并且数字资产对象304D可以包括用于由多租户服务器104管理的每个区块链网络的交换对象502。在一些实施方案中,每个租户系统102的租户级对象104B可以包括映射对象316。每个映射对象316包括对应租户系统102的映射元数据。例如,对应于租户系统102₁的映射对象316₁包括将交换字段504₁映射到物理对象306₁的字段406₂的映射元数据;将交换字段504₂映射到物理对象306₁的字段406_N的映射元数据;以及将交换字段504₃映射到物理对象306₁的字段406₁的映射元数据。相反,对应于租户系统102₂的映射对象316₂包括将交换字段504₁映射到物理对象306₂的字段412_H的映射元数据;将交换字段504₂映射到物理对象306₂的字段412₁的映射元数据;以及将交换字段504₃映射到物理对象306₂的字段412₂的映射元数据。最后,对应于租户系统102₃的映射对象316₃包括将交换字段504₁映射到物理对象306₃的字段418₂的映射元数据;以及将交换字段504₃映射到物理对象306₃的字段418₁的映射元数据。因此,每个映射对象316仅包括与对应租户系统102相关联的映射元数据。

[0045] 在操作208,安全服务112可以确定每个交换字段504和租户系统102的许可/权限(有时称为许可/权限级别)。例如,区块链网络108可提供每个交换字段504的读取、更新和插入权限。在该示例中,安全服务112可以确定租户系统102₁已经读取、更新和插入用于交

换字段504₁-504₃的许可。相反,租户系统102₂可以仅具有对交换字段504₁的读取许可以及对交换字段504₂和504₃的读取和更新许可。最后,租户系统102₃可以不具有与交换字段504₁相关的许可/权限,并且可以具有用于交换字段504₂和504₃的读取、更新和插入权限。在操作208处的权限/许可的确定可以基于来自租户系统102的管理员或订阅级别的指示。

[0046] 在操作210中,安全服务112可以为每个租户系统102生成成组的许可钥。许可钥的组可以由租户系统102使用或代表租户系统102用于访问一个或多个交换字段504。例如,每组许可钥可以包括用于租户系统102的每个交换字段504和每个许可/权限级别的单独钥。例如,图6示出了分别用于每个租户系统102₁-102₃的安全对象318₁-318₃。如图所示,针对与对应租户系统102相关联的每个许可/权限级别606,为每个交换字段504提密钥的组604₁-604₃。这些密钥的组604₁-604₃可以基于每个对应租户系统102的公钥和私钥中的一个或多个来生成,并且可以用于经由对应的交易对象和对等分类账310将交换字段504读取、更新和插入到区块链网络108中。

[0047] 在操作212中,区块链服务104D的交易管理服务302B可接收(1)要添加到物理对象306₁-306₃的提议的新记录或(2)对物理对象306₁-306₃的现有记录的修改。例如,如以上示例中所述,物理对象306₁可以对应于医学实验室报告,并且虚拟空间/组织314₁的交易管理服务302B可以在操作212中从租户系统102₁接收添加/插入新的实验室报告记录404的请求。在另一示例中,物理对象306₁也可以对应于医学实验室报告,并且在操作212中,虚拟空间/组织314₁的交易管理服务302B可以从租户系统102₁接收修改现有实验室报告记录404的请求。出于解释的目的,将关于在操作212中从租户系统102₁接收向物理对象306₁添加/插入记录的请求的虚拟空间/组织314₁的交易管理服务302B来描述方法200。然而,对于物理对象306的修改,方法200可以以类似的方式工作。

[0048] 在操作214中,安全服务112可以确定租户系统102₁是否具有足够的许可/权限来执行从操作212接收的请求(即,安全服务112确定租户系统102₁是否被授权添加/插入新的实验室报告记录404)。在一个实施方案中,该确定基于安全对象318₁,安全对象318₁包括用于租户系统102₁的每个许可/权限级别606的钥。具体地,响应于未能为被请求插入的每个交换字段504定位许可钥并对应于插入许可/权限606,安全服务112可以在操作214中确定,租户系统102₁没有足够的许可/权限来执行从操作212接收的请求,并且方法200可以移至操作216以拒绝来自操作212的请求。

[0049] 相反,响应于为被请求插入的每个交换字段504定位许可钥并对应于插入许可/权限606,安全服务112可以在操作214中确定租户系统102₁具有足够的许可/权限来执行从操作212接收的请求,并且方法200可以移至操作218。

[0050] 在操作218中,虚拟空间/组织314₁的交易管理服务302B在与操作212的接收到的请求(即新记录)相对应的影子对象308₁中生成记录。影子对象308₁可以对应于租户系统102₁并且可以包括物理对象306₁的所有字段406₁-406_N。与物理对象306₁相反,物理对象306₁存储也在租户系统102₁的对等分类账310₁中表示的已提交数据(例如对租户系统102₁的物理对象306₁的记录404的添加/修改),影子对象308₁表示未提交给物理对象306₁的数据。如将在下面更详细地描述的,租户系统102₁的影子对象308₁中的数据在被提交给物理对象306₁并由租户系统102₁的对等分类账310₁表示之前需要由其他租户系统102₂和102₃通过共识来验证/证实。该承诺和表示还可以扩展到租户系统102₂和102₃的物理对象306₂和306₃。

以及对等分类账310₂和310₃,这将在下面更详细地描述。

[0051] 图7示出了根据一个示例实施方案的对应于租户系统102₁和物理对象306₁的影子对象308₁的示例。如图所示,影子对象308₁包括两个记录704₁和704₂,对应于对物理对象306₁的两个单独提出的改变。例如,第一记录704₁对应于物理对象306₁中的记录404的添加/插入,并且第二记录704₂对应于物理对象306₁中的新添加/插入的记录404的一个或多个字段值408的修改/更新。例如,第一记录704₁可以提出添加/插入对应于医学实验室报告的记录404,而第二记录704₂可以提出修改新的医学实验室报告记录404的若干字段值408(例如,修改/更新对应于医学实验室报告的状态的字段值408)。

[0052] 在操作220中,事件管理服务302C和/或交易队列104A可以基于(1)在操作218中添加到影子对象308₁的记录704₁和(2)对等区块链网络108的交换对象502来生成交易对象。具体地,交易对象可以包括对应的交易字段504₁-504₃中的交易字段504₁-504₃中的每一个的值和在操作218中添加到影子对象308₁的来自记录704₁的数据/字段值。例如,图8示出根据一个示例性实施方案的交易对象802的示例。

[0053] 如图8所示,交易对象802基于交换字段504₁-504₃和物理对象306₁的字段406之间的映射将交换对象502的所有交换字段504₁-504₃和来自影子对象308₁中的记录704₁的字段值706包括在适当位置中。虽然相对于记录704₁示出,但是可以为记录704₂生成单独的交易对象802。如下面将描述的,将在下文中用于说明目的的交易对象802可以被传递或以其他方式可用于其他租户系统102₂和102₃,以确定在区块链网络108中是否存在共识来提交所提出的记录404(例如以验证/证实交易对象802)。

[0054] 在一个实施方案中,交易对象802的生成可以包括基于(1)来自影子对象308₁的记录704₁、(2)交易对象802的唯一分配的标识符(例如在生成时被顺序地分配给交易对象802的标识符)以及(3)租户系统102₁的私钥(即提出改变的租户系统102的私钥)向交易对象添加签名。例如,记录704₁和交易对象802的唯一分配的标识符可以合并或者以其他方式组合在一起以形成单个消息,并且租户系统102₁的私钥可以用于(例如使用单向密码散列函数,诸如SH 256)加密消息以形成数字签名。因此,交易对象802包括来自影子对象308₁的记录704₁以及使用租户系统102₁的私钥生成的签名。

[0055] 在一些实施方案中,安全服务112可以使用(1)租户系统102₁的私钥(即,提出改变的租户系统102私钥;(2)具有与交换字段504相关的许可/权限606的每个租户系统102的许可钥(即,已经读取、更新和/或插入与交换字段504相关的权限的租户系统102的许可钥);和/或(3)具有与交换字段504相关的许可/权限的每个租户系统102的公钥来对交易对象802的每个交换字段504单独地加密。在这些实施方案中,使用具有与交换字段504相关的许可/权限的每个租户系统102的许可钥确保仅这些租户系统102具有对对应交换字段504的访问(例如,读取访问)。在一些实施方案中,私钥、公钥和/或许可钥可与密码功能(例如SHA256)一起使用以生成加密数据。

[0056] 在操作222中,事件管理服务302C和交易队列104A可以使交易对象802对其他租户系统102₂和102₃可用。在一些实施方案中,使交易对象802对其他租户系统102₂和102₃可用包括交易队列104A将交易对象802放置在对租户系统102₂和102₃可用的多租户服务器104的一部分/分区中。例如,如上所述,多租户服务器104可以包括用于每个租户系统102₁-102₃的单独的虚拟空间/组织314。每个虚拟空间/组织314包括仅对该租户系统102₁-102₃可访问并

且对其他租户系统 102_1-102_3 不可访问的数据和服务。在操作222中,多租户服务器104可以将来自租户系统 102_1 的虚拟空间/组织 314_1 的交易对象802传递到租户系统 102_2 和 102_3 的虚拟空间/组织 314_2 和 314_3 ,使得租户系统 102_2 和 102_3 的虚拟空间/组织 314_2 和 314_3 可以处理/分析交易对象802以用于可能的验证/确认。如上所述,由于交换字段504可以使用私钥、公钥和/或许可钥来加密,因此仅具有对交换字段504的读取访问的那些租户系统102或许能够确定该交换字段504的内容。

[0057] 在操作224,交易管理服务302B可以监视来自租户系统 102_2 和 102_3 的响应,以确定是否已经达成关于交易对象802的共识或者是否未能达成共识。在一个实施方案中,共识管理服务302D可以定义交易管理服务302B在确定关于交易对象802的租户系统 102_2 和 102_3 何时达成共识时使用的阈值或规则。例如在一些实施方案中,共识管理服务302D可以指示共识要求所有租户系统 102_2 和 102_3 来验证/确认交易对象802,而在其他实施方案中,共识管理服务302D可以指示共识要求大部分租户系统 102_2 和 102_3 来验证/确认交易对象802。在一些实施方案中,共识管理服务302E指示由租户系统 102_2 和 102_3 使用的规则和/或操作,特别是与租户系统 102_2 和 102_3 关联的虚拟空间/组织 314_2 和 314_3 ,以确定交易对象802的验证/确认是否适当。例如共识管理服务302E可以指示租户系统 102_1 的公钥与交易对象802中的签名和消息一起用于确定交易对象802中的信息是否源自租户系统 102_1 并由租户系统 102_1 授权。

[0058] 在操作226,交易管理服务302B和交易队列104A可以响应于未能从租户系统 102_2 和 102_3 获得共识而放弃交易对象802(例如未能获得由共识管理服务302D定义/指示的共识)。在一些实施方案中,放弃交易对象802可包括向租户系统 102_1 指示交易对象802和物理对象 306_1 的对应改变(即将新记录404添加到物理对象 306_1 或将现有记录404修改到物理对象 306_1)已被对等区块链网络108拒绝(即未实现/获得对等区块链网络108中的共识)。响应于接收到交易对象802和对物理对象的对应更改已被对等区块链网络108拒绝的通知,虚拟空间/组织 314_1 可删除影子对象 308_1 中对应于交易对象802的记录704₁。

[0059] 在操作228中,交易管理服务302B可以代表领导租户系统 102_1-102_3 提交交易对象802和/或与已经对其达成共识的交易对象802相对应的影子对象 308_1 中的记录704₁。在一些实施方案中,领导租户系统 102_1-102_3 可以由成员资格服务302A从对等区块链网络108中的租户系统 102_1-102_3 中随机选择。当领导租户系统 102_1-102_3 是租户系统 102_1 (即在操作212中发起或以其他方式与对物理对象 306_1 的改变相关联的租户系统 102_1-102_3)时,租户系统 102_1 的虚拟空间/组织 314_1 中的交易管理服务302B可以提交影子对象 308_1 中的记录704₁,在操作220中,代表租户系统 102_1 ,影子对象 308_1 对应于达成共识的交易对象802。在这种情况下,承诺可以包括将来自影子对象 308_1 的记录704₁添加到物理对象 306_1 。当领导租户系统 102_1-102_3 是租户系统 102_2 或租户系统 102_3 时,租户系统 102_2 和 102_3 的对应虚拟空间/组织 314_2 和 314_3 中的交易管理服务302B可以在操作220中代表租户系统 $102_2/102_3$ 提交达成共识的交易对象802。在这种情况下,承诺可以包括将记录410/416添加到物理对象 $306_2/306_3$ 中的记录410/416,或者修改物理对象 $306_2/306_3$ 中的记录410/416,该记录410/416包括来自映射到物理对象 $306_2/306_3$ 中的对应字段412/418的影子对象 308_1 的字段值706,如交换对象502或对应映射对象316所指示的。

[0060] 在操作230中,交易管理服务302B可以代表领导租户系统 102_1-102_3 在对应于交易对象802的对等分类账 310_1-310_3 中添加条目/块。具体地,领导租户系统 102_1-102_3 的虚拟空

间/组织314₁-314₃的交易管理服务302B可以代表领导租户系统102₁-102₃在对应于交易对象802的对等分类账310₁-310₃中添加条目/块。添加到对等分类账310₁-310₃的条目/块可以包括多条信息。例如如图9所示,对等分类账310₁中的每个条目/块904₁-904_T可以包括对对等分类账310₁中的前一个条目/块904、交易对象802(以及一个或多个其他交易对象)以及临时数(即,用于满足对等链区块链网络108的要求的任意数)的引用。

[0061] 在操作232中,交易管理服务302B和/或交易队列104A可以代表领导租户系统102₁-102₃发送请求或者以其他方式触发其他租户系统102₁-102₃来向对应的物理对象306₁-306₃提交交易对象802并将块/条目添加到对应等分类账310₁-310₃。特别地,领导租户系统102₁-102₃的虚拟空间/组织314₁-314₃的交易管理服务302B传递请求或以其他方式做出请求或以其他方式触发其他租户系统102₁-102₃的虚拟空间/组织314₁-314₃的交易管理服务302B,以向对应的物理对象306₁-306₃提交交易对象802和向对应的对等分类账310₁-310₃添加块/条目。对等分类账310₁-310₃允许计算环境100、300A和/或300B维护数据的透明度和可审计性。具体地,多租户服务器104通过在对等分类账310₁-310₃中记录/反映交易来为每个交易提供不可变性,对等分类账310₁-310₃在所有租户系统102₁-102₃上被复制。如上所述,租户系统102₁-102₃参与共识机制以验证/确认交易/交易对象802对象,并且仅在验证/确认交易/交易对象802对象之后,才将交易/交易对象802对象提交给对等分类账310₁-310₃。在一些实施方案中,对等分类账310₁-310₃可以存储在Merkle有向无环图(DAG)结构中。Merkle DAG可以以Oracle和/或HBase存储器表示。在数据被提交给对等分类账310₁-310₃时、在数据被提交给对等分类账310₁-310₃后,或在数据被提交给对等分类账310₁-310₃的条件下,相关物理对象306₁-306₃将与对等分类账310₁-310₃中的最近数据一起更新。在一些实施方案中,对等分类账310₁-310₃还可以保存描述租户/租户系统102₁-102₃的数据,该租户/租户系统102₁-102₃可以查看数据或以其他方式在对等区块链网络108中操作。

[0062] 在操作234中,一个或多个租户系统102可以尝试读取对应的对等分类账310中的一个或多个交换字段504。例如,添加到上述示例中的租户系统102₁-102₃的对等分类账310₁-310₃的事务对象802包括交换字段504₁-504₃。如上所述,租户系统102₁-102₃中的每一个已经分配了在相应的安全对象318₁-318₃中所指示的许可/权限级别。因此,与交换字段504相关的租户系统102₁-102₃的许可/权限级别是独立的。例如,在操作234中,租户系统102₁的虚拟空间/组织314₁可以尝试读取存储在对应等分类账310₁中的交易对象802的交换字段504₁。由于租户系统102₁的安全对象318₁包括用于读取交换字段504₁的许可键(即KEY_A),因此租户系统102₁的虚拟空间/组织314₁将能够基于该许可键(即KEY_A)针对存储在对应等分类账310₁中的交易对象802成功地解码交换字段504₁中的值。类似地,由于租户系统102₂的安全对象318₂包括用于读取交换字段504₁的许可键(即KEY_J),因此租户系统102₂的虚拟空间/组织314₂将能够基于许可键(即KEY_J)针对存储在对应等分类器310₂中的交易对象802成功地解码交换字段504₁中的值。然而,由于租户系统102₃的安全对象318₃不包括用于读取交换字段504₁的许可键,因此租户系统102₃的虚拟空间/组织314₃将不能针对存储在对应等分类账310₃中的交易对象802成功地解码交换字段504₁的值。

[0063] 如上所述,方法200允许多租户服务器104代表租户系统102₁-102₃管理对等区块链网络108中的数据。具体地,由多租户服务器104提供的云环境可以用于保护存储在对应等分类账310中的交易对象802中的数据,使得未经授权的用户/租户/对等方不能查看敏感数

据。

[0064] 在一些实施方案中,计算环境300A和/或300B可以构建在平台312之上,该平台312包括用于实现多租户服务器104的其他部件的服务和/或元数据。在一些实施方案中,区块链服务104D可以包括附加服务,诸如用于跟踪与每个租户/对等方相关联的记录和项目的硬币服务302F。

[0065] 如以上所使用的,术语“用户”是指使用系统和/或服务的实体(例如个人)。多租户架构向每个租户提供软件实例的专用共享以及(通常)为用户管理、租户特定功能、配置、定制、非功能属性、相关联的应用等输入租户特定数据的能力。多租户与多实例架构形成对比,在多实例架构中,独立的软件实例代表不同的租户进行操作。租户包括成组的用户,该组用户共享对提供服务的软件实例的具有特定权限的公共访问。租户可以是组织(例如公司、公司内的部门等)。租户可以具有相对于系统和/或服务的一个或多个角色。例如在客户关系管理(CRM)系统或服务的上下文中,租户可以是使用CRM系统或服务来管理租户关于供应商的一个或多个客户的信息的供应商。作为另一个示例,在数据即服务(DAAS)的上下文中,成组的租户可以是提供数据的销售商,而另成组的租户可以是不同销售商的客户或所有销售商的数据。作为另一个示例,在平台即服务(PAAS)的上下文中,成组的租户可以是提供应用/服务的第三方应用开发者,而另成组的租户可以是不同第三方应用开发者或所有第三方应用开发者的客户。用户可以具有相对于系统和/或服务的一个或多个角色。为了提供一些示例,用户可以是租户(例如供应商或客户)的代表(有时被称为“最终用户”)、提供系统和/或服务的公司的代表(例如管理员),和/或正在平台上创建和维护平台即服务(PAAS)的第三方应用开发者的代表(例如程序员)。

[0066] 上述实施方案的一个或多个部分可以包括软件和/或软件和硬件的组合。电子装置(也称为计算装置、计算机等)包括硬件和软件,诸如耦合到一个或多个机器可读存储介质(例如磁盘、光盘、只读存储器(ROM)、闪存、相变存储器、固态驱动器(SSD))的一个或多个处理器的集合,以存储用于在处理器的集合上执行的代码(其由软件指令组成并且其有时称为计算机程序代码或计算机程序)和/或存储数据。例如电子装置可以包括非易失性存储器(具有较慢的读/写时间,例如磁盘、光盘、只读存储器(ROM)、闪存、相变存储器、SSD)和易失性存储器(例如、快闪存储器、动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM),其中非易失性存储器即使在电子装置存在时也保持代码/数据因为易失性存储器通常具有更快的读/写时间,所以在操作期间,电子装置将要由该电子装置的该组处理器执行的那部分代码从非易失性存储器复制到该电子装置的易失性存储器中。作为另一个示例,电子装置可以包括非易失性存储器(例如相变存储器),当电子装置关闭时,该非易失性存储器保存代码/数据,并且该非易失性存储器具有足够快的读/写时间,使得不是将要执行的代码/数据的部分复制到易失性存储器中,该代码/数据可以被直接提供给该组处理器(例如未被加载到该组处理器的高速缓存中);换言之,该非易失性存储器既用作长期存储又用作主存储器,因此电子装置可以不具有或者仅具有少量的用于主存储器的易失性存储器。除了在机器可读存储介质上存储代码和/或数据之外,典型的电子装置可以在一个或多个机器可读传输介质(也称为载波)(例如电、光、无线电、声或其他形式的传播信号-诸如载波、红外信号)上传输代码和/或数据。例如典型的电子装置还包括成组的一个或多个物理网络接口,以与其他电子装置建立网络连接(以使用传播信号来传输和/或接收代码和/或数据)。

因此,电子装置可以存储代码和/或与一个或多个机器可读介质(也称为计算机可读介质)一起传输(内部地和/或通过网络与其他电子装置一起传输)代码和/或数据。

[0067] 电子装置用于各种目的。例如电子装置(有时称为服务器电子装置)可以执行使其作为用于向另一电子装置(有时称为客户端电子装置、客户端计算装置,或客户端装置),执行客户端软件(有时称为客户端代码或租户系统)以与服务通信。服务器和客户端电子装置可以分别由处于管理员(也称为管理用户)和终端用户角色的用户操作。

[0068] 图10A是示出根据一些示例性实施方案的电子装置1000的框图。图10A包括硬件1020,其包括成组的一个或多个处理器1022、成组的一个或多个网络接口1024(无线和/或有线),以及其中存储有软件1028(其包括可由成组的一个或多个处理器1022执行的指令)的非瞬态机器可读存储介质1026。先前描述的租户系统102和交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D中的每一者可以在一个或多个电子装置1000中实施。在一个实施方案中:1)每个租户系统102在电子装置1000中的单独一个中实施(例如在由用户操作的用户电子装置中,其中软件1028表示实施租户系统102以与交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D接口的软件(例如web浏览器、本地客户端、门户、命令行接口和/或基于诸如简单对象访问协议(SOAP)、表述性状态转移(REST)等协议的应用程序接口(API));2)在电子装置1000中的一个或多个的单独集合(例如成组的一个或多个服务器电子装置,其中软件1028表示用于实施交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D的软件)中实施交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D;以及3)在操作中,实施租户系统102和交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D的电子装置将通信地耦合(例如通过网络)并且将在它们之间(或通过一个或多个其他层)建立连接,以用于向多租户服务器104委托所提议的新记录或对物理对象中的现有记录的所提议的修改。在其他实施方案(例如租户系统102和多租户服务器104在单个电子装置1000上实施的实施方案)中,可以使用电子装置的其他配置。

[0069] 在使用计算虚拟化的电子装置中,一个或多个处理器1022的集合通常执行软件以实例化虚拟化层1008和软件容器1004A-R(例如利用操作系统级虚拟化,虚拟化层1008表示操作系统的内核(或在基本操作系统上执行的垫片),其允许创建多个软件容器1004A-R(表示单独的用户空间实例并且也被称为虚拟化引擎、虚拟专用服务器或监狱),这些软件容器可以各自被用于执行成组的一个或多个应用;利用完全虚拟化,虚拟化层1008表示在主机操作系统之上执行的管理程序(有时被称为虚拟机监视器(VMM))或管理程序,并且软件容器1004A-R各自表示被称为虚拟机的软件容器的紧密隔离形式,该虚拟机由管理程序运行并且可以包括访客操作系统;对于准虚拟化,与虚拟机一起运行的操作系统或应用程序可能知道存在用于优化目的的虚拟化。同样,在使用计算虚拟化的电子装置中,在操作期间,软件1028的实例(示为实例1006A)在虚拟化层1008上的软件容器1004A内执行。在没有使用计算虚拟化的电子装置中,在“裸金属”电子装置1000上执行主机操作系统之上的实例1006A。实例1006A的实例化,以及虚拟化层1008和软件容器1004A-R(如果实施的话)被统称为软件实例1002。

[0070] 电子装置的可替代实施方案可以具有与上述实施方案不同的多种变化。例如定制的硬件和/或加速器也可以用于电子装置中。

[0071] 网络装置 (ND) 是可通信地互连网络上的其他电子装置 (例如其他网络装置、用户电子装置、服务器电子装置等) 的电子装置。一些网络装置是“多业务网络装置”, 其为多联网功能 (例如路由、桥接、交换、第2层聚合、会话边界控制、服务质量和/或用户管理) 提供支持, 和/或为多应用服务 (例如数据、语音和视频) 提供支持。

[0072] 图10B是根据一些实施方案的其中可以部署租户系统102₁-102₃和多租户服务器104的环境的框图。系统1040包括用于提供服务1042的硬件 (成组的一个或多个电子装置) 和软件, 该服务942包括交易队列104A、租户级对象104B、网络级对象104C和区块链服务104D。系统1040通过网络1082耦合到用户电子装置1080A-S。服务1042可以是使其对一个或多个其他组织 (有时称为外部用户) 工作的用户1084A-S中的一个或多个可用的按需服务, 以使得这些组织不必关心构建和/或维护系统, 而是替代地在需要时 (例如按用户1084A-S的需求) 使用服务1042。服务1042可以经由一个或多个应用编程接口 (API) (例如表述性状态转移 (REST) API) 彼此通信和/或与用户电子装置1080A-S中的一个或多个通信。用户电子装置1080A-S由用户1084A-S操作。

[0073] 在一个实施方案中, 系统1040是支持多个服务的多租户云计算架构, 诸如客户关系管理 (CRM) 服务 (例如由salesforce.com公司销售的Sales Cloud)、合同/建议/报价服务 (例如由salesforce.com公司销售的Salesforce CPQ)、客户支持服务 (例如由salesforce.com公司销售的Service Cloud和Field Service Lightning)、营销服务 (例如由salesforce.com公司销售的Marketing Cloud、Salesforce DMP和Pardot)、商城服务 (例如由salesforce.com公司销售的Commerce Cloud Digital、Commerce Cloud Order Management和Commerce Cloud Store)、与外部商业数据源的通信 (例如由salesforce.com公司销售的Salesforce Connect)、生产力服务 (例如由salesforce.com公司销售的Quip)、数据即服务 (DAAS) (例如由salesforce.com公司销售的Database.com™)、平台即服务 (PAAS) (例如由salesforce.com公司销售的执行运行时和应用程序开发工具, 诸如Heroku™ Enterprise、Thunder和Force.com®以及Lightning)、分析服务 (例如由salesforce.com公司销售的Einstein Analytics、Sales Analytics和/或Service Analytics)、社区服务 (例如由salesforce.com公司销售的Community Cloud和Chatter)、物联网 (IoT) 服务 (例如由salesforce.com公司销售的Salesforce IoT和IoT Cloud)、行业特定服务 (例如由salesforce.com公司销售的Financial Services Cloud和Health Cloud) 和/或基础设施即服务 (IAAS) (例如虚拟机、服务器和/或存储)。例如系统1040可以包括使得PAAS能够创建、管理和执行由应用平台1044的提供者开发的一个或多个应用的应用平台1044、经由一个或多个用户电子装置1080A-S访问系统1040的用户, 或者经由一个或多个用户电子装置1080A-S访问系统1040的第三方应用开发者。

[0074] 在一些实施方案中, 一个或多个服务1042可以利用用于租户数据1048的一个或多个多租户数据库1046, 以及用于系统1040可用的系统数据1052的系统数据存储1050。在某些实施方案中, 系统1040包括成组的一个或多个服务器, 其在服务器电子装置上运行并且被配置为处理针对与任何租户相关联的任何授权用户的请求 (用户和/或租户与特定服务器没有服务器亲缘关系)。用户电子装置1080A-S与系统1040的服务器通信以请求和更新由系统1040托管的租户级数据和系统级数据, 并且作为响应, 系统1040 (例如系统1040中的一个或多个服务器) 可以自动生成被设计为从一个或多个多租户数据库1046和/或系统数据

存储1050访问期望信息的一个或多个结构化查询语言 (SQL) 语句 (例如一个或多个SQL查询)。

[0075] 在一些实施方案中,服务1042使用响应于来自用户电子装置1080A-S的查询并根据元数据在运行时动态创建的虚拟应用来实施,包括:1) 描述多个租户共同的构造 (例如表单、报告、工作流、用户访问权限、业务逻辑) 的元数据;以及/或2) 租户特定的并且描述租户特定构造 (例如表、报告、仪表板、接口等) 的元数据,并且存储在多租户数据库中。为此,程序代码1060可以是将来自元数据的应用数据具体化的运行时引擎;也就是说,编译后的运行时引擎 (也称为系统内核)、租户数据和元数据存在明显的分离,这使得可以独立地更新系统内核和租户特定的应用程序和架构,而实际上没有一个影响其他应用程序和架构的风险。此外,在一个实施方案中,应用程序平台1044包括支持应用程序开发者创建和管理应用程序的应用程序设置机制,应用程序开发者可以通过保存例程将其保存为元数据。可使用提供编程语言风格接口的过程语言/结构化对象查询语言 (PL/SOQL) 来编码对包括交易队列104A、租户级对象104B、网络级别对象104C和区块链服务104D的这些应用的调用。在由Craig Weissman于2007年9月21日委托的标题为“METHOD AND SYSTEM FOR ALLOWING ACCESS TO DEVELOPED APPLICATIONS VIA A MULTI-TENANT ON-DEMAND DATABASE SERVICE”的美国专利第7,730,478号中讨论了一些PL/SOQL语言实施方案的详细描述。对应用的调用可以由一个或多个系统进程检测,该系统进程管理获取进行调用的租户的应用元数据并且作为软件容器 (例如虚拟机) 中的应用执行元数据。

[0076] 网络1082可以是LAN (局域网)、WAN (广域网)、电话网络、无线网络、点对点网络、星形网络、令牌环网络、集线器网络或其他适当配置中的任何一者或任何组合。该网络可以遵循一个或多个网络协议,包括电气和电子工程师协会 (IEEE) 协议,第三代合作伙伴计划 (3GPP) 协议,或类似的有线和/或无线协议,并且可以包括用于在系统1040和用户电子装置1080A-S之间路由数据的一个或多个中间装置。

[0077] 每个用户电子装置1080A-S (诸如台式个人计算机、工作站、膝上型计算机、个人数字助理 (PDA)、智能电话等) 通常包括一个或多个用户接口装置,诸如键盘、鼠标、轨迹球、触摸板、触摸屏、笔等,用于与在显示器 (例如监视器屏幕、液晶显示器 (LCD) 等) 上提供的图形用户界面 (GUI) 结合系统1040提供的页面、表格、应用和其他信息进行交互。例如用户接口装置可用于访问由系统1040主存的数据和应用,并对所存储的数据执行搜索,否则允许用户1084与可呈现给用户1084的各种GUI页面交互。用户电子装置1080A-S可以使用TCP/IP (传输控制协议和网际协议) 与系统1040通信,并且在更高的网络级使用其他联网协议来通信,诸如超文本传输协议 (HTTP)、FTP、Andrew文件系统 (AFS)、无线应用协议 (WAP)、文件传输协议 (FTP)、网络文件系统 (NFS)、基于诸如简单对象访问协议 (SOAP)、表述性状态传输 (REST) 等协议的应用程序接口 (API)。在使用HTTP的示例中,一个或多个用户电子装置1080A-S可以包括HTTP客户端 (通常称为“浏览器”),用于向系统1040的服务器发送HTTP消息和从其接收HTTP消息,从而允许用户电子装置1080A-S的用户1084通过网络1082访问、处理和查看来自系统1040的对其可用的信息、页面和应用。

[0078] 在以上描述中,为了提供更透彻的理解,阐述了许多具体细节,诸如资源分区/共享/复制实施方案,系统部件的类型和相互关系,以及逻辑分区/集成选择。然而,本领域的技术人员应当理解,可以在没有这些具体细节的情况下实施本发明。在其他实例中,没有详

细示出控制结构、逻辑实现、操作码、指定操作数的装置,以及完整的软件指令序列,因为本领域的普通技术人员通过所包括的描述将能够实施所描述的内容而无需过多的实验。

[0079] 说明书中对“一个实施方案”、“示例性实施方案”等的引用指示所描述的实施方案可以包括特定特征、结构或特性,但是每种实施方案可以不一定包括该特定特征、结构或特性。此外,这样的短语不一定指同一实施方案。此外,当结合实施方案描述特定特征、结构或特性时,认为结合其他实施方案影响这样的特征、结构或特性是在本领域技术人员知识范围内的,无论是否明确描述。

[0080] 本文中可使用带虚线边框(例如大破折号、小破折号、点破折号和点)的括号文本和块来说明向一些实施方案添加额外特征的任选操作和/或结构。然而,这种表示法不应被认为意味着这些是唯一的选项或可替代操作,和/或具有实心边界的区块在某些实施方案中不是可替代的。

[0081] 在下面的描述和权利要求中,可以使用术语“耦合”及其派生词。“耦合”用于表示两个或多个元件彼此可以直接物理或电接触、彼此协作或交互,也可以不直接物理或电接触。

[0082] 参照其他附图中的示例性实施方案来描述流程图中的操作。然而,可以由不同于参考其他附图所讨论的那些的实施方案来执行流程图的操作,并且参考这些其他附图所讨论的实施方案可以执行不同于参考流程图所讨论的那些的操作。

[0083] 虽然附图中的流程图示出了由某些实施方案执行的操作的特定顺序,但是应当理解,这样的顺序是示例性的(例如可替代实施方案可以以不同的顺序执行操作、组合某些操作、重叠某些操作等)。

[0084] 虽然以上描述包括若干示例性实施方案,但是本领域的技术人员将认识到,本发明不限于所描述的实施方案,并且可以在所附权利要求的精神和范围内通过修改和改变来实现。因此该描述是说明性的而不是限制性的。

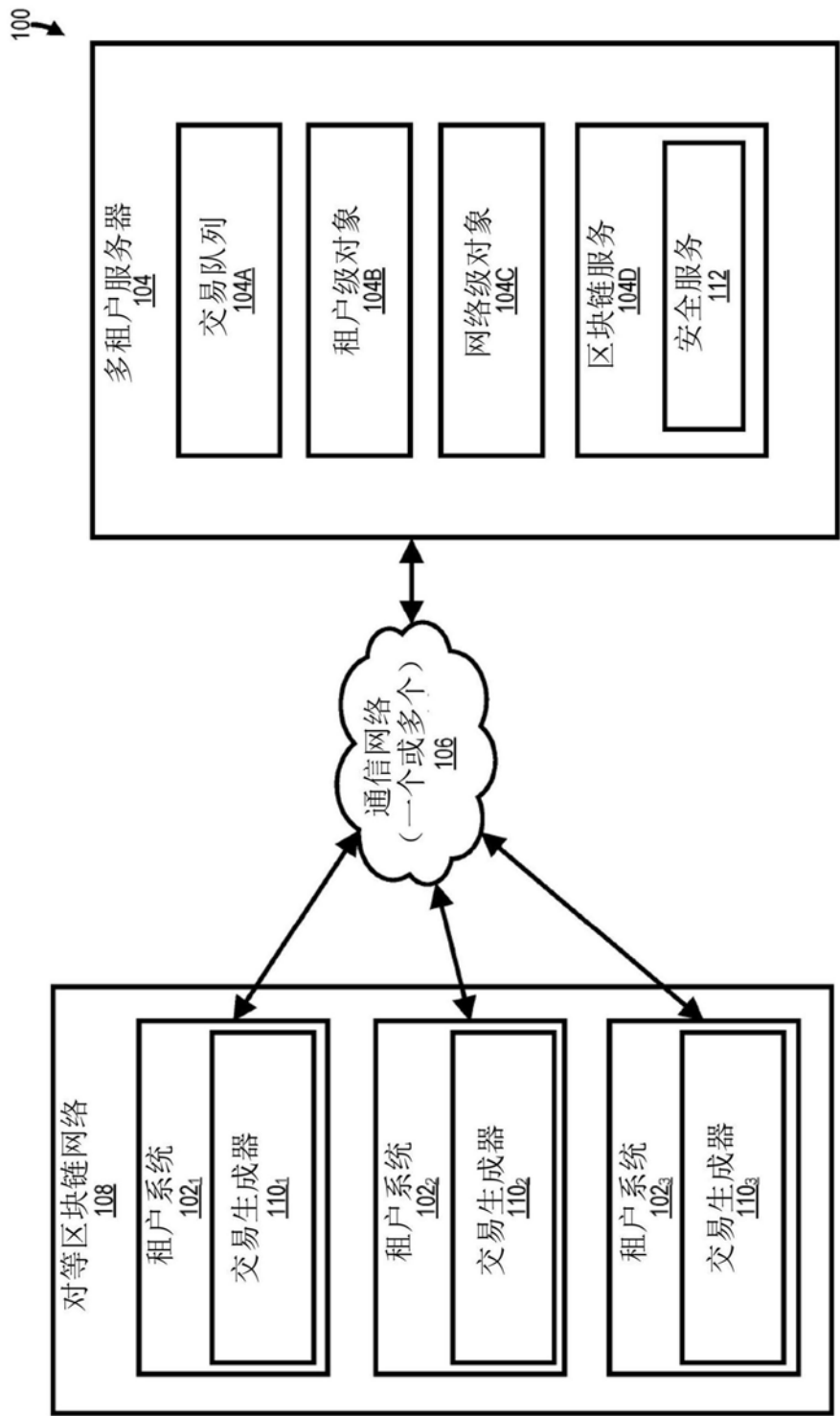


图1

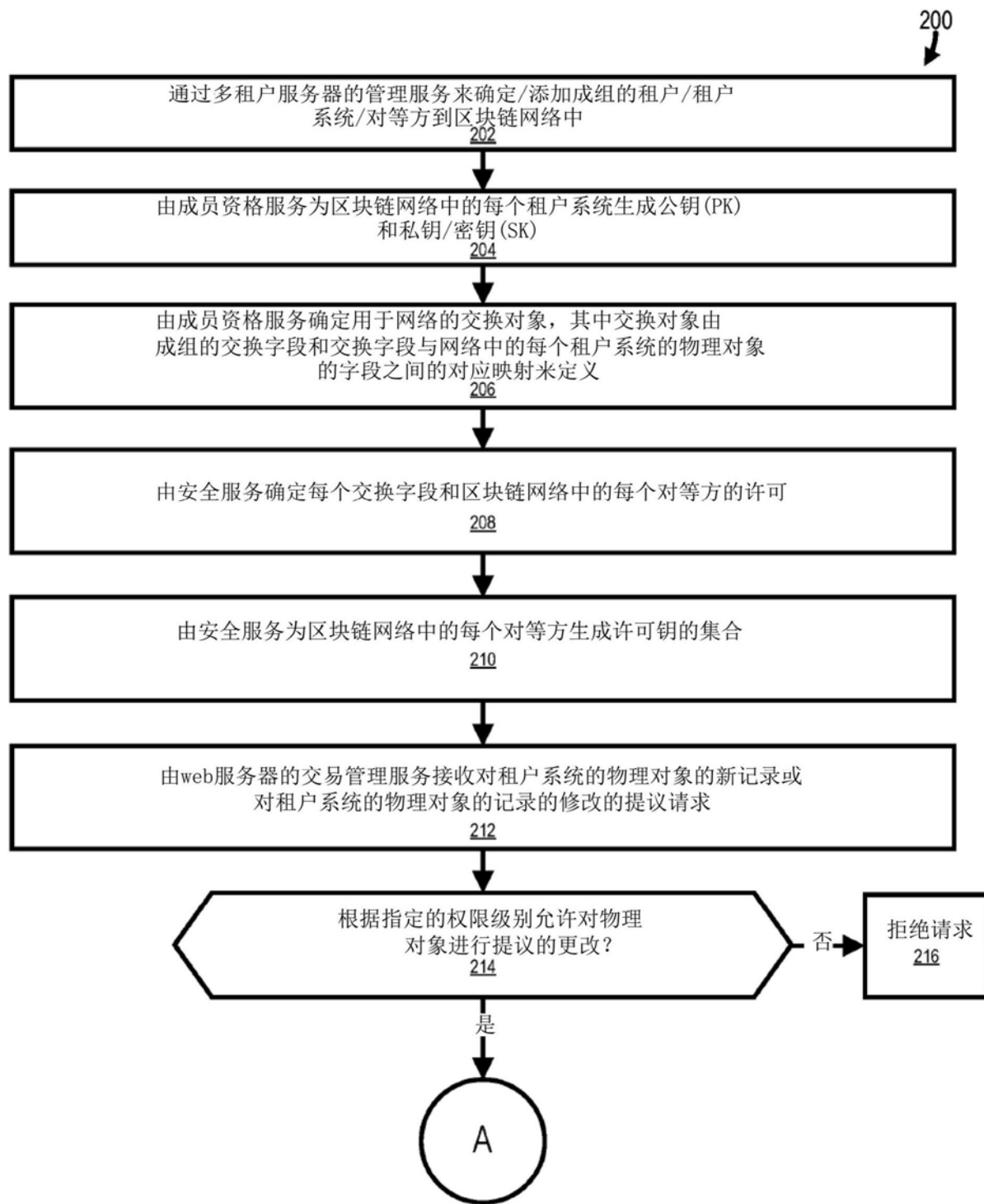
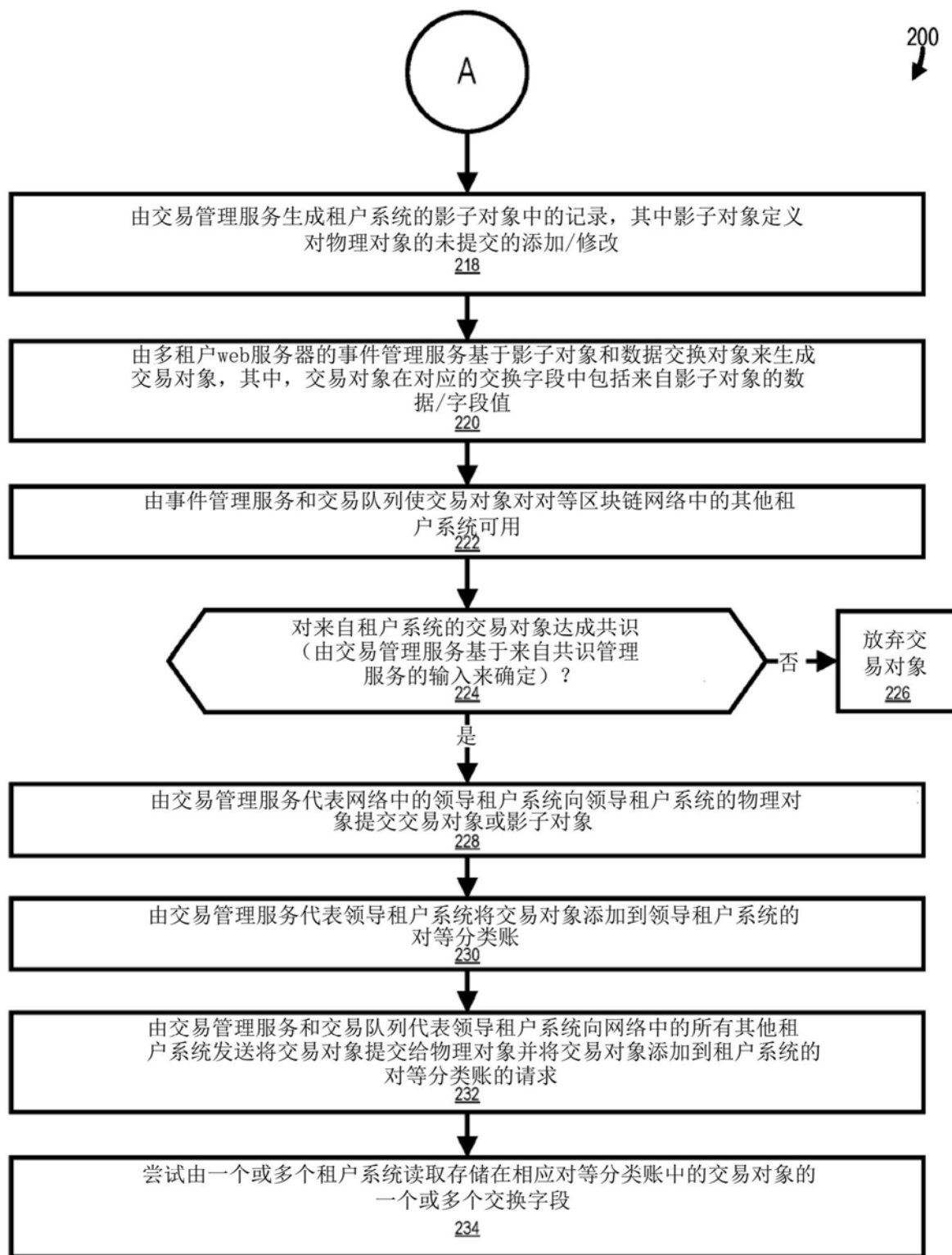


图2A



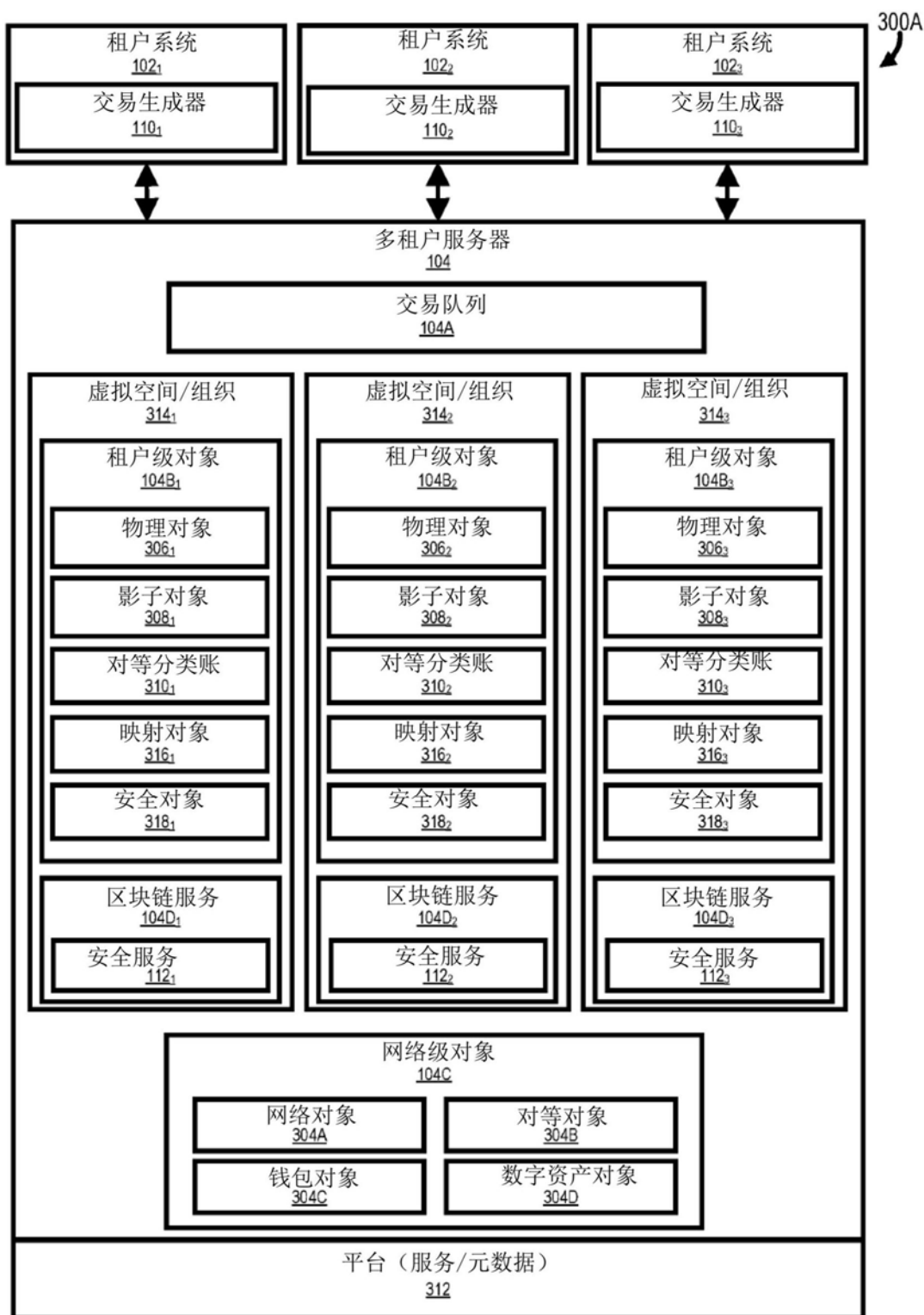


图3A

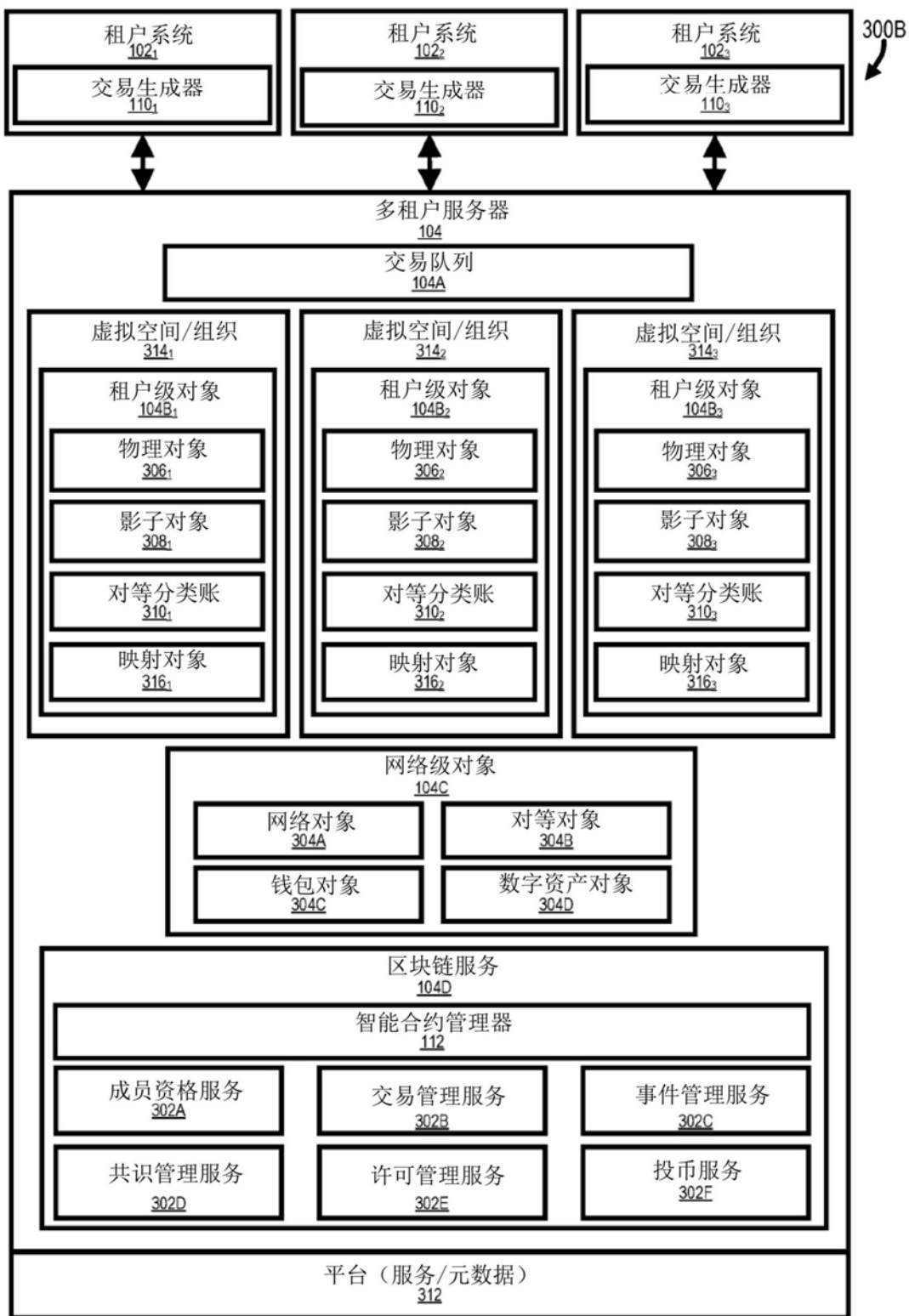


图3B

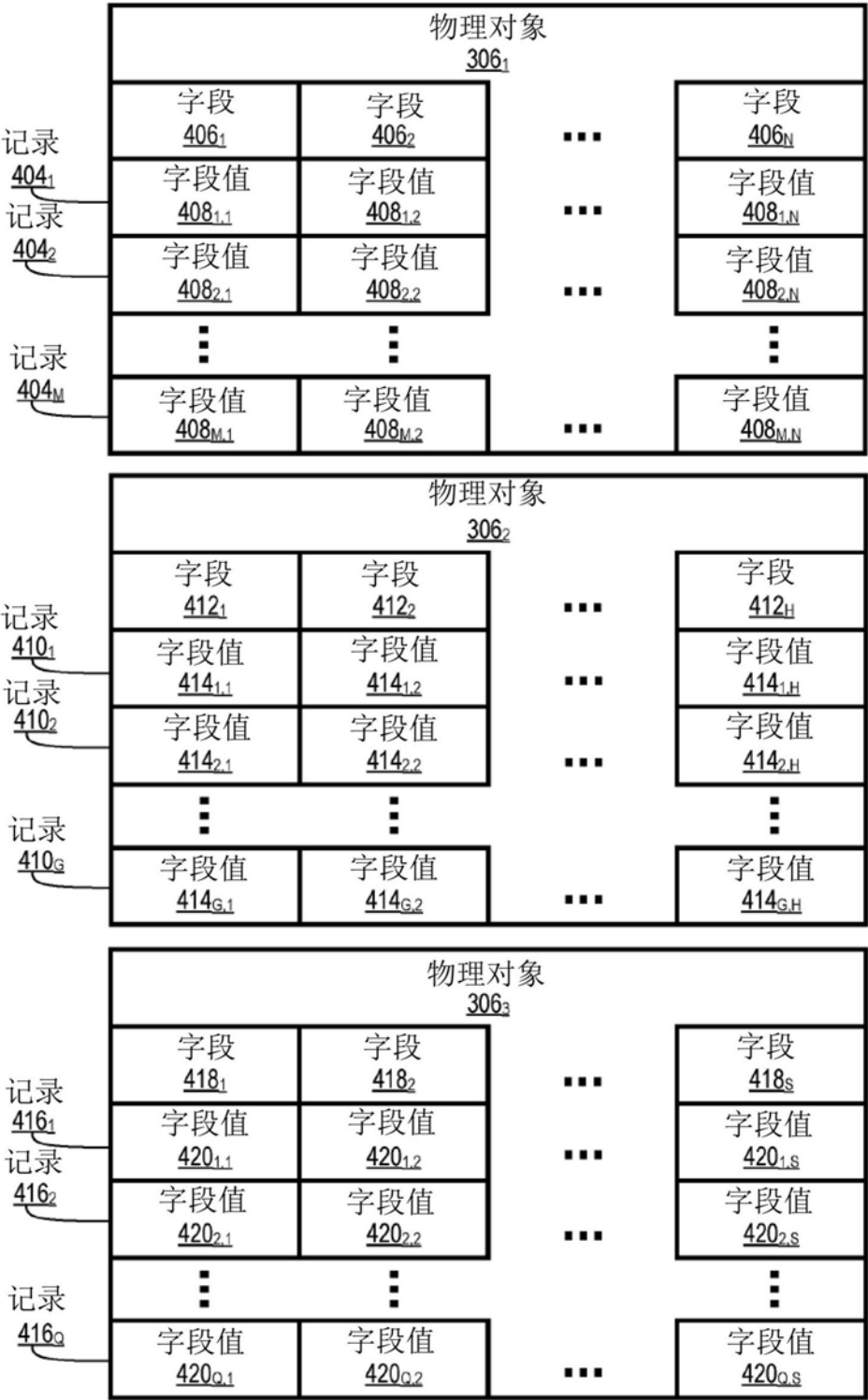


图4

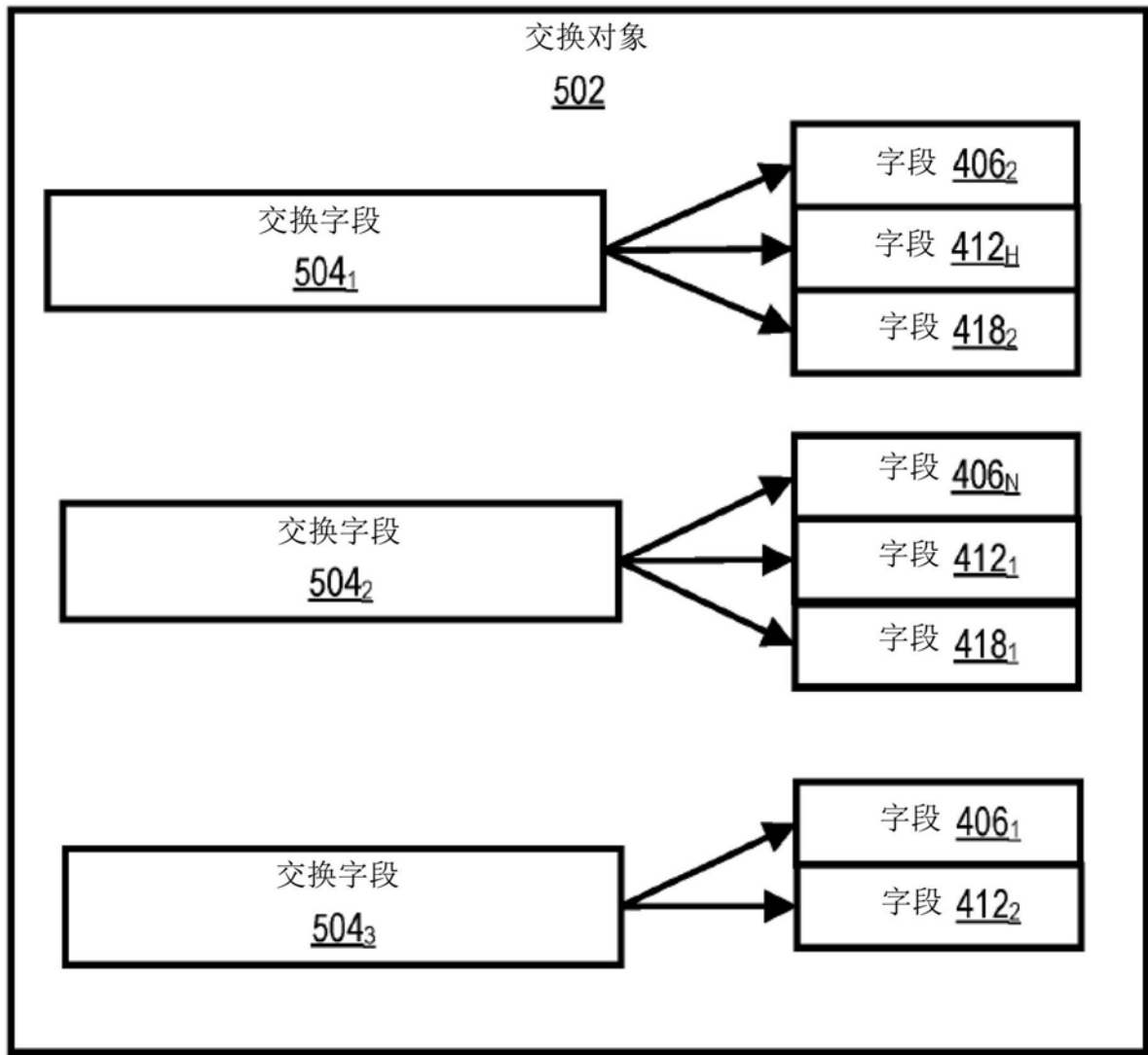


图5

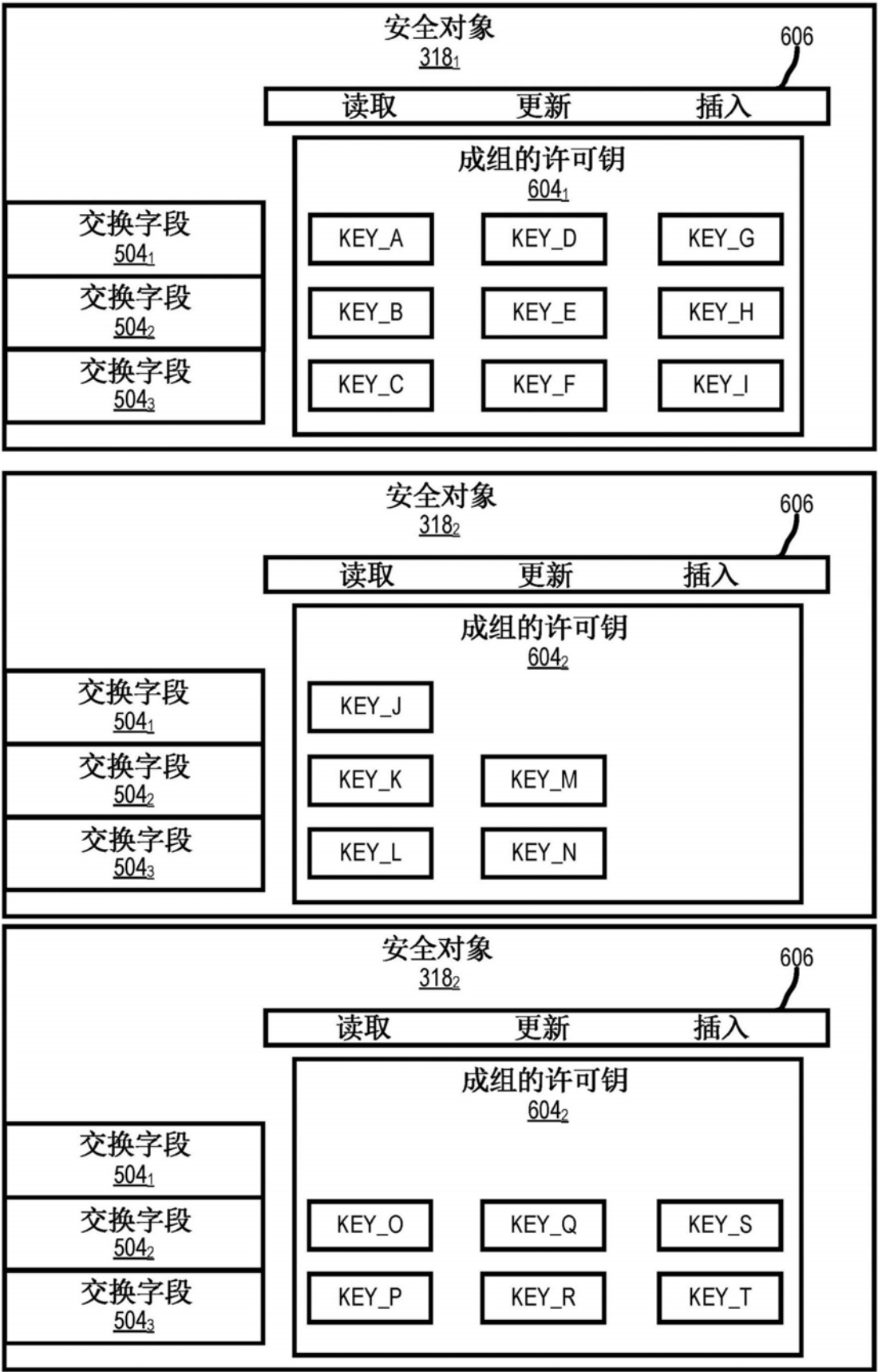


图6

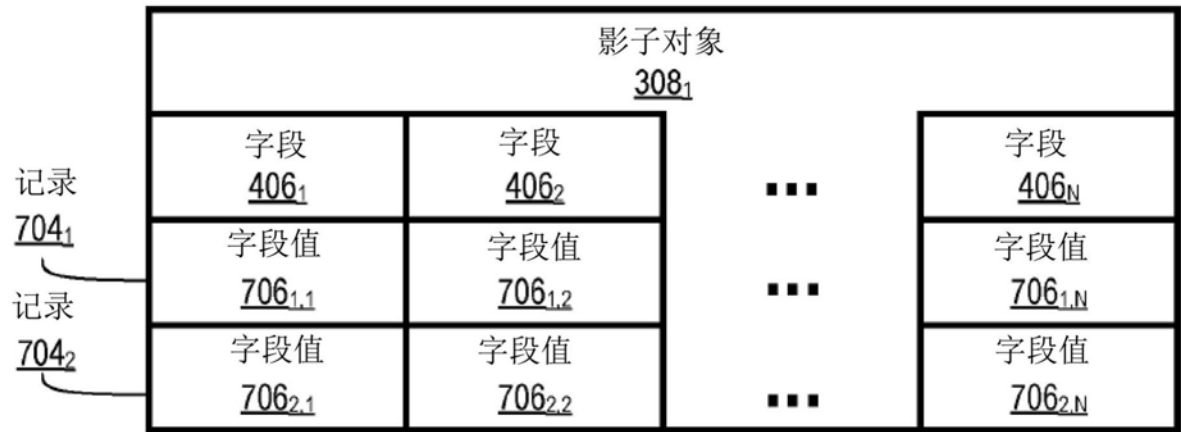


图7



图8

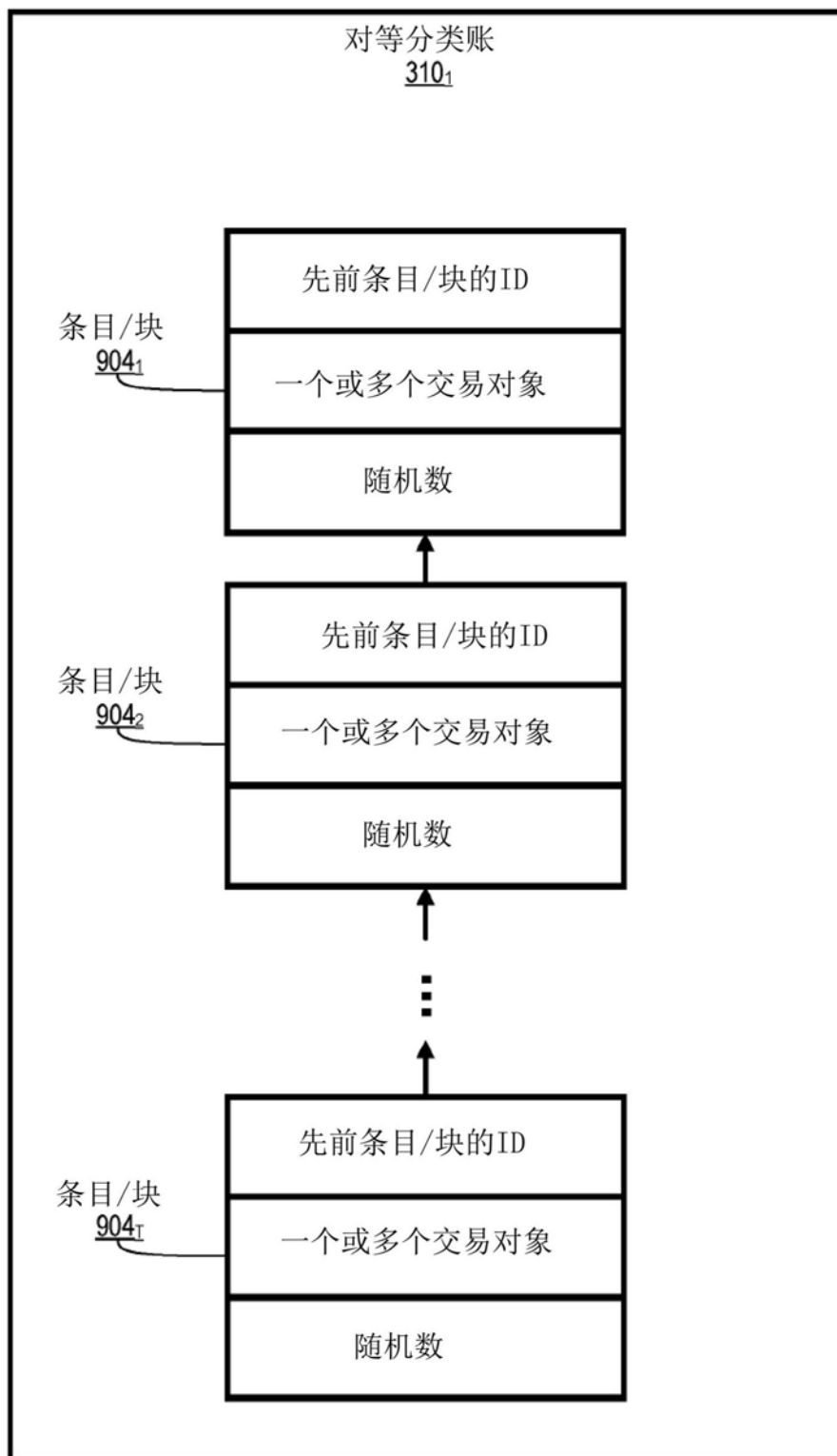


图9

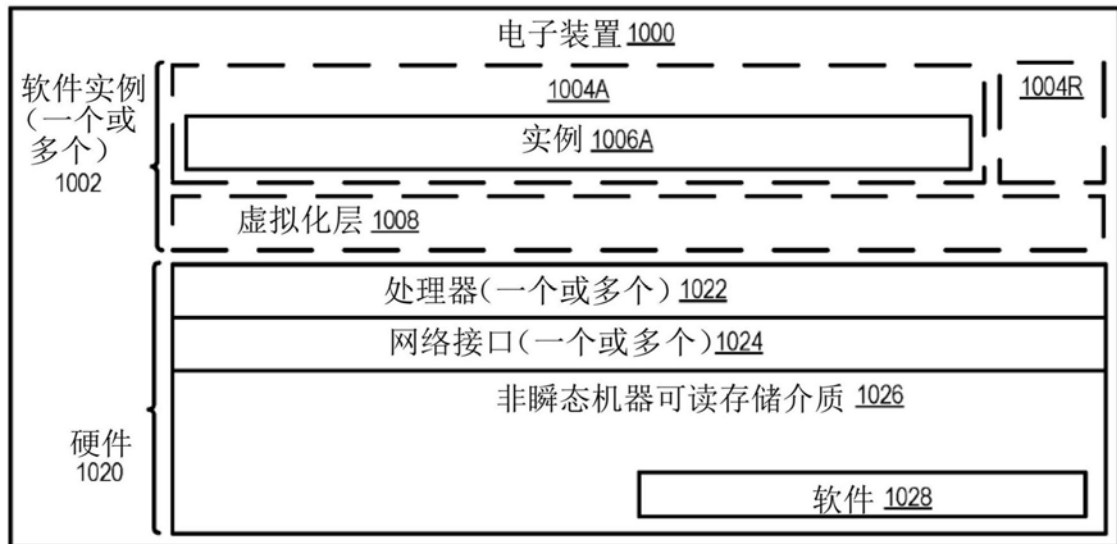


图10A

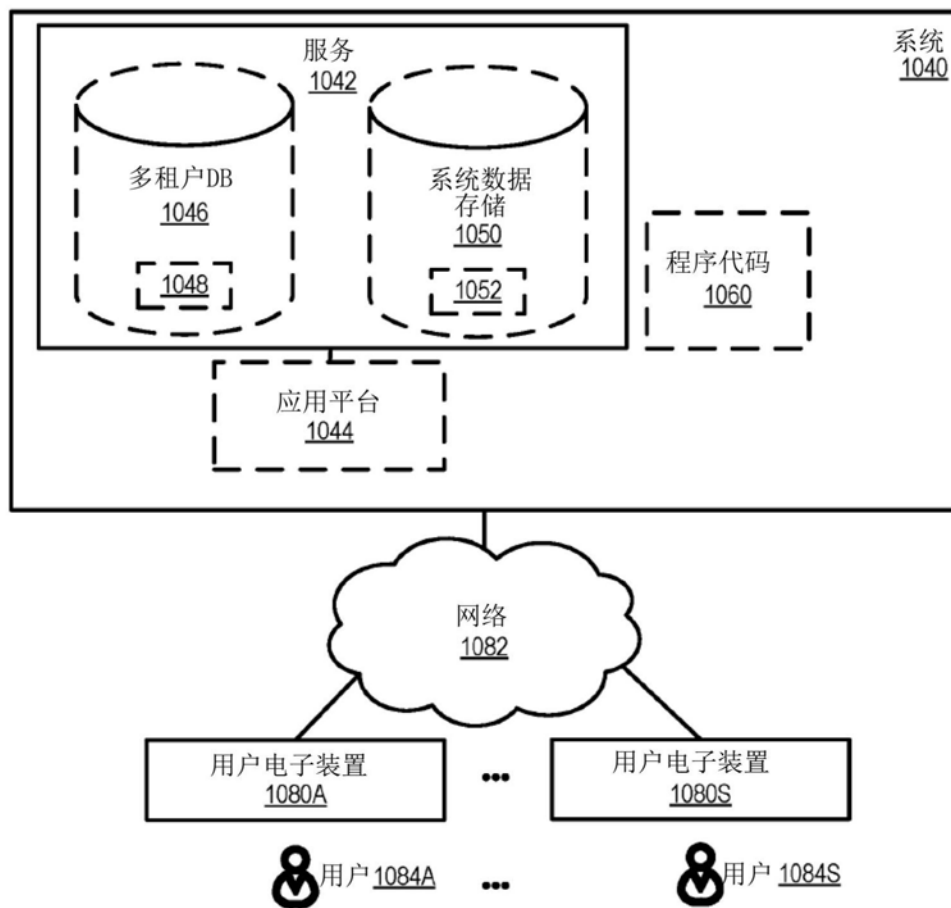


图10B