[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
G07F 7/00
G07F 7/10 G06F 17/60

[12]发明专利申请公开说明书

[21]申请号 96180487.4

[43]公开日 1999年11月10日

[11]公开号 CN 1234892A

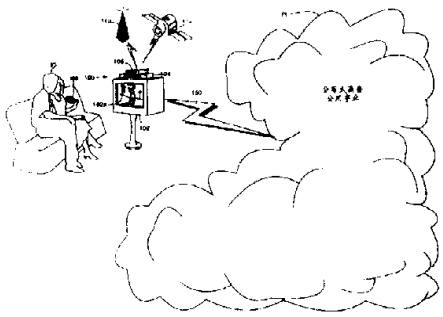
[22]申请日 96.9.4 [21]申请号 96180487.4
[86]国际申请 PCT/US96/14262 96.9.4
[87]国际公布 WO98/10381 英 98.3.12
[85]进入国家阶段日期 99.4.30
[71]申请人 英特托拉斯技术公司
地址 美国加利福尼亚州
[72]发明人 V·H·希尔 D·M·范韦
R·韦伯
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 张志醒

权利要求书3页 说明书157页 附图页数98页

[54]发明名称 用于安全电子商务、电子交易、商务处理控制及自动化、分布式计算和权利管理的可信架构支持系统,方法和技术

[57]摘要

本发明提供了管理和支持服务的一种集成的、模块化阵列,用于 电子商务和电子权利和交易管理。这些管理和支持服务为在庞大的电 子网络,如 Internet 和/或组织内部的 Intranet 上从事金融管理、权 利管理、凭证机构、规则结算、使用结算、安全目录服务以及其它与 交易有关的能力,提供了安全的基石。这些管理和支持服务可适应电 子商务价值链的具体要求。电子商务参与者可以利用这些管理和支持 服务来支持他们的利益,并能按照竞争性的商业现实,调整和重新利 用这些服务。具有安全、可编程和分布式的架构的一分布式商务公共事业系统提供了管理和支持服务。该商务公共事业系统充分利用商业 管理资源,并能以切实可行的方式扩展,以满足电子商务成长性的要 求。该分布式商务公共事业系统可包括许多商务公共事业系统。这些 商务公共事业系统提供了架构支持网,可为整个电子社区和/或其许 多或全部参与者利用和重复利用。可以按分级和/或联网关系收集不 同的支持功能,以适应各种商业模式和/或其它目的。可以将模块化 支持功能综合不同的阵列,以形成用于不同设计方案和目的的不同的 商务公共事业系统。这些商务公共事业系统可以按不同的分布程度,分布在大量的电器中。



ISSN1008-4274

权　利　要　求　书

1、一种用于至少执行一种结算操作的电子商务和/或权利管理系统，该系统包括:

第一电器（100），

第二电器（100'），以及

允许第一和第二电器（100、100'）交换数字信号的电子通信网络（150），

其特征在于:

第一电器（100）至少执行第一部分结算操作，以及

第二电器（100'）至少执行第二部分结算操作。

2、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作的第一部分至少包括一项小额支付汇总任务，结算操作的第二部分至少包括一项支付清算任务。

3、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一电器（100）包括消费者的电器，第二电器（100'）至少部分安装在结算机构中。

4、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，至少第一电器（100）包括一受保护的处理环境（154）。

5、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作的第一部分包括使用计量任务（116）.

6、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作的第一部分至少包括一项以数字凭证（504）为条件的任务。

7、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作的第一部分至少包括一项权利管理任务。

8、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作的第一部分至少包括一项电子货币的管理任务。

9、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，大多数结算操作都是由第一电器（100）来执行的。

10、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，大多数结算操作都是由第二电器（100'）来执行的。

11、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，系统还包括通过网络（150）与第一、第二电器（100、100'）中的至少一个联接的第三电器（100''），第三电器执行结算操作的第三部分。

12、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一、第二电器（100、100'）中每一个都能够执行金融结算操作、使用结算操作、权利及许可结算操作、认证机构操作、交易机构操作、以及安全目录服务操作中的任一种操作，所述操作中每一种操作都能以不同的方法，分布在第一和第二电器（100、100'）之间。

13、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，电子网络（150）将第一和第二电器（100、100'）联接至商务公共事业系统网。

14、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，电子权利持有者可以用电子方式，在第一电器（100）和第二电器（100'）之间选择。

15、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一和第二电器（100、100'）共同执行整个交易的结算。

16、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一和第二电器（100、100'）中每一个都执行以下操作之一：至少一个金融结算操作、至少一个使用结算操作、至少一个权利及许可结算操作、至少一个认证机构操作、至少一个交易机构操作、以及至少一个安全目录服务操作。

17、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一电器（100）包括若干商务公共事业系统（90（1），…，90（N））的分级结构。

18、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一电器（100）是因组织而异的。

19、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一电器（100）是专用的。

20、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一电器（100）是领地和/或辖区专用的。

21、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，第一和第二电器（100、100'）以对等和分级的方式通信协调。

22、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括处理与支付有关的信息和执行至少一项与支付有关的交易。

23、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括处理与使用有关的信息和执行至少一项使用报告活动。

24、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括接收至少一个请求和执行至少一个相关的权利管理交易。

25、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括颁发至少一个数字凭证。

26、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括安全地提供目录信息。

27、根据权利要求1的一种电子商务和/或权利管理系统，其特征进一步在于，结算操作包括执行至少一个处理管理交易。

28、根据权利要求1的一种电子商务和/或权利管理系统，其中结算操作的第一部分和第二部分相互支持。

29、根据权利要求1的一种电子商务和/或权利管理系统，其中第一和第二电器（100、100'）中至少有一个包括权利操作系统，该系统支持规定至少一项服务功能的服务应用程序组件的集合。

说　明　书

用于安全电子商务、电子交易、商务处理控制及自动化、分布式计算和权利管理的可信架构支持系统、方法和技术

发明领域

本发明一般涉及将现代计算和网络的效率理想地带入电子交易的管理和支持，并进一步涉及一种能够对电子商务进行分布式可信管理的安全架构。

这些发明更具体地涉及“分布式商务公共事业”－管理和支持电子商务及其它电子交易和关系环境的基础。

更具体地说，这些发明一般涉及：

- 电子商务和通信的有效管理和支持；
- 用于电子权利管理和支持服务的方法和技术；
- 用于分布式管理和支持服务的技术和装置，这些管理和支持服务如安全电子交易管理、电子处理控制和自动化以及在电子网络和/或虚拟分布环境内或跨网络和/或虚拟分布环境的清除功能；以及/或
- 清除、控制、自动化和其它管理性、架构和支持能力，共同使在人类数字化社区内高效、安全、对等地收集商业参与者的操作成为能够并支持这种操作。

背景

高效实用的社会必须具有使它们的居民能够控制他们参与交易的本质和结果的能力。每个社区都需要这些基本的服务、设施和设备：

- 邮局传递信件，
- 学校为儿童提供教育，
- 公路部门使道路通畅并保持良好的路况，
- 消防部门负责灭火，
- 电力公司为家庭提供电力，
- 电话公司将人们和远近的电子设备联系在一起并在你不知道正确的号码时提供号码簿服务，
- 银行保证钱财的安全，

- 有线电视和广播电台向家庭提供新闻和娱乐节目，
- 环境卫生部门收集废弃物，以及
- 社会性的服务支持针对贫困人口的社会政策。

这些和其它重要的“后台”管理和支持服务提供了一个基石或基础，使我们所知道的现代生活的便利和必需品成为可能并行之有效，并使商业的转轮平稳地转动。

假设你想在本地的面包房购买面包。面包师无须做与制作面包有关的所有事，因为他可以依赖社区所提供的支持和管理服务。例如：

● 面包师不需要种植或碾碎谷物来生产烤面包的面粉。相反，他可以从用卡车供货的供应商那里购买面粉。

● 同样，面包师不必种植或生产油料来使烘箱保持热；可以由专门生产和供应油料的人以管道或罐装的形式提供。

●你大可相信本地面包房的洁净性，因为它展示了一个检查通知，证明它已经得到了本地健康部门的检查。

对于确保人们会因他们的努力而得到补偿来说，支持和管理服务也非常重要。例如：

●你和面包师可以安全地相信政府维护你从钱包或钱夹中取出用于支付面包的货币。

●如果你用支票支付，银行系统连夜将与支票等量的钱从你的银行帐户中扣除并将钱付给面包房。

●如果你和面包房使用的是不同的银行，你的支票能够由一种自动化的“结算所”系统来处理，这种系统使不同的银行可以交换支票并处理帐户－高效地在银行之间转帐并退回从钱不够的帐户开出的支票。

●如果面包房接收信用卡支付方式，会提高在交换面包房产品过程中采用的支付方式的灵活性，并增加顾客的便利和购买力。

从尺度和范围上来说，这些支持和管理服务都提供了巨大的经济性－使我们的经济更有效率。例如，这些重要的支持和管理服务使面包师能够将精力集中于如何做得最好－制作和烘烤面包。由面包房和有经验的面包师在其大型的商业烤箱中制作许多块面包，与在各个家庭中用自己的烤箱分别烘烤各自的面包，或者与谷物的种植者也烘烤

面包和抽取烤面包所须的油料并进行易货交换，例如以小鸡交换面包相比，要更为有效。结果，你和面包房就能用信用卡完成购买交易，因为你和面包房都相信这种支付系统运作良好，并且相信能够作为非现金交易的高效、便利的基础高效“自动地”运行。

电子社区需要管理和支持服务

现在已经形成了一个世界性的电子社区。在电子世界中，电子社区的参与者需要塑造、控制和自动进行他们的交易的能力。他们急需可靠、安全、可信任的支持和管理服务。

越来越多的世界贸易是通过电子方式进行的。Internet－一个庞大的、联接了全世界数以百万计计算机的电子网络－正日益成为商务交易的途径。很大程度上得益于易于使用的界面（如那些允许消费者“点击”项目开始购买，然后完成一个简单的表格，提供信用卡信息），Internet正迅速成为消费者到商业和商业到商业采购的焦点。它也正成为包括信息、软件、游戏和娱乐在内的各种电子资产和服务的销售和发布的一个重要“渠道”。

与此同时，大公司使用专用和公共数据网络与它们的供应商和消费者们联系。受计算性能和网络能力成本显著而无情地下降的驱动，电子商务的重要性将随着世界越来越计算机化而增长。这个全新的电子社区－它具有广泛的电子商务－正为电子管理、支持和“票据交换”服务带来巨大的、全新的需求。

这个电子社区急需一个基础，以支持商业的和个人的电子交易和交往关系。在任何重要的尺度上，电子商务都需要第三方支持和管理服务提供者的一个可靠的、高效的、可扩展的、安全的网络和机制，以便为交易过程的重要部分提供便利。例如：

●为电子社区贡献价值的人要求无缝的、高效的机制，使他们能从他们的付出中得到补偿。

●向电子社区出售商品或服务的提供者需要可靠、高效的电子支付系统，为他们自己和其它价值链的参与者服务。

●电子市场中的购买者，虽然常常不会留意支付交易活动背后的详情，但要求与支付机制和金融债务履行系统具有易于使用的、高效灵活的界面。

●在所有的电子“内容”（例如，代表文字、图形、电影、动画、图象、视频、数字化线性运动图象、声音和录音、静止图象、软件计算机程序、数据的模拟或数字信息）中，对于许多种电子控制过程，权利持有者需要安全、灵活和广泛地互操作的机制，用于管理他们的权利并管理他们的商业模型，包括在需要时收集各种使用他们内容的支付和相关的使用信息。

●所有各方都需要一个即使在商业交易显著增长时也能保持可靠、可信任和安全的架构支持服务。

因此，成功的电子交易管理和商务的一个重要基石，在于一整套管理和支持服务的开发和操作，支持这些目标并利于普遍适用于电子商务的更加多样、灵活、可扩展和高效的商务模式的出现。

Ginter专利说明书描述了一种综合的解决方案

上述引用的Ginter等人的专利说明书描述了有关技术，该技术提供了对开发安全的、分布式交易基础上的电子商务和权利管理有益的独特而强大的能力。这项技术可在支持现有的商业模式和惯例的同时，在电子商务参与者这一部分使许多新的、重要的商业模式和商业惯例成为可能。

Ginter等人的说明书描述了全面的总体系统和许多个参与方法、技术、结构和方案，使在Internet（Intranet）上、大小公司的内部、起居室及家庭办公室内安全、高效的分布式电子商务和权利管理成为可能。这些技术、系统和方案给电子商务和电子权利管理，带来了前所未有的安全性、可靠性、效率和灵活性。

Ginter等人的专利说明书还描述“信息公共事业”－支持和管理性的服务、设施和设备的网络，为电子商务的轮子提供润滑剂，支持这个全新电子社区中的电子交易。例如，Ginter等人详细说明了广泛的支持和管理服务的提供者，用来与安全的“虚拟分布环境”接口并提供支持。这些支持和管理服务提供者包括:

●交易员

●使用分析员

●接受报告者

●创建报告者

●系统管理器

●许可代理

●认证机构

●内容和消息库

●金融结算所

●消费者/作者登录系统

●模板库

●控制结构库

●支付系统

●电子资金转帐、信用卡、书面记帐系统，以及

●收据、应答、交易和分析审核系统。

本发明建立在Ginter专利说明书中描述的解决方案的基础上并加以扩展

本发明建立在Ginter等人的专利说明书中描述的基本概念的基础上，同时对这些发明进行了扩展，以进一步提高效率、灵活性和能力。它们提供了分布式电子管理和支持服务（“分布式商业公共事业”）的重叠。在它们的优选实施方案中，它们能够利用“虚拟分布环境”和Ginter等人专利说明书中描述的其它能力的优势，它们位于这些能力的顶部并加以扩展。

本发明的一些特性和优点的简要说明

本发明为电子商务和电子权利以及交易的管理提供了一系列集成的、模块化的管理和服务。这些管理和支持服务，为在巨大的电子网络如Internet和/或机构内部的Intranet、甚至在家中的电器网络上进行的从事金融管理、权利管理、授权认证、规则结算、使用结算、安全目录服务以及其它与交易有关的能力，提供了安全的基础。

这些管理和支持服务能够适应电子商务价值链的特殊要求。电子商务的参与者可以使用这些管理和支持服务，维持他们的利益，并能根据竞争性的商业现实调整和重复利用这些服务。

本发明提供了一个具有安全、可编程的分布式结构的“分布式电子商务公共事业”系统，提供管理和支持服务。该分布式电子商务公共事业能够有效地优化利用商业管理资源，并能根据实际情况进行扩展，以满足电子商务成长的要求。

该分布式电子商务公共事业可包括若干商务公共事业系统。这些商务公共事业系统提供了一个能够为整个电子社区和/或其许多和/或所有参与者利用和重复使用的架构支持网。

可以按等级制度和/或联网关系将不同的支持功能集中在一起，以适应各种商业模式和/或其它目标。可以以不同阵列的形式将模块化支持功能综合在一起，为不同的设计实施和目的形成不同的商务公共事业系统。这些商务公共事业系统可按各种分布程度分布在大量的电器中。

本发明所提供的全面的“分布式商务公共事业”系统包括:

●使实际有效的电子商务和权利管理成为可能。

●提供安全地管理和支持电子交互作用和结果的服务。

●为电子商务和其它形式的人类电子交易和相互关系提供架构。

●优化利用现代分布式计算和网络的效率。

●提供电子自动化和分布式处理。

●支持模块化、可编程、分布式和优化计算的电子商务及通信架构.

●提供各种全面的功能，能够综合起来支持执行各种管理和支持作用的服务。

●最大限度地从电子自动化和分布式处理中获取利益，从而在整个系统或网络上实现资源的最佳分配和利用。

●高效、灵活、成本有效、可配置、可重复利用、可调整及通用性。

●能够经济地反映用户的商业和个人需求。

●能够最佳地分布处理－使商务模式可根据要求灵活扩展，满足用户的需求。

●能够有效地全面处理大量的活动和服务。

●能够根据每一种商务模式塑造和运作为分布式和集中式处理的混合体。

●提供本地、集中式和网络化能力的综合，能够被独特地塑造或重新塑造，以符合不断变化的情况。

●支持通用目的的资源，并且对许多不同的商业模式而言是可以重复利用的；架构可以为具有不同需求的不同价值链重复利用。

●能够支持任何数量的商业和通信模式.

●高效地利用本地的、集中式的和联网的资源来满足每个价值链的需求.

●公共资源的共享分散了成本并最大限度地提高了效率.

●支持混和、分布式、对等和集中式的联网能力.

●能够在本地、远程和/或集中运作。

●能够同步、异步运作或支持两种运作模式。

●轻松、灵活地适应快速变化的商海机遇、关系和“电脑空间”的约束。

总而言之，分布式商务公共事业系统为安全电子商务和其它形式的电子交互提供了全面的、集成的管理和支持服务。

本发明提供的分布式商务公共事业系统包括如下优点和特征:

●分布式商务公共事业支持可编程、分布式、优化计算了的商务和通信管理。它独特地提供了一系列执行各种管理和支持任务的服务-提供从电子自动化、分布式处理和系统（如网络）广泛的最佳资源利用中实现最大利益所必须的管理覆盖。

●分布式商务公共事业尤其适合为涉及分布式数字信息创建者、用户和服务系统的Internet、机构Intranet和类似的环境提供管理基础。

●分布式商务公共事业架构为电子商务和通信的管理及支持服务提供了高效的、成本有效的、灵活的、可构造的、可重复利用和通用的基础。提供这些能力对建立支持商业和个人的最佳电子关系模式的人类电子交易的基础而言至关重要。

●分布式商务公共事业架构提供了一个电子商务和通信支持服务的基础，能够针对任何特定的模式进行塑造和运作作为分布式和集中式处理的混合体。

●分布式商务公共事业支持的模式能够被整形和重新整形，以不断反映本地、集中式和联网的分布式商务公共事业管理能力的最佳组合。

●分布式商务公共事业独创性的电子管理能力支持混合的、分布式的、对等和集中式的联网能力。这些能力的组合能够分别在任何本地、远程和中央的异步和/或同步的联网组合中运作，在任何给定的

时候为一定目的，这些联网组合一同包括商业上最能实现的、最经济的和最能推销的－也就是商业上所最期望的－模式。

●分布式商务公共事业的架构是 通用的。它能够支持任何数量的商务和通信模式，这些模式共享（如重复利用）合理的、本地的、集中式的和联网的资源。结果，分布式商务公共事业使实用的有效的电子商务和权利管理模式成为可能，能够通过相同或重叠的资源库的公共利用来分期偿还资源的维护成本。

●一个或多个分布式商务公共事业的商务模式可以共享一个或多个其它模式的某些或全部资源。一个或多个模式也可以转换它们分布式的管理运作的混合和属性，以适应电脑空间－一个迅速变化的商海机遇、关系和限制－的要求。

●分布式商务公共事业通过允许将传统的商务处理转换成电子商务处理，从而支持传统的商务处理。分布式商务公共事业通过采用高效、商业上切实可行的电子商务模式可能必须的分布式处理、与权利有关的“结算所”管理、安全性设计、面向对象的设计、管理性的智能代理、协商和电子决策技术和/或电子自动化控制技术，进一步增强了这些处理。

●这些分布式商务公共事业的运作（金融支付、使用审核等）可以在参与者的用户电器安全执行空间中进行，如在Ginter等人公开的“受保护的处理环境”中进行。

●分布式结算所的运作可以通过“虚拟联网和/或分等级”的商务公共事业系统结点的阵列来进行，这些地址采用通用的、可互操作的（如对等的）虚拟分布环境作为基础。

●对于给定的应用或模式，可以授权对分布式商务公共事业服务阵列的变更，以提供不同的管理和/或支持功能。

●分布式商务公共事业所支持的任何或全部作用，都可通过相同的机构、论坛或其它机构组织、或者其它电子社区参与者如个人用户的站点来进行和/或利用。

●分布式商务公共事业的一个或多个部分可由分布式的受保护的处理环境组成，执行一种或多种具有分等级和/或对等关系的作用。

●多个受分布式商务公共事业保护的处理环境可执行服务、基础成分和/或结算所的完整任务。

●在一个优选实施方案中，对分布式商务公共事业的作用有贡献的分布式受保护的处理环境可以分布为VDE参与者受保护的处理环境的数量，以及/或者可以具有针对这种参与者受保护的处理环境的特定的分级、联网和/或集中管理和支持关系。

●在一定的模式中，某一种或多种分布式商务公共事业作用可以是完全分布式的，其它某一个或多个作用可以更加和/或完全集中（如等级制），其它的作用可以是部分分布式部分集中式的。

●分布式商务公共事业所提供的这种基本的对等控制，使得可以任意组合分布式作用，集体提供重要的、切实可行的、可扩展的和/或必需的商业管理、安全性和自动化服务。

●可以在可编程的分布式和集中式的混合布置中采用分布式商务公共事业的特性、布置和/或能力的组合，并具有在最终用户受保护的处理环境，和/或“中间”基础受保护的处理环境（本地、区域、特定等级等），和/或集中式的服务受保护的处理环境中运作的各种特性、布置和能力。

●对于支持具有分布式信息创建者、用户和服务提供者的Internet和其它电子环境而言，分布式商务公共事业特别有用。通过帮助人们将他们的活动转移到电子世界中，它在将这些非电子化的人类活动转到Internet、Intranet和其它电子交互网络的迁移过程中扮演了根本性的重要角色。这些网络用户需要分布式商务公共事业的基础和支持服务，以经济地实现他们的商业和个人需求。如果想要最佳地支持电子商务模式的能力，以便有意义地满足要求并有效地全面处理所希望的大量活动和服务，那么这个安全的分布式的处理基础是必需的。

●本发明提供的这个分布式商务公共事业技术，为电子商务、权利管理和分布式计算和过程控制提供了一整套安全的、分布式的支持和管理服务。

●分布式商务公共事业的支持服务包括高度安全的、复杂的技术和/或契约服务，可以被电子商务和价值链的参与者以无缝、便利和相当透明的方式所调用，用户是看不到底层操作的复杂性的。

●分布式商务公共事业能够确保适当高级别的物理、计算机、网络、处理和基于政策的安全性和自动化，同时提供了增强的、高效的、

可靠的、易于使用的、便利的功能，而这恰恰是有序地、有效地支持电子社区需求所必需（或高度希望的）的。

●在其优选实施方案中，分布式商务公共事业支持在一个基于VDE的“开放的”数字市场中运作的有竞争力的商务模式的创建。

●分布式商务公共事业能够向它们的价值链参与者提供便利性和运作效率。例如，它们可以提供一套完整的、集成的、重要的“结算”功能，这些功能是可编程的，并能够通过一个无缝的、“分布式的”界面（如一个分布式的应用程序）进行修正，以最佳地支持多个参与方商业关系。正如所希望的那样，结算和/或支持功能和/或子功能能够被单独和/或分开利用，以便为商务、保密、效率或其它目标服务。

●分布式商务公共事业能够使供应商、批发商、经销商、转销商、消费者和其它价值链参与者很容易就能联接、调用和使用分布式商务公共事业的服务。接续（Hookup）可以是简易、无缝和全面的（一个hookup可以提供广泛的互补性的服务）。

●通过提供或者支持参与管理机构提供的用于结算服务的用户标记图案，分布式商务公共事业就能进一步增强便利性和效率，但利用的是共享架构和处理，。

●通过支持电子化地、无缝地采用多个参与方特殊服务和能力的“虚拟”模式，分布式商务公共事业能够从参与管理机构的规模和专长中实现重要的效率。

●分布式商务公共事业使消费者能够便利地得到诸如服务或产品上的好处，这里所指的服务或产品是从调用各种支持服务的“组织”获得的－每一服务都可由更专业的服务和/或参与的组元服务提供者的分布式组织构成（对价值链的参与者来说总的组织是可见的，底层的复杂性基本或完全是（或可能是）不可见的）。

●在它们的优选实施方案中，分布式商务公共事业服务和能力能够以合理的方式采用并与Ginter等人描述的任何一个或多个虚拟分布式环境能力相结合，包括：

A. 处理和控制的VDE链，

B. 安全可信的节点间通信和互操作性，

C. 安全的数据库，

D. 授权，

E. 密码，

F. 指纹，

G. 其它VDE安全技术，

H. 权利操作系统，

I. 对象设计和安全的容器技术，

J. 容器控制结构，

K. 权利和过程控制语言，

L. 电子协商，

M. 安全的硬件，和

N. 智能代理（智能对象）技术（例如，用作支持分布式节点管理集成的过程控制、多个参与方和/或其它管理性代理能力的智能代理）。

商务公共事业系统可能是分布式的和混合式的

分布式商务公共事业所提供的支持和管理服务功能，能够以各种方式综合和/或分布在电子社区、系统或网络中。优选实施方案采用了Ginter等人描述的基于受保护的处理环境的虚拟分布环境，以便于这种综合与分布。由于所有这种受虚拟分布环境保护的处理环境都至少在一定程度上是可信的，每个受保护的处理环境都能够作为结算所或结算所的一部分。符合VDE商务节点用户利益和意愿的商务模式能够支持分布式商务公共事业服务，这些服务被通过各种途径，推送给采用如其它VDE受保护处理环境、安全通信技术和其它VDE能力（如其它地方描述的那样，VDE能力能够直接与本发明集成）的最终用户的电器中。这些电器与更多集中式的价值链节点一起，能够共同形成虚拟结算受保护的处理环境的组合。最终，电脑空间将部分充满大的、“虚拟”计算机，其中对资源的访问基于“可达性”和权利。

分布式商务公共事业是模块化、可编程和通用化的环境，它能支持这些虚拟计算机。分布式商务公共事业是一种独特的、设计电子商务价值链模式和虚拟计算机的架构基础。具体实现手段的可编程性，能够为相同和/或类似的服务支持不同的实际（逻辑的和/或物理的）和/或不同程度的分布，例如：

●集中式的商务公共事业系统和服务可以用来有效地从集中的位置提供一定的支持服务功能或功能的结合。

●其它商务公共事业系统可以用部分或完全分布式的方式提供。

●一些支持和管理性的服务功能可以分布于和/或跨越现有或新的通信架构或其它电子网络支持组元。

●其它支持服务可以利用对等通信和交互，在任何或所有用户的电器上的安全执行空间（如受保护的处理环境中）中运作，用来提供支持服务组织的安全网。

●其它支持服务在网络支持架构和用户的电器中都可以运作。

这些分布式支持服务可以补充更加集中的支持服务设施（和/或消除对后者的需要）。可以提供相同和/或不同的、非分布式和以不同方式分布的服务的不同组合，用以支持不同的活动。此外，一个总模式的服务性质和分布可以因实现的不同而异。如有必要，这些不同模式的实现可以共享相同的商务公共事业系统和服务，以及/或任何具体的分布式商务公共事业管理和/或支持功能和/或它们的任何组合。

另外，一个具体的商务公共事业系统和服务架构可以以不同的方式为不同的价值链所利用（如商业模式或关系）。例如，某个价值链可以从效率、安全性、控制或其它原因出发，选择使该支持服务的功能更加集中，而其它价值链则可能选择更加分布的和/或不同的分布式模式。

例如，只要支付方法和权利拥有者和/或其它价值链参与者同意，分布式商务公共事业安全架构的任意一个或多个支持服务都可以向最终用户和/或价值链电器的任意集合或组合，分布和/或委派它们的部分或全部功能和授权。分布和委派这些服务和功能具有各种优点，如能够灵活有效地创建临时的、专门的安全电子商务网，其中，集合或组合中的任一、若干或全部电器都可以至少作为同一商务网组织中的其它电器的部分（如果不是完全）对等物进行参与。

本发明提供了下列与分布管理和支持服务有关的附加特性的非穷举的列表：

●任何管理和/或支持功能的任意混合都可以与任何其它管理和/或支持功能的混合集成。

●在一个集成设计中，商务公共事业系统功能的任意集合或子集可以与商务公共事业系统功能的任何其它混合相结合。这些混合可以

以任何所希望的程度进行分布，且该混合中任意一个或多个部分的分布与其它任何一个或多个部分相比，可多可少。这就允许价值链采用最佳的和/或切实可行的设计。可以提供包括任意程度的分布在内的权利结算、金融结算、使用累积、使用报告和/或其它结算和/或其它分布式商务公共事业功能的任意混合。这些分布式商务公共事业功能和/或管理和/或支持服务，能够与其它任何期望的分布式商务公共事业功能和/或管理和/或支持服务相结合。

●任何一个或多个管理和/或支持服务和/或功能都能作为商务公共事业系统运作，并且支持商务公共事业系统节点的网络，每个节点至少支持这些商务公共事业的管理服务活动的一部分。每个商务公共事业系统都能向其它商务公共事业系统和/或节点批准授权和/或提供服务和/或与之安全地互操作。

●每个商务公共事业系统（或商务公共事业系统的组合）都可参与有多个商务公共事业系统组成的“虚拟的结算所”。在优选实施方案中，在依据VDE规则和控制时，这些“虚拟的结算所”可以以这些规则和控制所规定的方式，与参与同一网络的其它商务公共事业系统和/或其它虚拟结算所互操作。这些“虚拟的结算所”可以从电子控制装置中内建的安全处理控制链中获取授权，并可参与从这种处理控制链和其它VDE能力获得的电子商务处理自动化。

这种以任何期望的程度跨系统或网络分布任何支持服务功能并在期望时随后加以修改（调整）的能力，提供了巨大的功能、灵活性并提高了效率。例如，诸如结算功能等支持服务的分布方面将有助于避免“瓶颈”，即如果它没有足够的能力来应付处理负荷，就会创建集中式的结算设施。利用许多价值链参与者的设备的分布式处理能力，还在改进效果和系统响应时间、更低的运作开销、更高的容错性、应用实现中的多功能性、以及通常从本发明对每个价值链参与者的需求和要求的适应性获得更多的价值链吸引力等方面，具有巨大的好处。

分布式商务公共事业提供的管理和/或支持服务的一些实例

可以将分布式商务公共事业组织成若干不同的、专门和/或通用的“商务公共事业系统”。商务公共事业系统可以是集中式的、分布式的或部分分布部分集中式的，以提供实际的商务管理层所需要的管

理、安全和其它服务。一些商务公共事业系统包括一些公知的管理服务功能，如金融结算所和认证机构等分布式商务公共事业的实现形式。其它商务公共事业系统涉及针对公知的服务活动的新型服务和新的组合及设计。商务公共事业系统是支持具体电子商务模式的分布式商务公共事业的任何示例，商务公共事业系统本身可以由商务公共事业系统的组元构成。商务公共事业系统可以包括以下以任何形式组合的任何或所有能力和分布设计，例如：

●金融结算所，

●使用结算所，

●权利及许可结算所，

●认证机构，

●安全目录服务，

●安全交易管理机构，

●包括上面紧接着列出的系统能力的任意组合在内的多用途、通用和/或商务公共事业系统的组合，以及

●其它商务公共事业系统。

这些商务公共事业系统的设施和适用性的范围很广。例如，它们可以为以下列出的任一或所有项目提供管理支持：

●可信的电子事件管理，

●联网的、自动化的、分布式的、安全的处理管理和控制，

●虚拟的分布环境处理链和控制，以及

●跨包括“未联”、虚拟联接或周期性联接的网络在内的电子网络和/或在此网络内的权利管理和使用（如事件）管理（如审核、控制、权利履行等）。

商务公共事业系统可以监管电子处理链和与下列有关的电子事件结果，如：

●电子广告，

●市场和使用分析，

●电子货币，

●金融交易结算和通信，

●生产和其它的分布式处理控制模式，

●金融结算

●使至少部分基于内容、处理控制（事件）和/或权利管理的支付履行或其它报酬的规定（包括服务费用、产品费用或其它任何费用和/或收费）成为可能，

●执行审核、记帐、支付履行（或其它报酬的规定）和/或其它结算活动，

●编译、积累、使用和/或提供与一个或多个安全容器和/或内容和/或处理（事件）有关的信息，包括安全容器的内容和/或其它任何内容，

●根据使用审核、用户情况和/或与一个或多个安全容器和/或内容和/或处理（事件）有关的市场调研提供信息，

●采用从用户对内容透露的情况（包括广告）和/或处理（事件）的利用中获取的信息，

●为已登记和/或正在登记的对象提供对象登记服务以及/或权利、许可、价格和/或其它规则和控制信息；

●与规则和控制一起使用和/或为规则和控制所需要的电子认证信息，如验证身份、等级隶属关系和/或其它分类方式（例如自动处理的类别验证）的属性，如与权利有关的基于管理管辖范围（纳税）、雇佣和/或其它包括获得的等级权利（如购买的折扣买主俱乐部的会员资格）的金融交易的履行；

●第三方存档和/或验证用于安全备份和不可拒付的交易和/或交易信息，

●提供商务公共事业系统处理控制和自动服务的可编程混合阵列，其中不同的商务公共事业系统支持不同价值链和/或商业模式的要求，且这种商务公共事业系统还支持分布式的、可扩展的、高效联网的和/或等级关系固定的和/或虚拟的结算所模式，这些模式在商务公共事业系统的分布式结算所受保护的处理环境中采用了安全通信，用以传递与结算所有关的规则和控制以及导出、总结和/或详细的交易信息，

●EDI、电子贸易模式和分布式的计算布置，其中参与者需要可信的基础，使交易价值链高效的分布式管理、自动化和控制成为可能，以及

●其它支持和/或支持服务和/或功能。

附图简述

通过结合附图学习下面关于当前优选实施方案的详细描述，将可以更好更彻底地理解本发明提供的这些和其它特性及优点，这些图为：

图1示出了一个支持消费者的示例性电器的分布式商务公共事业实例；

图1A示出了消费者电器内的一个受保护的处理环境（“PPE”）；

图1B显示分布式商务公共事业可以包括许多示例性商务公共事业系统；

图2A－2E示出了怎样才能分布管理和支持服务功能的实例；

图3A－3C示出了示例性的分布式商务公共事业系统；

图4示出了商务公共事业系统的示例性网络；

图4A示出了消费者电器和商务公共事业系统的一个无限的网络；

图5示出了权利拥有者怎样才能在与电子“信息高速公路”相联的多个商务公共事业系统之间选择；

图6示出了怎样才能使不同的商务公共事业系统一起工作的一个实例；

图7示出了怎样才能将多个管理和支持服务功能综合集成到商务公共事业系统内的一个实例；

图7A示出了组合功能的商务公共事业系统的一个示例性网络；

图8A－8B示出了示例性的商务公共事业系统的层次结构；

图9示出了多功能商务公共事业系统的一个示例性层次结构；

图10示出了一个示例性的金融结算所；

图11示出了一个示例性的使用结算所；

图12示出了一个示例性的权利及许可结算所；

图13示出了一个示例性的认证机构；

图14示出了一个示例性的安全目录服务；

图15示出了一个示例性的交易机关；

图16A－16F示出本发明商务公共事业系统能够支持其它商务公共事业系统；

图17A到17D－3示出了一个示例性的商务公共事业系统的架构；

图17E－1到17E－4示出了商务公共事业系统的示例性交互模式；

图17F示出了管理和支持服务运作的分布部分的一个示例性布置；

图18示出了一个示例性的金融结算所的商务公共事业系统；

图19示出了一个示例性的金融结算所的布置；

图20示出了一个示例性的金融结算处理；

图20A－20F示出了金融结算活动和处理的另一个实例；

图21示出了一个简化的价值链（支付）的分解实例；

图22示出了怎样在金融结算所环境中实现图21的分解的一个实例；

图22A示出了在用户受保护的处理环境中实现支付分解的一个示例性布置；

图23示出了一个更加复杂的价值链（支付）分解的实例；

图24示出了怎样在金融结算所环境中实现分解的一个实例；

图25示出了一个价值链分解的实例，该实例还详细说明了对分布式商务公共事业的补偿。

图26示出了针对任何数量的受款人分解的示例性价值链（支付）；

图27示出了通过金融结算所实现价值链（支付）分解和重新分配的另一个实例；

图28示出了利用金融结算所进行金融结算的示例性超级分配支付和重新分配的方案；

图29示出了一个示例性的、在消费者受保护的处理环境或其它地方进行的价值链（支付）汇总；

图30示出了示例性的、跨多项交易的价值链（支付）归并；

图31示出了示例性的、跨多项交易和多个消费者的价值链（支付）归并；

图32示出了一个提供支付归并的示例性商务公共事业系统的架构；

图33示出了一个示例性的使用结算所的商务公共事业系统；

图34示出了一个示例性的使用结算所的架构；

图35示出了一个示例性的使用结算处理;

图36示出了利用多个使用结算所的另一个示例性的使用结算处理;

图37示出了利用使用和金融结算所的一个示例性的使用结算处理;

图38示出了一个示例性的使用结算所的媒介布局过程;

图39示出了一个根据不同等级消费者使用信息的公开提供折扣的示例性使用结算处理;

图40示出了一个示例性的权利及许可结算所商务公共事业系统;

图41示出了一个示例性的权利及许可结算所的架构;

图42示出了一个示例性权利和许可结算处理;

图42A示出了一个示例性的控制集的更新登记处理;

图43示出了另一个示例性的权利和许可结算处理;

图44A－44E示出了另一个权利和许可结算的实例;

图45A和45B示出了示例性的权利模板;

图45C示出了一个示例性的、与示例性权利模板对应的控制集;

图46示出了另一个示例性的权利和许可结算处理;

图47示出了一个示例性的认证机关商务公共事业系统;

图48示出了一个示例性的认证机关的架构;

图49示出了一个示例性的认证处理;

图50示出了一个示例性的分布式认证处理;

图50A示出了一个示例性的、在存在数字凭证时调整性能和/或其它结果的控制集;

图51A－51D示出了示例性的数字凭证的数据结构;

图51E示出了一个示例性的、用于根据其它数字凭证和可信数据库生成数字凭证的技术;

图51F－51H示出了一个用于规定虚拟实体的示例性的技术;

图52示出了一个示例性的安全目录服务商务公共事业系统;

图53示出了一个示例性的安全目录服务结构;

图54示出了一个示例性的安全目录服务处理;

图55示出了一个示例性的交易机构商务公共事业系统;

图56示出了一个示例性的交易机构架构；

图57示出了一个示例性的交易机构处理；

图58A示出了交易机构怎样创建控制超集的一个实例；

图58B示出了交易机构所执行的示范步骤；

图58C和58D示出了一个示例性的安全检验点的商务公共事业系统；

图59和60示出了分布式商务公共事业怎样才能支持不同电子价值链的实例；

图61示出了一个采购、特许和/或租借的实例；

图62示出了一个实物采购和支付的实例；

图63示出了一个消费者安全地支付服务的实例；

图64示出了实物购买的示例性价值链分解；

图65示出了机构内部和外部的商务公共事业系统之间合作的一个实例；

图66示出了机构之间和内部的一个示例性交易机构的实例；

图67示出了一个国际贸易的实例。

示例性实施方案的详细描述

分布式商务公共事业

图1示出了　与分布式商务公共事业75电连接的用户电器100。在该实例中，电子网络150将电器100与分布式商务公共事业75连接在一起。分布式商务公共事业75支持用户电器100中进行的各种活动。

分布式商务公共事业75为电子商务和通信提供了管理和支持服务的基础。这个基础高效、成本有效、灵活、可配置、可重复利用、可编程且可以通用。它支持个人和商业应用的所有各种电子关系、交互和通信。

分布式商务公共事业能够支持任何电器

电器100可以为任何种类的电子或电气设备，如计算机、娱乐系统、电视机或视频播放机－这里只提到了几个实例的名称。在图1所示的具体的实例中，用户电器100为一台家用彩色电视机102、一台录像机104和一台机顶盒106。电器100可由手持遥控器108所控制。机顶盒106可以通过有线电视网络114从电视广播设备110和/或卫星112接收电视节目。录像机104能够播放磁带、光盘或其它媒质的各种节目

资料，并且还可以具有记录通过机顶盒106接收到的节目资料的能力。

电器100可以具有“受保护的处理环境”

电器100优选地为Ginter等人的专利说明书中图7和图8中所示的那种安全电器。它优选地为Ginter等人的专利说明书中描述的“虚拟分布环境”的组成部分。图1A显示，电视机102、机顶盒106、媒体播/录机104和遥控器108都可具有“受保护的处理环境”（“PPE”）154。分布式商务公共事业75可以与这些受保护的处理环境154中的任一环境内进行的处理交互并提供支持。

受保护的处理环境154可以以一个或多个计算机芯片为基础，如Ginter等人的专利说明书图9所示的基于硬件和/或软件的“安全处理单元”。受保护的处理环境154提供高度安全可信的环境，其中，可以在没有显著的损坏或其它折衷的情况下可靠地执行电子处理和交易。Ginter等人的专利公开书描述了设计、构建和维护受保护的处理环境154的技术、系统和方法，使权利拥有者和其它价值链参与者（包括消费者95）可以信任其安全性和完整性。在优选实施方案中，这种信任对分布式商务公共事业75和电器100之间的交互是重要的。

分布式商务公共事业可由许多“商务公共事业系统”组成

图1B显示分布式商务公共事业75可以由许多商务公共事业系统90组成。商务公共事业系统有不同的种类，如：

- 金融结算所200;
- 使用结算所300;
- 权利及许可结算所400;
- 认证机构500;
- 安全目录服务600;
- 交易机构700;
- VDE管理器800; 以及
- 其它种类的商务公共事业系统90。

商务公共事业系统90可支持和管理受保护处理环境154内的功能或运作。如：

- 电器100受保护的处理环境154可提供自动化的电子支付机制118，该机制根据节目消费将消费者的银行或其它钱财帐户计入借

方．分布式商务公共事业75可包括一种称作“金融结算所”200的专用商务公共事业系统90a，它支持受保护的处理环境154运作的金融方面－确保权利拥有者和其它人得到适当数量的报酬，并确保消费者95不过多付费．

● 电视节目102a的广播商可能需要电器100的受保护的处理环境154，以便利用电子使用 计量机制，计量消费者95观看多少视频节目和它们所观看的视频节目．分布式商务公共事业75可包括一个称作“使用结算所”300的专用商务公共事业系统90b，它接收受保护的处理环境154内的使用 计量器116所计量的使用信息，加以分析并提供报告。

● 视频节目102a的权利拥有者可坚持要求受保护的处理环境154提供一种复制保护机制120，安全地阻止复制视频节目102a。分布式商务公共事业75可包括一个称作“权利及许可结算所”400的专用商务公共事业系统90c，它向受保护的处理环境154提供必要的许可，使消费者95可以观看特定的节目（例如，按观看的次数付费），并为加强禁止复制保护机制120提供援助。

● 视频节目102a的权利拥有者还可以要求电器100受保护的处理环境154在消费者95能够观看视频节目102a之前，处理识别消费者的身份、年龄等信息的“数字凭证”122。分布式商务公共事业75可包括一个称作“认证机构”500的专用商务公共事业系统90d，它向受保护的处理环境154创建和提供“数字凭证”504－使消费者可以有效地与权利拥有者提供的许可交互。

图1B所示的其它商务公共事业系统90包括：

● 一“安全目录服务”600，它可以协助受保护的处理环境154通过网络150与其它计算机和电器进行通信；

● “交易机构”700，它可以用于处理控制和自动化，如安全地审核和监视涉及受保护的处理环境154的复杂电子交易；以及

● 虚拟分布环境（“VDE”）的“管理器”800，在优选实施方案中，它可以使受保护的处理环境154平稳安全地运行。

也可以采用图1B中未示出的其它商务公共事业系统90来管理和/或支持附加的功能和运作。各个商务公共事业系统90可以一起工作，分担全部工作，以便高效、有效地支持消费者95。

商务公共事业系统可以是分布式的

图2A-2E示出了怎样才能分布分布式商务公共事业75。商务公共事业系统90的一些管理和支持功能可在消费者的电器100内－或者甚至以“分散”的方式在大量一同合作的不同电器上执行。

如上所述，电器100分别提供了一个受保护的处理环境154，此环境能抵抗损害并提供一个安全的地点，其中可以执行管理和支持运作。这使得消费者家中的电器100可以执行为他方，如权利拥有者、电子商务的参与者等所信任的运作。鉴于受保护处理环境154的可信的、受保护的特性，商务公共事业系统90的部分、扩展甚至全部都可存在于整个系统中的每个或任一受保护的处理环境154和有关的电器中。

图2A－2E代表了一个示例性商务公共事业系统90，如四块拼图玩具的使用结算所300的全部功能。图2A－2E显示，这些商务公共事业系统的功能可以以不同的程度分布。例如：

- 图2A示出了一个实例，其中商务公共事业系统90的所有功能都是在一个安全的中心设施中进行的。
- 图2B示出了一个实例，其中商务公共事业系统90的大部分功能是在一个安全的中心设施中进行的，但有一些功能是在用户电器100的受保护的处理环境154中进行的。
- 图2C示出了一个实例，其中商务公共事业系统90的一些功能是在一个安全的中心设施中进行的，但大部分功能是在用户电器100的受保护的处理环境154中进行的。
- 图2D示出了一个实例，其中商务公共事业系统90的一些功能是在一个安全的中心设施中进行的，有些功能是在第一个用户电器100A的受保护的处理环境154A中进行的，还有一些功能是在第二个用户电器100B的受保护的处理环境154B中进行的。
- 图2E示出了一个实例，其中商务公共事业系统90的功能没有一个是在一个安全的中心设施中进行的；有些功能是在第一个用户电器100（1）的受保护的处理环境154（1）中进行的，有些功能是在第二个用户电器100（2）的受保护的处理环境154（2）中进行的，有些功能是在第二个用户电器100（3）的受保护的处理环境154（3）中进行

的，还有一些功能是在第N个用户电器100（N）的受保护的处理环境154（N）中进行的。

另一方面或者另外，商务公共事业系统90的一些功能可以分布于网络150内－例如，在用于在电器100之间传输数据的装置中。

分布多个管理和支持功能

图3A示出了怎样才能将商务公共事业系统90的多个功能或子功能分布于同一个受保护的处理环境154中。例如：

● 运作于消费者电器100A的受保护的处理环境154a中的金融结算所功能200a，可提供一定的金融结算如审核，能够取代和/或提供支持集中式金融结算所200所执行的一些金融结算操作。

● 运作于消费者电器100A的受保护的处理环境154a中的使用结算所功能300a，可执行一定的使用信息结算操作，如综合或分析所收集的使用信息，以补充、取代或添加由使用结算所300所执行的使用结算操作。

● 电器100A受保护的处理环境154a可以在消费者地址处，执行一定的权利和许可结算操作400a、一定的认证机构操作500a和一定的安全目录服务支持操作600a，以补充、添加或取代由权利及许可结算所400、认证机构500和安全目录服务600所执行的操作。

图3B显示，另一个示例性的消费电器100（2），…，100N（此例中为个人计算机124）可执行本地支持或管理功能的不同组合（例如交易机构700执行的部分或全部功能）。例如：

● 受保护的处理环境154（1）中的处理可依赖于部分分布式部分集中式的金融结算所200A、部分分布式部分集中式的使用结算所300A、部分分布式部分集中式的权利及许可结算所400A、部分分布式部分集中式的认证机构500A、集中式的安全目录服务600A、以及集中式的交易机构700A。

● 受保护的处理环境154（2）中的处理可依赖于集中式的金融结算所200B、部分分布式部分集中式的使用结算所300B、部分分布式部分集中式的权利及许可结算所400B、集中式的认证机构500B、集中式的安全目录服务600B、以及部分分布式部分集中式的交易机构700B。

● 受保护的处理环境154（N）中的处理可依赖于部分分布式部分集中式的金融结算所200N、部分分布式部分集中式的使用结算所

300N、部分分布式部分集中式的权利及许可结算所400N、部分分布式部分集中式的认证机构500N、部分分布式部分集中式的安全目录服务600N、以及部分分布式部分集中式的交易机构700N。

进一步推广分布式结算服务这个概念，将有可能如图3C中所示完全地分布分布式商务公共事业75－主要或完全地依赖于用户电器100的受保护的安全处理环境154中的管理和支持服务的运作和活动。这样，用户自己的电器100就能－以分布式的方式－执行金融、使用、权利和许可结算、以及认证、安全目录服务和交易机构服务中的任一项或全部功能。这种“本地”和/或并行和/或分布式的处理交易结算能够更有效地满足个人消费者的需求。例如，这是一种允许消费者提供控制的方法，保护从他们自己的电器出来的一些私人数据，同时仍然向权利拥有者提供他们所需要的简明信息。

图2A－2E和3A－3C中所示的分布式的布置与提供集中式商务公共事业系统90并非是互相排斥的方法。相反，提供混合布置可能更加有利，其中一些管理和服务功能（如少量支付的汇总、使用数据的保密功能、以及凭证的颁发，如父亲为他们的孩子颁发凭证）是广泛分布的，而其它管理和支持服务功能（如重要数字凭证的颁发、支持安全目录服务的大型数据库的维护等等）则更加集中。任何具体的管理和支持服务、结算所或功能的分布程度，可以取决于各种非常重要的课目，包括效率、可信度、可扩展性、资源的要求、商业模式以及其它因素。此外，分布的程度涉及多级结构，此分级结构基于由其后是具体的商业子模式的具体商业模式决定的子集，或者地理和/或管理机构和/或地区。

由于给定的电器100能够参与多种活动，其不同的活动有可能依赖于分布式和集中式商务公共事业系统90的不同组合。例如，对于某个活动，受保护的处理环境154可以依赖于集中式的金融结算所200，对另一个活动，它可能依赖于部分分布式部分集中式的金融结算所200，而对又一个活动，又可能依赖于完全分布式的金融结算所200。不同的活动或商业模式可以采用不同程度的分布。

商务公共事业系统网

图4显示商务公共事业系统75可包括一个巨大的分布式、部分分布式和/或集中式的商务公共事业系统90的“网”。网络150可用来将

商务公共事业系统90的这个网与各种不同的电器100相联，电器100可以完全共享分布式商务公共事业75。例如，电子网络150可接到：

- 机顶盒106和/或媒体播放机104，
- 个人计算机124，
- 计算机图形工作站126，
- 多媒体、视频游戏系统128，或者
- 其它任何种类的电器100，例如包括生产控制设备、家用电器、过程控制装置、电子网络和/或其它通信架构的设备、主机和/或微型计算机等。

在这个实例中，同一个分布式商务公共事业75可支持许多不同的消费者、作者、发行者、供应商、经销商以及其他人的各种不同的活动－分布式商务公共事业75可支持数量庞大的不同电子活动。图4还显示，通过交换Ginter等人公开的那种用于安全（如保密性、可靠性和完整性）目的电子“容器”152，商务公共事业系统90可与电器100（也可以相互之间）进行通信，容器152是通过利用在受保护的处理环境中处理的安全规则和控制来管理的。

商务公共事业系统网实际上可以是无限的

图4A显示，商务公共事业系统网可以非常庞大甚至是无限的。事实上，网络150可以是一个无缝的网，它延伸到世界各地，利用任意数量的商务公共事业系统90联接了成千上万的电器。

商务公共事业系统90的网可提供与各种不同的电器非常复杂的互联，这些电器执行的是各种不同的电子功能和交易。如上所述，任一电器100都可能与任一商务公共事业系统90或其它任何电器进行通信。这使得可以最有效、最灵活地将不同的商务公共事业系统分配给不同的电子交易。例如：

- 地理位置相近的商务公共事业系统最能用来尽量减少来回获取数据所需的时间。
- 在一些情况下，较远的商务公共事业系统可以更好地用于有效地处理某些专门的交易。
- 政府规章也可以至少部分地指定选择一定的商务公共事业系统而非其它系统。（例如，如果一个日本消费者尝试使用位于Cayman

岛的金融结算所200，她就可能遇到法律上的问题－或者一个新泽西的居民可能被法律要求使用报告新泽西消费税的金融结算所200）。

● 各方很可能推出不同的、相互竞争的商务公共事业系统，这些不同的系统将充满包括分布式商务公共事业75的网。对于效率和电子商务资源的重复利用来说，这些系统和/或它们的节点之间的互操作性非常重要。

权利拥有者和提供者可以在商务公共事业系统之间选择

图5显示权利拥有者怎样才能在不同的商务公共事业系统系统90之间作选择。在这个实例中，Bob运作第一使用结算所300a，Alice运作第二使用结算所300b，Helen运作第三使用结算所300c。这些不同的使用结算服务提供者可以在质量和/或价格上相互竞争，或者，它们可以是互补的（例如，它们在不同的交易方面各有专长）。

由于电子网络150可将电器100联到许多不同的商务公共事业系统90上，消费者正在使用的数字财产的权利拥有者可以有许多不同的商务公共事业系统供选择。内容提供者和权利拥有者可授权特定的（或成组的）商务公共事业系统90处理交易的不同方面。例如：

● 计算机软件发行者可以规定个人计算机124向Helen的使用结算所300c发送计量信息116a，以监视计算机软件或个人计算机所执行的其它活动的使用。

● 视频节目102的权利拥有者可以指定机顶盒106向Alice的使用结算所发送有关视频的计量信息116。

● 多媒体内容提供者可指定利用Bob的使用结算所300a来处理由多媒体播放机128作生成的使用数据116c。

某些情况下，特定的消费者95也可在提前指定他们喜爱的特定结算所或其它商务公共事业系统90时起作用。图5示出了提供者（和/或消费者的）的选择，通过一个“警察”将计量业务流量引向选定的使用结算所300（这里所述的和Ginter等人所述的电子控制将优选地为实际控制如何引导业务流量的机制）。

内容提供者或权利拥有者能够让消费者95从一组商务公共事业系统90（和/或商务公共事业系统90的提供者）中，选择想要作交易的内容提供者和/或权利拥有者。例如：

● 电视工作室可授权特定的个别或种类的商务公共事业系统90，处理与电视节目有关的交易，以及/或者指定不想由它们处理其交易的具体的个别或种类的商务公共事业系统90。

● 具体的商务公共事业系统90可为个别（或某些种类的）提供者和/或消费者95设立要求或标准。

● 价值链的参与者能够参与法律协议和/或不同商务公共事业系统90的商业关系。

商务公共事业系统可以一同工作

图6显示，不同的商务公共事业系统90可以一同工作，以支持不同的运作。在此实例中：

● 使用结算所300a、权利及许可结算所400a、认证机构500a和金融结算所200a（图的左侧），可以用来支持机顶盒106和电视机102的具体运作。

● 相同的金融结算所200a、不同的使用结算所300b、不同的认证机构500b和不同的权利及许可结算所400b（图的上部），可以用来支持个人计算机124上的一些服务。

● 不同的金融结算所200c、认证机构500c、使用结算所300c和相同的权利及许可结算所400b（图的右侧），可以用来支持多媒体系统128的电子活动.

● 商务公共事业系统的不同组合（在此例中，使用结算所300、金融结算所200d、权利及许可结算所400c和认证机构500a－沿图的底部），可以用来支持声音系统130。

这个实例显示，各种商务公共事业系统90组合起来工作，商务公共事业系统的不同组合可用来支持不同电子交易。

为效率或方便起见可将管理和支持服务综合在通用的商务公共事业系统中

图7显示，出于获得最大的方便性、效率或其它原因，不同的专用商务公共事业系统90的管理和支持服务功能或子功能可以集成在一起，形成更加通用或多用途的商务公共事业系统90。例如：

● Bob可以运作一个集成的或综合的商务公共事业系统90a，该系统提供了金融结算所200a的功能、认证机构500a的功能以及使用结算所300a的功能。

● Anne可以运作一个集成的或综合的商务公共事业系统90b，该系统提供了金融结算所200b的功能、权利及许可结算所的功能400b和交易机构的功能700b.

● Helen可以运作一个集成的或综合的商务公共事业系统90c，该系统提供了权利及许可结算所的功能400c和认证机构功能500c。

● Roger可以运作一个集成的或综合的商务公共事业系统90d，该系统提供了安全目录服务600d、使用结算所服务300d、金融结算所服务200d和权利及许可结算所400d。

操作电器100的消费者可以访问这些不同的商务公共事业系统90或其组合的任意一个或全体。例如，机顶盒106可从Helen的商务公共事业系统90c获得权利、许可及认证，但也能利用Bob的商务公共事业系统90a的金融结算和使用分析。

商务公共事业系统90可提供运作管理和支持功能或子功能的任何组合，以执行一定的商业模式所需要的运作，提供最高的效率和/或便利性。例如，Anne的商务公共事业系统90（2）可以只提供金融结算所功能的一个专门的子集。

图7A示出了一个商务公共事业系统系统90怎样才能提供广泛的、不同的管理和支持功能组合或部分组合的另一个实例。在图7A中，每个管理和支持服务功能都以不同种类的简单积木（child's play block）代表（示意图）：

● 金融结算所200用方块表示，

● 使用结算功能300用半圆块表示，

● 权利及许可结算功能400用矩形块表示，

● 认证机构的功能500用三角块表示，

● 安全目录服务功能600用隧道块表示，

● 交易机构的功能700用圆柱体表示。

图中消费者和用户电器100以竖立着的矩形柱表示。电子网络150用道路来表示，它将各个商务公共事业系统彼此相联，并与消费者的电器100相联。电子数据容器152可沿这个电子网络或不同的电子设施之间的“信息高速公路”150传送。

图7A只示出了许多可能用到的管理和支持服务组合的一部分。例如：

● 在左上方，商务公共事业系统90A至少提供了一些金融结算功能200a、至少一些权利及许可结算功能功能400a和至少一些认证功能500a。这样完整的电子商务公共事业系统90A可以用于代表权利拥有者从事商业管理和授权业务，并根据这些权利处理支付问题。

● 紧挨着设施90A的右侧是商务公共事业系统90D，它包括金融结算服务200d和交易机构服务700a。在审核和/或管理全面复杂的、多步骤的交易，同时还确保交易各方得到应有的报酬时，它显得特别有用。

● 在图的中下方，商务公共事业系统90B包括金融结算功能200f和使用结算功能300c。在处理与电子使用交易有关的支付和其它金融明细帐并根据电子使用提供审核和报告服务时，商务公共事业系统90B显得特别有用。

● 图的中底部示出了商务公共事业系统90C，它将认证服务机构500与使用结算服务机构300相结合。在颁发数字凭证然后记录这些凭证的使用（例如，为评估风险、潜在的债务、保险费用等）时，它显得特别有用。

图7A所示的各种实例是出于演示的目的。取决于商业目标、便利性和其它因素，其它组合是可能或非常可能的。

商务公共事业系统的等级结构

图8A显示，商务公共事业系统90或功能可以分级布置。例如，总金融（或其它）结算所200（N）可以监视和/或对其余的无数金融（或其它）分结算所200（1），200（2），…负总责任。在图8A这个实例中，消费电器100可与结算所200（1）交互，后者可接着与结算所200（2）交互，诸如此类。管理和支持服务的这个“分级结构” 可被认为在某些方式上与大公司或军队中的命令链相类似－具有一些结算所的训练和/或委派能力、控制和/或监管其它结算所。

图8B示出了管理和支持服务的分级结构的另一个实例。在此实例中，若干集中式的总结算所和/或其它商务公共事业系统90将它们的一些或全部职责委托给其它商务公共事业系统90。在图示的这个具体的实例中，公司、非盈利组织等机构可以拥有自己的商务公共事业系统156。一些的电子商务或其它活动（如娱乐业）可以拥有自己的直属专业商务公共事业系统158。一些地理、地区或管辖组织（如威斯

康星州内所有购买某种商品的个人）可以拥有自己的地区性的/管辖性的专业商务公共事业系统160。反过来，分级结构中级别较低的商务公共事业系统156、158和160，可以进一步将职权或职责委托给特定的消费者、机构或其它实体。

在一个实例布置中，被委托了职权的商务公共事业系统90可执行几乎所有的实际支持工作，但却可以通过报告或其它手段通知更多的拱形商务公共事业系统90。在另外一个布置中，拱形商务公共事业系统90无论如何都与受委托的商务公共事业系统的日常活动无关。在又一个实例布置中，更加专门的商务公共事业系统做一些工作，而更多的拱形商务公共事业系统则做其余部分的工作。在具体的方案中，工作和职权的具体划分在很大程度上依赖于有些因素，如效率、可信度、资源的可利用性、受管理的交易类型、以及其它各种因素。可以部分委托结算职权（如委托使用汇总，但不委托金融或权利管理职责），并可以和对等处理一致（如在保留某些集中式的重要功能的同时，将某些功能置于消费者的电器内）。

多功能商务公共事业系统可以分级或对等地组织

图9示出了一个不同的、更加复杂的商务公共事业系统环境，包括一个分级的命令链单元和在不同的多功能商务公共事业系统90之间水平方向上的一个高度合作的单元。在这个实例中，有五个不同等级的职责，第一级的主（拱形）商务公共事业系统90（1）（例如，金融结算所200）拥有最多的职权，2、3、4、5级的其它商务公共事业系统的能力、权力、控制、范围和/或职责依次降低。图9还显示，同一级的不同商务公共事业系统可以具有不同的功能、职责范围和/或地区。例如：

- 商务公共事业系统90(2)(1)可以是“A类”商务公共事业系统，
- 商务公共事业系统90(2)(2)可以是“ B类”商务公共事业系统，
- 商务公共事业系统90(2)(3)可以是“C类”商务公共事业系统。

在下一级上，商务公共事业系统可以是A类商务公共事业系统（如90(3)(1)和90(3)(2)），可以是B类商务公共事业系统（如90(3)(4)），

可以是C类商务公共事业系统（90(3)(5)和90(3)(6)），也可以是混合型的－如商务公共事业系统90(3)(3)可为具有A类和B类功能的商务公共事业系统。

图9还显示，4、5级上的其它结算所可分为各种类型和分类型。例如，在金融结算所200的环境中，A类负责消费者的信贷，B类负责电子支票、C类则负责商务信贷。其它划分可以是Visa（A类）、MasterCard（B类）和American Express（C类）卡的结算。那么A/B类的结算所将负责结算委托，能够处理消费者的信贷和电子支票的结算。B类的分类型I可负责商务电子支票。C类的分类型I负责商业信用卡交易，分类型III则负责信用汇票（credit draft）。多情况的基本原理可以基于管辖的边界（如法国、德国、纽约及阿拉巴马），以及/或者协议的安排（不良贷款风险、小规模购买者、大型交易等职责的委托等）。对等规模反映了协调总交易的需要（如在小规模购买者的结算所和大型交易商的结算所之间）。

权利及许可结算所400可打破内容的类型的限制（如电影；科学、技术和医学类；软件）。子类型A可包括首轮上映的电影、古董和艺术胶片；子类型B可处理杂志和课本；C类可负责游戏、办公和教育内容。结算所之间的对等通信可能涉及多媒体演示的许可（如多媒体演示可将许可储存在一个结算所中，该结算所利用后备通道联到其它结算所，以确保分布最新的许可）。

一些示例性的商务公共事业系统

如上所述，商务公共事业系统90是通用化且可编程的－因此能提供不同的支持和管理功能的混合，以满足给定交易的要求。因此，实际实现的许多或大多数商务公共事业系统90可提供一定范围的不同支持和管理功能，这使得难以将实现手段相互对比分类为特定“种类”的商务公共事业系统。

尽管如此，对广泛的模式、交易和应用来说，某些理想化的专门商务公共事业系统90特别有用。它对描述不同类型的这些“纯粹”的商务公共事业系统的一些特性有帮助并为此提供便利－承认实际的实现手段可以混合一些理想化模式的功能或功能的子集。以下为这些“纯粹”的、理想化的商务公共事业系统的一些特性的简介。

金融结算所200

图10详细地示出了一个示例性的金融结算所200. 金融结算所200处理支付，以确保价值提供者可以获得公正补偿。在执行此项任务的过程中，金融结算所200可以安全地与其它商务公共事业系统90协调。

在这个实例中，金融结算所200可通过电子网络150，利用Ginter等人的专利说明书中结合图5A和5B所描述的那种电子容器152，以安全的方式，与电器受保护的处理环境154通信。金融结算所200可从这些安全的容器152中受保护的处理环境154接收支付信息202，并与各个银行业、信用卡或其它机构电子地交互，以确保进行了合理的支付。

例如，金融结算所200可与消费者的银行206a、提供者的银行206b和消费者的信用卡公司206c交互。例如，金融结算所200可将消费者的银行206a的资金和借贷资金划入权利拥有者的银行206b，以支付消费者看电影、电视节目或其它内容的费用. 此外或在另一方面，金融结算所200可与消费者的信用卡公司206c交互，以请求调查信用、获得信贷授权、支付等。

金融结算所200可向消费者95提供支付报表204 - 例如，通过向安全电子容器152b中的电器100发送报表，以保持报表信息的机密性。在这个实例中，消费者95可利用他们电器100受保护的处理环境154查看报表204，并且还能够将它们打印或保存下来，以便保留记录。

在一个实例中，受保护的处理环境154所提供的支付机制可以是提供电子货币的电子钱包，以便在支付电子服务或内容时使用。这个电子钱包可以存放数字形式的货币。消费者95可将数字货币花在它们想要的任何东西上。当电子钱包空了时，消费者95就能通过授权金融结算所从他们的银行206a中的消费者帐户划拨资金来充实钱包。金融结算所200可处理电子货币的支付，当消费者化光了上一次存的钱后，就安排自动地重新充实电子钱包（例如基于消费者的预先授权），并且向消费者提供他们是怎样花费电子货币的详细报告和报表204。

使用结算所300

图11示出了一个示例性的使用结算所300。在这个实例中，使用结算所300从使用 计量器116接收使用信息，分析使用信息并根据所

进行的分析提供报告．在实现这些任务时，使用结算所300可以安全地与其它商务公共事业系统90协调．

例如，使用结算所300可以向消费者95发送用户上月所观看的所有电影、电视节目和其它内容的详细报告304a。受保护的处理环境154和使用结算所300之间的通信可以是安全容器152的形式。如Ginter等人的专利说明书所述，使用 计量器116能够根据许多不同的因素计量使用情况，并且可从非常详细到完全切断．如果消费者希望，他们就能在他们的电视机102上查看详细的使用报告304a。

使用结算所300可向其它结算所报告符合保护消费者隐私的消费者观赏习惯．还可以在安全容器152中传送这些报告．例如，使用结算所300可向广告客户306提供总结报告304b，该报告没有暴露消费者的身份，但却向广告客户提供了有关消费者观赏习惯的有价值的信息。另一方面，如果消费者同意，使用结算所300就能向广告客户306或其它特定人提供揭示消费者身份的更详细的报告。消费者95回过来又能得到奖励，例如折扣、现金、免费电影或其它补偿。

使用结算所300还可以向权利拥有者308－如消费者95正在观看的视频节目的制片人或导演，发布报告304c。这些报告使权利拥有者得以核实哪些人观看了他们的节目和其它创作。这在确保支付或在向消费者发送他们可能感兴趣的其它类似节目方面可能非常有用。

使用结算所300还向收视情况调查公司310发送报告304d，以便自动地调查节目受欢迎的程度。使用结算所300还可向其它市场研究机构312发送报告，供科学、市场或其它研究使用。

权利及许可结算所400

图12示出了一个示例性的权利及许可结算所400．权利及许可结算所400储存并分布电子许可404（在这些图中以交通指示灯表示）。许可404批准并保留许可，它也规定了结果。权利及许可结算所400可与其它商务公共事业系统90一同协作，以完成其任务。

在这个实例中，权利及许可结算所400可以担当与数字内容相关的集中式“知识库”或权利结算所。例如，广播台、作者和其它内容创作者及权利拥有者可以用电子“控制集”的形式，向权利及许可结算所400登记许可。这些许可能规定消费者能或不能使用数字财产，在什么情况下能够运用许可，并可以规定运用许可的结果。权利及许

可结算所400可从电器受保护的处理环境154，相应地交付许可（控制集），对请求402作出响应。

例如，假设消费者95想在电视机102上观看一场音乐会或战斗片。他们可以操作他们的遥控器108，请求获得观看一定节目的权利。受保护的处理环境154可自动通过网络150与权利及许可结算所400联系，发送电子请求402。权利及许可结算所400可在自己的库或知识库中“查找”，看它是否已经从节目的权利拥有者400那里获得了（且被授权提供）必要的权限404b。然后，它就可以将请求的许可188发给受保护的处理环境154。

例如，许可188可以允许消费者只看一遍音乐会或战斗片，并且用复制保护机制120禁止复制。许可188也可以（或者另外）规定观看节目的价格（例如，从消费者的电子钱包中减去5.95美元）。电器100可向消费者95询问他们是否愿意付5.95美元看这个节目。如果答案为“是”（例如，用遥控器108指示），电器100可自动地将消费者的电子钱包计入借方并“释放”节目，这样，消费者就能观看节目了。

权利及许可结算所400可以在安全容器152b内移交许可188，容器152b也可以包含由许可所控制的信息－或者许可188可在不同的时刻经由与节目或其它内容不同的路径，到达电器100。例如，可以在网络150上发送许可，而与其有关的节目可从卫星112或经由其它路径到达，如有线电视网络114（参见图1）。

权利及许可结算所400还可以向权利拥有者或其它人发布报告406，指明批准或拒绝了哪些许可。例如，书或视频节目的作者可以与消费者的私人喜好保持一致，能够准确地知道有多少人已经请求发行他或她的作品的摘录。这类报告能补充使用结算所300所提供的报告。

认证机构500

图13示出了一个示例性的认证机构500。认证机构500颁发数字认证504，为电子权利的管理提供了环境。认证机构500可与其它的商务公共事业系统90协作，完成其任务。

认证机构500颁发识别特定事实的数字认证504。数字凭证122在某些方面就象驾照或高中毕业证，因为它们每个都提供了一定事实的证明。例如，我们可以出示驾照以便表明我们已经达到了投票、购买

酒精饮料或观看“R”级电影的年龄．该同一驾照表明了一个事实，即我们有自己的姓名并居住在一定的地址，并且具有一定的知识（州的机动车辆法）和技巧（驾驶机动车辆的能力）．数字凭证504类似于驾照的这个方面，即证实执照持有人的身份和有关事实，只不过数字凭证是用数字信息而不是卡片制作。

在这个实例中，认证机构500可接收消费者的请求和有关的证据502，并可颁发证实特定事实的相关数字凭证504．认证机构500还可从其它人如官方机构506、专业机构508和大学510那里，接收证据和凭证，还能够接收凭证的定义。举一个例子，认证机构500可从官方机构506那里获得出生证或其它身份信息．根据这个身份信息，认证机构500就能预备和颁发数字凭证504，表明个人的身份和年龄。认证机构500还可根据从各人那里得到的各种证据和输入，颁发数字凭证504，表明工作状况、职业、居留国或其它各种分类和级别。

认证机构500可识别组织和机器乃至人。例如，认证机构500能够颁发一项凭证，表明斯坦福大学是一所受人推崇的高等学府，或ACME运输公司是一个声誉良好的公司并被批准运输危险物品这样一个事实．认证机构500还可以，例如，向计算机颁发凭证504，表明计算机具有一定级别的安全性或被授权代表一定的个人或组织处理消息。

认证机构500可通过交换电子容器152，与受保护的处理环境154和其它各方进行通信．电器100的受保护处理环境154可使用认证机构500颁发的数字凭证504，以便管理和运用诸如权利及许可结算所400所发布的那些许可188．例如，机顶盒106可自动防止任何17岁以下的消费者观看某些种类的节目资料，或向观看教育资料的学生提供折扣－这一切都是以认证机构500所颁发的凭证504为依据的。

安全目录服务

图14示出了安全目录服务600的一个实例。安全目录服务600的作用类似于计算机化的电话或名称服务目录。消费者95可发送一个请求602，指出他们所需要的信息。安全目录服务600可以“查找”这个信息并向消费者95提供答复604。安全目录服务600可与其它商务公共事业系统90一同协作，以执行其任务。

例如，假设消费者95想用电子方式从Joe's Pizza店定购比萨饼。他们决定想要的比萨饼的类型（例如加香肠和洋葱的大奶酪比萨

饼）. 然而，他们并不知道Joe's Pizza店的电子地址（该地址就象一个电话号码）. 消费者95可以利用遥控器108输入关于他们想要查找的信息（"Joe's Pizza, Lakeville, Connecticut）. 受保护的处理环境154可生成包含这个识别信息的请求602，并将该请求发送给安全目录服务600. 它可以在安全容器152a中发送这个请求.

安全目录服务600收到请求602后，它就可以访问数据库，找到请求的信息. 安全目录服务600以前可能已经从Joe或它处直接得到了Joe的电子地址. 安全目录服务600可在响应604中，将这个请求的信息发回给电器100. 响应604也可以在安全容器152b中. 消费者95可以利用这个信息用电子方式将他们的订单发给Joe's Pizza店—在消费者发出订单后的几秒钟内，该订单就可以显示在Joe's Pizza店的定购终端上. 几分钟以后，Joe就可以向消费者95送去热烘烘的奶酪、香肠和洋葱的比萨饼（用车而不是用电子的方式，因为实实在在的比萨饼远比电子比萨饼更令人满意）.

安全目录服务600可帮助与网络150相联的任何人与其它任何人联系. 举一个例子，安全目录服务600可告诉使用结算所300怎样在网络150上找到金融结算所200. 与网络150相联的任何电器100都能借助安全目录服务600与其它任何电器联系.

如上所述，发送给安全目录服务600的请求602和它发回的响应604可以封装在Ginter等人的专利说明书所描述的那种安全容器152中. 使用安全容器152有助于防止偷听者窃听消费者95和安全目录服务600之间的交换. 这样就保护了消费者的隐私. 如果有人窃听消费者95的比萨饼订单，他们可以不在意，但他们可能更关心保护这样一个事实，即他们正用电子的方式与其它一些人（如医生、银行、律师或其它与他们有保密和信任关系的人）进行通信. 安全容器152还有助于确保跨网络150传送的消息是真实的、未经变更的. 电子容器152使Joe's Pizza店确信刚刚收到的比萨饼订单确实来自于消费者95（而不是其它人），且订单未经变更，而消费者则可以比较相信没有人会以他的名义给Joe比萨饼店发一个假的比萨饼订单. 在这个优选的实施方案中，如果消费者95确实从Joe's Pizza店定购了比萨饼，采用安全容器152和受保护的处理环境154还能确保消费者95不能事后不承认.

交易机构700

图15示出了一个示例性的交易机构700. 在该实例中，交易机构700提供了过程控制及自动化。它有助于确保过程和交易能顺利完成。交易机构700可与其它商务公共事业系统90一同协作，以完成其任务。

更详细地说，在这个实例中，交易机构700监视电子交易和/或处理的状况，同时维护到目前为止发生了什么和为完成整个交易和/或处理还需要发生些什么的安全、可靠的记录。如有必要，交易机构700还可以通过如生成发生特定活动的请求，来起一个更积极的作用。某些情况下，交易机构700可以是复杂交易或处理中的唯一参与者，它“通晓”处理的所有步骤。交易机构700还可根据过程控制中各参与者所提供的电子控制，利用电子方式规定全部处理。

图15示出了怎样利用交易机构700使消费者95能够定购商品（如毛衣）的一个实例。在整个具体的电子化的家庭购物实例中（仅用于示例目的，但并不仅限于此），消费者95可使用遥控器108选择具体的零售商、想以一定的价格定购的毛衣的款式和颜色。在这个家庭购物实例中，电器100的受保护的处理环境154可生成电子订单702，该订单被发送给电子“邮购”公司的订单收取部门704. 可以在安全容器152中发送订单702.

在这个实例中，交易机构700可协助电子邮购公司协调商业活动并确认已经准确及时地完成了交付毛衣所需的所有步骤。例如：

- 收到电子订单702后，订单收取部门704可以给交易机构700发一个电子通知706. 交易机构700储存电子通知706并可能发一个“要求”708.
- 在下单之前，交易机构700可能已经发布了要求708，使订单收取部门704知道订单进来时该怎么做。
- 根据“要求”708，订单收取部门704可向生产部门712发订单710的电子和/或书面（或其它）版本。
- 交易机构700可向生产部门发一个生产要求714，以根据消费者的喜好生产毛衣。

● 交易机构700还可向供应商718发供货要求716。例如，交易机构700可要求供应商718供应物资，如线球711，使生产部门712具有生产毛衣所必须的原材料。

● 当供应商718已经提供了所需物资时，它就可以发出通知720，通知交易机构700。

● 当生产部门712做完了毛衣后，它就向交易机构700发一个通知722，提示交易机构700。

● 交易机构700可根据生产部门712发来的通知722，向发货部门724发一个通知726，例如，要求发货部门从生产部门那里取回完工的毛衣，并将毛衣交付到消费者手中。

● 交易机构700可与其它商务公共事业系统90，如金融结算所200协作，以安排支付问题。

当然，本实例仅用于示例的目的。交易机构700可用于所有各种不同的处理和自动化，如商业机构内部或商业机构之间的电子订单及销售的处理、电子数据交换（EDI）、电子合同的协商和/或履行、电子文档的交付、公司之间及公司内部的交易、商务处理的安全电子集成－这里只列出了许多有用的应用中的几个。

VDE管理服务800

在该优选实施方案中，VDE管理器800（参见本说明书的图1和图1A以及Ginter等人的说明书中的有关讨论）可提供各种电子维护和其它功能，以使网络150、电器100受保护的处理环境154和分布式商务公共事业75安全、平稳、高效地运作。例如，VDE管理器800可管理整个网络150的电子安全密匙，并且可通过电器100、各商务公共事业系统90和其它电器，提供与安全数据的维护有关的服务。如Ginter等人的专利说明书中详细描述的那样，VDE管理器800所担当的其它重要功能包括安装及配置受保护的处理环境154，以及协助受保护的处理环境安全地维护储存的许可和/或使用数据。VDE管理器800可与其它商务公共事业系统90一同协作。

商务公共事业系统90可以相互支持

除了支持消费者95以外，商务公共事业系统90还可以支持其它商务公共事业系统。图16A－16F对此作了显示。例如：

● 金融结算所200有助于确保其它商务公共事业系统90为它们的付出而获得报酬（参见图16A）；

● 使用结算所300（参见图16B）可向其它商务公共事业系统90通告它们所提供的支持是怎样使用的．例如，使用结算所300可告诉认证机构500是怎样使用它的凭证的（这对认证机构随时了解其担保的潜在债务或协助检测虚假凭证非常有用）。

● 图16C显示，权利及许可结算所400可支持其它商务公共事业系统90，如金融结算所200、使用结算所300、其它的权利及许可结算所400'、认证机构500、安全目录服务600、以及交易机构700。

● 认证机构500可发布数字凭证504，证实其它一个或多个商务公共事业系统90（参见图16D）的运作－支持其它商务公共事业系统90，如金融结算所200、使用结算所300、权利及许可结算所400、其它认证机构500'、安全目录服务600、以及交易机构700。

● 图16E显示安全目录服务600可支持其它商务公共事业系统90，如金融结算所200、使用结算所300、权利及许可结算所400、认证机构500、其它安全目录服务600'、以及交易机构700。

● 图17F显示交易机构700可支持其它商务公共事业系统90，如金融结算所200、使用结算所300、权利及许可结算所400、认证机构500、安全目录服务600、以及其它交易机构700'。

"A piece of the tick"

此处描述的商务公共事业系统90提供了有价值的、重要的服务和功能。这些服务的运作者能够并且应当从它们所提供的服务中获得补偿。金融结算所商务公共事业系统200可确保他们和其它支持服务的提供者获得这种补偿，并且不会给其它电子社区和价值链参与者带来不便。

在协助或补偿价值链参与者过程中，商务公共事业系统90可以（根据业已批准的协议安排）提取它自己的那一部分或百分比，以便补偿它所提供的结算服务．可以根据少量归于每次电子交易("a piece of the tick"）的支付（即"小额支付"）补偿支持服务。提供者可以以各种方式将这些费用部分或全部转交给它们各自的价值链参与者。

可以调用几种不同等级的价值链参与者补偿商务公共事业系统90，这些参与者包括：

● 信息消费者（例如，包括利用电子商务、电子交易管理和权利管理活动产生的信息“消耗”的人）；

● 内容的权利拥有者和其它电子提供者；

● 最广泛的安全、分布式电子商务交易的参与者；

● 此外，各个支持服务提供者可能还必须以各种方式相互支持－因此可能需要彼此补偿。例如：

● 一个商务公共事业系统90可以作为另一个商务公共事业系统90的消费者的中介；

● 一个商务公共事业系统90可能被要求支持另一个商务公共事业系统90的运作；和/或

● 商务公共事业系统90可能必须一同工作，以支持公共的交易。

不同的商务公共事业系统90可以合作建立公共的费用，然后在它们之间进行分配。在另外一个方案中，每个商务公共事业系统90可单独从自己的服务中收费。不同的商务公共事业系统90之间，依据服务的质量和价格可以存在竞争－就象信用卡公司现在竞争供应商和消费者的生意一样。

示例性的分布式商务公共事业系统的架构

在Ginter等人的专利说明书的第180页及以后的部分描述并在图10－12中示出了一个“权利操作系统”，该系统提供了一个小型的、安全的、由事件驱动的、隔开的、基于服务的、面向“组件”的、分布式的多处理操作系统环境，该环境集成了带有传统操作系统概念的VDE安全性控制信息、组件和协议。根据这些发明所提供的优选的示例性商务公共事业系统90的架构建立在Ginter等人描述的权利操作系统的基础上并加以扩充。

例如，优选的示例性商务公共事业系统90的架构提供了服务功能的集合，权利操作系统可作为应用来运行。这些服务功能定义了各种有用的、任何和/或所有商务公共事业系统90可能需要执行的任务。这些服务功能是可分布的、可扩展的和可重复利用的。它们可以综合为各种组合和分组合－例如取决于商业模式－以提供实现任何特定的商务公共事业系统90所期望的总功能。

图17A示出了一个示例性的商务公共事业系统90的总体架构，图17B示出了商务公共事业系统的应用架构的一个实例，图17C则示出了服务功能的具体细节.

首先参照图17B，在这个实例中，商务公共事业系统90的应用软件架构包含商务公共事业系统描述器90A。商务公共事业系统描述器90A包含关于商务公共事业系统90的信息，该系统可用于识别该系统及其能力，以及描述、汇总任何数量的服务功能90B(1)、90B(2)，…和/或提供接口。商务公共事业系统描述器90A和服务功能90B可以，例如，用面向对象的编程技术，以及将实际上怎样实施和/或实现所请求的商务公共事业系统90的活动抽象化来实现，用面向对象的编程技术协助确保这种描述器和服务功能为模块化且是可重复利用的.

商务公共事业系统描述器90A(1)还可负责协调服务功能90B的活动。在这个实例中，描述器90A用于将请求和其它系统活动定向到适当的服务功能90B，以便通过调和接口、数据类型等可能存在于服务功能90B之间的差异，以及协助在各种服务功能90B之间定向总的处理流，确保需要一种以上服务的活动被协调。这些服务功能90B的实例的非穷举性的列表包括如下:

- ●审核，
- ●维护记录，
- ●监督处理，
- ●监视状态，
- ●完成处理定义，
- ●处理控制，
- ●清算服务的接口，
- ●资金转帐，
- ●货币兑换，
- ●计税及应用，
- ●帐户创建及标识符的分配，
- ●支付汇总，
- ●支付的分解，
- ●预算的预授权，
- ●状况通知，

●证实，
●未完成事件的记录，
●要求的生成，
●报告的生成，
●事件的后果，
●帐户调节，
●身份验证，
●电子货币的创建，
●事件数据库的管理
●路由数据库，
●生成请求，
●复制，
●传播，
●使用数据库的管理，
●帐单的创建和处理，
●市场研究，
●协商，
●控制集数据库的管理，
●控制集的生成，
●处理控制逻辑，
●事件流的生成，
●路由，
●归档，
●权利及许可数据库的管理，
●模板数据库的管理，
●商务管理语言的处理，
●权利管理语言的处理，
●广告数据库的管理，
●自动级别的生成，
●自动级别的分配，
●公证，
●印章生成器，

●数字时间戳，

●指纹/水印，

●出价和还价，

●对象登记

●对象标识符的分配，

●版权登记，

●控制集登记，

●模板登记，

●凭证的创建，

●撤单的维护，

●定向器数据库的管理，

●数据库查询和响应的处理，

●其它服务功能。

图17C更详细地示出了服务功能90B。在这个实例中，服务功能90B由服务功能描述器90C和任意数量的服务应用组件90D(1)，90D(2)，…组成。服务功能描述器90C起着类似于商务公共事业系统描述器90A的作用，只不过它用于服务功能90B和服务应用组件90D。服务功能描述器90C和服务应用组件90D也可以利用面向对象的编程技术，以及将实际上怎样实施和/或实现所请求的服务功能90B的活动抽象化来实现，用面向对象的技术协助确保这种描述器和服务应用组件为模块化且可重复利用。在这个实例中，服务应用组件90D通过执行服务功能90B的步骤或子功能，实现服务功能90B的绝大多数能力。

图17A示出了一个示例性的商务公共事业系统90的总架构。该实例所示的总架构为面向对象的系统，其中总的商务公共事业系统90为单一的对象，而它又是由可重复利用的服务功能90B对象组成的。这些服务功能90B对象是由可重复利用的服务应用组件（对象）90D组成。如下详细描述的那样，任一或所有对象可利用商务公共事业支持服务层90－4所提供的服务。所示优选设施方案的商务公共事业系统架构90建立在Ginter等人的专利说明书中详细描述的权利操作系统90－1之上（例如，参见Ginter等人的图12）。一组服务功能90B包括权利操作系统90－1所执行的“应用”。服务功能90B的数量是任意的。

图17A所示的面向对象设计的商务公共事业系统90架构有几项可取的特性。例如，商务公共事业系统90可以容易地添加、移去和/或更换服务功能90B，以改变、扩充和/或增强其能力。类似地，该架构允许添加、移去和/或更换服务应用的组件90D，以便使服务功能具有相似的灵活性。此外，面向对象的设计显著改善了服务功能和/或服务应用组件在不同商务公共事业系统90中或不同服务功能90B（如图17A所示）中重复利用的简易性和效率。

应用层由服务功能层90－2和服务应用组件层90－3（包括组件90DA），如果需要，可以由商务公共事业的支持服务层90－4来支持。商务公共事业的支持服务层90－4可提高大量交易的效率。这些商务公共事业的支持服务90－4可包括，如：

●对话管理，

●容错

●内存管理，

●负荷平衡，

●数据库的桥接，以及

●其它商务公共事业的支持服务。

在这个实例中，服务功能90B是以组件为基础的，并利用了可重复利用且基于组件的服务应用组件90D。服务应用组件90D通常执行服务功能90B的步骤或子功能。每个服务应用组件90D都可以有一个或两个部分：

组件90－B_a，它不必在受保护的处理环境154中执行；以及

安全组件90－B_b，必须在受保护的处理环境154中执行。

在这个示例性的架构中，在组件$90D_a$和组件$90D_b$之间可以存在对应关系。例如，至少有一个组件$90D_a$可与至少一个$90D_b$对应。在组件$90D_a$和组件$90D_b$（如图17中以公共的几何形状所示）之间可以有一对一的对应。在这个优选实施方案中，这种功能上的隔离使得可以在必须和/或必要时，在PPE 154中运作的安全处理和服务应用组件90D之间交互。利用这种架构，可以更加容易、更有效地创建实现同时需要应用层及安全处理能力的服务功能。例如，在这个优选实施方案中，商务公共事业系统90提供的一些性能上的管理和/或支持功能，可以涉及应用层数据库功能以及得到受保护的处理环境（“PPE”）154保护

的信息的利用．这样的一个具体实例可以是金融结算所200的使用者的支付记录．如果金融结算所200的运作者选择在应用层数据库中保存支付的历史信息，但是需要受到PPE 154保护的信息，以便精确地确定消费者帐户的目前状况，用单一的对象来实现服务应用组件$90D_A$，可以明显简化给定服务功能90B中利用信息的任务（如延长额外贷款的决定），组件$90D_A$使应用层数据库中的信息与受PPE 154保护并由服务应用组件$90D_B$处理的信息相一致．此外，这个示例性的服务应用组件可以在其它服务功能90B中重复利用。

在另一个实例中，服务应用组件$90D_A$可以主要充当相应的PPE 154对象$90D_B$的应用层接口对象。例如，如果公证服务功能90B要求应用数字签名，那么服务应用组件$90D_A$可以主要提供一个接口，该接口从对应的服务应用组件$90D_B$收发信息，组件$90D_B$执行创建和实施数字签名的几乎所有实际工作。此外，应用层服务组件$90D_A$可另外提供异常处理、协议转换或其它功能，用来协助更加容易地或以与最初为服务功能90B设计的方式不同的方式来集成能力。

图17D－1示出了服务功能90B和有用的、普通类型的示例性商务公共事业系统90之间示例性的对应关系。示例性的服务功能90B（“审核”、“记录维护”，…）在水平方向表示。这些示例性服务功能90B对商务公共事业系统90的实例类型（“金融结算所”、“使用结算所”，…）的实现有用处，这些实例垂直地写在图表上面那一行的方框中。图17D－1的图表并没有列全－可能还有其它类型的有用的商务公共事业系统，也可能还有其它的服务功能90B。的确，商务公共事业系统90的架构确保在商业模式或其它因素改变时，其类型和服务功能90B都能加以扩充。

在几乎所有的实现方案中，尽管一些商业要求和模式可能会激发重要服务功能的组合和集合的使用，商务公共事业系统90的架构本质上是灵活的－使实施者能够按照他们的需要自由地混合及组合各种不同的功能。例如，提供扮演“金融结算所200”角色－提供支付处理、通信、数据库管理和其它相关服务的商务公共事业系统90是有用的。商务公共事业系统的架构能提供这样的“金融结算所”－本质上也更加通用化和更具有通用性。例如，“金融结算所”的具体的商务公共事业系统90实现方案，还可以将“非金融”服务功能与金融服务

功能相结合．商务公共事业系统90任何给定的实现方案中所实现的具体功能或功能集，取决于实施者的单独要求－例如由商业模式或功能决定．

例如，图17D－2显示，“金融结算所”200这一示例性的商务公共事业系统的全部功能可以从示例性的服务功能90B中建立．在这个实例中，用黑线包围的服务功能90B就包括在图17B所示的商务公共事业系统描述器90a中．图17D－3示出了建立在黑线包围（图17D－1所示）的服务功能90B的不同子集上的使用结算所300这一示例性商务公共事业系统。比较图17D－2和图17D－3，可以看出，有些服务功能90B（如“审核”、“状况通知”、“事件数据库管理”等）可以在金融和使用结算操作中重复利用．金融和使用结算所商务公共事业系统90的综合可以使用图17D－2中黑线包围的服务功能90B和图17D－3中黑线包围的服务功能90B的并集。简单地提供和调用或多或少和/或不同的服务功能90B，就能向具体的商务公共事业系统90提供或多或少和/或不同的功能。

商务公共事业系统90的分布

在优选实施方案中，上述安全应用组件90－3可包括或包含Ginter等人的专利说明书中图41A－41D和48所示的互惠控制结构和有关的规则及方法。这些互惠控制结构可用于互联运作于相同或不同的商务公共事业系统90或其它的电器100上的不同或相同控制集。因此，每个操作者都可能与其它操作者－即各种操作中的一些作用所涉及的商务公共事业系统90，有一种或多种互惠关系。

图17E－1到17E－4示出了不同交互模式的实例，商务公共事业系统90可利用这些交互模式，与正在进行的部分基于这些互惠控制结构的交易或处理交互：

●图17E－1示出了一个事件中介模式，其中商务公共事业系统90收到来自安全实体（如第一个受保护的处理环境）的一个事件通知748，生成一个事件758，事件758引发另一个（和/或同一）安全实体（如第二和/或第一个受保护的处理环境）的活动。

●图17E－2示出了一个不同的商务公共事业系统交互模式，其中第一个安全实体向商务公共事业系统90和其它安全实体提供事件通

知748，执行某个步骤，但第二实体在实际执行下一步处理之前，要等到从商务公共事业系统90收到授权之后才继续进行。

●图17E－3示出了一个通知模式，其中从安全审核目的出发，商务公共事业系统90更多是作为一个被动的旁观者，接收事件通知748，除非要解决异常问题（如出错），否则不会直接与正在进行的处理或交易进行交互。

●图17E－4示出了一个以前的授权模式，其中商务公共事业系统90收到某个安全实体的事件通知748之后，必须在实体将该事件通知748传给下一个安全实体以执行整个处理或交易的下一步之前，向该实体发布一个通知748'。

图17E－1到图17E－4所示的商务公共事业系统90的各种交互模式并不是全部，也不是相互排斥的－任何给定的交易或处理都可以根据商业模式或其它要求，包括这些模式的不同组合的部分或全部。如上所述，本发明为在系统50或网络中分布具体服务功能90－2或服务应用组件90－3的运作提供了技术－例如，包括向个人消费者95的电器提供。图17F示出了控制集188的一个实例，该控制集可用于控制远处的受保护的处理环境（如消费者的电器）执行结算操作的“本地”部分。商务公共事业系统90可以向消费者的电器、其它商务公共事业系统90、或其它某种电器（如隶属于通信架构的组成部分）交付这种控制集188.例如，商务公共事业系统90可以把它的部分结算职权（例如，用一个或多个服务功能90－2来实现，每个功能都包括一个或多个服务应用组件90－3），委托给一个过程控制，该过程控制可在用户电器的受保护的处理环境154中执行。

图17F实例就是方法850（如计量、记帐或预算），其AUDIT事件852（1）是由审核方法854处理的。例如，示例性的计量方法850可能有：

●USE事件852（2）（如“点击”计量），

●INITIALIZE事件852（1）（如准备计量供使用），

●RESET事件852（3）（如在出错以后将计量器恢复到已知的良好状态），

●AUDIT事件852（4）（如收集USE事件中生成的记录以及当前UDE值的副本，并安排向审核员交付），

●READ USE RECORD事件852（5）（如返回所请求的使用记录的副本），

●READ UDE事件852（6）（如返回当前UDE的副本），

●READ MDE事件852（7）（如返回所请求的MDE的副本），以及

●各种各样的其它事件。

在该实例中，AUDIT事件852（4）可联接到审核方法854。在该实例中，为了访问该数据，商务公共事业系统90可能需要获得访问标签和/或适当的PERC控制集形式的许可，以及计量方法850的USE事件852（2）所写的记录格式的语义知识，PERC控制集定义了更加详细的使用许可。语义知识可以来自段外（out of band）协议（如标准），或通过访问描述使用记录格式的计量方法850的MDE（或有关的MDE部分）获得。

审核方法854的事件包括USE事件856（2），该事件执行调用方法的事件所预期的功能－在此情况下，收集使用记录和当前MDE的副本并将它们发出去。在该实例中，假设这个方法中还有一个INITIALIZE事件856（1）。当被调用时，INITIALIZE事件856（1）将被送进去，其相关的装载模块将回叫计量方法850的READ MDE事件852（7），了解使用记录的语义。然后，调用USE事件856（2），与处理该事件有关的装载模块852（2）将调用计量方法850的适当事件（如重复调用READ USE RECORD事件，调用READ UDE一次）。此时，除管理对象的封装和传递以外，调用方法所期望的目的已经达到。

为实现更加分布的结算功能，USE事件856（2）可能要作更多的处理。例如，在读取计量器的USE记录的过程中，审核方法854可实现分析功能（如将使用的对象加以分类，将就结算链所报告的信息减少为访问了各类内容多少次这一简单的计数）。不感兴趣的内容类型记录则被抛弃。详细的记录本身在分析以后也可以被抛弃。在另一个实例中，可以将UDE值（如记录了多少次点击）与检索到的用户记录数量加以对比，如果两者不一致，就能就地汇报或采取措施（如在进一步的交互之前禁止使用给定提供者的对象）。在又一个实例中，记录可以将用户的身份信息去掉，以保障隐私。在另一个实例中，可以就地处理和分析某些使用记录（然后抛弃），而其它详细信息则被保存下来，供以后处理。

一旦执行了分布式的结算功能，信息就能被封装在一个或多个管理对象中，以便沿结算链上传到集中的地点。这可能涉及向提供者直接报告，和/或向其它结算功能报告。在接收、处理、发送或受件人的确认收到以后，可以用审核方法854将处理过的记录释放（利用计量方法删除、总结或提交）。

在另一个采用图17F所示的计量方法850的实例中，AUDIT事件854可由计量方法850“内部”执行。在该实例中，用户记录和UDE将被捆绑在一个或多个管理对象中，利用与计量方法850的AUDIT事件854（4）有关的装载模块853传送给审核员。然而，它们也可以不将这些对象发出去，而是就地处理。为此，ROS（参见Ginter等人的图12和图13）采用的、用来寻找指定的审核员的名称服务记录被重新定向回本地PPE 154。在PPE 154中，可以创建（以代表它们所交付的方法和/或装载模块为基础）由商务公共事业系统90所控制的处理，执行上述的本地结算功能，只不过采用的是管理对象的内容，而不是调用计量方法的事件。由于这种运作是在管理对象和它们的内容之上进行的，更象是在远处的结算设施中执行的功能，但处理能够在本地消费者的电器和联网的电器中进行。

用这种方式分布支持服务提供了集中式架构所没有或不具备的附加能力。例如，权利及许可结算所可以委托机构内的一台本地服务器记录请求并缓存机构以前请求的许可的副本。这样一种本地权利及许可结算所能够降低网络的通信量，并且针对具体机构的许可提供便利的本地知识库（如计算机软件的现场许可）。权利拥有者、权利及许可代理机构或其它权利分布组织，可以授权本地的权利及许可服务器根据请求批准许可。

另外一个例子，许多安全的、高度自动化的管理和支持服务可以全部和/或部分地分布在一个至少不定期联接的电器中－不管该电器是计算机、机顶盒、个人数字助理（PDA）、数字电话、智能化的数字电视，还是其它任何数字电器。这些电器可以利用受保护的处理环境来保证支持服务的执行安全可靠，不会被篡改和干扰（如Ginter等人的专利说明书所述的那样）。

在另一个实例中，一个可能的VDE内容分布方案涉及执行初始封装作用的内容提供者、执行分布功能的分布者、记载使用记录的用

户、以及处理使用和金融信息的结算所。这与集中式的处理模式形成对比，其中所有这些功能都是由集中的一方执行的。

还有一个例子，通过跨个人用户的电器、局域网（LAN）服务器、和/或公司里联接公司的LAN/WAN环境和外部世界的“网关”机器、以及商用的“主干”服务器，分布结算所的功能，可以实现效率的提高。

还有一个例子，核心凭证管理机构可以授权公司的计算机批准某些数字凭证。例如，公司可以是某个贸易组织的成员。贸易组织的认证机构可以给予这个公司一个数字凭证，表明这个事实，并委托该公司自己的计算机作颁发凭证的认证机构，表明该公司的每个员工都是该贸易组织的一员这一事实。类似地，父母可被授权颁发代表他们后代的数字凭证。

上述技术通过采用商务公共事业系统90的架构，阐明了怎样能够跨多个商务公共事业系统分布分布式商务公共事业。此外，一个或多个商务公共事业系统90所提供的服务功能90－2，可以分解成在其它整个或部分商务公共事业系统90或给定方案的参与者所选定的其它任何系统（包括最终用户系统）中执行的整个或者甚至部分处理步骤（如服务应用组件90－2）。

示例性商务公共事业系统的类型

金融结算所200

图18示出了金融结算所商务公共事业系统200的一个实例。“金融结算所”支持电子交易的自动化的、高效的金融履行。例如，金融结算所200可收集与支付有关的信息和细节，并有效地安排转帐和其它补偿，以确保价值的提供者得到报酬，包括将支付自动地、有选择地分解成定向到适当的价值链参与者的支付部分。金融结算所200还可以向参与者（如最终用户）受保护的处理环境提供贷款、预算限制，和/或电子货币，其中，为了操作的安全和本地性能，金融结算所可能已经将它的一些操作分布到这些受保护的处理环境中了。以下就是可以通过利用本发明来提供的示例性的金融结算支持功能：

●以安全、高效、及时和精确的方式对金融交易进行结算。

●向受到价值提供者和用户/消费者信任且便利的支付机制提供安全的金融结算。

●保证向权利拥有者和其它价值链参与者（例如，在从创建到分布、销售及到交付的过程控制的某些部分中向电子社区提供价值的提供者）支付，不要求他们承担管理大量与广泛分布的消费者和/或各种常常复杂的金融服务标准和协议打交道的金融工作。

●允许内容的消费者使用各种不同的支付媒介，通过公共的、可信的接口支付信息产品和相关的服务的费用。

●允许交易中的每一方确认指定的交换已经按照双方的意愿发生，并且防止任一方否认交易。

●在购买或使用报告时协调帐户（如从价值链参与者的帐户转移资金到一个或多个提供者的帐户上）。

●支持频繁的小额交易结算活动。

●向所有的价值链参与者（如各种数字内容的购买者、发行者和经销商，以及实物商品的购买者、发行者和经销商和其它服务的使用者）提供金融结算服务。

●将分布式的电子商务域与现有的电子、书面和/或其它支付和/或结算服务接口，包括但并不限于信用卡系统、银行签帐卡系统、智能卡系统、电子数据交换、自动化的结算所、数字货币等。

●通过一个或多个银行和/或其它组织，使结算和协调生效，和/或直接与可能合法地执行结算服务的实体接口。

●通过一个或多个银行和/或其它组织，给数字处理和/或数字信息的创建者、信息分布和/或修改者、和/或消费者、和/或其它资金、贷款和债务的用户帐户，创建和分配识别标志、数字、名称或其它唯一的标志符。

●在提供安全的金融结算服务的任何步骤、部分或过程控制中使用安全容器。

●控制至少部分基于规则和控制的安全金融结算处理，这些规则和控制促进了在分布式金融结算所系统（如用户受保护的处理环境、Web服务器、集中式的结算设施）的每个受保护的处理环境中执行的处理的分布。

●高效安全地处理一种货币到另一种货币的转换。

●根据包括服务费用、产品费用和/或其它至少部分基于内容、处理控制和/或权利管理的使用的任何费用或收费在内的其它报酬，履行支付。

●支持至少部分基于内容、处理控制和/或其它使用交易的小额费用和小额支付的广泛使用，其中这种支持可包括小额交易活动的分布式的、安全的累积和/或处理，以及周期性地通过结算所网络传递与这种活动有关的信息，供进一步处理和/或累积。

●在尽可能地减少交易开销的同时，高效地测量和管理小额支付活动。

●尽可能地减少处理小额支付交易的等待时间。

●汇总或“捆绑”与本地价值商店或其它支付媒介（方法）的交易。

●采用价值链规则和控制以及处理和控制链，以便高效地管理支付的分解（分割），包括根据控制使用和/或其它许可（如在启动具体的支付方法之前，按照规则和控制的要求，在价值链各方之间分散支付金额，从而安全地控制支付的结果）的相同或不同的电子控制集，将支付分配或转移给不同的价值链提供者。

●通过，如分布式的交易处理和/或交易活动的累积，减少（如尽可能减少）支持给定的电子交易集所需的电子消息的数量。

●支持在价值链参与者处就地累积多个支付或小额支付（捆绑或综合在一起）。

●允许价值提供者（如价值链的参与者）在赊帐提供服务或商品（实物的和/或电子的）之前，有效地核对其它价值链参与者的支付能力。

●允许价值提供者在价值链参与者偏爱的支付媒介上，为估计的购买水平授权适当级别的资金，例如，包括允许提供贷款和/或货币预算，该预算可以花费在全部和/或有限种类的交易上（如内容和/或处理控制类），例如，包括支付明显指定了开支类型的预算，如仅用于G和PG电影。

●提供潜在的价值链参与者的身份识别，并将这个身份与价值链参与者选择的支付媒介绑定在一起。

●周期性地提供交易活动的报告，以便结算所协调和记录。执行审核、记帐、履行支付和/或其它报酬和/或其它结算活动。

●按照时间、地点、本地资金的损耗、以及/或支付活动的种类如目的（商用、娱乐、旅行、家庭开支）、家庭成员或其它个人或组织的身份、所获得的内容或其它商品和/或服务的分类、和/或任何类型的支付活动的分类，提供事件驱动的报告。

●从电子控制集中内嵌的安全处理链和控制获得授权。

●向一个或多个分布式金融结算所批准授权和/或提供服务和/或一起协作，这些金融结算所是一个或多个这种结算所的下属机构的某种组合，以及/或者与它们为对等关系。

●跨网络或其它系统，根据Ginter等人的专利说明书所述的规则、控制以及其它VDE技术，分布金融结算功能（例如，每个消费者或其它价值链参与者的节点都能够执行分布式的金融结算服务，而且，参与者的节点可以向其它一个或多个参与者直接传送金融结算信息）。

●向一个或多个金融分结算所授权和/或提供服务和/或一起协作，这些分结算所逻辑上和/或物理上可以在任何地方运作，例如公司和/或政府机构的内部，以及/或者一个或多个辖区内和/或高级金融结算所的总业务集中区的附属服务设备中。

●跨系统或网络分布和/或授权金融结算功能，例如，每个消费者和/或其它某些或所有价值链参与者的节点都可能支持分布式使用结算服务，该结算服务在整个结算所网络的环境中启动了自己的安全的金融结算交易和功能，包括结算所与其它一个或多个参与者的可互操作的节点、以及列表中其它地方所有采用VDE技术的活动的互操作.

●高效地计算、总结和分散销售额以及由至少一个辖区征收的“增值税”。

●支持金融结算所网络，其中一种（组）或多种（组）结算所有着可互操作的、对等的关系，并且不同组所拥有的与其它组成员互操作的权利可以不同，例如，最终用户受保护的处理环境中金融结算所可能只具有与“主”金融结算所互操作的有限的权利。

●支持结算所受保护的处理环境的网络，其中该受保护的处理环境包括谨慎周全的“银行”或银行业受保护的处理环境，这里该受保

护的处理环境可利用VDE能力安全地监管、执行银行功能，如国家货币的安全储备（本地和/或远处地）、向最终用户和/或其它结算所受保护的处理环境“出借”储备货币的权利、起动电子货币对象的权利、用本地或远处货币储备履行支付的权利、接收代表应付的债务的通信（如电子帐单）的能力、履行这类支付的能力、以及作为一个或多个虚拟银行（或银行网络）的银行“分支机构”，其中这些虚拟银行执行着许多现在由传统银行所执行的作用。

●支持金融结算所创建电子货币的能力，这种电子货币有条件地为匿名的，此货币可用于履行支付债务，并且此货币被当作真实的货币对待，不需要收方在收到之后与远处的银行机构联系鉴定货币的真伪或已经授权使用。

●支持分布式结算所受保护的处理环境与上述一个或多个功能在便携式设备如智能卡（如电子钱包等）中协同运作的能力，其中蜂窝或陆地通信装置（或其它传输机制）支持与当前或多项交易如记帐有关的信息，或涉及包括购买者、经销商和/或发行者身份识别在内的商务活动的其它审核信息，以及与这些活动有关的授权信息、预算信息、贷款供应、货币供应和/或支付等信息的在线或异步通信。

●支持向价值链参与者，例如向消费者提供折扣、补贴和/或优惠券，以此交换使用数据或更加精心整理的使用数据（例如，改善某些环境中对隐私的关注）。

●可以按分级、对等或混合模式进行组织，这里，可以针对不同的商务模式和/或活动和/或价值链，以不同的方式分布金融结算的职责，并且，在某一种或几种情况下，某一方或几方在级别上可以高于其它方，而在其它某一种或几种情况下，则为同级别或级别较低。

●参与者之间的关系是可编程的，并且可以设置（并在以后调整），以便体现针对给定的商务活动、价值链或模式的一个或多个期望的金融结算安排。

●向多个参与方分布支付，例如，包括向一个或多个政府部门（如市政府、州政府和联邦政府）缴纳的税收。

图18示出了一个示例性的面向功能的金融结算所200的图表。在该实例中，金融结算所200是高度自动化的，它运作在一个可信的、安全的域中，用以提供一个受保护的处理环境。它有效地为所有各种

电子商务链提供了金融结算服务。它还扮演着高度安全的虚拟分布环境（VDE）域和其它域之间的网关的角色－为现有的架构提供协议支持。网关功能可使高度灵活的、分布式VDE受保护的处理环境得以利用不灵活的、集中式的，然而却无处不在的、可信的现有金融架构服务。

金融结算所200的核心功能涉及支付处理208、支付汇总212、支付分解214、以及小额支付管理216－因为这些功能将钱从消费者和其它价值链参与者那里收集起来，并向价值链服务或产品的提供者如经销商支付钱财。

更具体地说，在该实例中，金融结算所200可执行如下功能：

- 支付处理208，
- 信用检查210，
- 支付汇总212，
- 支付分解214，
- 小额支付处理216，
- 事件驱动的报告218，
- 协调220，
- 数据库的维护/管理222，
- 复制224，以及
- 传播226。

金融结算所200可接收来自外部世界的支付信息202、消费者信息230、提供者信息232、汇总报告和帐单234。它可以生成赊购订单236、信用订单238、报表204和报告240、释放信号242以及信用调查和授权244。

数据库管理222和事件驱动报告218可用于向价值链参与者安全地提供精确的金融报告。协调功能220－与报告和金融管理都有关联－使金融结算所200能够提供更加可靠的金融管理。复制功能224和传播功能226被金融结算所200用来促进与其它金融结算所200和/或其它安全或不安全的受保护的处理环境的分布式处理，允许金融结算所安全地与其它商务公共事业系统或其它参与者一起共享状况及更新信息。

在所示的实例中，支付信息202（可到达一个或多个安全容器152中）是支付处理块208的主要输入信息。如果需要，支付信息202还可包括发送给使用结算所300的某些或所有使用信息－或者包括与金融审核和交易跟踪联系更密切的不同类型的使用信息。该支付信息202可实时或延时到达（如周期性地或由其它事件驱动）。

金融结算所200利用提供者信息232和消费者信息230实现消费者和提供者之间的资金转帐。金融结算所200利用汇总报告及帐单234指导总的支付处理208以及支付汇总212和支付分解214。例如，金融结算所200可向第三方的金融团体，如银行、信用卡公司等发布赊购和贷款订单236、238，以便将消费者的帐户计入借方并相应地将提供者的帐户计入贷方。金融结算所200可发布报表204和报告240，用于安全审核和/或提供信息的目的。金融结算所200可在执行信用调查210之后发布信贷授权244，由此将贷款扩展到合适的价值链参与者。这种授权244可包括输入/输出功能，除非它们完全是在本地进行的（即授权请求进来，结算所200是贷款和/或贷款限制信息的源）。

金融结算所200可在适当情况下发布释放信号242，使电器100在金融结算所200传送、分析和/或处理完金融信息后，中止维护和/或保留“待处理的”信息。在一个实例中，用户电器100可以在商业模式的限度内，储存金融信息，即使该信息已被“释放”，将该信息缩减为概述。当然，它也许已经用数据的副本完成了这项工作（如，如果以前允许访问它）。例如，假设金融使用信息的本地副本含有机密的商业模式信息。查看一次可能就要花1美元，这1美元又可能被分给多个参与方。通常，用户只知道总的底线，但并不了解分配的细节－尽管在本地可能存在这次交易的每个参与者的记录。

图19示出了金融结算所200的一个示例性的架构图。在该实例中，金融结算所200包括安全通信处理器246、交易处理器248、数据库管理器250、交换机252以及其它一个或多个接口块244。金融结算所的这个示例性架构可以基于Ginter等人的专利说明书的图12、13所示的操作系统架构（在那个实例中，通用的外部服务管理器172可支持结算服务的接口254）。安全通信处理器246使金融结算所200能够与其它电器100（1）…100（N）安全地通信。这种通信可通过安全的数字容器152进行。大多数商务公共事业系统90都希望（包括金融结算

所200）支持实时和异步地接收容器152．另外，金融结算所200还可支持实时联接的协议，在简单的交易，如在没有分解要求的用信用卡支付时，该协议不需要容器152．使用实时联接的优点在于结果是实时的。这对用户因为花光了钱而需要更多的钱或贷款的情况有利（不是简单地报告或周期性地补充未用光的预算），在提供者（如内容或预算的提供者）坚持要求在允许任何活动所启动的交易继续进行之前结清交易时也有利。

用于实时交易的联接并不总是需要安全容器152，但即使在这种情况下使用容器152也可其优点。例如，容器152允许将规则和控制添加到内容中，使用户能够指定怎样使用内容。另外，容器152的使用提升了受保护处理环境的现有能力。利用诸如电子邮件这样的技术传递容器152（如作为SMTP邮件消息的附件，或其它任何支持附件的e-mail协议的附件）使得可以异步处理内容，从而使商务公共事业系统90能平缓它们的最高处理负荷。商务结算所的运行成本就是设备的折旧费。设备的数量主要是由最高负荷要求决定的。可以想象负荷有显著的差异（例如，将星期五晚上8时和星期二早晨3时的负荷进行比较）。平缓功能能够大量地节省设备和有关成本（电费、人力、维护等）。

交易处理器248可处理分析收到的信息，数据库管理器250可将收到的信息储存在数据库中，供以后分析和/或供历史分析（以提高贷款的限额、分析支付的过程等）。另外，数据库管理器250还可储存与现有贷款限额有关的信息、通信地址（物理的和/或电子的）、以及其它帐户信息。例如，Ginter等人的专利说明书讨论了预算保留数（encumbrance）。数据库管理器250可用于储存用来跟踪保留数等信息。还可以有安全信息组，用于和受保护的处理环境和/或采用这些受保护的处理环境的用户通信，并可以有结算服务。与和结算服务通信有关的记录也可以储存在那里。数据库250还可配备与其内容有关的报告设施。

交易处理器248和数据库管理器开250一同执行图18所示的大多数功能。交换机252用于在接口块244之间来回路由信息。接口块244用于和第三方的结算服务，如信用卡公司、银行结算的自动清算所（ACH）、签帐卡帐户等通信。或者，联邦储备银行256所提供的内部

结算服务可用来代替或补充所示的第三方结算服务，以根据通行的银行协议和法律要求，提供帐户的结算服务。按照可行的金融和银行制度，金融结算所200所采用的支付机制可以是对称的（如告诉VISA向消费者A的收费帐户和贷款提供者Y的帐户的帐户收费），也可以是不对称的（如告诉VISA将消费者A的收费帐户计入借方，向将把使用其它某种支付机制的提供者Y的帐户计入贷方的金融结算所付款）。

示例性的金融结算处理

图20示出了一个示例性的金融结算所的过程控制。在该实例中，提供者164向消费者95供应商品、服务或内容。例如，提供者164可提供一个或多个数字财产1029和在电子安全容器152内的有关控制404。消费者95处的受保护的安全处理环境154记录支付、使用和其它信息，并可提供指明该信息的查账索引228。查账索引228可从消费者95所在处传送到一个或多个安全容器152b内的金融结算所200。查账索引228可能包括，如正在报告的电器100的身份识别；支付金额；提供者身份识别；消费者所希望的支付方式；电器用户的姓名或其它身验证；以及涉及的交易的类型。报告的时间和/或频率可以依据许多不同的事件，如年、月、周、日或其它时间间隔；一些相关或无关事件的发生（如要求预先批准购买，一定数量的购买已经发生，本地电子钱夹中的钱已经花光，出于其它某种原因必须报告等等）；或上述这些的组合。

金融结算所200分析查账索引228，生成一个或多个总结报告240。金融结算所200可以通过在安全容器152c中利用电子手段传送总结报告240，向提供者164提供这个总结报告。金融结算所200还可以与金融中介机构258和一个或多个金融处理器260协作，实现将消费者95所拥有的银行或其它帐户计入借方，并相应地将提供者164所拥有的银行或其它帐户计入贷方。

例如，金融结算所200可以接收审核信息，分解交易（分解为创建者、分布者和其它人以及税务部门和其它政府实体的价值链数额），然后计算从每个交易受益人应得的数额。然后，如果希望或有必要（由于交易的规模、每项交易的费用或其它效率和/或成本上的考虑），可以将每一方的交易累积成总额，提交给金融中介机构258（与适当的帐户信息一起），由中介机构负责信用卡交易的执行。然后，

金融中介机构258（可能收取费用或提取一定的百分比）就可能使交易在金融处理器260中发生，使得每个受益人都能获得合理的数额。或者，如果金融结算所200拥有向信用卡公司直接提交信用卡交易所必须的能力和职权，它就可以使交易在金融处理器260（如VISA）中直接发生。

金融处理器260可以向提供者164（和/或消费者95）报表204，详细说明业已发生的金融借贷和支付。如果希望的话，它可以在安全容器（未示出）内部提供报表204。金融结算所200可以得到计入借方的部分或一定百分比的资金，以补偿它所提供金融结算服务。

图20A－20F示出了一个示例性的金融结算活动，该活动利用了维护于消费者的电器100中的本地电子货币钱包262。在该实例中，金融结算所200最初可以通过在一个或多个安全容器152中传送电子现金，向消费者95提供电子现金形式的电子货币。金融结算所200可自动将消费者的银行206a或其它帐户计入借方，以获得这些资金，并可根据消费者的请求这样做（参见图20A）。

消费者的电器100在收到电子资金后，就可以将它们存在电器100在其受保护的处理环境154中维护的电子现金钱夹262中（如Ginter等人描述的“MDE”）（参见图20B）。消费者的电器100可使用这个储存在本地的电子货币支付消费者所消费的商品和服务。例如，出版商68可通过在一个或多个安全容器152b传输作品166，向消费者的电器提供作品166，如书籍、影片、电视节目等。消费者可操作他或她的电器100打开此容器并访问作品166，使消费者能够以它的有关电子控制所指定的方式使用该作品（参见图20C）。

假设权利拥有者要求为作品166的使用付款，消费者的电器100可自动将电子钱包262中需要的支付额计入借方（此情况为5美元）（参见图20C）。另外，电器100可自动地生成记录该使用事件的使用记录264。根据时间和/或其它事件的发生，消费者的电器100可自动地以一个或多个电子容器152c的形式，向金融结算所200发送查账索引264－它可能包括在审核时间发送的一批审核记录或储存在安全数据库中的相关记录集－（或其概述，以保护消费者的隐私）（参见图20D）。

金融结算所200收到使用记录262并成功地将它储存在自己的数据库250中后，就可在电子容器152d中发送一个释放信号242（参见图20D）。这个释放信号242使消费者的电器100能够删除它以前所维护的使用记录264（参见图20D）。

消费者可以再次使用相同或不同的作品166，以提示另一个使用记录264'的生成，并利用另一个使用收费来削减电子钱包262（在此情况下就是花光钱包的内容）（参见图20E）。花完电子钱包262可以提示消费者的电器100再次与金融结算所200联系，以要求获得追加的资金（参见请求228'）并提供使用记录264'（在该实例中，两块信息都是在相同电子容器152e中传送的）（参见图20F）。

金融结算所200可通过传送追加的电子资金进行响应（在将消费者的银行或其它帐户计入借方以后），并且还可以提供允许消费者的电器100删除使用记录264'的其它释放信号（参见图20F）。可以将收的钱付给权利拥有者（在减去任何合理的数额以补偿商务公共事业系统90之后）。

支付分解

图21示出了一个涉及价值链“分解”的示例性的金融结算活动。在该实例中，金融结算所200高效、可靠、安全地支持价值链内的支付分解。图21示出了一个向发行者168交付作品166的内容创建者，如作者。发行者向消费者95发行（例如，在电子书籍166'中）并交付作品。在该实例中，消费者95为他的这份作品166'的副本支付了20美元。消费者的支付在作者164和发行者168之间根据如合同协议被“分解”或瓜分。在该实例中，发行者得到消费者的20美元中的4美元，其余的归作者。

分解使金融结算所200可以自动地在任何数量的价值链参与者之间瓜分消费者的支付。这对确保所有对产品或服务有贡献的各方能够可靠、高效地从它们各自的贡献中获得补偿来说极其有用。

图22显示了金融结算所200怎样才能支持图21所示的价值链分解。在图22的电子实例中，消费者95可以用电子方式将他的支付交付金融结算所200。该支付可以是封装在安全电子容器152a中的电子货币的形式，或者其它某种形式（如所报告的与已有的授权结合的使用信息，以便金融结算所200将消费者95的银行帐户计入借方）。

金融结算所200可以根据作者和发行者之间的协议，将消费者所支付费用的适当份额分配给作者164和发行者168。是什么告诉金融结算所200谁应当获得支付的分解部分呢？在图22的这个实例中，作品166可以在一个或多个安全电子容器152中以电子的形式从作者164传递给发行者168，又从发行者168传递给消费者。一个或多个电子控制集188可以容纳在相同或不同的容器中，这些控制集与作品166或其它财产有关。控制集188可以在其它事项中指定消费者95必须支付的数额，以便能够使用作品166。

控制188还可指定及控制怎样在其它价值链参与者之间分解消费者的支付。例如，作者164可在她提供的控制188b中，指定她将从最终消费者95购买的作品166的每份副本中获得16美元。由于有根据虚拟分布环境提供的安全处理链和控制（参见Ginter等人的专利说明书），作者164就能确信（其程度取决于作者的商务优先级要求和总系统的实力许可）发行者168、消费者95和其它任何消费者或财产166的潜在用户将受控制188b的支配。发行者168可将它自己的控制添加到作者164指定的控制中，发行者的控制188c（例如）提供4美元加价，用于品牌、分布和营销服务。

图22A示出了怎样在消费者的受保护的处理环境154中利用Ginter等人的专利说明书中描述的控制集188执行支付分解。Ginter等人在图48和有关的文本中，说明了控制集怎样在用户的受保护的处理环境154中实现和控制全部计量、记帐和预算处理。图22A示出了根据提供给消费者的受保护的处理环境154的一个或多个控制集188的分解支付。图22所示的每个处理块可以响应用户打开和访问内容的请求（事件）。

在这个具体的实例中，计量方法275设计用于在消费者第一次使用特定片段的内容时，给记帐方法277发送一个事件（如果需要，计量事件275还可以或者替换地在消费者每次使用该内容时传送该事件，以提供“按观看次数付费”功能）。

在该实例中，记帐方法277包括两种不同的记帐方法277a和277b。方法277a、277可以独立交付－例如，作者164可以交付记帐的子方法227a，发行者168可以交付记帐的子方法277b。记帐方法277a将信息写入规定应当向作者164付多少钱（在该实例中为16美元）的

记帐索引数据结构中。记帐方法277b将信息写入规定应当向发行者168付多少钱（在该实例中为4美元）的相同或不同的记帐索引数据结构中。记帐方法277a、277b可分别接收计量方法275传递的公开事件，并且都可以将记帐记录写入相同（或不同的）的记帐索引数据结构。

在该实例中，预算方法279可以在记帐方法277a和277b之外独立交付。预算方法279可以将记录写入规定（在其它事项中）支付分解协定（即在作者和发行者之间瓜分16/4美元）的预算索引数据结构281，记帐方法277a、277b对这种协定作了规定。可以将预算索引数据结构281（与记帐方法277a、277b维护的数据结构分开维护，因此不能由作者164和/或发行者168所泄露）送到金融结算所200。金融结算所200将执行支付并将上述的金融结算计入借方，将消费者帐户中的20美元计入借方，将16美元登入作者的帐户，4美元登入发行者的帐户（从而在作者164和发行者168之间分解用户支付的20美元）。与此同时，可以将记帐索引数据结构发送给作者164和/或发行者168指定的使用结算所300。使用结算所300能够分析这个记帐索引数据结构并让作者164和/或发行者168知道他们将从金融结算所200得到多少钱。

这样，在该实例中，电子控制集188可以在其中指定或规定：(i)具体数字对象中可用的权利，(ii)行使这种权利的开支，以及(iii)怎样在权利拥有者之间划分（分解）行使权利的支付。这种预先（在启动消费者的支付方法和安排之前）规定支付分解的能力提供了高度的效率和灵活性－因为它能够使用消费者的支付方法，自动地将消费者的部分支付定向到需要得到补偿的有关人员。由于用来行使权利的相同电器100还可用于协助将支付定向到各个不同的价值链参与者，整个金融结算所的一部分有效地遍布在大量并行计算资源中。例如，由于Ginter等人的专利说明书所公开的系统能够提供高度的可信度，因此权利拥有者能够用拨款将这种控制集188颁布给商务流，实施他们的支付安排。金融结算所200可协助确保这种分解支付能有效、迅速地到达它们应到达的目的地。

消费者95处的受保护的处理环境154安全地加强了控制188，在允许消费者95访问作品166之前，该控制需要来自消费者95的全额支付和/或支付授权。控制188c还可指定使用哪个金融结算所200从事支付

处理，并在选择支付方法方面为消费者95提供灵活性的同时，指定哪些支付方法是可行的。然后，消费者的受保护的处理环境154c就可以自动将适当的支付或支付授权190a发送给金融结算所200，以便根据控制188a分解，控制188a可以与作者和/或发行者指定的控制（或者与支付分解有关的那些控制的子集）相同。

由于消费者的受保护的处理环境154c生成针对发行者和作者指定的控制188c、188b的控制188a（参见图22），因而可以委托这些支付控制188a执行作者和发行者的支付意愿，反映两者之间的支付划分协议。消费者的受保护的处理环境154c可在一个或多个安全电子容器152a中，将消费者的支付或支付授权152a以及这些支付控制188a发送给金融结算所200。

金融结算所200根据控制188a处理支付或支付授权152a，按照作者和发行者之间达成的支付划分协议，将支付152b分配给发行者，将支付152c分配给作者。这样，例如，金融结算所200就能将4美元的电子货币发送给发行者，并将16美元的电子货币发送给作者；或者将这些数额的钱登入作者和发行者的银行或其它帐户。由于整个处理是在一个安全、可信的虚拟分布环境中发生的，价值链的每个参与者都能相信他们将实际获得他们所要求的支付，处理可以按非常有效的方法自动地、电子化地进行，这种方法可以灵活地适应各种不同的商业模式和特别的关系。

图23示出了一个另外的、在某种程度上更加复杂的支付分解实例，该实例在价值链中加入了内容分布者或汇总者170。在该实例中，消费者95的20美元现在可能要分成三部分而不是两部分，作者164仍然得到16美元，发行者只得到3美元，而内容分布者/汇总者170则因他或她的努力得到1美元。图24表明，图22所示相同的基本方案仍可用于满足这个新的价值链参与者的支付或其它利益。

图25示出了又一个支付分解实例。图25示出了怎样用分解对商务公共事业系统90在维护和管理价值链过程中所起的作用进行补偿。如上所述，分布式商务公共事业75提供了非常重要的服务，如金融结算、使用审核、许可、身份识别等等。整个商业或产业都可以依赖于高效、可靠地提供的这类管理和支持服务。商务公共事业系统应当从它们自身的投资和努力中获得补偿。一种使它们得到补偿的方法，是

从每次交易中获得少量份额－“a piece of the tick”。上述相同的支付分解机制还可用于支持给商务公共事业系统90提供这种小额支付。

图23示出了一个实例，其中商务公共事业系统90获得每次交易值的3%（在所示的实例中为0.6美元）。由于上述电子控制集188可用于实现这种小额支付能力，可以灵活有效地适应任何期望的商业安排或目的。

图26表明，支付分解可用于将单个用户的支付分解或瓜分成任意个不同的数额（甚至以不同类型的货币来记录数额，用于国际贸易目的），这些不同的金额位于在各个不同的目的地，并采用了各种不同的支付机制（如信用卡、银行帐户、电子货币等）。

图27和28示出了支付分解的其它实例，以进一步表明分布式商务公共事业75可以怎样灵活地处理这些及其它安排。图27的实例显示在作者164、发行者168、汇总者170、再打包者174和另外两个作者164、164b之间瓜分消费者的支付，作者164a、164b提供的额外的作品被合并在提供给消费者的电子产权中。图27的实例特别适用于再打包者174从涉及相关问题的多个原始资料中提取内容并将它们综合成混合的原始资料产品，如多媒体组合、“最新情报通报”合集、或销售给感兴趣的各方的简报类的出版物。

例如，再打包者 174可以出版一份关于当代政治的简报，它选择了作者164的一篇文章，将它与作者164a、164b写的其它两篇作品一起，在下一期简报中出版。作者164、164a、164b可以授权再打包者 174重新编排和重新发行作品。再打包者可以利用重新编排这一权利，制作最新一期简报，并将它分布在安全的电子容器中供消费者95阅读。在这个实例中，安全电子容器152a至少可包含商业要求的四种独立“交付的”集合－三个作品分别用一个（由作者164、作者164a、作者164b中的每个人指定），一个用于整个简报（由再打包者174指定）。或者，可以在独立的安全容器152中发送和交付适用于他们的各个作品和/或控制，并且/或者某些作品或全部作品以及/或控制也可以位于远处。

要阅读这份简报，消费者95得打开电子容器152a。假设每一期简报的价格（由再打包者定价）为10美元。消费者的10美元支付或支付

授权就被发给金融结算所200，金融结算所200将这10美元分解开来，给价值链的每个参与者予以补偿，例如，作者164可得到1美元，发行者168可得到1美元，汇总者170可得到0.5美元，另外两个作者164a、164b分别得到1美元，再打包者可得到其余款项－所有这一切都是由适用的电子控制指挥的。这样，再打包者就能得到补偿，以便选择合适的专题文章并将它们综合成一篇容易阅读的出版物，再打包者还可以用自己的识别品牌作为总体质量的标志，并可以加入自己独创的内容。

图28示出了一个“超级分布”实例。权利拥有者非常担心来自“pass-along”的版权侵犯－就是说，非法复制和重新发布。pass-along问题在数字环境如Internet中较为严重。Ginter等人的专利说明书中所公开的虚拟分布环境和该说明书中公开的管理及服务安排，从根本上使pass-along从明显的威胁转变为一种重要的机会。在优选的实施方案中，由于虚拟分布环境提供了对价值链权利的独特的、自动的、安全的电子管理，消费者可被当作价值链可信的成员对待。这使得超级分布模式成为可能，其中所有消费者都成为潜在的分布者。由于超级分布的收入只带来了最低的权利拥有者成本，超级分布为成功作品的权利拥有者提供了巨大收益的可能性。

参见图28，假设消费者95从汇总者170那里得到一部作品，她非常喜欢，就想把这部作品传给她的几个朋友和同事。假设汇总者170已经批准消费者95有重新分布作品的权利，那么消费者很容易就能将这部作品的副本发给其它任意数量潜在的消费者95(1)，…，95(N)。其他这些人知道消费者95，相信她不会给他们发可能没有趣且质量不高的东西。另外，下游的消费者不用付款就能阅读作品的梗概或看它的摘录（如看一部电影的预告片、阅读一部小说的第一章等等）。

在免费读完梗概或看完电影的前5分钟之后，假设有6个下游消费者95（3）－95（8）同意每个人为这个内容支付3.25没美元。金融结算所200可确保作者164、发行者168和汇总者170分别能得到适当份额的收入（如7美元给作者，7美元给发行者，8.75美元给汇总者）。

超级分布使任意个等级的重新分布成为可能。例如，假设在这6个下游消费者95（3）－95（8）中，有三个人决定将这部作品分别传给另外6个潜在的消费者－这样就有18个其它的人收到副本。由于重

新分布的作品有相应的命令相同支付安排的控制结构，因此作者164、发行者168和汇总者170每人都能从每个新消费者那里得到额外的支付。重新分布的滚雪球效应可以按这种方式在任意数量的消费者中继续相当长的时间，并能以最低的额外成本大幅度增加价值链成员的收入。

支付汇总或绑定

小额费用和小额支付可成为内容使用交易的重要基础。例如，消费者可按她所观看的特定作品、使用一段计算机软件、或听到的一段音乐的次数付费。可以灵活地提供不同的支付方式，使消费者可以选择支付较大数额的初始费用获得无限的使用，或以每次使用为单位支付数额较小的小额支付。另外，对商务公共事业系统90来说，小额支付是用来补偿系统所提供的服务的最易负担和最实际的方法。因此，在支持和实施小额收费方面，这种有效地处理小额支付的能力是非常重要的。

传统的金融支付机制，如信用卡、支票等，不适合管理小额支付。这些系统通常有分级交易开销，这对以许多5美元以下的购买为基础的商业模式而言是一个沉重的负担。例如，如果处理某个支付交易要花费0.5美元，那么对处理低于一定数额（有可能为2美元）的支付来说就显得不经济，因为处理支付的开支占了交易额的很大一部分，甚至超过了交易本身。因此，传统的金融支付机制更适合大额购买，不适合小额购买。

图29显示怎样利用支付汇总或绑定，通过减少需要结算的个别金融交易的数量，以及/或者通过减少结算这些交易所需的消息收发的数量，消除这种担心。图29所示的示例性支付汇总可以在消费者自己的位于受保护的处理环境154中的电器100中进行；或者在集中式的金融结算所200中进行；或部分在电器中进行，部分在集中式的结算所中进行。这种支付汇总处理可以将许多小额支付汇总或合并在一起，形成较大的支付－或者形成一批可以一次处理的小额支付。这种较大的支付和/或批量的小额支付可以周期性地与其它交易数据一起汇报，如果需要，就由商务公共事业75协调和记录。这种汇总小额支付的能力在提高效率、减少需要结算的个别交易的数量、以及降低电子网络150上的消息收发量等方面，都有重要的有利作用。当然，支付

汇总不必适合每一个交易（例如，一些大的、关键的或有风险的交易可能需要实时的结算），但可以用于大量常规性的交易中，以减少对商务公共事业系统90和总系统50的负担。

在这种概念的一个变例中，支付汇总可保留每次个别交易的数额，以获得高度的详实性，但可以用于触发何时发生报告（如已经收了X美元，或已经发生了Y次交易），这样就能把许多个别交易捆在一起传送和/或处理。这种汇总对减少在电子网络150上传播的个别消息的数量和频率都有用。在这种情况下，汇报的电器100可以报告：(i)个别交易汇总后的总额，或者(ii)每次个别交易，或者(iii)两者，或者(iv)两者的结合。

图29表明消费者可以使用他或她的电器100从事许多不同的活动，例如阅读小说、观看视频节目、获取和查看研究结果、交互享受多媒体演示、以及家庭理财如支票簿的平衡。每次使用的小额支付可与这些活动中的每一个有关。例如，消费者每次访问由作者写作并由发行者发行的作品的电子版，就向发行者A支付1美元，向作者A支付1.5美元。假设作者A的作品非常受欢迎，被改编成电影。消费者可以按使用的次数为基础观看其中一部电影－支付发行者A5美元，作者3美元，以及分布式商务公共事业75 0.5美元。

支付汇总者266（如果希望，可以在消费者处由消费者电器100提供的受保护的处理环境154中运作）可将支付汇总给公共实体，保存归发行者A的钱数、归作者A的钱数、以及归分布式商务公共事业75的钱数的流水总额。消费者每次触发另外的支付事件时，该流水总额就增加。可以周期性地或用其它方式以一定的时间间隔将汇总后的支付额报告给金融结算所200或其它商务公共事业系统90（例如每周一次、每月一次或每日一次），一定事件的出现（例如，消费者超越了她的贷款授权并需要一个新的授权，某个电子控制到期等），以及/或者这些技术的任一或全部的混合。

图30示出了跨若干消费者交易的支付汇总。在该实例中，付给同一价值链参与者并采用同一支付方法的支付被汇总在一起作为总额。这种支付汇总－可以在消费者处和/或金融结算所中发生－减少了需要结算的总金融交易的数量。这提高了效率和吞吐量，降低了处理每一个别消费者交易的成本。

图31示出了另外一个支付汇总的实例，其中汇总是对许多不同消费者的交易进行的。例如，金融结算所200可以汇总采用属于特定提供者的特定支付方法的所有交易。注意图29－31所示的支付汇总技术不一定会导致失去个别交易的详情。换句话说，消费者的电器100仍然能够记录和报告每次交易的详细信息，金融结算所200和/或使用结算所300仍然能够一次交易一次交易地报告信息的使用信息－尽管个别交易的支付被综合在一起以便更有效地处理和操作支付。这种在汇总支付的同时单独操作和处理更详细、更详实的使用信息的能力，可以在不过度增加支付处理机制负担的前提下，提供高级的审核责任。在某些情况下，失去详细的记录会在结算所这边得到存款。可以将它们抛弃，但将它们保留在用户的系统和/或商务公共事业系统90的知识库中也有好处。例如，如果出现记帐纠纷，详细记录的本地副本就能作为有用的证据，证明实际上发生了什么－即使从来没有将它们发送给结算所。

图32示出了怎样改造一个示例性的金融结算所200，使其包括支付汇总者组件268。支付汇总者268可用于汇总来自许多不同的消费者电器100或其它来源的支付收入，并将这些汇总后支付提供给交换机200，以便用第三方的结算服务来处理。支付汇总者268可以选择性地只汇总某些支付，与此同时其它支付则直接送到交换机200，以便不作汇总就直接处理。支付的汇总可以根据许多不同的因素。例如，可以根据消费者、提供者、支付方法、任意或全部因素的组合来汇总支付。这种汇总功能可以完全或部分地在消费者95的电器中进行，或者由集中式的结算所200集中进行。

使用结算所300

图33示出了示例性的使用结算所这一商务公共事业系统300。使用结算所的服务和功能通常可收集、分析和“再定向”详细的、总结的和/或推导的有关数字财产和/或数字处理的使用和/或执行的使用信息。该信息可包括任何描述电子交易活动的信息。使用结算所和/或支持服务可提供和/或促进以下：

●独立审核和报告（可独立于金融结算服务提供）；

●一般的市场研究；

●向与使用信息有关的消费者和价值链参与者提供协商、实施、确定和通信的隐私和保密级别;

●按照群体制定的市场营销和统一的目录销售、租赁或颁发许可。

更具体地说，根据本发明的使用结算服务可提供，例如下列详细特性和/或功能的任意组合:

●总结、汇总、利用、导出和/或提供描述和/或涉及安全容器、安全容器的内容、和/或其它任何内容和/或任何数字控制处理的使用的信息，其中这种信息描述和/或涉及(a)内容和/或处理的一个或多个用户，(b)一种或多种内容、控制处理、内容的使用和/或用户，以及/或者这种使用信息的一个或多个接收者。

●使在高度详实(如详细)的水平上跟踪和报告内容和/或处理控制的使用和/或处理信息成为可能。

●能够收集、汇总、分析、总结、摘录、报告、分布、租赁、许可、和/或出售使用信息。

●利用从用户对内容如广告、信息资料、娱乐、培训资料、商业效率软件应用程序等暴露得出的信息，通过利用优选实施方案中的VDE机制，安全地向使用信息汇总和/或分析结算所至少提供一部分这样得出的信息和/或与之有关的信息，这里，这种结算所安全地向另外至少一个结算所和/或价值链权利拥有者提供上述使用信息、或从该信息得出的信息的至少一部分;其中，所述结算所可安全地向具有结算所或其它权利拥有者作用的不同的其它各方提供所得到的不同使用信息。

●利用用户受保护的处理环境根据各种不同的技术计量创建和/或得出的“信息消耗”查账索引(例如，采用Ginter等人公开的技术)。

●收集和分析详细使用信息，如打开、提取、嵌入或执行数字财产或其任何部分的次数;或者价值链参与者使用财产，如交互式游戏或多媒体演示、计算机软件、或这些产品的模块或附属部分的时间长度。

●为来自消费者或其它受保护的安全处理环境的使用信息提供各种再定向能力。

●提供有利于存档和认可的独立的、第三方审核能力。

●在优选实施例中根据使用审核、用户情况和/或与一个或多个安全容器和/或内容和/或VDE管理的 处理控制的使用有关的市场调研提供信息。

●为权利拥有者、消费者、和/或其它价值链参与者和/或感兴趣的各方如政府部门，提供中立的、可信的第三方审核使用汇总和报告服务（税务、执法、商业调查与统计等）。

●连同规则和控制的权利以及许可结算一起提供审核机会（例如，提供一份报告，指出运用了哪些规则和控制的许可和权利，例如由谁做、做什么、什么时候做－由此将实际用户的活动与特定的许可和权利和/或规则和控制模板紧密联系在一起）。

●在该优选实施方案中，向每个和/或任意一组或多组内容创建者、内容分布者、业界分析者、贸易协会、以及其它任何投机商和价值链参与者、和/或其它任何感兴趣的各方如政府统计人员、调控机构、和/或税务管理机关，提供根据VDE规则和控制并在VDE容器中生产和交付的标准化的和定制的报告和分析。

●提供原始的、提炼过的、总结过的、推导出的和汇总的可信数据报告，以便支持任何价值链内、和/或跨和/或多个价值链的多种商业模式。

●将使用信息与金融结算服务分开或一起分布给电子社区内部或外部的价值链参与者和其它各方。

●支持隐私和保密控制，完全保护价值链参与者所有与使用信息有关的利益的权利，例如，包括处理和控制受管理的商业模式的VDE链的固有权利。

●能够满足隐私方面的要求，（如不披露超出消费者或价值链内容的分布者、汇总者、再定向者、或电子设备的其它用户以外的信息，在该设施方案中，该设备为安全的、受管理的内容或其它处理控制、授权采用了VDE，以便通知授权的用户正在收集和/或结算什么样的信息）。

●可被信任用于至少部分以规则和控制为依据，在进一步处理秘密或私人的使用信息或将这种信息传送给其它一方或多个参与方（包括另外的任何使用结算所）之前，自动地隐蔽（如加密）、去除和/或

转换这种信息的一个或多个部分，从而有效地保护隐私和秘密，包括保护商业贸易的机密信息。

●保护关键的商业模式信息，防止有利害关系的其它各方进行刺探，以及/或者防止无意中披露给利害关系的其它各方和/或公众，从而为真正可信的商用网络奠定坚实的基础。

●允许包括发行者和分布者、以及/或者消费者和服务和/或产品的供应组织在内的价值链参与者，协商即将传达给任何指定的价值链权利拥有者的使用信息的详细等级，其中，详细等级可根据具体的接收方是谁以及使用信息的具体类型和/或子类型而有所不同，这里，可以向指定的使用信息接收者提供这种使用信息的不同部分的若干不同的详细等级，或作为指定的可交付的详细等级，这样确定的详情至少部分是由指定一方的权利决定的，指定的这一方至少部分是由优选实施方案中VDE规则和控制信息描述。

●允许消费者和组织协商传送给价值链权利拥有者的信息的详细等级。

●允许消费者或其它价值链参与者－创建者、发行者、分布者、再定向者－指定和/或协商详细等级、他们期望的与使用的任何给定片断的内容、内容的分级、具体的处理、处理分级、和/或支付要求有关的使用信息的汇总和/或匿名（例如，匿名和/或与某些或所有使用详细资料有关的隐私的维护可能要求支付加价，以弥补这种信息的价值的损失）。

●允许信息消费者和/或其它价值链参与者定制他们的“信息消耗”，并设立规则和控制，规定怎样按照意愿将他们的使用信息汇总或加以利用－根据有权接收信息的权利拥有者的竞争要求，以及/或者将用户和权利拥有者双方用电子方法同意的接收信息提供给权利拥有者。用户和/或一个或多个权利拥有者可以有权指定对一个或多个权利拥有者的限额，以及/或者描述可以或必须传递给一个或多个权利拥有者的具体使用信息。

●支持真实的价值链参与者控制汇总价值链参与者的哪类使用信息，谁可以访问什么信息以及怎样才可以使用这些信息，怎样收集和处理这些信息，以及使用记录与特定价值链参与者或组织的联系程度。

●在提供安全的使用结算服务的任何步骤、部分和/或过程控制中，安全地使用容器（如结合Ginter等人描述的VDE受保护的处理环境和安全通信能力使用VDE安全容器）。

●支持在交换使用数据或更加精心整理的使用数据（例如，改善某些环境中对隐私的关注）的过程中，向价值链参与者，如向消费者、分布者、再定向者等提供折扣、补助和/或优惠券。

●生成并向有利害关系的各方提供销售研究和报告和综合的销售目录（针对性的邮寄、直销和其它形式的针对性的销售）。这些资料通常类似于独立杂志和报纸的发行量审核、电视的观众收视率报告、和/或商业上针对性的销售列表，但它们是在一个高效的、分布式的和安全的电子环境中生成的。需要时，根据受方的请求、支付、权利、和/或与在底层信息的一部分或多个部分中有权利拥有者利益的一方或多个参与方的利益冲突，这些资料可以具有重要的、新形式的详细资料（如观看、打印、提取、重复利用、电子储蓄、重新分布等），更加详实的信息，以及定制的、选择性的报告资料。

●利用详细的使用信息，自动地生成分级结构、方案、组和/或等级，并自动地向连同优选实施方案中的至少一个安全容器和/或VDE一起创建、收集、传送的使用数据中得出的一个或多个等级，分派个人、个人组、机构、机构组、数字和/或模拟内容、或成组的数字和/或模拟内容。

●支持广告和营销，包括支持高效的价值链自动化，以自动交付服务，如自动寻找目标，或向规定的消费者、专业人士、员工和公司的集合（如一个或多个等级）投递广告和/或其它销售资料，其中集合可通过自我选择、使用数据、使用数据的情况、或其它方法确定，其中这些集合可由任一或多个价值链参与者（如创建者、消费者、分布者、提供服务者、站点、分布式结算所）组成，所述的一个或多个参与者可接收不同的、定制的资料，而且如果接收资料的参与者获得了规则和控制的授权，就可重新分布这些资料，这些参与者可从这种重新分布中获得贷款、优惠券、现金支付、和/或其它形式的报酬，这种重新分布可采取至少部分依据自我选择、使用数据、使用数据的情况或其它方法，将接收到的一些或所有这种资料定向到其它某一方

或多个参与方，并且，所有这些处理都可通过优选实施方案中节点间的处理控制VDE链安全地管理（如支持）。

●根据价值链用户对广告的暴露，确定权利拥有者从广告客户那里应当得到的支付和/或其它报酬，并且至少部分地在拥有与作为确定报酬的依据的内容和/或处理有关的权利拥有者利益的若干方中，安全地自动分布部分这些报酬。

●依据直接的、更加详细具体的使用数据以及从使用信息、用户情况、分类识别信息等暗示的、明确的、和/或自动得出的消费者和价值链的偏好，支持高级的、有针对性的市场分割以及更合适的信息产品和商业模式的设计。

●使“专用的”使用结算所（某个组织控制和/或运作的使用结算所）能够获取某些详细的使用信息，这里，这些使用结算所可执行使用分析和/或这些信息的其它处理，并且从这些部分或全部使用信息中，向更加集中的和/或它方的结算所和/或其它价值链参与者，提供选择性地限制的使用信息（如采用更高级别的摘要，概述信息，限制使用信息的使用和/或使用方式－查看、打印、保存、重新分布等），对这些使用信息的不同限制，可适用于从不同种类的内容、处理、用户、和/或用户组的使用中得出的使用信息，这种限制能力通过隐蔽某些内部活动的详情，为公司或其它组织的秘密贸易的机密信息提供了额外的重要保护，而且，价值链的其它一方或多个参与方可以要求获得支付和/或其它报酬，作为对保存这些详细的使用信息的回报。

●使组织能够在公司的Intranet上采用专用的使用数据结算所，这里这些结算所与组织的文档工作流和/或数据仓库系统集成在一起。

●通过专用使用组织（如公司、政府机关、合作伙伴、或其它任何有组织的运营实体）的结算所，从组织内部的电器中接受使用信息，并将记录汇总为供内部使用的详细报告，以及/或者报告供内部使用的原始的详细数据，但只将使用数据汇总为总结性的报告，供外部分布，例如，分布给权利拥有者、和/或其它的价值链参与者、和/或一个或多个商业性的结算所，在优选实施方案中，供内部使用的详细数据是受到保护的，至少部分根据由指定的各方安全维护的电子身份，将以及存取或这些内容的其它使用限于指定的各方和/或以指定

的方式，这些电子身份包括任何有关方的类别识别信息（如某个研究组织的成员，高级行政官员），该信息具有使用相关的特定信息的特权。

●通过专用的使用结算所，识别和提供与使用有关的信息，这些信息提供了重要价值的使用数据，用于分配组织内部的资源、方向研究、以及其它重要的商业目的。

●分布使用结算（如出于效率和/或其它原因）。

●在优选实施方案中，根据Ginter等人的专利说明书所描述的规则、控制和其它VDE技术，跨网络或其它系统分布结算功能。（例如，每个消费者和/或其它价值链参与者的节点都可能是一个分布式的使用结算服务，它至少部分启动自己的安全使用结算，这里，参与者的这种节点可直接将使用信息传送给其它一方或多个参与方）

●分级组织使用结算所，在分级结构的每一层中至少部分地保密。

●向一个或多个分布式的使用分结算所（或与这些结算所一起）批准授权和/或提供服务，这些结算所在逻辑上和/或物理上可以在其它地方运作，如公司或政府机构的内部，以及/或者一个或多个辖区和/或高级使用结算所的总业务集中区域的服务子集内。

●跨系统或网络分布和/或授权使用结算功能，这里，每个消费者和/或其它某些或所有的价值链参与者受保护的处理环境（节点），都有可能在总的分布式商务公共事业的环境中，支持分布式的使用结算服务和功能。

●启动它自己的、直接与其它一个或多个参与者的安全的使用交易。

●使用采用虚拟分布环境技术的任何或所有活动，将可互操作的运作提供给其它参与者的一个或多个可互操作的节点。

●利用结算所生成使用所用的信息，该信息在产品和/或与产品有关的服务和/或其使用由这些使用信息描述的设计和/或销售过程中至少部分得到利用。

●可以按分级、对等、或组合模式加以组织，这里，可以针对不同的商务模式和/或活动和/或价值链，以不同的方式分布使用结算的职责，并且，在一种或多种情况下，某一方或某几方可以在等级上高

于其它各方，而在其它一种或多种情况下，则为同级别或较低的级别，就是说，参与者之间的关系是可编程的，并且可以设置（以后修改），以代表一定的商务活动、价值链或模式的一个或多个希望的使用结算安排。

图33从处理的观点示出了一个示例性的使用结算所300。在该实例中，使用结算所300收集、分析和报告数字信息的使用，包括但并不限于数字内容的使用。在该实例中，使用结算所300执行以下功能：

- ●数据收集314，
- ●数据库管理316，
- ●隐私控制318，
- ●安全审核320，
- ●安全报告322，
- ●数据汇总324，
- ●广告和营销326，
- ●使用分析328，
- ●复制330，以及
- ●传播332。

如果需要的话，使用结算所300和其它电器100之间的通信可通过安全电子容器152来进行。就象上面结合金融结算所200所解释的那样，使用结算所300可以实时和/或异步的方式接收容器。在使用结算所300中，实时的需求可能涉及广告或收视率信息，这些信息会失去其作为时间函数的部分或全部价值（如，如果没有在特定的时间之前递交某收视率信息，它就可能再也和指定的市场分析无关；或者，如果广告客户没有即使地收到使用信息，他们就可能无法有效地迎合消费者的口味）。另一个情况可能涉及必须递交使用信息（如度假的用户回来后发现他们所需要的审核数据和付款宽限期都已到期了，而且除非进行审核，否则他们就无法使用这些财产）。在某些情况下，出于和上面结合金融结算所200相同的原因，异步递交情况仍将是更可取的。

数据收集功能314用于收集使用记录302及其它类型的信息，如规则和控制188（例如，可提供关于价格和许可的信息）、金融报表240a、详细的金融报告240b、使用信息和/或分析请求336。数据收集功能314

可以与数据库管理功能316密切地交互－得到被储存和维护于使用或其它数据库中的各类信息。复制和传播功能330、332可用于将数据库316的内容与其它数据库同步（例如，其它使用结算所300维护的数据库），以及/或者跨许多安全网络受保护的处理环境或电器提供分布式数据库。

数据汇总324和分析328可用于分析数据收集功能314所收集的和/或储存在数据库316中的数据的内容，使使用结算所300能够执行审核320和/或报告322。隐私控制318可与报告功能322一起，用于向第三方只披露某些信息，而不披露其它信息－从而保护消费者对隐私和保密的关心，使用信息就是为消费者而收集的。这种未定控制316能够以与信息到达的容器有关的规则来表述。

报告功能322可生成各种使用审核报告304。另外，使用结算所300可用于提供广告和/或营销支持326（如协助使广告专门针对适当人口的消费者，以及/或者提供市场和广告研究）。这样，在一个实例中，使用结算所300自身可生成和/或发布广告340，有针对性地供一定的消费者观看，或者替其它使用结算所交付这种广告。使用结算所300还可根据信息请求336，生成定制的响应342，而且，一旦有关的审核记录被传输到使用结算所300且这种传输得到证实，还能生成释放信号344，授权电器100从本地数据库中删除和/或制作“不再等待”的使用信息。在这个使用信息被“释放”以后，消费者95可能有兴趣保留而不是删除该信息（如出于监视其它人（员工、儿童等）行为的好奇心）。

使用结算所300可删除它自己的控制188b，以便，例如管理使用信息、市场分析信息或其它信息怎样为其余各方所用。例如，使用结算所300可以准备一份产权报告或分析，将这份报告提供给第三方，并从中获得补偿。使用结算所300可坚持要求他们为之提供报告的人员不得向其它任何人再分布这份报告。使用结算所300可通过在一个或多个安全容器152中传递此报告和将电子控制188b与此报告关联，用电子手段实施这个要求。这些电子控制188b可与其它准许条件和/或限制（如不得修改此报告，可以打印和查看此报告，可以摘录此报告等）一起，实施这个“不得再分布”禁令。

如上所述，使用结算所300还可接收金融报表240a和/或详细的金融记录240b或其它金融信息－并可生成自己的金融报表240c和/或详细的金融记录240d。例如，使用结算所300可向内容提供者提供服务，其中使用结算所300从内容提供者那里获得控制188a，此控制类似于交付给消费者95的控制。在比较这些数据的基础上，使用结算所300可以对内容提供者预计将从金融结算所200获得的钱数进行估计。使用结算所300可以这样提供独立的审核功能－重复检查金融结算所200并提供欺诈检测功能（如可以利用使用结算所300查明提交了没有相关支付或支付额不正确的使用记录的人）。另外，控制188可代表内容提供者正在考虑实施的秘密模式，然后，使用结算所300就可提供一种服务，与实际收集的使用数据进行比较，以便建立一个模式，其金融结果就象内容提供者果真已经建立了提议的这个模式一样。

图34示出了使用结算所300的一个示例性架构。在该实例中，使用结算所300包括安全通信实施346、数据库和交易处理器348、验证者350、授权检验者354和数据汇总354。使用结算所300的架构可基于Ginter等人的专利说明的图12、13所示的权利操作系统架构。

在该实例中，安全通信346提供了在电子网络150上通过安全容器152与各种电器100的通信。在该实例中，数据库和交易处理器348执行图33的大多数功能。验证者350可用于验证消费者和/或数据，授权检验者352可用于检验授权，数据汇总者354则可用于执行数据汇总功能324。验证者350和授权检验者352与安全电器和受保护的处理环境一起，执行Ginter等人的说明书中所描述的验证功能。

图35示出了一个示例性的总使用结算过程。在该实例中，提供者164向消费者95（1），95（2），95（3）提供数字财产。例如，提供者164可在电子容器152中向消费者95中每个人提供一部小说或其它作品。可以有一个或多个控制集188与作品166关联（在一个实例中，可以在用于交付作品166的相同电子容器152中交付）。控制188可以指定必须以查账索引的形式收集某些类型的使用信息，并且必须根据一定的时间和/或其它事件报告该查账索引。

由于容器152只能在受保护的安全处理环境154中打开，受保护的处理环境154是上面引用的Ginter等人的专利说明书中所描述的虚拟分布环境的组成部分，提供者164就能相信，要求的查账索引将按照

他或她的指示生成或报告。在消费者95使用财产166时，他们的电器100自动收集、储存查账索引302形式的使用信息。然后，在发生指定事件（如每月一次、每周一次、使用一定次数后等）之后，消费者的电器100就在数字容器中向使用结算所300发送查账索引信息302。

使用结算所300收集查账索引信息302，可以将该信息存在其数据库316中，分析查账索引信息以生成报告304，该报告可在另一个电子容器152中发送给提供者164。

提供者164通过使用结算所300，自动获得审核他或她的作品被使用的次数和怎样使用这些作品的安全信息，从而将该提供者从收集或分析这些详细使用信息的负担中解脱出来。另外，通过只披露经消费者95许可的简要情况（例如，有多少人已经使用了作品166，但不披露他们的姓名或地址），使用结算所300可以保护他们的隐私。如果提供者164自己尝试分析详细的使用记录，这种保密功能将更加困难或问题更多。

图36示出了一个较详细的示例性的使用结算处理，该处理涉及两个不同的使用结算所300（1）和300（2）。在该实例中，提供者164将作品166直接交付给消费者95和可以将该作品再次分布给消费者的分布者168。与分布式的内容166有关的控制188可指定使用结算所300（1）收集和分析与创建者164直接分布的内容166的使用有关的信息，另一个使用结算所300（2）则收集和分析与再分布者168所分布的作品166的使用有关的信息。或者，使用结算所300（1）、300（2）可收集与同一电子财产166有关的不同类型的使用信息（例如，可以一个使用结算所收集与“按观看次数付费”有关的信息，另一个使用结算所收集所有一次性购买的信息）。使用结算所300（1）、300（2）可分别向创建者164和/或分布者168和/或消费者95发布报告304。

图37示出了使用结算所300是怎样与金融结算所200一起使用的。在该实例中，消费者的电器100可以：

●向使用结算所300发送与电子内容的使用有关的查账索引信息302，以及

●向金融结算所200发送与金融结算活动有关的使用和支付查账索引信息228。

如果希望的话，使用结算所300和金融结算所200可由相同的商业运作（在此情况下，可以在相同的电子容器152中发送使用和金融查账索引信息）。使用结算所300所执行的使用结算功能可以和金融结算所200执行的金融结算功能并行运作，以支持详细的使用报告和高效的金融结算。

图38示出了另一个示例性的根据媒介和/或广告内容的定位的使用结算操作。消费者95（1）、95（2）、95（N）可以订阅各种信息分布服务170A，170B，…。信息分布服务170可以分布由内容提供者164制作的节目资料和广告（商业性内容）。消费者95消费分布的内容，他们的电器100收集并向使用结算所300（1）、300（2）…报告有关的使用数据。

使用结算所可对接收到的使用数据进行人口统计分析，根据这种人口统计分析，将其它商业性内容164的特定广告定位作为特定信息服务170。例如，信息服务170A可以向长跑爱好者和其它健康爱好者分布节目资料和商业性内容164。使用结算所300（1）可以分析订阅和观看这类信息的消费者95所提供使用信息。这样，使用结算所300（1）就处于一个独特的位置，将广告放在相同兴趣的群体可能感兴趣的其它商业性和非商业性内容中。与此相似，信息服务170B可以专门广播汽车发烧友感兴趣的信息。使用结算所300（2）可以收集关于这类信息的使用的使用数据－这样就处于一个独特而有利的位置，向这组消费者分布和发布广告、商业性和非商业性内容。

图39示出了另一个可由使用结算所300执行的示例性的使用结算操作。在该实例中，权利拥有者164可以授权使用结算所300，按照消费者95愿意公开的使用信息量来提供折扣。这可以利用财产控制188，通过从控制集中选择和/或加入电子协商来实现（参见Ginter等人的图76A和76B）。权利拥有者可以预先将它考虑作为他们财产的普遍规则－或者可以授权某个权利及许可结算所400交付这些控制集（如根据它们作为特定类别使用信息的收集者的特殊地位）。

有一个例子，消费者的电器可以是一台个人计算机，分布计算机软件的权利拥有者164除了知道他们自己正在分布的软件以外，可能还想知道消费者95正在使用哪些软件程序。另一方面，消费者95可能不想披露他或她的个人计算机上的所有软件程序的详细信息。

另外一个例子，数字广播权利拥有者164可能想知道消费者95观看的每一个广播节目，而消费者则不想让其它任何人知道他或她感兴趣的节目类型。

使用结算所300可以向消费者95提供经济上的奖励，鼓励更全面地公开，但也给消费者一个选择，从而有效地调解这些对立的利益。

在该实例中，权利拥有者164向消费者95分布电子内容及有关的控制。这些控制可指定披露使用信息的选择。消费者可以选择:

●全额支付并保留除确保该支付绝对秘密所必须的信息以外的所有使用信息;

●允许有限的使用广告，以此换取价格上的小折扣;

●利用大折扣，作为允许完全公开使用信息的回报。

某些秘密的消费者可能想尽可能地让外界少知道他们的使用习惯，并且愿意全额支付以保护他们的隐私。其它消费者则可能不在意外界知道他们的使用习惯，并且愿意根据更全面的公开而获得大的折扣。可以提供任意数量的这种选择等级，使消费者能够，例如，精确地选择应该公开什么类型的信息，哪些应该保守秘密。由于使用信息是在作为消费者的电器100组成部分的受保护的安全处理环境154中收集的，消费者可以相信使用信息会被安全地处理，而且未经他或她的同意，不会发生未经授权的公开。

例如，根据向消费者的受保护处理环境154提供的一个或多个控制集188，和/或通过这些控制而成为可能的消费者的选择，消费者的受保护处理环境154可以不向使用结算所300披露（或披露最少的）使用信息。然后，使用结算所300就可以自由地分析它所收集的有限的使用信息或完整的使用信息，向权利拥有者164和其它第三方，如市场研究人员、经纪人、广告客户、审核员、科学家、以及其它人员，提供报告分析。

权利及许可结算所400

图40示出了权利及许可结算所这一商务公共事业系统400的一个实例。权利及许可结算所的服务可以执行以下所有功能的任意组合:

●登记数字对象和有关的许可、价格和/或其它允许和/或要求的运作，支持进行和/或未能进行这些运作的因果关系的执行;

●根据指定的情况和/或其它要求，如许可请求者的类别、履行支付要求的情况或履行能力等，按要求提供预先批准的许可；

●安全高效地支持向一个或多个国家和/其它辖区的适当机构登记电子版权；

●报告功能。

更具体地说，根据这些发明的权利及许可支持服务可包括，例如，下列某些或全部功能及特性：

●沿数字化的电子价值链识别、分布和确认特定的产权和/或其它商业规则和控制。

●为登记的对象提供对象登记服务和权利、价格和/或其它控制信息。

●根据它自己的编号和/或命名方案，和/或根据其它一个或多个组织、协会（如标准化团体）、公司、和/或机构（如政府管理机关）规定的一个或多个编号和/或命名方案，向每个数字对象分配至少一个识别数字和/或名称。

●从电子控制集中内建的安全处理链和控制获得授权。

●安全地为已经登记的数字财产提供许可（如依据规则和控制对许可的运作和有关结果如价格所作的描述），并支持这些登记的财产自动地与规则和控制集关联（如更新规则和控制、采用根据财产的类别预设的模板等），这些许可可以至少部分地远程提供并在登记过程中或作为这种登记的结果，安全地下载到登记地点。

●允许数字内容的权利拥有者确定并灵活地规定和安全地向一个或多个权利及许可结算所提供他们想怎样使用和不使用他们的知识产权（例如，VDE受保护的数字财产）的方法，以及使用和/或误用的任何结果。

●沿一个特别的电子价值链，提供VDE支持，以分布和管理权利及商业规则（包括预先批准的和其它许可），这里，这些权利和商业规则不断得到支持。

●按要求向经授权使用数字对象的人员提供数字对象许可。

●可以根据与一个或多个组合类别的用户（如不同年龄组、辖区、商业年龄、消费者、创建者、提供者、合作伙伴、政府、非盈利性组织、教育组织、组织成员等）安全关联的不同许可，提供不同的条款。

●向权利拥有者提供担保，即他们设立的条款正在得到潜在不同的和分布式的价值链参与者基础的遵守.

●可以提供控制，这些控制不包括所有可能的许可，并且/或者根据请求者的权利（按类别和/或按个体），在特殊的和/或预先计划好的基础上，按照要求进一步分布所需的和/或所希望的许可，如允许权利拥有者选择只分布与特定的数字财产有关的最常用的许可，以及根据权利拥有者的模式，允许适当的各方获得新的许可.

●通过使用结算所的数据库机制和自动化的提供和/或消息收发，根据请求和/或自动识别这些权利的到期，从而更新到期的许可，提供这些许可，并且/或者在优选实施方案中，通知VDE价值链参与者应当取得这些许可（在用户主动尝试使用有关信息和/或电子控制处理之前，通知这个用户，从而避免用户遭受挫折和效率低下）.

●在提供安全的权利结算服务的任一步骤、部分或处理中，使用Ginter等人描述的那些安全容器。

●创建、储存、分布、以及接收允许权利拥有者充分地指定权利、条件和结果的权利和许可“模板”，（如补偿），这些模板与涉及他们数字财产的使用（和/或VDE处理控制的电子事件）的运作有关.

●模板能够直接响应与财产、内容用户、用户类别、和/或其它数字信息和/或物理或虚拟地址和/或用于事件和事件结果监控的处理控制有关的数字控制集。

●模板能够自我执行.

●模板可适用于多个对象/情况。

●模板可以和他们与之有关的任何数字对象独立交付。

●可以扩展模板以预期新的运作和方案，包括但并不限于新的支付方法、定价模式和定价级别、以及新的许可.

●模板能够灵活地识别包括分布和发送和/或再发送权利在内的所有各种数字权利。

●模板能够灵活地识别个体身分和类别身分的权利.

●不同的模板可适用于不同的内容和/或处理控制安排的财产类型.

●多个模板可适用于相同的财产和/或处理控制安排.

●权利及许可结算所可维护超集模板，允许价值链参与者和/或分级结构中的子结算所修改一个或多个这样的超集模板，以创建采用所述的一个或多个超集模板的子集和/或扩展集的模板。

●可以利用图形用户界面和/或权利管理语言，以许多不同的方法来完成模板。

●可以通过使用拓扑图、示意图、可直接编辑的图形表示的价值链规则和控制来创建和/或修改模板“应用”，这些规则和控制以及价值链关系是通过显示混合图标、位置信息、流程图、以及文字信息来表现的，其中规则和控制是通过使用权利管理语言来实现的，并且，例如，权利语言的要素或这些要素的高级表现形式可直接对应于用图形表现的组件。

●多个价值链参与者可以参加和/或修改模板，以及/或者参加和/或修改适用于相同的数字信息的不同模板。

●用户们可在适用于相同数字信息的不同模板之间作选择，这些信息包括，例如，描述和/或控制通过如安全的VDE处理链和控制管理的控制过程的数字信息（如事件管理信息）。

●跨网络或其它系统分布权利结算功能（例如，每个消费者和/或其它价值链参与者的节点都可能是分布式的权利结算服务，该服务至少部分启动它自己的安全的权利结算，其中所述参与者的节点可将权利信息直接传送给其它一个或多个参与者、可互操作的结算节点，在优选实施方案中，所有活动都采用了Ginter等人的专利说明书中描述的那种VDE技术）。

●向一个或多个分布式的权利分结算所（或与这些结算所一起）批准授权和/或提供服务，这些结算所的运作逻辑上和/或物理上可以位于其它地方，如公司或政府机构的内部，以及/或者一个或多个辖区，和/或跨系统或网络分布和/或授权权利结算功能的高级权利结算所的总业务集中区域的服务子集内，例如，每个消费者和/或其它某些或全部价值链参与者的节点都有可能支持分布式的使用结算服务，在总结算所网络的环境中启动它自己的、安全的权利结算交易和功能，包括结算所与其它一个或多个参与者的可互操作的节点、以及列表中其它地方所有采用VDE技术的活动的互操作。

●可以至少部分地根据内容和/或处理控制的使用的某些方面，自动地向参与者提供一个或多个权利，这样提供的一个或多个权利可用作提供优惠券补偿这些使用（如购买）情况的奖励成分，此情况可直接从使用信息中得知，也可以从涉及多个变量的加权公式中导出。

●可以按分级、对等或混合模式进行组织，这里，可以针对不同的商务模式和/或活动和/或价值链，以不同的方式分布权利结算的职责，并且，在某一种或几种情况下，某一方或几方在级别上可以高于其它方，而在其它某一种或几种情况下，则低于其它方。就是说，参与者之间的关系是可编程的，并且可以设置（并在以后调整），以便体现针对给定的商务活动、价值链或模式的一个或多个希望的权利结算安排。

图40从功能的角度示出了一个示例性的权利及许可结算所400。在该实例中，权利及许可结算所400可执行以下四种主要功能的部分或全部功能:

●对象登记。权利及许可结算所400登记数字财产和与他们有关的许可及价格。

●按需许可。权利及许可结算所400响应查询，在安全电子容器152中一同提供许可188及相关的价格。许可控制188可在内容以外独立提供。

●协商许可。权利及许可结算所400响应查询和请求，代表已经将这种职责委托给权利及许可结算所的权利拥有者协商许可和/或价格。权利及许可结算所400也可以是权利拥有者和权利用户之间协商的中介。权利拥有者和权利用户之间可以协商并向权利及许可结算所报告这些协商的结果。

●报告。权利及许可结算所400可提供报告，以累积金融结算所200和/或使用结算所300执行的报告。

在该实例中，权利及许可结算所400可提供以下部分或全部功能:

●许可的创建、更新或变更408,

●许可的分布410,

●数据库管理412,

●模板的定义和/或管理414,

●协商许可416，

●报告417，

●复制418，

●登记419，以及

●传播420。

权利及许可结算所400的对象登记的主要任务是由数据库管理412完成的。在这一关系上，权利及许可结算所400可在相同或不同的电子容器152中，接收控制集188和相应的对象身份识别422，然后将该信息“登记”在数据库412中，供以后参考。权利及许可结算所400可通过提供模板功能414，协助权利拥有者定义控制集188，该控制集规定了与权利拥有者的电子财产有关的权利及许可。除对象或财产166以外，登记处理419和数据库412还可登记控制集188。

权利及许可结算所400的数据库功能412和分布功能410可用于响应请求412，按要求分布许可，还可负责分布所有与特定财产有关的许可这一任务（利用分布功能410）。由于许可和/或价格可能会到期或变更，权利及许可结算所400还可负责更新规定以前发布的许可和/或价格的控制集188，并分布那些更新过的控制集。

权利及许可结算所400还可提供报告功能417，例如，发布关于它已经发布或分布的许可和/或价格的报告406。在该实例中，权利及许可结算所400的运作提供了审核的机会，即一个渠道，通过它附加使用信息。这种审核运作（例如，可通过将权利及许可结算所400的功能与使用结算所300的功能相结合来提供）可用于创建关于提供了哪些许可、运用了哪些许可的综合报告－对市场研究和商业结果以及向权利拥有者提供额外的责任来说是很有价值的信息。

该权利及许可结算所400的审核功能对保守秘密来说可能非常有利。例如，可以将专用的权利及许可结算所400加以扩展，提供支付汇总，以便隐藏来自金融结算所200的秘密的个别交易等级的信息。在另外一个实例中，权利及许可结算所400可发布报告426，指出例如在报告期间的初始时刻数据库412中所登记的对象的数目、新登记对象的数目、以及关于和这些对象和/或某些种类对象的平均或中间价格有关的许可的种数的一些统计汇总。

权利及许可结算所400还可用响应428来响应查询402。例如，一个请求可能由许可请求构成－可以自动批准这种请求；或者可能需要权利及许可结算所400授予资格，以确定请求者是否有资格获得这些许可。可以通过出示一个或多个有效的凭证来建立资格，可以简单地检验或将这些凭证储存在数据库412中，与其它关于结算所批准的许可的信息一起传送给提供者。在该优选实施方案中，其它资格可以根据请求者的PPE54和权利及许可结算所400所知道的共享的秘密（如请求者持有的来自控制集188的一个或多个标签）。这个共享的秘密可与凭证一起使用，或者，在资格要求较低或已经建立（如已经获得了第一个地方的共享秘密）的情况下，共享的秘密单独就足以获得许可，取代或更新到期的许可。

权利及许可结算所400还包括许可协商机制416，可用于协商没有预先得到权利拥有者批准的许可188。例如，假设消费者95想运用不在数据库412中的某项权利。消费者95可以请求获得这项权利。相应地，权利及许可结算所400可以确认权利拥有者是否已经授于它代表权利拥有者协商的这个权利。如果权利拥有者没有提供这个权利，也没有给予权利及许可结算所400协商的权利，那么该结算所就可以与权利拥有者联系，请求获得授权和/或许可。如果权利拥有者同意给权利及许可结算所400的协商权，该结算所就能进入消费者的控制集和权利拥有者的控制集之间的电子协商（参见Ginter等人的图75A－76B）。可以将最终协商的控制集发送给消费者，使消费者能够运用此项权利。

图41示出了权利及许可结算所400的一个示例性的架构。在该实例中，权利及许可结算所400包括安全通信设施430、数据库及交易处理器432、验证者434、授权检验者436、以及登记处理器438。如上所述，权利及许可结算所400的架构可以基于Ginter等人专利说明书的图12和13所示和相关文字描述的权利操作系统架构。

数据库及交易处理器432执行图40所示的大多数功能。登记处理器438可执行登记功能419。在电子网络150上，安全通信设施430通过安全容器152，安全地与消费者95、作者164、发行者168、汇总者170、再打包者174、以及其它价值链参与者进行通信。验证者434和授权检

验者436与安全电器和受保护的处理环境一起，执行Ginter等人的专利说明书所描述的验证功能。

图42示出了一个示例性的权利及许可结算处理。在该实例中，作者164用包括控制A的控制集188A向发行者168发送作品166。发行者168－根据安全的处理链和控制－将控制B添加到控制集中，形成新的控制集188AB。发行者168利用控制集188AB向消费者95发行作品166。发行者168还可以在一个更全面的控制集188ABC中，指定不常使用的，但有时又必不可少的附加许可集C（例如，控制C可允许新闻记者根据一定的目的，摘录作品166的部分章节）。

发行者168可以向权利及许可结算所400登记控制集188ABC（如果希望的话，也可以登记控制集188AB和控制集188A）。发行者168还可以与控制168ABC一起，包括附加的“控制的控制”或“许可的许可”“D”（如分布结合Ginter等人的专利公开书的图79－85描述的控制）。这些附加的“D”控制可指定批准权利A、B和/或C的条件（给定用户的资信、再发布的频率、控制的数目等）。

消费者95（或其它任何提供者，如汇总者、再打包者、作者、或其它发行者）可以请求获得在权利及许可结算所400登记过的这些各种控制集的任一个的副本。例如，如果消费者95是一个新闻记者，她根据控制集188AB使用作品166，出于某种目的，她想摘录这部作品，那她就可以请求发行者168以前在权利及许可结算所400登记过的控制超集188ABC。另一个例子，在德国的消费者95收到的可能是供在美国分布的控制集188，可能需要请求获得符合欧洲的法律和货币环境的不同控制集。另外，权利拥有者可能会在后来某一天，通过负责或按要求分布新的控制集的权利及许可结算所400，修改以前分布的控制，以便增加新的权利、提供“销售”、撤消权利等。

图42A示出了另一个实例，其中消费者95可以向权利及许可结算所400登记一个与某个对象，如消费者95已经收到的文件或软件程序有关的控制集188X。只要为权利及许可结算所400的对象而登记的控制被修改，新的控制集188X就请求权利及许可结算所400，为命名的对象向消费者95发送一个新的控制集188Y。权利及许可结算所400可自动地向特定数字财产的所有已登记的用户发送更新的控制集188Y。

在不同的实例中，发行者168可能会用非常有限的控制集188X分布作品166，控制集188X只允许消费者95观看摘要，并指定权利及许可结算所400作为获得观看或使用整个内容的许可的联系点。然后，消费者95可以和权利及许可结算所400联系，获得允许其它等级使用的一个更广泛的控制集188Y。由于它要求消费者95与权利及许可结算所400联系，以便实际地使用以前分布的财产，这就提供了高度的可计算性和不断扩展的审核能力。与此相似，权利及许可结算所400可通过更新的控制集188Y，取代到期控制集。这种机制可以用来，例如按时间对特定的项目提供各种折扣（例如允许电影发行商在电影始发日的6个月以后，对首轮上映的电影进行打折，无需在电影始发之时决定该提供多少折扣）。

图43示出了权利及许可结算所400所执行的另一个示例性的权利及许可结算操作。在图43实例中，作者164、发行者168、汇总者170、或者其它另外的价值链参与者中的每一个都分别向权利及许可结算所400登记他们自己控制集188A、188B、188C－可能还登记另外的控制，控制他们提供者的控制的分布。然后，权利及许可结算所400就分布一个与各个控制集188A、188B、188C一致的、新的组合控制集188ABC－将每个价值链参与者从制定不是他们特别关心的控制集的负担中解脱出来。在该实例中，权利及许可结算所400与其它组织（如与政府机构440，如版权局－或与其它类型的组织如专业协会）之间可以有接口。权利及许可结算所400可自动地登记已经在权利及许可结算所400中登记的作品和其它对象中的版权－减少或消除权利拥有者自己做这些工作的负担。权利及许可结算所400和政府机构440之间的版权登记交互可以，例如，利用VDE和安全容器152。

图44A－44E示出了另外一个可通过使用权利及许可结算所400来完成的权利及许可结算处理。在该实例中，发行者168可以向消费者95提供财产166和有关的控制集188a（参见图44A）。消费者可以使用她的电器100和有关的受保护的处理环境154尝试访问使用控制集188a的财产166，但可能确定她需要另外一个控制集188b，以便按她希望的方式访问该财产。消费者的电器100可以生成给权利及许可结算所400的请求402，（参见图44B）。作为响应，权利及许可结算所400可以分布请求的控制188b，该控制包含了消费者95所请求的许可和定

价信息（参见图44C）。然后，消费者就可以依据控制集188使用财产166，并根据消费者的使用生成使用/查账索引信息302（参见图44D）。消费者的电器100可以向使用结算所300报告这个使用信息，并可以在从适当的结算所收到释放信号时，就删除和/或将内部储存使用信息释放为“待处理”（参见图44E）。

权利模板

图45A和45B示出了示例性的权利模板450，图45C示出了示例性的、对应的控制集188。权利模板450在某些方面与“在空白处填写”表格相似。权利拥有者可以使用权利模板450高效率地、有效地定义与特定的数字财产相关的权利。模板450受具体的内容行业、提供者、内容类型等影响很大，模板450可用于构造Ginter等人的专利公开书所描述的虚拟分布环境技术的通用能力。这使得象提供者这样的用户可以与资源的集中菜单一起出现，这里的资源适用于特定目的或对此目的有用。

例如，模板450可以对内容或其它受控的信息作一些猜测，它是怎样划分的或组织的，以及/或者这些实体组织都有些什么性质。模板450简化了定义许可的过程，减少或消除了利用虚拟分布环境的底层能力所需的专业知识和大量的时间投入。在该实例中，用户能够避免总是使用模板450，相反，他们可以用权利管理语言来定义许可188（例如，自然的或基于计算机的语言）－但大量百分比的用户将会喜欢模板450所提供的易于使用的图形界面－当日复一日地从事规定大量不同内容的许可这样的职业时，他们不会介意放弃其它的灵活性和有关的复杂性。

图45A所示的示例性的权利模板450（例如，可能适合文字和/或图形提供者）定义了与具体的数字财产有关的许多不同种类的使用/动作，例如，“观看标题”、“观看摘要”、“修改标题”、“再分布”、“备份”、“观看内容”、以及“打印内容”。权利模板450可进一步提供一个“菜单”或对应于每种使用的选项列表。这些不同的选项使权利拥有者能够定义其它人可以运用该财产的权利。例如，可包括如下权利：

- 无条件的许可，
- 以支付为条件的许可，

●根据内容的许可，

●无条件的禁止，以及

●根据其它因素的禁止和/或许可。

权利拥有者可以“填写”或在各种选项之间选择，定义对应于他们的特定财产的“权利配置文件”。在该实例中，权利模板450可以深化按支付条件运作的权利的模式和/或等级。这样的定价模式和等级可以灵活地定义各种不同类型的商业定价，例如，一次性收费、按观看的次数付费、降低成本等。参见图45B，图中为怎样使用图形化的界面指定定价模式和等级的一个实例。

在该实例中，权利模板450可以自我执行和/或被自动“翻译”或编译成一个或多个控制集188，提供实现权利拥有者的选择所必须的控制。例如，图45B有一个“观看标题”控制188a，允许象图45A的权利模板450规定的那样无条件地观看标题。与此相似，图45B的示例性控制188b包括另外的控制集单元188（2）…188（N），这些单元对应于权利拥有者根据图45A的权利模板450定义的其它权利和许可188。

在该实例中，权利模板450是可扩展的。例如，当新技术使新的运作成为可能和/或产生新的运作，权利模板450就能扩展，以适应新的运作，与此同时，仍然“向上兼容”以前的权利模板。不同的权利模板450可用于不同类型的财产、不同的价值链参与者，等等－与此同时，一定的权利模板可能适用于多个对象或财产、多个价值链参与者，等等。某些权利模板450可能是其它权利模板的超集。例如，总权利许可模板450可以定义适用于特定的财产或特定类型财产的所有可能的权利，子模板则可进一步定义与不同的消费者、不同阶层的消费者或不同的权利拥有者有关的权利。这样，例如，作者就能使用一个与分布者使用的子模板不同的子模板。模板也可以是递归的，即他们可以用来引用其它模板（类似地，他们定义的控制集也可以引用其它控制集）。

权利及许可结算所400可以填写权利模板450的一部分－或者，可以使用一种自动处理（例如，根据权利拥有者预设的指令）来完成和/或复制权利模板。权利拥有者可以使用图形用户界面完成权利模板450（如在用户的计算机屏幕上显示选项列表，用鼠标指点设备点击，填充希望的选项）。在另外一个实例中，权利拥有者可以定义他或她

在使用计算机能够自动编译或处理的权利管理语言填写权利模板450和/或构造有关控制集188时的参数选择。

图46示出了利用权利模板450的一个示例性的权利及许可结算过程控制。在该实例中，权利及许可结算所400和/或各个权利拥有者定义权利模板450（参见图46，方块452（1））。然后将这些权利填入权利模板450，定义批准的和保留的权利、以及有关的定价模式和等级。（方块452（2））。权利拥有者将权利模板定义的许可与对象关联（如通过创建一个或多个引用和/或适用于受控的财产的控制集188）（方块452（3））。然后，权利拥有者就可以将许可（控制集188）与对象（方块452（4））一起或分开传送。权利拥有者可以将这些控制集188直接发送给消费者95（方块452（5）），并且/或者可将它们发送给权利及许可结算所400，以便在数据库（方块452（6））登记和储存。权利及许可结算所400可以在收到消费者的请求（452（8））后，按照要求向消费者（方块452（7））提供这种经过预先授权的许可。

如上所述，提供者可以通过权利及许可结算所400，利用附加提供“分布控制”的机制，即指导和/或控制分布处理，控制这种预先授权的许可的分布。

认证机构

图47示出了一个示例性的认证机构商务公共事业系统500。通常，认证服务机构可以创建“证实”、担保、和/或证明某些事实的数字文档。所谓事实包括，例如，在特定团体如某个组织中的身份识别和/或成员资格；年龄组、拥有的资信；隶属某一个或多个辖区；以及/或者具有经过证实的一种或多种权利，可以在固定的时间段或特定的时间之前使用内容和/或处理。

更具体地说，根据这些发明的认证机构可提供以下有利特性和功能的任意组合，例如以凭证的形式：

●电子认证信息，为规则和/或控制所需要或它们一起使用，如证明、身份、成员资格、和/或身份和/或环境的其它属性等规则和控制，并且包括按照这些信息的来源（如一个或多个认证过的提供者身份）和/或分类自动地认证该信息。

●提供可信的验证，即消费者或其它价值链参与者的确是她自称的那个人和/或说自己是一个或多个特定的团体、类别和/或组织成员的那个人。

●提供可信的验证，即一组价值链参与者的确是他们自称的那些人，其中来自不同方面的大量凭证被汇总检验，在某些要使用内容和/或执行一个或多个控制过程控制的情况下，将这些凭证汇总是必须的。

●自动生成凭证，代表一个价值链或部分价值链的证明，以此作为多个这样的凭证的总结。

●通过使用规则和控制，预见从能够形成实际上代表认证过的特定团体的凭证的多个参与方，正当地收集凭证，在出现某些凭证的情况下，识别两个以上预料中的和/或符合一定标准—如足够的交易收入、足够的信誉等—的各方，新的凭证就会自动生成并起着复合凭证的作用，证实多个参与方的集体和协同的存在，其中所述凭证可与某些规则和控制关联，这些规则和控制允许某些电子活动，如使用内容和/或控制过程控制，在多个参与方EDI、内容分布、贸易系统和/或金融交易系统中进行。

●生成一个或多个凭证，以此至少部分作为规则和控制对凭证创建进行管理的结果，其中，这样生成的一个或多个凭证是在满足所需的一些标准，如多个参与方中每一方的某些特定的活动－如提供一个或多个凭证和/或授权和/或使用活动和/或贷款和/或支付活动和/或报告活动和/或VDE支持的电子协议活动（例如，包括电子协商活动）－之后，作为基于安全规则和控制的一个或多个指令的结果而产生。

●认证其它支持服务（如金融结算所、使用结算所、权利及许可结算所、交易许可以及其它认证机构等）。

●根据其它凭证（如身份）和安全数据库的自动查找进行认证，自动查找可以在本地、跨分布式的数据库布置、或远程进行。

●提供非自动进行（即至少有些部分由人提供或协助）的服务，即根据颁发从属凭证的自动服务以外的实际证据，颁发更为基本的凭证（如身份证）。

●可以使用公共密匙加密技术、私人密匙、以及/或安全的VDE虚拟网络，支持（如创建）数字凭证。

●能颁发凭证，支持一个自动的、可信的、分布式的、对等的安全电子环境中权利使用的环境，该环境支持处理链和控制。

●与其它分布式商务公共事业服务一起，利用通用的、可重复使用的、可编程的、分布式的、模块化的架构，支持无限多样的不同商业模式和方案。

●能颁发支持控制集的凭证，控制集具有其使用依赖于存在和/或缺少特定的和/或特定类别的和/或非特定的一个或多个表明一定事实的数字凭证的单元，并且，关于存在或缺少与不同颁发有关的凭证，可能共同存在不同的要求。

●能颁发一个或多个凭证，这些凭证与有条件的电子控制集协作，只向某些消费者和/或包括消费者在内的其它价值链参与者批准某些权利。

●更新到期的凭证，支持复杂的时间和/或使用和/或其它事件驱动的凭证到期（包括终止）－例如，到期的判据可以根据特定的凭证、凭证的类别、特定的和/或特定类别的用户、用户节点等而变化。

●维护和分布，包括根据节点上分布的情况和/或规则和控制，选择性地向分布式的节点分布撤消目录信息。

●在可互操作的、对等联网的分布式公共事业节点上，根据时间、其它事件分布撤消目录信息，其中，根据议定的撤消信息要求，将信息选择性地分布到某个或某几个节点，以及/或者不加选择地将撤消信息分布到每个或某几个节点。

●从电子控制集内嵌的处理控制安全链获得授权。

●跨网络或其它系统分布凭证机构功能（例如，对于某些种类的凭证而言，每个消费者的节点都可能是一个凭证机构；父亲可以有权给他们的孩子颁发凭证）。

●分级组织凭证机构，包括依靠其它凭证机构颁发的至少部分有这种目的的凭证，允许自动地验证一些凭证机构（就是说，他们所颁发的凭证和关于可信度、合理程度等的相关确定）。

●向一个或多个分布式的凭证机构分结算所授权和/或提供服务和/或一起协作，这些分结算所逻辑上和/或物理上可以在任何地方运作，例如公司和/或政府机构的内部，以及/或者一个或多个辖区内和

/或跨系统或网络分布和/或授权权利结算功能的高级凭证机构结算所的总业务集中区的附属服务设备中。

●每个消费者和/或其它某些或所有价值链参与者的节点都可能支持分布式凭证机构结算服务，该结算服务在整个结算所网络的环境中启动了自己的安全凭证和功能，包括结算所与其它一个或多个参与者的可互操作的节点、以及列表中其它地方所有采用VDE技术的活动的互操作。

●提供责任承兑控制（即根据发布人承诺的责任数额确保数字凭证），可以包括安全地维护与这种责任承兑有关的信息，并向凭证的收受人提供关于这些凭证所承担的责任保护的提示，并可以进一步包括通过VDE管理的明确的电子承兑或通过连续的暗示承兑，对承保数额以上的任何责任进行承兑的承保凭证的收受人。

●可以按分级、对等、或组合模式加以组织，这里，可以针对不同的商务模式和/或活动和/或价值链，以不同的方式分布凭证机构活动的职责，并且，在一种或多种情况下，某一方或某几方可以在等级上高于其它各方，而在其它一种或多种情况下，则为同级别或较低的级别，就是说，参与者之间的关系是可编程的，并且可以设置（以后修改），以代表一定的商务活动、价值链或模式的一个或多个希望的特定凭证机构安排。

图47从处理的角度示出了一个示例性的认证机构500。在该实例中，认证机构500创建了称作凭证504的数字文档，凭证504“证实”某些事实，如身份或类别成员资格。例如，一个可信的第三方认证机构500可以提供安全的数字证明，即消费者的确是声称她就是的那个人或具有某些特征、属性、类别成员资格等。例如，某些属性可以表示在特定类别（如某公司的员工）中的成员资格，某个日期以前出生的人，身体有一定残疾的人，学校的教职工、管理或学生机构的人员、或军队的退役人员。

在该实例中，认证机构500颁发的数字凭证504被当作权利使用和交易授权环境的传送者。如Ginter等人的专利说明书所述的那样，凭证504在虚拟分布环境中能力特别大，因为它们为权利使用提供了环境。例如，基于类别的凭证使用和商业权利的自动的、分布式的管理，可以从根本上提高可信网络的效率。例如，假设内容发行者想对所有

不在高教部门的学术期刊的订阅者按商业价格收费，而对大学的学生和教授则给予20%的折扣。可信认证机构500颁发的数字凭证504可用于自动地提供证明－在分布式电子网络的环境中－即只有那些确实有资格享受折扣的人才能运用它（在该实例中，只有那些经证实属于某个高等教育机构的人才能运用它）。

在图47的实例中，认证机构500可执行以下所有功能：

●事实的收集和检验522，

●凭证的生成524，

●撤销目录的维护526，

●凭证和撤销目录的分布528，

●验证530，

●凭证的更新532，

●授权534，

●复制536，

●传播538，以及

●归档554。

认证机构500可收集证据502，作为向谁颁发数字凭证504的依据。在该实例中，证据502可包括其它数字凭证504'（以便可以在一个凭证的基础上建立另一个凭证）。事实的收集和检验功能522可承认证据502以及其它可信度数据540（如关于协议的或以前误用的凭证的信息）。凭证生成功能524可根据事实的收集和检验处理522，生成新的数字凭证504。然后，分布功能528就可以分布新的数字凭证504，并发布帐单542，对承担与颁发凭证有关的工作和责任的认证机构予以补偿。

认证机构500还可以根据可信度数据540维护撤销目录542，指出那些协议的或以前证实的事实已不再真实（例如，Smith先生过去曾是Stanford大学的教授，但现在已经从该所大学离职）的凭证。撤销目录的维护这一功能526之所以非常重要，在于它提供了一种机制，即一旦发现有些凭证是“坏的”就确保他们不能继续使用。认证机构500颁发的凭证504可能会过期，认证机构可以（例如，收费）通过执行凭证更新功能532，更新以前颁发的凭证。认证机构500可以维护它所颁发的凭证的记录或数据库，该数据库可以是分布式的－得益于复

制功能536和传播功能538，精确、高效地跨若干不同的地点分布数据库。

图48示出了认证机构500的一个示例性的架构。在该实例中，认证机构500可包括安全通信设施544、加密/解密处理器546、记帐系统548、密匙生成器550、查询机制552、以及电子归档554。在该实例中，安全通信设施544用于和其它电器100和/或其它商务公共事业系统90通信。电子归档554储存密匙、凭证504和其它维护认证机构500的运作所需要的信息。加密/解密处理器546用于通过使用牢靠的密码技术，创建数字凭证504。记帐系统548发布帐单542。查询机制552用于查询电子归档554。密匙生成器550用于生成认证机构500自身运作所需的密匙。

图49示出了一个示例性的认证机构处理。在该实例中，发行者可以向消费者95发送一个电子安全容器152。要想使用安全容器152中的某些许可188a，消费者可能需要从认证机构500获得一个凭证，证实有关消费者的特定事实（如消费者为美国的公民，消费者是军队的退役人员，消费者已经年满18岁等）。消费者可生成一个给认证机构500的请求502，要求颁发一个合适的证实。认证机构可以检验消费者95或某个第三方提供的证据502，只要认证机构500感到满意，就向该消费者颁发所需的数字凭证504。数字凭证504不仅可以和发行者的控制集188a一起使用，而且可以和需要证实同一事实并且已经同意委托认证机构500作为凭证的颁发者的其它权利拥有者一起使用。

认证机构500可以利用安全容器152与消费者95进行通信。它可以生成并向控制集188b提供凭证504。控制集188b可控制凭证504使用的某些方面（如不可以再分布和/或修改）和/或定义从属凭证的颁发（如父母授权为他们的后代颁发凭证）的处理链和控制。

一个认证机构500可以“受委托”代表另一个认证机构颁发凭证－如在由一个或多个电子控制集188所定义处理链和控制中。跨若干不同的电器分布认证机构500具有效率方面的优势。图50示出了分布式凭证颁发方案的一个有用的实例。

图50表明，权利拥有者164（和/或权利及许可结算所400）可以请求（如通过在安全容器152a中发布电子控制188a）认证机构500，向认可的高等教育机构如学院1060颁发数字凭证504(1)。控制集188a

可以建立查明某个特定的学院实际上是否正式得到认可的所必需的策略和程序。根据控制集188a和学院1060提交的证据502，认证机构500就可以颁发一个数字凭证504A，表明已获认可这样一个事实。

为了利用凭证504A，学院1060的学生、教师、和/或职工需要提供另一个凭证，表明他或她属于学院1060这一事实。由 持有凭证504A的每个学院1060向它自己的教师、职工和学生颁发从属凭证504（2），而不是让认证机构500给学院1060的每一个学生、教师和职工再颁发一个凭证504，显得更为有效和/或可行。例如，学院1060可以维护所有学生、教师和职工的当前目录。不需要请求认证机构500给学院1060的每一个学生、教师和职工单独颁发凭证504（1），学院自己就能承担这个职责。

例如，学院1060可以选择运行自己的分布式认证机构500A。在一个实例中，认证机构500可以发布控制集188b（例如，从属于权利拥有者164发布的控制188a），该控制集向学院的认证机构500A委托在一定限度内（如表明有限多样的事实，如“这个人在职务上与学院1060有关”）颁发从属凭证504（2）的权力和职责。这些从属凭证504（2）可以是凭证504（1）的副本，并追加声明特定个人与学院1060有关以及具体的期满日期（如当前的学期结束）。然后，学院的认证机构500A就可以向当前花名册上的每个教师、学生和职工颁发这样的从属凭证504（2）。

凭证504（2）的收受人还需要另外一个凭证504（1）来表明他们的身份。这是因为认证机构500A所颁发的凭证504（2）表明的是叫这个名字的人属于学院1060这一事实－而不是此凭证的特定收受人就是那个人这一事实。收受人必须从政府，如州政府或联邦政府运作的认证机构500那里获得另一个“身份”凭证504（1）。

权利拥有者164（和/或权利及许可结算所400，未示出）可为数字财产166发布控制集188c，向那些能够提供有效数字凭证504的组合，表明他们在“认可的高校”这一类别中的成员资格的人，同意给予折扣或提供其它好处。学院1060内获得凭证504（2）的每个学生、教师和职工都可享受这些折扣或其它好处。图50A表明了这些不同的数字凭证是怎样用于支持以凭证为条件的控制188的－就是说，其单元依赖于存在或缺乏表明一定事实的凭证504的控制集。

在图50A的这个实例中，一个或多个控制集188c包括适用于同一数字财产166或同一组财产的分立的控制188（1）…188（N）. 控制188（3）可以向Stanford大学的所有学生、教师和职工提供附加的和/或不同的权利。在图50A的这个实例中，可以同时使用多个凭证来提供所请求的证明。例如，可以同时使用图50实例中所示的凭证504（1）、540（2）、504A，使具体的个人能够享受向认可高校的学生、教师和职工提供的折扣。例如：

●凭证504（1）可表明John Alexander此人的确是自称的那个人这一事实。

●另一凭证504A表明Stanford大学是一所得到认可的高校这一事实。

●另一凭证504（2）表明John Alexander本学期是Stanford大学的一名学生。

这些不同的凭证504中的每一个都可由不同的认证机构500颁发。例如，一个认证机构500（如政府机构运作的）可颁发证明消费者身份的凭证504（1），而另一个认证机构可颁发表明学生情况的凭证504（2），第三个认证机构可颁发凭证，表明Stanford是一所认可的（参见图50）大学这一事实。

另外一个例子，图50A所示的控制集188（1）可向加州的居民提供一定的好处。消费者只要出示一个证实其居民身份（如与“身份”证504（1）一起）的数字凭证504（3），就能满足其条件。通过出示表明美国公民身份的凭证504（5），就能满足图50A所示的另外又一个许可180（N）。凭证504（3）、504（5）证明指定的个人确实属于某个或某几个辖区（例如，特定城市、州、国家或其他行政单位的居民或作在那里作生意－因此，要缴纳该单位的销售、收入或其他税收，或缴纳一定的管理费），这对州之间和/或跨国商业贸易来说非常重要。例如，认证机构500可以向英国的金融结算所200颁发凭证504. 此凭证504可与控制集188结合使用，控制集188是由权利拥有者和/或规定只有英国的金融结算所200才有权接收英镑支付的权利及许可结算所400分布的. 想用英镑支付的消费者只有在所使用的金融结算所具有适当的英国凭证时，才可能完成支付交易. 然后，这个英国结算所可

能要交一定的税－将提供者从弄清他或她的哪些交易应交英国税、哪些不用交英国税这样的负担中解脱出来。

图50A还示出了另一个凭证504(4)，证实某人与另外某个人结婚了。要使用凭证504(4)，还必须出示证实身份的第一个凭证504(1)。在允许家庭成员使用家庭其他成员的凭证方面（如一个人可以依据他或她的配偶或父母的经证实的凭证而收益），这些表明个人之间或个人与组织之间的关系的凭证非常有用。

图51－51D示出了各种数字凭证504的示例性的详细格式。图51A的数字凭证504（1）可证实某个人的确是他自称的那个人。该凭证可包括，例如；

●陈述个人姓名的字段560（1），

●指出个人出生日期的字段560（2），

●指出数字凭证何时期满的期满字段560（3），

●对应于个人公用密匙的公用密匙字段560（4），ID代码560（5）（在该实例中，可以是公用密匙字段560（3）的散列），以及

●提供错误校验功能的校验和字段560（6）。

在该实例中，数字凭证504（1）被认证机构500利用该认证机构的公用密匙－私用密匙密码系统的的私用密匙，如RSA或EI Gamal加密。认证机构500的相应的公用密匙可以公开（如将它发布在一些公开的WWW站点上或其它广泛分布的环境中），或者予以保密，不向受保护的处理环境154的外部披露。在其中任意一种情况下，将数字凭证504(1)成功地解密，揭示其原始的明文信息，这提供了高度的保障，即该数字凭证的确是认证机构500颁发的（假设认证机构的私用密匙尚未泄密）。

期满字段560（3）之所以有用，是因为忽略撤销目录校验的人至少有一点相信，即如果凭证必须周期性地更新，那么它就是好的。期满字段560（3）通过确保凭证不会永远持续有效，提供了另外一层保护－使认证机构500可以使用不同的密匙对来提供认证处理的完整性和可信度。变更认证机构500的密匙减少了对手破译某个密匙的动机，因为受密匙保护的信息量是有限的，欺诈性地使用泄密的密匙将只有有限的有效时间。而且，（目前）数学上尚未预见到的进展可能会使某些加密算法无用武之地，因为它们依赖的是（目前）理论上可

以难以处理的计算。如果启用新的算法重新颁发凭证，那么内建的变更认证机构500密匙的机制，就会将这种破解密匙的影响限制在一段时间内（或者，可以使用根据不同算法生成的多个不对称的密匙对，给密匙作标记并使之生效，从而消除这个风险，其代价是额外的加密时间）。

图51B、51C和51D示出了另外一个含有不同种类信息（如在凭证504（5）情况下为专业凭证字段560（7），在凭证504（3）情况下为地址字段信息560（8），以及在学生证504（2）情况下为学生凭证信息504（9））的数字凭证的实例。这些凭证504（2）、504（3）、504（5）通过公用ID字段560（5）与身份证504（1）结合在一起，通常要求同时出示身份证和独立的凭证。

图51E示出了认证机构所颁发的示例性的数字凭证怎样能够－与可信的数据库一起－成为其它认证机构批准其它凭证的依据。认证机构500A能够，例如，使用户身份生效并创建图51A所示的身份证504（1）。用户可以向其它认证机构500B提交此身份证504（1），认证机构500B有一个具有特定属性的人员和/或组织的数据库554a。例如，认证机构500B可由维护内部数据库554a的专业机构来运作。认证机构500B信任内部数据库554a的内容，因为认证机构500B维护它并使它准确无误。

通过比较图51A凭证中的身份信息和可信数据库554a的内容，认证机构500B无须从图51A凭证的拥有者那里获得任何实际证据，就能颁发图51B的凭证。这解决了用户每次需要一个高度可信的凭证时自己都必须“露面”这样一个重要问题－还使得第二个凭证的生成可以自动进行。

图51E还显示，认证机构500B颁发的凭证504（2）可以（与身份证504（1）一起）作为另一个认证机构500c根据其在可信数据库554b中的查询结果颁发另一个凭证504（3）的充足依据。

另一个实例将是一个公司，该公司已经向它所在辖区的国务秘书表明了其身份。如果该公司已经符合处置危险材料的要求，它就可以向有关机构（负责维护目前哪些公司有资格并被授权处置危险材料的数据库554a的认证机构500B）提交国务秘书颁发的身份证504（1）。

然后，认证机构500B就能颁发表明这一事实的凭证504（2），如果希望的话，这一切可以全部自动地进行。

插在219页的安全目录服务（图52所示）的标题之前。

允许参与者担当某个实体的代理的证明

有时，特定价值链的或与其它参与者有特定关系的一个或多个参与者，需要被授权代表集体参与者行事。例如，多个参与方可能希望依据来自它们属于其中一员的合营或合资企业的授权来行事－或者特定价值链中的所有参与者都可能需要代表整个价值链行事。从该实体接收这种授权的每个参与者可能需要该实体的授权来行事。

本发明提供了一种机制，其中数字凭证504可用于创建“虚拟实体”，该虚拟实体可向参与者的任意组合批准在受控的使用条件下运用指定权力的相同或不同能力的任意组合。更具体地说，数字凭证授予虚拟实体中的每个参与者代表该实体行事的权力－受使用条件的约束，并且利用了与容器相关的控制集规定的使用条件中定义的任何因果关系。

图51F示出了一个示例性的电子容器152，该容器封装了以下信息：

标识“虚拟实体”的值564，

签名566（1）－566（N）－实体的每个成员各有一个，

与实体有关的其它信息568，

数字凭证504（1）－504（N）－实体的每个成员各有一个，

规定权力（如权力或许可）和“使用条件”的控制信息188。

值564提供了唯一地标识实体的标识符。“其它信息”字段568可提供关于实体的进一步的信息（如实体名称，每个参与者的姓名和地址，实体终止存在的期满日期，以及其它信息）。签名566（1）－566（N）如同合作协议上的签名－虚拟实体的每个成员都要附上他或她的签名，表明同意成为实体的一员，并且同意授予每个参与者的条件。

在该实例中，容器152进一步包括描述可以运用该权力的条件的电子控制集188. 控制188定义了授予每个参与者的权力－包括（在该实例中）运用这些权力的条件或限制。控制188可为每个参与者提供

相同的权力和/或使用条件，或者它们可以向每个参与者提供不同的权力和/或使用条件。

例如，控制188可授权虚拟实体中的每个参与者代表实体担当认证机构500的角色。在这个具体的实例中，控制188可以允许虚拟实体的每一方代表虚拟实体制作凭证－受使用条件的约束，并且 利用了控制规定的使用条件中定义的因果关系。如上所述，授予凭证的权力只是一个例子－根据任何类型的电子使用条件，可以授予任何类型的电子权力或许可。

图51G示出了创建图51F的容器152的一个示例性的过程。在该实例中，虚拟实体的各方可以协商根据如Ginter等人专利说明书的图75A－76B所示的电子协商技术管理集体活动的控制信息（图51G，方块570）。所得到的控制信息188规定了“使用条件”，如实体中的每个参与者可以运用的权力，以及对这些权力的限制（可以一个参与者一个参与者地分别规定）。

启动数字容器152（实际上是参与者的受保护的处理环境154）的发布的参与者，可以选一个随机数作为实体标识符的值564（图51G，方块572）。接下来，参与者的PPE 154可以通过将实体标识符的值564与其它信息568（图51G，方块574）关联，为虚拟实体创建凭证信息。接着，参与者的PPE 154就可以给虚拟实体的凭证信息签名，表明参与者同意成为虚拟实体的一员，并且同意使用控制信息188的条件（图51G，方块576）。

接下来，参与者的PPE 154就可以做成电子容器152，将它置于控制信息188、虚拟实体凭证信息564、566、568、以及参与者自己的、指定该参与者可以利用以便运用权力的密匙的凭证504中（图51G，方块578）。然后，参与者就能决定是否将更多的参与者加到实体凭证中（图51G，方块580）。如果是，就可以将容器152传送（图51G，方块582）给虚拟实体的其它参与成员，并可被下一个参与者访问和验证（图51G，方块586）。接下来的这个参与者可以类似地通过加上自己的签名566（2），给虚拟实体凭证信息签名－表明她也同意控制188并同意加入该虚拟实体（图51G，方块588）。这个新的信息被添加到该实体凭证信息564、566、568中和/或取代该信息（图51G，方块590）。

接下来的这个参与者还将他们自己的凭证504(2)加到容器152中(图51G，方块592).

可以不断地重复步骤580－592，直到虚拟实体中的每个参与者都对容器152被作了标记(判断方块580的“否”出口)。然后，可以将完成的容器152传送个给所有参与者(图51G，方块594)。

图51H示出了虚拟实体的参与者可能会利用以便根据图51F所示的控制188代表虚拟实体运用权力的一个示例性的过程。图51H的实例过程是由参与者的受保护的处理环境154根据请求而执行的。参与者的受保护的处理环境154记录审核记录(图51H，方块594a)，然后利用控制188所规定的使用条件评估请求(图51H，方块594b)。如果该请求为控制188所允许(图51H的判断方块594c的“是”出口)，参与者的受保护的处理环境154就从容器152访问虚拟实体的值564(图51H，方块594d)，并且利用与使用条件有关的控制信息188，实现该请求和完成适当的结果(图51H，方块594e)。在一个实例中，参与者的受保护的处理环境154可通过根据使用条件颁发数字凭证504，代表虚拟实体起认证机构500的作用－通过用与容器152中参与者自己的凭证504对应的密匙解密实体标识符值564，给数字凭证做上数字标记，并使该数字凭证成为新颁发的凭证的一部分。然后，该实例就可以记录附加的审核信息594H，报告它的活动。

如果所请求的活动未得到控制188的许可(图51H，判断方块594c的“否”出口)，图51H的实例过程就确定错误是否严重(判断方块594f)。如果错误严重(判断方块594f的“是”出口)，该过程可以禁止在容器152中进一步使用信息(方块594g)，记录附加的审核信息(方块594h)，然后终止(图51H，方块594i)。如果错误不严重(判断方块594f的“否”出口)，受保护的处理环境154就记录附加的审核信息(方块594h)，然后就能结束这项任务(图51H，方块594i)。

图51F－51H所示的过程和技术具有各种不同的使用。有一个例子，假设第一个发行者出版发行了一部包括他自己的内容和第二个发行者提供的内容的演绎作品。这两个发行者就可构成一个虚拟实体，允许第一个发行者代表该实体活动－但只能按照双方协商同意的使用条件进行。例如，第二个发行者可能乐意让第一个发行者重新出版发行第二个发行者的内容，并允许消费者95摘录和选编内容－但只有

在消费者出示了适当的、由该虚拟实体颁发的表明消费者被允许运用此项权利这一事实凭证504才行。例如，只有具有一定特征的特殊订户才有权获得凭证504。上面的技术使第一个发行者能够代表包括由第一和第二发行者组成的虚拟实体，向订户颁发凭证504。第二个发行者可以相信第一个发行者将只按照这两个发行者协商同意的使用条件颁发凭证。

另一个实例是包括多个参与者的制造过程。控制188提供的使用条件使制造过程价值链中的价值链参与者能够代表整个价值链执行一定的活动。例如，一材料制造商，一成品供应商和在它们之间运输材料的一运输公司可以形成一个虚拟实体。然后，这个虚拟实体就可以向描述某个处理的交易机构提交控制集，该处理描述了共同行动的所有三个参与者。例如，根据适用于它们的虚拟实体的使用条件创建的控制集，可允许联合展示材料的要求、最终的外观以及交付时间表，作为一个简单的例子。

在另外一个实例中，一家半导体公司、一家系统集成商、三家不同的软件供应商可形成一个虚拟实体，支持半导体公司的芯片设计、仿真和设计测试应用程序。在该实例中，可向组成该示例性实体的每家公司和每家公司中的具体人员颁发凭证。公司之间协商的规则和控制可规定谁能够访问软件应用程序和相关数据库的哪些部分，谁可以修改软件和/或数据。利用这种方法，半导体公司就能授权外部的承包商和/或供应商和代表这些外部公司的特定人员访问该公司。可以只向这些人授予足够解决典型问题和执行系统维护任务所的访问权利。而且，可以在有限的时间内授予他们附加的权利（授权），以便解决特定的问题，解决这些问题需要访问那些不包括在他们的默认许可中的某些可执行文件和/或数据。

本发明的虚拟实体的特性部分，代表了建立在Ginter等人公开的处理链和控制技术之上的扩展。例如，根据本发明的这个方面生成的凭证可以利用VDE处理链和控制的能力来管理凭证链。

安全目录服务

图52示出了安全目录服务商务公共事业系统600的一个实例。安全目录服务可以安全地提供电子的和/或其它目录信息，如姓名、地址、公用密匙、凭证等。安全地传送这样的信息（如在优选实施方案

中，通过使用虚拟分布环境）有助于防止窃听，有利于保守秘密，并通过使重要的参与者有效地交互，提供了重要的架构支持。

更具体地说，根据这些方面提供的安全目录服务可提供以下示例性的有利特性和功能：

●根据各种不同的参数，安全可靠地提供包括各种分类信息在内的目录信息。

●可以根据姓名、功能、物理位置和/或其它属性，安全地提供消费者的、内容提供者的、结算所的和/或其它方的电子地址和/或其它通信路径。

●可以根据，例如姓名、功能、物理位置和/或其它属性，提供消费者的、内容提供者的、结算所的和/或其它方的公用密匙和/或凭证。

●保护（适当隐藏）与身份有关的信息，同时有效地管理和/或使安全容器中请求和响应的秘密通信自动地进行。

●利用安全容器和规则及控制保证内容的完整性和非规范性（nonreputability）。

●从电子控制集中内建的安全处理链和控制中获得授权。

●跨网络或其它系统分布安全目录服务功能（例如，每个消费者和/或其它价值链参与者的节点都可能是分布式的安全目录服务，该服务象Ginter等人专利说明书中所描述的那样，利用VDE启动与其它一个或多个参与者的安全目录服务交易。）

●向一个或多个分布式的安全目录服务分结算所授权和/或提供服务和/或一起协作，这些分结算所逻辑上和/或物理上可以在任何地方运作，例如公司和/或政府机构的内部，以及/或者一个或多个辖区内和/或跨系统或网络分布和/或授权安全目录服务功能的高级安全目录服务机构的总业务集中区的附属服务设备中。

●每个消费者和/或其它某些或所有价值链参与者的节点都可能支持安全目录服务机构，该机构在总的命名服务网络的环境中提供命名和有关的服务功能，包括与其它一个或多个参与者的可互操作的节点、以及列表中其它地方所有采用VDE技术的活动的互操作.

●可以分级组织，以根据姓名、功能、物理位置和/或其它属性，委托总目录的子集的职责和安全目录服务的运作。

●例如，可以分级组织以提供目录的目录。

●可以按分级、对等、或组合模式加以组织，这里，可以针对不同的商务模式和/或活动和/或价值链，以不同的方式分布目录服务的职责，并且，在一种或多种情况下，某一方或某几方可以在等级上高于其它各方，而在其它一种或多种情况下，则为同级别或较低的级别，就是说，参与者之间的关系是可编程的，并且可以设置（以后修改）为针对一定的商务活动、价值链和/或模式的一个或多个希望的具体目录服务安排。

图52从处理角度示出了有关示例性的安全目录服务600。在该实例中，安全目录服务600是安全地保存关于消费者、价值链参与者和/或电器的目录信息并根据合格的要求提供该信息的档案。在该实例中，安全目录服务600可提供以下的功能:

●数据库管理606,

●数据库搜索/检索608,

●数据库复制610,

●数据库传播612,

●验证614，以及

●授权616。

可以通过搜索和检索引擎608访问数据库606，将消费者提供的输入信息作为源并利用它检索相关的记录。例如，安全目录服务600可以获得个人、组织、服务和/或设备的身份618；电子地址620；凭证622；和/或密匙624。该信息可储存在数据库606中。

响应于请求602，安全目录服务搜索及检索引擎608可访问数据库606，检索其余信息（例如，某人或组织的电子邮件地址、某人的公用密匙、拥有某个电子邮件地址的个人的身份、拥有某个公用密匙的个人的身份和地址等）。

另外，安全目录服务600可返回访问控制、审核要求等。例如，某个用户可能被要求出示有效证件（如凭证504），以便访问公司的内部email地址。数据库606已知的信息的某些字段不能为所有来访者知晓（如办公地点或特定的员工，他们在公司服务器上的主目录等；或者出示凭证504的人可以知道消费者的实际地址，该凭证是由担当他

自己的认证机构500的消费者颁发的，其它人的都不行）. 这些控制可在给安全目录服务600传递信息的安全容器中指定.

在向请求者提供信息时，他们可能被要求只能以授权的方式使用该信息。例如，他们可能被允许使用该信息来拟定email消息，而不是摘录邮寄目录的物理地址。这些限制可由控制188b来实施，安全目录服务600通过它提供的信息与该控制集关联。

如图53所示，安全目录服务600除提供安全通信设施626之外，还能提供数据库606和搜索及检索引擎608. 安全目录服务600的架构可以以Ginter等人的专利说明书的图12和图13为基础。

图54示出了安全目录服务600所执行的安全目录服务处理. 在该实例中，发信者95（1）想给收信者95（2）发一个消息. 发信者和收信者可以是消费者、结算所等所拥有的电器100。发信者95（1）可向提供某些信息和请求其它信息的安全目录服务600发送一个地址请求。安全目录服务600响应这个请求，给发信者95（1）提供请求的信息，发信者可以利用该信息给收信者95（2）发送消息。在该实例中，地址请求602和响应信息604包含在安全电子容器152中，以便维护保持请求和响应的机密性和完整性。例如，利用这种方式，外部的窃听者就无法知道发信者95（1）想跟谁通信，他或她需要什么样的信息来进行通信－目录响应不会“受骗”而将请求的消息定向到其它地点。另外，如上所述，目录服务600可能包括控制188连同其响应，和/或请求或要求控制188成为它的部分输入。

交易机构700

图55示出了一个示例性的交易机构商务公共事业系统700。这些发明还使安全“交易机构”具有提供以下所有的功能的能力:

●在一个总的多事件交易或处理链和控制过程中，安全地批准、证实、和/或审核事件（例如，包括验证和认可的目的）;

●为多事件交易或处理链和控制过程安全地储存、批准、证实和/或分布控制集（例如，包括包括验证和认可的目的）;

●发布任一或所有交易和/或处理步骤的要求；以及

●如果希望的话，主动地参与交易或处理（如通过管理、定向、中介、仲裁、启动等，包括为分布式的计算、过程管理、EDI、参照货币等，参与采用互易控制的方法和分布式的、自动的事件的模式）.

●可以证实步骤和/或路径，包括证实为经过交易机构的通信交换机的电子信息正确路由，该交换机适合证实一定的信息，其中，凭证证实遵循的是要求的路径，并且/或者是按照规定的规则和控制发送这种电子信息的，例如获得一定的归档信息和/或不超出预算和/或其它限制和/或约束，例如：在指定时间内“付运”的信息容器的数量，当前容器中和/或在一定时间内容器所包含（代表）的电子货币的数额，订货购买时拨付的金额，正当的定购机构等。

交易机构可以仅仅是电子交易和/或交易步骤（全部交易步骤的次序）的安全的、警惕的旁观者和证明者，它可以是多个参与方安全电子交易的一个安全的服务商，并且/或者可以积极地直接参与电子交易。

更具体地说，根据这些发明的交易机构可提供以下的有利特性和/或功能：

●安全地维护和批准与多级交易和/或处理链和控制过程有关的事件通知信息。

●可以通过要求其证明或验证，根据商务处理要素的组成表示，强迫执行一系列所需的交易和/或处理链和控制过程，例如，这里一个或多个交易机构在交易顺序的一个或多个步骤“位置”，分别证实和/或验证一个或多个特定的事件。

●可以从若干不同参与者所提供的若干分立的子控制集中，形成总的交易控制集。

●利用互惠方法协调所需的交易事件，例如，包括价值链参与者之间的事件的顺序。

●从电子控制集中内建的安全处理链和控制中获得授权。

●可以主动地干预管理交易和/或处理链以及控制过程。

●能够协调工作流和/或处理链和控制过程和/或其它商业过程。

●能够以可信的、安全的分布式电子商务环境为基础，提供自动化的、高效的管理，包括分布式的所有权信息、EDI、金融交易、和/或贸易系统价值链的活动中的证实和/或验证步骤，非常显著地改善分布式权利管理的安全性，其中，这种安全性可能达到或超过集中式在线商务模式所能提供的安全性。

●可以管理价值链参与者（组织、个人消费者、虚拟团体等）内部和/或之间的至少部分交易。

●可以至少部分通过使用规则和控制，规定和/或监视满足基本交易的条件和/或结果。

●可以根据错误的情形和/或交易情况的分析（如通过使用推导引擎和/或专家系统），命令该发生些什么。

●能够秘密地协调安全性、路由、优先次序、和协商过程，利用秘密的、可信的接口，使不同的、分布式的各方共同高效运作。

●为安全文档和/或处理控制提供适当的公证、批准、证实、和/或传递。

●可以证实步骤和/或路径，包括证实为经过交易机构的通信交换机的电子信息正确路由，该交换机适合证实一定的信息，其中，凭证证实遵循的是要求的路径，并且/或者是按照规定的规则和控制发送这种电子信息的，例如不超出预算和/或其它限制：在指定时间内“付运”的信息容器的数量，当前容器和/或在一定时间内容器所代表的电子货币的数额，订货购买时拨付的金额，正当的定购机构等，之所以发布这些规则和控制，是为了满足关于在获得这种路由信息的节点处获得正当的证明或验证的要求。

●跨网络或其它系统，根据Ginter等人的专利说明书所述的规则和控制以及其它VDE技术，分布交易机构的功能（例如，每个消费者和/或其它价值链参与者的节点都可能是分布式的使用结算服务，该服务至少部分启动它自己的交易机构功能，其中参与者的节点可直接向其它一个或多个参与者传送使用信息）。

●可提供电子式或其它形式的仲裁、调解和协商服务。

图55从总体功能的角度示出了交易机构700的一个具体的实例。交易机构700提供了安全的审核设施，以便根据它从此项交易的参与者那里收到的事件通知，维护总交易或处理的当前状况。

在这个具体的实例中，交易机构700执行如下功能：

●事件通知的收集730，

●有效事件数据库的管理732，

●要求的生成734，

●验证过的安全审核736，

●报告738，

●通知740，

●复制742，以及

●传播744。

在该实例中，交易机构700收到事件通知748形式的通知，告知事件已经发生，事件通知可以装在一个或多个安全电子容器152中。事件通知的收集过程730收集这些事件通知748，并可将他们储存在一个有效事件数据库732中。交易机构700可依据其有效事件数据库732，生成另外的通知748'，并可以响应请求752和/或按照其它要求，发布表明交易或处理的当前状况的回答750。另外，交易机构700可以根据审核功能736分析的有效事件数据库732的内容，生成和输出表明交易或处理的进展和状况的审核记录754。交易机构700还可以根据其报告功能738，发布报告736。有效事件数据库732可以是一个分布式的事件通知数据库，在此情况下，复制过程742和传播过程744被用于以分布式的方式维护和更新该数据库。

在该实例中，交易机构700的另外一个主要功能是发布新的或修改过的事件要求758，该要求可用于控制或影响总处理或交易。交易机构700可获得控制集188、价格和许可188'、事件流的要求760、以及/或处理路由要求762。事件流的要求760和处理路由要求762都能在一个或多个控制集中规定，交易机构700响应此信息和有效事件数据库732的内容，可使用它的要求生成处理734创建新的或修改过的事件要求758。交易机构700还可以创建新的或修改过的控制集188"和新的或修改过的价格和/或许可188"'。交易机构700可以用金融报表764作为其安全审核功能736的输入。

图56示出了交易机构700的一个示例性的架构。在该实例中，交易机构700（可以以Ginter等人的图12和图13所示的VDE权利操作系统（ROS）为基础）包括安全通信设施770、数据库和交易处理器772、处理控制逻辑774、路由表776、以及自适应的控制集数据库778（这些功能可以在一个或多个控制地点用各种方法来实现）。另外，交易机构700还可包括一个文档公证员780，内有一印章生成器782、一数字时间戳生成器784、以及一指纹/水印生成器786。

安全通信设施770使交易机构700能够以安全的方式（例如，通过安全电子容器152），在电子网络150上进行通信。数据库和交易处理器772执行图55所示的大多数处理。自适应的控制集数据库778可执行有效事件数据库的功能。路由表776可用作要求生成功能734的组成部分，将适当的消息路由给适当的实体。

处理控制逻辑774可包括推导引擎或专家系统，用来处理事件流要求760和/或处理路由要求762没有完全预料到或规定的那些错误情况。处理控制逻辑774可以按照基于规则的原理、模糊逻辑、神经网络、或以上这些的部分或全部的组合来运作－或者其它任何处理控制逻辑方法。处理控制逻辑774确定即将在总交易或处理中发生下一个事件。

文档公证人780可用于生成验证过的文档，以便将数字印章和/或速记信息加到记录的和/或数字文档中。

图57示出了一个示例性的交易机构处理。在这个简化的实例中，交易机构700可以是公司内部用来安全地审核和指导整个商品交付过程的一个实体。在该实例中，消费者95发出一份订货单788。订单收取部门704收到订单788，就向交易机构700发布一个订单事件710。交易机构700响应订单事件710，发布一个或多个电子控制集188形式的规则和/或要求，规定订单收取部门704怎样处理这份订单。这些规则188可以规定处理链的顺序，并指导执行部门709A、仓库709B、运输公司726、以及支付收集部门709C的活动。规则188－可在安全电子容器152中从一个部门传递到另一个部门－这样就规定了即将发生的交易的要求和总的处理流。然后，每个部门就可以将安全控制188与规则和/或交易机构700指定的路由一起，传递给下一个部门。每个部门还可以发布事件通知748，警告交易机构700留意整个处理目前的状况。交易机构700可以将该状态信息储存在其安全的有效事件数据库732中，供审核和/或允许交易机构700指导下一步处理。

交易机构700可以，例如，使用图17E－1到17E－4所示的交互模式，与正在进行的交易或处理交互。交易机构700的一个特别有用的情景，是管理由多个参与方如在联营企业或为其它共同目的工作的公司执行的处理。在这类商业情景中，多家公司可能正朝着共同的总目标而工作，但他们也可能也有自己的内定目标，例如，保护它们自己

的秘密交易的机密信息。交易机构700可用作一个独立的第三方调停者/仲裁者，以协调多个公司之间的活动，无须任一公司将详细的处理信息披露给其它任何交易机构700。

例如，交易机构700可以生成规定事件流和/或处理的路由要求758的控制集和/或在不同环境中意味着不同事情的控制集188。有一个例子，交易机构700发布的一个控制集可能使某个公司执行一个步骤，另一个公司执行另外一个步骤－每个公司从来都不知道其它公司所执行的具体步骤或步骤的顺序。因此，交易机构700就能开发控制集188，可用于只在不同的个人或公司活动者之间部分公开。

图58A和58B示出了交易机构所执行的用于“基本交易”的示例性步骤和过程。在该实例中，交易机构700在某种程度上扮演着类似于足球队教练的角色。通过接收技巧集和每个个人“游戏者”的要求，并将它们结合成一个总的“游戏计划”，交易机构700就能在一个总的“基本交易”过程中涉及任意数量的价值链参与者。

在该实例中，在交易机构700管理的一个处理中的每个价值链参与者164（1），…164（N），可以贡献控制集188（1），…188（N），这些控制集规定或管理参与者自己对交易的商业要求、限制和过程（图58A和58B，方块750）。这些个别的控制集188（1），188（N）规定了每个个人参与者怎样担当自己的角色。每个参与者164（1），…164（N）都知道它在总交易中的作用，但可能不知道其它参与者所起的作用，或者不太清楚怎样去形成其它参与者的“团队”－因此，这些个别的控制集188（1），188（N）通常只描述子交易，可能并没有将总交易考虑在内。

交易机构700还收到另一个控制集188X，该控制集规定了怎样将各个参与者的控制集与要求和限制一起，结合在总的交易过程中（图58A和58B，方块752）。这个总交易控制集188Y规定了怎样解决个人参与者提供的子交易控制集188（1），188（N）之间的冲突（例如，这可能涉及Ginter等人的专利说明书的图75A－76A所示的电子协商过程798）。交易机构700将参与者的个别控制集综合在一起－利用另外的逻辑将它们结合在一起，以创建一个总交易控制超集188Y（图58A和58B，方块752）。交易机构将最终获得的控制超集188Y储存在本地

存储器中（图58B，方块754）。这个总控制超集控制交易机构700怎样处理事件，以执行“微小”的交易。

交易机构700在收到进来的要求处理的事件后（图58B，方块756），就可以启动总交易控制超集188Y（图58B，方块758）。然后，交易机构700就可以向交易中的每个参与者交付相应的互易控制集，该控制集对应于总交易控制集超集188Y的部分－从而使每个参与者都能与超集通信（图58B，方块760）。或者，在该实例中，每个参与者都可以－在它向交易机构700提供它的控制集188（1），188（N）时－维护一个互易控制集，该控制集可与该参与者送给交易机构700的控制集进行通信。

然后，交易机构700就可以开始监视利用启动的控制超集所收到的事件（图58B，方块762）。如果进来的事件不是错误情况（图58B，判断方块764的“否”出口），那么交易机构700就要弄清楚该事件是否表明基本交易已经完成（图58B，方块765）。如果基本交易尚未完成（图58B，判断方块765的“否”出口），控制就返回方块762，继续监视事件。如果基本交易已经完成（判断方块765的“是”出口），交易机构700就认定交易已经结束（图58B，方块774）。

如果进来的事件为错误情况（图58B，判断方块764的“Y”出口），交易机构700就在控制超集188Y中处理这个错误事件（图58B，方块766）。如果错误不太严重（图58B，判断方块767的“否”出口），那么控制就返回方块762，等待下一个事件通知的到来。

如果错误比较严重（图58B，判断方块767的“是”出口），交易机构700就可能调用一个严重错误处理例程（图58B，方块768）。严重错误处理例程768按照控制超集188Y中的规则和/或按照推理引擎774或其它处理控制逻辑，试图消除这个错误。这样的推理引擎或其它处理控制逻辑774可以按总交易的商业模式进行编程，这样它就有足够的信息依据错误情况，选择适当的措施。

图58B所示的过程可以嵌套进行。例如，某个“参与者”定义的子交易自身可能就是一个以许多参与者的贡献为基础的基本交易－所有这些都是由同一个或不同的交易机构700管理的。

安全检验点商务公共事业系统

一个商务公共事业系统90可以包括使其能起“安全检验点系统6000”（参见图58C）作用的服务功能，该安全检验点系统提供安全性、归档、和能以某些方法证实和/或验证通信信息的许可服务。安全检验点系统6000能够:

●为电子商务交互提供了分布式的、高效的、自动的审核和归档层，以及

●增强分布式安全环境如VDE和分布式商务公共事业层的安全深度。

这样，安全检验点系统6000可执行安全和/或管理功能。商务公共事业系统的这种能力利用了集中式安全模式的优点（如让中心机构实际地控制处理节点的能力），并将这些能力部署在分布式的“用户空间”模式中，该模式能达到最大的效率和灵活性，支持安全的和可管理的伸缩性（集中式系统的主要弱点），并提供多个独立的安全环境层的增强的安全性优点。后一个能力特别适合极其需要安全保障的高度敏感的通信。需要一个或多个独立的安全检验点保护的处理环境的参与和安全处理，这些安全层才能起作用，这种安全处理巩固了基础性的分布式安全环境。

可以证实和/或验证经过一个或多个安全检验点系统6000的信息，以便让信息的收受人（如收到容器中的信息的一方）相信在收到信息之前，某些通信功能和/或安全步骤（过程）已经发生的。这种证实和/或验证可以包括，例如，通过所需的和/或授权的、受保护的安全检验点系统6000处理，证实或验证正确的通信路由。检验点可以分布在整个通信网络中，或者在最终用户的VDE节点的物理和/或逻辑地点“本地”（参见图58C）。

安全检验点系统6000可采用适合证实和/或验证一定的信息和过程的通信交换机。例如，安全检验点系统6000颁发的凭证可以证实遵循的是所需的路径，且所需的检验点已经检查过了相连的安全电子容器，以及/或者已经按照某些规定的规则和控制，完成了这种容器或其它电子信息的发送。例如，这种服务可以协助确保和/或证实和/验证没有超过一定的预算、其它限制和/或约束，并且/或者满足了其它某些要求。

例如，安全检验点系统6000可以协助保障以下要求（包括不超出限制或其它约束）：在给定时间内“付运”的信息容器的数量；当前容器和/或在一定时间内容器所包含（或代表）的电子货币的数额（对减少不合理的电子货币活动来说非常重要）；订货购买时拨付的全额，包括正确的定购机构在场；诸如此类。例如，当VDE安全容器经过适合的一个或多个通信交换机时，这种要求评估可以依据从一定的逻辑和/或物理区域、节点、节点组、用户或用户组织、和/或其它用户团体传送来的容器（或其它数字信息通信）活动进行，其中的依据是通过引用安全节点和/或个人用户和/或组织和/或区域的识别信息确定的。这些商务公共事业系统的“通信检验点”能力可以通过沿通信路径提供一个或多个“独立”分布的安全“检验点”，提供有用的安全特性，通信路径要求存在由这个检验点安全地提供并安全地与该容器关联和/或通过该检验点（或一组检验点）管理的过程插入该容器的正确的凭证和/或验证，从而显著提高了安全的可靠性。可以由收取节点检测这种存在－例如，根据规则和控制，可以在这个收取节点即将处理收取的一种或多种容器的至少部分内容之前，要求必须存在正确的凭证或验证。容器的这些种类可以包括，例如，来自特定的个人和/或组织的容器，以及/或者具有某种或某几种特定属性的容器和/或容器内容。

从安全性的角度来看，安全检验点系统6000可以“独立于”最终用户的虚拟分布环境节点。例如，从安全性的角度来看，这些节点可以是独立的，因为它们为了检验点的管理，使用了密匙管理来维护它们受保护的处理环境中的多个安全的执行段，使得最终用户节点处的安全破坏不会直接危及检验点运作的安全性，并有助于确保涉及安全执行段的破坏将不会危及其它段。

安全检验点系统6000还可收集审核信息，例如，包括检索预定的容器收受人的身份信息、容器信息的类别、用于供将来证实（认可）的校验和和/或其它信息，以及/或者归档所述容器的部分或全部内容。可以对一些这样的信息至少部分加密，这样，如果没有一个或多个容器发送者、预定的和/或实际的容器收受人、以及/或者有权访问这些信息的政府机构的合作，这些信息的一个或多个部分就不会被解密。

图58C和58D示出了“检验点安全性”商务公共事业系统6000的安排的一个实例，该实例在联接用户95（1）、95（2）、95（3）的通信网络的环境中，提供了通信检验点安全性、认可和归档服务。在该实例中，安全检验点系统6000可以是通信架构的组成部分。例如，安全检验点系统6000可以是一个或多个通信交换机或其它设计用于根据它们所包含的标题信息检测安全电子容器152的装置的组成部分。

在该实例中，安全检验点系统6000具有安全能力，控制是否允许经由通信架构传输的安全容器152通过－以及经过通信架构路由该容器的结果。在一个实例中，与用户95（1）受保护的处理环境一同运作的控制可以要求有些种类的容器152（如携带电子货币的容器）包括控制404，控制404要求将它们路由经过安全检验点系统6000（或某种安全检验点系统）。这样的控制404能够防止使用容器152及其内容（如它包含的货币），除非它是经过适当的安全检验点系统6000路由的。

例如，假设用户95（1）想给用户95（2）发送一个安全容器152。在该实例中，用户95（1）通过通信架构向用户95（2）传送容器152。该通信架构可以检测到正在发送的信息是一个容器，并且可以路由该容器，以便让安全检验点系统截获（如系统6000（5））。

在截获容器152之后，安全检验点系统6000（5）可以检查容器内的控制信息，判断是否满足了将容器进一步传送给用户95（2）的要求。只有符合这些要求以后，安全检验点系统6000（5）才可以将容器转发给用户95（2）－或者，它可以修改容器，允许用户95（2）按照容器的控制404（例如，可能会限制使用）打开并使用容器。可以授权安全检验点系统6000至少修改容器控制404的一部分－例如，增加进一步使用的限制。

图58C的实例示出了安全检验点系统6000的两个“网”。在该实例中，这两个网代表了安全检验点系统6000的集合，每个安全检验点系统6000都被证实（例如，被认证机构500证实）为：

一个安全检验点系统，以及

特定级别的一个成员。

因此，在该实例中，“网1”代表证实过的安全检验点系统6000（1）－6000（5），6000（7）这一级别；“网2”代表安全检验点系统

6000（4）－6000（6）这一级别．作为一个例子，“网1”安全检验点系统6000被证实为能够处理包含电子货币6004的容器．

与容器152有关的控制信息内规定的要求之一，是它必须经过“网2”的安全检验点系统（如系统6000（5））－例如，使某些安全审核功能，如可信的电子货币跟踪成为可能．“网1”的一个安全检验点系统（如6000（3））可以拒绝按照这些控制404将容器152送给用户95（2）－或者它可以拒绝修改容器152使其能够为用户95（2）所使用．

作为另一个例子，假设用户95（2）想给另一个用户95（3）发容器152．在这个具体的实例中，与容器152有关的控制404可能要求容器152的下一步通信必须通过“网1”的安全检验点系统6000（7）．用户95（1）提供的控制404中可能已经有这样的路由要求，或者可能由安全检验点系统6000（5）或用户95（2）的受保护的处理环境添加。

在所示的具体实例中，控制404可以使“网1”的安全检验点系统6000（7）能够通过不包括安全检验点系统6000的另一个路由（如通过另一类的商务公共事业系统和/或非安全的通信交换机），将容器152发送给用户95（3）．

图58D示出了示例性的安全检验点系统所执行的一个实例过程．在这个示例性的过程中，安全检验点系统6000收到容器152（图58D，方块6002），判断是否已经满足了其有关控制404所规定的要求（图58D，判断方块6004）．如果要求已经满足，安全检验点系统6000就可执行“要求已满足”的结果，如修改控制404，以满足上述的路由要求（图58D，方块6006）．如果要求没有满足（图58D，判断方块6004的“否”出口），安全检验点系统就可以执行“要求未满足”结果（图58D，方块6008）．

每一组结果都可能涉及一些类型的安全审核。如果安全检验点6000通过了包含电子货币的容器152，安全检验点6000就可以记录以下一个或多个审核信息：

- 发送者的身份，
- 发送者节点的身份，
- 收受人的身份，
- 收受人节点的身份，
- 货币所基于的凭证，

●货币经过的其它安全检验点6000，

●以前的货币处理者的身份，

●传送的日期、时间和地点，

●接收的日期、时间和地点，

●货币运送了多长时间，以及

●其它安全审核信息。

如果安全检验点系统6000拒绝通过和/或修改容器152，它就有可能生成一个包括可利用的跟踪信息在内的审核报告，例如：

●发送者的姓名，

●亏差的本质，

●预定的收受人，以及

●其它跟踪信息。

它还可以通知发送者、预定的收受人、政府机关、或其它机构。它也可以向发送者收取“通信失败”费。

然后，安全检验点系统6000就能判断是否需要另外的通信（图58D，判断方块6010）。如果不，过程就可能结束。如果需要另外的通信（判断方块6010的“是”出口），安全检验点系统6000就可将容器152传送给下一个系统（图58D，方块6012）。下一个系统可以是另外一个执行别的处理的安全检验点系统6000（图58D，方块6016、6004、6006、6008）。

实例

示例－电子内容分布价值链

图59示出了示例性的分布式商务公共事业75怎样被用于支持一个示例性的电子内容分布价值链162。在图59的实例中，作者164可以创作一部有价值的作品，如小说、电视节目、音乐作品等。作者向发行者168提供了这部作品166（例如，以电子数字的形式）。

发行者可以利用他自己的品牌，名称识别和营销努力，向消费者95分布这部作品。发行者168还可以向内容“汇总者”170－向消费者提供广泛的、来自多个参与方内容的人－提供作品166。例如，汇总者的例子包括传统的在线信息数据库服务和存放来自许多个参与方面的内容的WWW站点。通常，消费者通过搜索与消费者定义的一个或

多个主题相关的信息来使用汇总者的服务．汇总者170可向消费者95提供搜索工具，由消费者自己选择．

汇总者170可直接向消费者95分布包含部分或全部原始作品166的作品172．汇总者170还可以将作品172分布给“再打包者”174．再打包者174可以从内容相关的几个作品中提取内容并将它们综合成混合的产品，如多媒体组合、新闻出版物、“最新情报通报”合集．在这些服务中，再打包者174根据听众表现的兴趣对内容加以选择和组织．消费者95可以订阅关于某个特定标题的电子版时事通讯，或者给再打包者174一个简短的目录，上面列出他们感兴趣的主题．再打包者174将筛选相关的信息并将信息传送给消费者．这里，再打包者是在为消费者作筛选．

例如，再打包者174可以是时事通讯的发行者，并且可以在时事通讯176中翻印作者的作品166的部分或全部．再打包者174可以将时事通讯176直接分布给消费者，或者时事通讯可能经过另外的通道．再打包者174可以使用汇总者170提供的搜索引擎寻找消费者95感兴趣的文章，并将这些文章综合成电子版时事通讯，上面带有汇总者170的品牌和再打包者174'的品牌，然后将时事通讯发给消费者95．

分布式的商务公共事业75能够以许多个参与方式支持图59的价值链．例如：

1、认证机构500能够颁发凭证，使每个价值链参与者都能识别他们是谁并表明他们是一个或多个特定类别的成员．例如，作者164和/或发行者168可以规定，只要支付合适的金额，任何经证实的汇总者或再打包者都有权摘录或选编作品166．认证机构500可以颁发数字凭证504，支持这个新希望的商业目的，凭证证明汇总者170的确是一个声誉颇佳的汇总者，而再打包者174也的确是一个名声不错的再打包者．只要作者164和/或发行者168信任总系统50和认证机构500颁发的凭证504的安全性，他们就不会担心作品166会被他们指定的适当类型的人员以外的其它任何人摘录或选编．

在另一个实例中，认证机构500可以向汇总者170或其它用户颁发凭证504．认证机构500可以在作者164或发行者168的指导下颁发这种凭证504．凭证504可以表明这样的事实，即作者164或发行者168同意授权汇总者170或其它用户修改某些许可404．作者164或发行者168

可以拥有特定的许可404，使得只有在存在“授权的汇总者”凭证的情况下，才允许修改这些许可.

在另一个实例中，认证机构500可以向一个或多个级别的用户颁发凭证，使他们能够利用内容和/或内容的特定部分和/或修改许可，通过采用作者或发行者或认证机构所提供的某些VDE规则和控制（为适当的规则和控制所允许），这种允许可以限于特定的利用和/或修改。

2、在该实例中，权利及许可结算所400可用于登记作品166和颁发与每个价值链参与者所提供的授权和指令一致的适当许可404。例如，作者164可以向权利及许可结算所400登记作品166，规定定义其它每个价值链参与者的权利的控制集404.

例如:

●有一个例子，控制集404可以规定，只要发行者为分布的每一份副本向作者164支付一定数额的美元，发行者168就可以分布无限数量的作品166的副本。

●控制集404可允许发行者168附加他自己的控制，使消费者95能够阅读作品166无限次，但禁止消费者复制或重新分布该作品。

●尽管电子控制集可以与作品166一起在电子容器152中传播，它还可以单独提供。例如，权利及许可结算所400可以根据请求，向请求获得控制集的任何人提供与作品166有关的控制集。

权利及许可结算所400可以为不同的用户级别维护不同版本的控制集404，例如，消费者95可以收到控制集404a，汇总者170可以收到另一控制集404b，而再打包者174则能收到又一个不同的控制集404c。这些控制集中每一个都可由作者164或其它权利拥有者168提前提供，提供“预先批准的许可”系统，该系统使作品166的广泛使用极其有效且高度安全，另外，这些控制集能够以无缝的方式，与VDE分布式的模板应用程序交互－一个或多个模板应用程序可以与控制集一起被这些控制集的分布者分布给控制集的收受人（或者可以被利用）。在一个具体的“超级分布”商业模式中，允许尽可能广泛地分布作品166，权利及许可结算所400所的工作为提供目前的控制集404，该控制集授权特定的价值链参与者在特定的条件下以特定的方式使用作品。

3、在这个具体的实例中，使用结算所300可以通过收集来自每个价值链参与者的使用信息，支持价值链．这样，使用结算所300就能提供安全的审核功能，生成记录作品166被使用了多少次和怎样被使用的报告．

有一个例子，使用结算所300可以分析使用信息，确定有多少消费者95阅读了这部作品。例如，使用结算所300可以根据每一方对隐私的要求和公认的商业权利，向各个价值链参与者报告不同详细程度的消费信息和/或特定种类的信息．有一个例子，使用结算所300可以向消费者95提供一个关于他或她自己使用作品166情况的报告，与此同时，向作者164或发行者168只提供总结报告信息，该信息可能不包括消费者的姓名、地址或其它直接的识别信息。

另外一个例子，报告还可直接从再打包者174流向汇总者170、发行者168和作者164。可以沿任何逻辑路线，直接地或按经过各方的任何顺序定向报告，该报告包含为价值链所承认的每一方信息的任意混合，并且可至少部分地由VDE规则和控制实施。

4、在该实例中，金融结算所200可提供交易的金融详情的安全结算－确保适当的价值链参与者补偿其它适当的价值链参与者．有一个例子，金融结算所200可以在至少部分由VDE规则和控制所管理的一个自动化的、高效的过程控制中，，根据消费者95使用作品166的情况，从消费者95那里得到支付，并将支付的各个部分合理地分配给作者164、发行者168和其它适当的价值链参与者．例如，金融结算所200可以和别的银行或金融机构交互，实现支付转帐的自动化，和/或协助管理在所示的总价值链中维护的电子货币．金融结算所200还可以协助确保它自身和其它商务公共事业系统90为他们提供的管理和支持服务而得到合理的补偿，就是说，例如，商务公共事业系统90中进行的安全VDE处理可自动地确保向这些管理和支持服务提供者支付。

5、在该实例中，安全目录服务600通过为价值链参与者和/或商务公共事业系统90之间的电子通信提供便利，支持该示例性的价值链。例如，安全目录服务600可以根据请求，提供电子地址和/或路由信息，使一个价值链参与者能够以电子方式与另一个参与者联系．有一个例子，假设消费者95想获得作品166的最新版本，但却发现发行者168的地址已经改变了。消费者95可以以电子方式与安全目录服务

600联系，后者能提供目前的地址信息。当然，在商务贸易系统应用中，安全目录服务提供更加精心的服务以识别希望的各方，如目录资源的多维搜索，以便根据分类属性识别各方。安全目录服务600还可以提供根据内容的类型和/或与之相关的规则及控制来识别内容的服务（定价，允许的使用参数，如重新分布的权利等）。

6、在该实例中，交易机构700可用于协助再打包者174开发新闻通讯176。例如，交易机构700可协助将许多不同作者创作的许多不同的作品全部汇总和摘录出版在新闻通讯中这一过程自动化。交易机构700可以安全地维护多步骤的总过程的当前状况，指出已经完成了哪些步骤，哪些步骤还没有进行。交易机构700还可以协助在这种多步骤的过程中，在不同的参与者之间仲裁和调解，在某些情况下，可以主动影响或控制这个过程（例如，通过根据错误或其它条件发布新的指令或要求）。

实例－制造链

图60示出了分布式商务公共事业75支持的一个示例性的制造价值链。在这个具体的实例中，消费者95向制造商180下订单并收到订单确认书。制造商可能从许多不同的供应商182（1）－182（N）那里定购零部件和必需品。供应商182（1）－182（N）转而又可能从另外的供应商182（a1），…那里定购另外的零部件或分组件。银行184根据定购证明和制造商将偿还预付款的保证，向供应商182提供资金。运输/储运公司186负责运输和储存必需品和/或成品。

在这个价值链中，认证机构500和交易机构700有助于电子订单、确认书、条款和条件、以及合同的安全传递，还协助确保每个价值链参与者在与其它价值链参与者交换必要的信息的同时，保持希望的一定程度的机密性。使用结算所300可协助安全地审核总的过程控制，跟踪价值链参与者之间的实际和电子包裹，以及与使用有关的其它信息。金融结算所200可以处理价值链参与者之间的金融安排，例如，帮助在电子网络世界150和纸件的或其它银行世界184之间协调。权利及许可结算所400可向定义部分或全部交易的电子控制404提供安全的归档。交易机构700可以安全地监视在价值链参与者中间发生的交易的总体进程，并向每个价值链参与者提供适当的周期状态报告。另外，交易机构700可协助指引或仲裁总交易，以确保实现实现所有步

骤和要求。安全目录服务600可协助在不同价值链参与者之间电子地路由信息。当然，如本发明前面所述，并且适用于整个说明书那样，VDE处理链和控制以及其它能力，包括规则和控制以及安全技术，将优选地作为上述活动的基础。

商务公共事业系统怎样相互支持的实例

上述图16A－16E示出了不同的商务公共事业系统90是怎样相互支持的。更具体地说，图16A显示，金融结算所200可以向其它一个或多个商务公共事业系统90提供服务，例如，包括使用结算所300、权利及许可结算所400、认证机构500、安全目录服务600、交易机构700和其它金融结算所200'。在这些情况下，多个商务公共事业系统构成了虚拟结算所和高级别的商务公共事业系统。

在每一情况下，金融结算所200收集因支持服务应得的资金，并将这些资金存在至少一个提供者的帐户中，该帐户至少采用一种支付方式。金融结算所200还可以提供VDE审核记录，证明资金的来源和数额，以及金融结算所200存入资金的提供者的帐户。金融结算所200可以帮助其它一个或多个支持服务机构建立提供者的帐户，并将帐户的号码和/或号码组以及适用的条款和条件传送给这一个或多个支持服务机构。发给金融结算所200的支持服务请求以及返回给正在请求的支持服务的响应，都可以在VDE安全容器中传送（如前所述），以利用它们牢靠的安全性、机密性、灵活的控制架构和可信度，并能够在每一地点由一个或多个VDE受保护的处理环境处理。可以由金融结算所200和/或其它一个或多个支持服务机构以VDE控制集的形式提供金融和帐户信息（以及/或者纳入VDE控制集）。金融结算所200还可以相互提供服务，进一步促进运作和管理效率。例如，金融结算所200可以向其它国家或其它地理区域的同行提供服务。在另一个实例中，金融结算所200可以让另一个金融结算所200使用这第二个金融结算所200不直接支持的一种或多种支付方法。

图16B示出了使用结算所300还可以向其它商务公共事业系统90提供服务。在一个实例中，使用结算所300可以向其它电子商务支持服务机构，如金融结算所200、权利及许可结算所400、认证机构500、安全目录服务600、交易机构700以及其它使用结算所300'，提供原始数据、汇总数据、至少部分推导出的数据、以及/或者报告。这些其

它架构的服务机构可将该信息作为独立的第三方对交易及其细节的证明，代表它们自己的服务机构作市场研究，以及/或者将该信息（很可能与它们自己的使用信息一起）转售给它人。在一个实例中，权利及许可结算所400可以向发行者出售报告，报告包含了它们自己的信息与来自金融结算所200和使用结算所300以及安全目录服务600和认证机构500的信息的组合。更具体地说，报告可以包含特定的发行者在权利及许可结算所400处登记的对象的列表，向权利及许可结算所请求更新或添加权利和许可的次数，金融结算所200为每个数字财产归总的收入数，认证机构500代表发行者颁发的指明用户已经过证实并具有发行者的数字作品的有效订阅的凭证数目，以及向安全目录服务600请求寻找发行者的在线Web服务器站点信息的次数。在每一种情况下，支持服务都向权利及许可结算所提供信息，以便将它合并在给发行者的报告中。

实例－分布式商务公共事业75可支持数字财产的购买、发放许可和/或租赁交易

在消费者为数字信息而付款的情形，分布式商务公共事业75提供了重要的可信度、安全性、方便性和效率。而且，信息的创建者和分布者可以按各种方法以及在不同的市场中以不同的方式，给该信息－当然是任何数字格式的数字财产－定价。

图61示出了信息交付服务装置1000的实例，其中信息提供者168提供电子内容，供购买、租赁和/或发放许可。在该实例中，信息服务公司168向全球数个市场（包括个人在内）发布信息166。它们的市场范围包括专业人士、家庭办公室用户和小型办公市场、以及大中型公司和家庭消费者。例如，提供者168可以向家庭消费者95（1）、专业人士如律师95（2）以及公司或其它组织95（3）交付电子形式的内容166。在一个实例中，:

●个人消费者95（1）从在线百科全书那里以订阅价格购买了3篇文章166（1）;

●律师95（2）购买了专利法专题文章的三章内容166（2）;

●大公司95（3）的两个产品市场经理收到了资产市场研究报告166（3）。

在信息交付交易之前，消费者95（1）、专业人士95（2）和公司95（3）可以利用安全目录服务600，查找信息提供者168的站点，并协助识别它们想用的内容。随后，各方面95可以向提供者168发一则电子消息，请求获得它们想要的特定信息。提供者168可以在VDE安全电子容器152中一并交付信息166以及控制定价和许可的有关规则和控制188。每一方95都有一个电器100，电器100内含执行执行控制188的受保护的处理环境154。

提供者168针对不同的市场对信息定不同的价格。例如：

●专业人士95（2）和SOHO（小型办公室/家庭办公室）支付交易费用；

●大公司95（3）支付订阅和交易费用之和（如公司85（3）每从一个大型报告中打印或摘录一页需支付10美元，可能还要付订阅费）；

●个人用户95（1）按平均订阅费用付费。

在每种情况下，本地、州和/或联邦消费税都包含在零售价格当中。可以在电子容器152中交付的电子控制集188中，与有关内容166（如Ginter等人所提供的）一起提供支付方法，也可以单独提供支付方法。

金融结算所200确保提供者168通过任何授权的支付方法得到支付。信息交付服务168接受广泛的支付方法。在有些市场中，某些形式的支付比在其它市场中更加流行。例如：

●在专业人士、SOHO和消费者市场中，信用卡（MasterCard和Visa）和赊帐（American Express）比较流行。

●消费者95（1）也喜欢信用卡，银行借记卡的使用也在不断增加。

●大型公司95（3）也使用信用卡和赊帐卡，通过自动化的结算所（ACHs）支付，通过基于X.12协议的传统和VDE安全电子数据交换（EDI）交易记帐和支付。

金融结算所200以多种方式使支付更有效率。例如，金融结算所200为提供者的几种支付方法提供便利的、“一站购买”的界面，并记录与给定提供者有关的至少一个帐号。

在这个具体的实例中，认证机构500可向每个消费者95交付数字凭证，指明消费者的一种或多种类别。例如，认证机构500可以交付：

●一个或多个凭证504（1），表明消费者95（1）是信息服务1000的个人消费者订户这一事实，并且进一步表明消费者是登记过的学校学生且为加利福利亚的居民（用于涉及交易的税收）这一事实，

●凭证504（2），表明专业人士95（2）是一名被加州的法律承认的律师这一事实，以及

●一个或多个凭证504（3），表明公司95（3）是一个法人实体并且拥有一定的信用等级这一事实。

控制集188可以根据所存在的适当的数字凭证504，启动不同的支付方法。例如，交付给消费者电器100（1）的控制集188（1）授权消费者95（1）使用这三篇文章166（1）中的每一部。控制集188（1）可以，例如，包含一个要求，即消费者95（1）必须有一个由独立认证机构500（或信息分布者或在一个更高级的认证机构授权之下担当认证机构作用的其它方）颁发的凭证504（1），表明消费者95（1）已经订阅了在线百科全书并且此订阅尚未过期这一事实。凭证504（1）可以，例如，与认证机构500（如可由美国政府或其它政府机构管理或授权）颁发的其它凭证一起使用，以表明消费者95（1）是美国公民、居住在美国、并且是加利福利亚州的合法居民这一事实。

个人消费者

消费者95（1）通过VDE电子容器152中发给金融结算所200的交易，向信息提供者168支付订阅费用。支付交易可能涉及，例如，向金融结算所200发送内含规则和控制188（4）以及审核记录302（1）的电子容器152的电器100。审核记录302（1）可指出，例如：

●应当向谁付费，

●交易额，

●具体的支付方法（如Visa卡），

●订阅者的Visa卡号码和到期日，

●信息订阅的标识符，

●接收付款的提供者的帐号。

安全容器152（7）还可能包含指明还应当征收市府、加利福利亚和美国联邦政府的销售税的规则和控制188（4）。金融结算所200征收适当的销售税并将这部分资金存入适当的帐户，例如，应当将这些资金存入属于加州税务机关1002的有关帐户。

在交换支付的过程中，订阅的消费者95（1）可以从认证机构500收到一个凭证504（1），表明她事实上已经是订户以及当前订阅的到期日。

专业人士

在该实例中，律师95（2）可能住在英国。他用MasterCard购买了关于专利的专题文章的三章内容166（2），但他是用英镑而不是美元支付。要完成这项购买交易，律师95（2）首先要预先从金融结算所200得到每月至多购买500美元（或等同的英镑数）的授权。可以从金融结算所200以安全容器152（8）中的预算控制188（5）的形式，将预先授权发送到律师的电器100（2）。律师的电器100（3）中受保护的处理环境154（2）可以打开容器152（8），验证预算记录188（5），并将该控制储存在PPE 154（2）维护的相关安全数据库中。

在得知这三章166（1）中每一章都已打开后，律师的受保护的处理环境154（2）就可以创建一个相关的审核记录，并从预算记录中现有的存款中扣除购买金额。一个月以后，或者当预先授权的这500美元的存款花完后，律师的PPE 154（2）可以向金融结算所200发送安全容器152（9），其附带的审核记录302（2）指明了所有的购买、他们的金额，以及提供者的帐户或应当计入贷方的帐户，这样有助于计算处理的高效自动化。金融结算所200可以打开安全容器152（9），将律师的信用卡帐户计入借方，并向适当的提供者支付它们应得的款项。

公司

在内容交易之前，公司95（3）内部的分布式的公司金融结算所200A在按照金融结算所200的授权运作的同时，向每个经理95（3）A、95（3）B发一个安全容器152，其中的预算记录188指出了目前批准的每月的信息和市场研究预算。公司的分布式认证机构500A（在该实例中，采用了与认证机构500相同的分级结构）还可以向公司的员工颁发数字凭证504（未示出）。

在该实例中，每个产品经理95（3）A、95（3）B都在他或她本地的电器100上选择性地打印报告和预算的有关部分，每打印一页就减去10美元。本地电器100（3）中受保护的处理环境154（3）安全地执行这个过程，利用控制188（3）进行调节，控制188（3）可能需要认

证机构500和/或分布式的公司认证机构500A颁发的数字凭证504（3）.

根据信息提供者所提供的控制188（3），在每个月的月底，或者该月的预算花完时，公司的电器100（3）就向公司内部的金融结算所200A发送审核记录（未示出），指出在报告间隔期间发生的任一购买事件、金额、以及这些购买的提供者的帐号。本地分布式的公司金融结算所200A汇总审核记录中的总额，并在安全容器152（12）中将至少一个审核记录302（3）发送给外部的金融结算所200，授权通过自动结算所（ACH）向市场研究报告的提供者支付应得的款项。另外，安全容器152（11）（如审核记录302（3）的组成部分）中有应当将资金计入借方的公司95（3）的帐号和发布报告的市场研究公司的帐号，资金应当拨入这个帐号。金融结算所200通过ACH完成支付过程并向内部的公司金融结算所200A发回VDE安全容器（提供至少一个审核记录）作为确认。分布式结算所200A又利用安全容器（未示出）向每个产品经理95（3）A、95（3）B发送至少一个确认审核记录。

实例：分布式商务公共事业75可支持消费者购买有形商品并付费的交易

电子商务的重要部分必然伴随着各类无形商品的销售、购买、分布管理、和/或支付。有形商品的商务就象无形商品（如数字信息）的商务一样，有许多相同的安全、可信度和效率的要求。要使计算机成为真正的商务工具，分布式的、安全的、可信的权利/事件管理软件层（如权利操作系统或中间软件），如Ginter等人描述的虚拟分布环境的规范就成为当务之急。因此，即使当有形而不是数字财产是安全电子商务的对象时，分布式商务公共事业75也能扮演重要角色。

图62示出了一个示例性的有形商品购买与支付系统1010。在图62的实例中，假想一个有名的服装和家居物品的提供者，例如，L. L. Bean或Lands End，通过数字网络如Internet/WWW网销售它们的货品。在该实例中，公司创建了：

●Web目录服务器1012，用于向消费者95提供服装的清单，

●Web履行服务器1014，作为履行功能的接口，以及

●第三台Web服务器1016，担当安全金融结算所200和多种支付方法（如MasterCard（“MC”），VISA，以及American Express（“AMEX”））的接口。

在这一个实例中，公司还：

●向安全目录服务600登记服务，

●通过金融结算所200，建立至少具有一种支付方法（如信用卡，贷款信用卡和/或银行）的提供者帐户，

●向交易机构700登记数种交易。

在该实例中，公司向交易机构700（可以是销售公司内部的分布式交易机构）登记至少包含一个电子控制集的基本交易，该控制集描述了，例如：

●向一个或多个履行处理机构如库房1018和后勤单位1020（可能是也可能不是同一个公司），

●收到期望的货物有存货的确认，

●收到订单的确认书，

●从下单的特定消费者的支付方法得到支付的预先授权，

●发货指示，

●确认货物已经发出，以及

●完成支付交易的控制。

在这一个实例中，公司还从认证机构500获得至少一个数字凭证504，至少表明以下一个事实，如：

●公司是在特拉华州（Delaware）登记注册的合法公司；

●公司没有破产并且/或者具有一定的资信；

●公司被分配了一个特定的联邦税收识别号码，以及

●公司具有几个州中每一个州的州税收识别号码、特定的州、和它们相应的识别号码。

消费者95利用他或她的具有Web浏览能力的电器100，在Internet的WWW网上访问目录服务器1012。目录服务器1012向消费者95发送Web页面1022，提供一页电子目录。可以在一个或多个安全电子容器152（1）中发送Web页面1022。消费者95利用他或她的电器100显示页面1022A，点击页面上显示男子短袖衫Oxford按钮部分，定购售价15.95

美元的衬衣．当前的Web页面被来自履行服务器1014的Web页面1022B替代．这第二个Web页面1022B可以在安全容器152（2）中发送．

消费者的电器100有一个受保护的处理环境154．PPE 154打开安全容器152，在屏幕上显示页面1022B．显示的页面1022B为一个表格，表格分几个栏目，包括目录号码以及衬衣和零售价格的描述．消费者95在栏目中填入颜色、领口尺寸、正常身高或高个人士、正常或量身定做、数量．消费者95还要指出衬衣的交付地点、交付服务的等级、以及消费者的地址．

在消费者95完成所需的信息之后，电器100将表格栏中的信息1024放入安全容器152（3），并将容器发回履行服务器1014．履行服务器打开容器152（3）并读取栏目信息1024．履行服务器1014创建VDE审核记录，表明收到了信息1024，履行服务器1014还可以创建控制集188和/或启动购买交易的事件通知．

履行服务器1014可以直接或通过交易机构700与库房1018通信．然后，履行服务器1014就要弄清楚需要的商品是否有货并能发货．如果履行服务器1014知道所需的商品有货且能够发货，并且消费者95提供的信息1024足以继续进行交易，履行服务器就向消费者发回另外一个Web页面1022C，表明：

- ●购买能够实现，
- ●各种销售税和运费，
- ●提供的地址和所选择的交付服务的等级，
- ●用于填写与支付有关的信息的新栏目，以及
- ●询问消费者是否想继续进行．

履行服务器1014还向消费者的PPE 154和交易机构700发送审核记录302（1），指出哪些部分较大的基本交易已经完毕．

在查看了履行细节之后，如果消费者95决定他或她不想继续交易，他或她的电器100就可以向履行服务器1014和交易机构700发送安全VDE容器152（5），指出交易已经取消．如果消费者95的回答为是，请继续交易，消费者被提示从提供的支付方法列表中选择一种支付方法．在该实例中，该列表对应于商品提供者和金融结算所200双方都支持的支付方法．消费者95填入信用卡或赊帐卡的号码，到期日以及寄送帐单的地址．

在完成了所需的信息之后，消费者的电器100就可以利用他或她的安全PPE，在安全VDE容器152（5）中，向金融结算所200发送该信息，并将附有审核记录的一个独立的VDE容器（未示出）发给交易机构700。

金融结算所200从信用卡处理公司那里获得预先授权，并且，例如，利用安全VDE容器152（6）将预先授权的批准信息1026返回给履行服务器1014。金融结算所200可以向交易机构700发送另一个附有审核记录302（2）的VDE容器152（7），表明预先授权步骤已经结束。

履行服务器1014可以向消费者95发送另一个附有新的Web页面1022D和审核记录信息302（3）的VDE安全容器152（8），表明：

●定购过程已经完成，

●销售已获支付方法的支持，

●在发货时，消费者的信用卡将付全部费用，

●交易确认号码，供以后参考，以便能够向履行服务器1014和/或交易机构700查询。

履行服务器1014（如与库房1018一起）包装货物、将它们交付给快递公司1020，并且，例如，发送附有审核记录302（4）、302（5）的安全容器152（9）、152（10），分别向金融结算所200和交易机构700表明货已发出。在该实例中，快递公司1010（“后勤部门”）也向交易机构700和履行服务器（如果希望的话，也可以向消费者95）发送VDE安全容器152（11），表明该快递公司1020已经拿到了货包。

在该实例中，在交付了货包之后，快递公司1020就向交易机构700发送包含表明货包的投递已经完成的审核记录302（7）的VDE安全容器152（12），然后，后者就给交易打上完成的标记，然后向金融结算所200、快递公司1020、履行服务器1014、以及在某些情况下向消费者95发送另一个VDE安全容器200，表明交易已经结束。

实例：分布式商务公共事业75可支持其中消费者为服务付费的交易

在本世纪末，发达的西方经济，尤其是美国经济的一个显要标记，就是从大量的制造、“烟囱”经济向“信息经济”以及“服务经济”的转变。分布式商务公共事业75可以支持消费者为消费或使用服务而付费的交易。

图63示出了一个示例性的在线服务系统1030. 在一个实例中，在线服务1032向安全目录服务600登记，从认证机构500那里获得表明该在线服务身份的数字凭证504（1）. 在线服务还同意认证机构500和认证机构500授权的各方所颁发的凭证504，为具体的事实颁发凭证.

例如，在线服务1032同意从经过认证机构500证实的（通过凭证504（2））父母那里接受分布式认证机构500A颁发的凭证504（3），以颁发凭证，表明他们有孩子并且这些孩子目前还是小儿童. 在线服务1032又不允许这样证实的儿童访问在线服务分布的某些主题问题的材料，也不允许用基于这些凭证的数字签名从事购买交易，除非儿童的监护人颁发了另一个凭证，表明他们愿意承担财务责任（如无限制条件，或每次交易的购买或者在给定时间内（在一个实例中，这个时间为一个月）花费的总额有一最高限额）. 可以从认证机构500将这些凭证504（2）、504（3）在VDE安全容器152中发给父母和/或至少一个儿童.

现在，假设儿童95（2）订阅了一个叫作“聊天”的在线游戏. 在线服务1032有一个专门为学龄儿童设计的Web界面. 服务1032提供的订阅每个季度都必须更新. 利用电器100如个人计算机或带有双向通信功能和受保护的处理环境154的电视机和机顶盒，儿童95（2）使用安全目录服务600查到在线服务1032，并发出一个请求订阅的消息. 作为响应，在线服务1032在VDE安全容器152（4）中发给父母95（1）或监护人一个支付要求1034、成员资格和成员信息. 父母或监护人和/或其它付费的个人95（1）在一个或多个别的安全容器152（5）中，向在线服务1032提供他或她（或他们）的信用卡号码、到期日、和寄送帐单的地址信息1036.

在该实例中，在线服务1032利用VDE安全容器152（6），将消费者的服务帐户、信用卡和/或其它支付信息1036发送给金融结算所（在本实例的一个变例中，父母95（1）可能已经在VDE安全容器152（5）中向金融结算所200直接提供金融及相关信息）. 在线服务提供者1032还向金融结算所200提供结算所的站点和提供者的帐号. 在受保护的处理环境中（例如，可能包括锁在安全的房间中或其它安全地方的一台通用的计算机），金融结算所200打开安全容器152（6），取出支付信息1036，并完成与信用卡公司的支付交易.

对该实例来说，金融结算所200继而又在至少一个安全VDE容器152（7）中，将下列信息1038（此列表只用于说明的目的，并不有损于一般情形，即其中任何可利用的信息都可能已经被传送）发送给在线服务1032:

- ●交易的VDE审核记录，
- ●交易的授权号码，
- ●提供者的帐号，
- ●获得服务的消费者的帐号，以及
- ●支付的数额。

在线服务1032继而又向消费者95（1）发送安全容器152（8），表明支付已获接受。在一个实例中，在线服务1032可以指导认证机构500颁发凭证504，表明在到期日之前订阅都有效。在线服务1032还提供从金融结算所200提供的信息1038中得出的审核记录302（1）。

儿童95（2）每次登录到在线信息服务1032上，儿童的PPE 154就检验确定是否存在或知道凭证504，如果是的话，是否:

- ●这些数字凭证表明当前订阅在线服务尚未到期，以及
- ●任何小儿童都有凭证且都有效（例如，因为儿童未满18岁，所以尚未到期）。

在线服务通过这些凭证504，确信儿童95（2）被授权使用在线服务1032并禁止访问某些“成人”内容后，就批准选择性地访问授权的部分。

在线服务的特性包括分布式的多人交互游戏。在该实例中，儿童95（2）与另外至少一个经授权和证实的儿童一起玩游戏－在该具体的实例中，成人被底层的VDE规则和控制禁止玩这些游戏。可以利用至少一个VDE安全容器152（9），从在线服务1032将实现至少一个游戏的至少一部分1040的软件的至少一部分（如可执行的代码和/或解释性代码如Java）下载到儿童的信息电器100（2）当中。

利用Ginter等人的说明书所描述的方法，确定这些程序和/或程序段1040真实可信且未经修改。用来计算单向散列函数（生成用于确定至少一个程序1040或程序至少一部分的完整性的数字签名）的密匙，至少有一个被认证机构500颁发的批准504绑定到在线服务1032的身份中。

在该实例中，当儿童95（2）玩游戏时，他或她的活动至少有一部分被按照共同等待批准的Ginter等人的申请中公开的方法进行计量，创建表明该儿童使用情况的审核记录302（2）。在一定的时候，将这些审核记录302（2）传送给在线服务1032，在该实例中，在线服务1032可能包括使用结算所300。使用结算所300分析这些使用记录302（2），并利用它们来确定向儿童95（2）收多少费。

实例：分布式商务公共事业75可用于为购买和/或使用有形商品提供价值链分解

分布式商务公共事业75可用于为涉及有形商品的购买或其它类型的交易提供便利。图64示出了一个示例性的有形商品交付系统1040。例如，公司1042利用包含PPE 154的电器100下单定购办公用品。定购的商品有一盒纸夹、一个订书机、订书钉、一箱8.5×11英寸的复印纸、以及一打法定尺寸的黄色笔记本。这些商品由制造商1050制造，由经销商1048经销，并由零售商1046卖给该公司。

在该实例中，金融结算所200从公司1042收到支付1052并将支付分解，将支付分成分解支付1052A、1052B、1052C，分别交付给零售商1046、经销商1048和制造商1050。

例如，公司1042在VDE安全容器152（1）中将订单1044发送给零售商1046。在该实例中，零售商1046提供履行服务，即收取订单1044，并相应地提供控制集188，该控制集指明了每种商品的经销商1048和/或制造商1050的帐号和每一方要从零售价格中收取的百分比。如果希望的话，零售商1046可以为定购的每种商品都提供一种不同的控制集188（不管数量是多少）-允许一项一项地执行不同的支付分解。零售商1046可以向公司1042提供这种控制集188a。

可以在存在认证机构500颁发的一个或多个数字凭证504时调节控制集188a。例如，控制集188a可要求公司1042提供认证机构500颁发的数字凭证504（1）。凭证504（1）表明定货的公司1042的身份。公司1042可以在与认证机构500相同的可信分级链中提供另一个凭证504（2），证明下单人已被授权下单，每个订单有指定的最高开支限额。公司1042可提供相同或不同的凭证504（2），该凭证还表明公司的采购人员已被授权使用公司的赊帐卡。

在该实例中，公司1042用公司的赊帐卡付款．在零售商1046发货之前，金融结算所200首先从信用卡公司得到支付授权．在收到预先授权的通知后，零售商1046就可以向公司1042发货1047．交货以后，零售商1046就在至少一个VDE安全容器152（2）中创建至少一个VDE审核和/或记帐记录1052，并将该容器传送给金融结算所200（还可以或者替换地将审核信息发送给零售商1046）。

然后，金融结算所200就将总的支付金额分配给（例如，可能是直接从零售商1046和/或通过公司1042收到的）控制集188a代表的每个价值链参与者，从而完成赊帐卡的交易。通过这种方法，经销商1048和/或制造商1050就在零售商1046收到它的支付的同时，收到它们的支付。控制集信息188a还可表明怎样分配总的支付和供应商的帐号，以便缴纳本地、州以及联邦的税收（如果要交税的话），并支付费用，如向快递公司付费。

图64的这个实例表明，价值链的分解可适用于有形商品和无形商品。如果需要，还可以使用类似的技术，进一步退到制造商1050的供应链（如提供用于制造纸夹的金属的供应商）。

实例：分布式商务公共事业75能通过提供对象登记和其它服务来协助分布数字财产

分布式商务公共事业75可以协助电子社区有效地分布电子或数字财产或内容．例如，利用配备受保护的处理单元154的电器100，创建者或其它权利拥有者164就可在安全容器中向权利及许可结算所400发送要登记的数字对象。

权利及许可结算所400利用它自己的VDE受保护的处理单元打开容器，分配一个统一的对象标识符，表明创建者身份、登记对象的类型（软件、视频、声音、文字、多媒体等）、以及对象的数字签名。统一的对象标识符可以是全世界独一无二的，或者只是在创建者或其它实体（如在线服务、数字图书馆或特定的辖区，如指定的国家）的名称空间域中为独一无二。

在该实例中，权利及许可结算所400利用其受保护的处理环境，用该权利及许可结算所的私用密匙给这个统一的对象标识符作上数字标记，并在VDE安全容器中将对象和标识符返还给登记它的个人或组织．权利及许可结算所400可以保留对象的副本，或者只保留对象

的统一对象标识符、对象及其统一对象标识符的签名。在另一个实例中，权利及许可结算所400给由原始对象和它的统一文件标识符组成的一个新对象作数字标记，并将这个新对象和/或它的签名保存在权利及许可结算所400的档案中。

创建者可能也已经在VDE安全容器中发送了许可及定价模板450（参见图45A－45C），指出批准了哪些许可、运用这些许可的收费价格，如果可行，还指出这些价格和许可所适用的个人、类别和/或辖区。在一个VDE安全容器152中可以发送一个以上的许可及定价模板450，或者，可以为每个许可及定价模板单独使用一个VDE安全容器152。

在该实例中，利用VDE安全容器152，对象就被从创建者传送到发行者168那里（参见图16）。利用凭证504，发行者168就能向解释创建者的控制集的VDE事例（PPE 154）证明，发行者确实已经被授权选择性地改变对象的许可及价格，以及创建新的许可及定价模板。然后，发行者168就向权利及许可结算所400发送VDE安全容器，容器内包含了伴随着新控制的统一对象标识符。在这个优选实施方案中，如果对象保持不变，发行者168就可以选择让该统一对象标识符不变；然而，如果发行者已经改变了该对象，有可能将它加入自己的品牌，那么就必须改变统一对象标识符，以反映发行者的情形。利用发行者的私用密匙重新计算数字签名。象前面一样，登记对象可以选择只储存数字签名或签名加实际对象。

实例：分布式商务公共事业75可用于为版权登记提供便利

作为增值服务，权利及许可结算所400可以提供版权登记服务（参见图43）。权利及许可结算所400可以将对象的副本发送到适当政府部门440，例如美国版权局的适当在线版权登记服务机构。如果登记或处理要收费的话，可以将对象和统一对象标识符与指明支付模式的控制一起，在VDE安全容器中发送。

在该实例中，版权登记服务机构可以向金融结算所200发送至少一个VDE安全容器，安全容器至少附带一个审核记录，表明应付的金额、支付方法和登记方的帐户、收取资金的政府部门的帐户，回过来，版权登记服务机构又在VDE安全容器内收到表明交易已获预先批准（或者由于何种原因，建议的交易未获批准）的审核记录。

如果金融结算所200已经预先批准了这项交易，在该实例中，美国版权局中具有VDE能力的计算机打开这个安全容器，将该统一对象标识符和对象添加到登记数据库中。在认证机构500发出的信托链下－在该实例中，该机构可由或代表美国政府运作管理－版权登记服务机构颁发至少一个数字凭证504，表明这些事实，即事实上一个具有指定的统一对象标识符和指定的数字签名的对象已经在登记机构登过记了，并且在登记该对象时事实上至少有一个人是该版权的拥有者。凭证504在VDE安全容器中被发送给登记对象的那个人（和/或指定接收通知的那个人）以及权利及许可结算所400，后者又可以根据请求在安全VDE容器中提供版权登记信息。

版权登记服务机构向金融结算所200发送至少一个VDE安全容器，该容器至少带有一审核记录，指导结算所200继续履行预先批准的交易（如果所有必需的信息都是预先批准的处理的组成部分）和/或向结算所200提供有关信息，如应付的金额、支付方法和登记方的帐户、收取资金的美国政府部门的帐户、以及应当完成此项支付交易，回过来，版权登记服务机构又在VDE安全容器中从金融结算所收到审核记录，表明交易已经完成且资金已经存入某个适当的帐户或多个帐户，或者表明支付交易失败以及无法完成交易的原因。

实例：分布式商务公共事业75可支持许可及价格的更新或调整

分布式商务公共事业75可以提供一种机制，用于更新已经到期的权利及许可，从而进一步为电子和数字财产的分布提供便利。参见图42A。

在一个实例中，假设一家进入幸福1000排名的公司的一名员工有一个过期的数字财产（可能是一段软件或Java小程序）的控制集。该员工计算机上的VDE受保护的处理环境可以向权利及许可结算所400发送一个VDE安全容器。

分布式商务公共事业75还可以提供一种机制，分布已经被分布链中的一个或多个参与者改变了的权利、许可及价格，从而为电子和数字财产的分布提供便利。在一个实例中，假设消费者在她的硬盘上有一数字对以及有发行者分布的VDE控制集。许可及价格最初表明为按使用次数付费的模式，其中用户每次操作对象如打印或查看，就要支付10美分。

要确定现在是否可以利用新的许可及价格，消费者PC中的受保护的处理环境可以利用从控制集获得的站点以及MIME兼容的电子邮件，向权利及许可结算所400发送一个VDE安全容器。消费者已经在VDE安全容器中向安全目录服务600发送了一个查询并且在VDE安全容器中收到了回答，由此获得了权利及许可结算所400的站点。

发给权利及许可结算所400的VDE安全容器包含对象标识符以及要求获得包括价格在内的当前控制的请求。权利及许可结算所400服务器处受保护的处理环境打开VDE安全容器，从控制数据库中检索最近的控制集，并通过回复电子邮件，将另一个带有所需控制的VDE安全容器发出去。消费者的受保护的处理环境打开这个容器，并用新的控制取代和/或扩充过期的控制。现在，消费者就能根据刚刚从权利及许可结算所收到并由本地计算机或其它电器中的VDE处理的控制集中所规定的规则和控制使用内容了。在该实例中，这些新的规则和控制将每次使用所支付的价格从每次操作10美分降至5美分。

实例：分布式商务公共事业75可支持分布新权利的模式

分布式商务公共事业75还可以支持有些交易，其中某些或全部权利最初并不是以内容的形式分布给最终消费者的，而是必须请求分布这些权利。在一个实例中，假设一个律师决定将他/她自己的文章与从法律信息分布者那里获得的其它材料综合在一起，进入出版。法律信息分布者已经选定了一个权利及许可结算所400，作为他们许多财产的控制集信息的分布者。他们每在权利及许可结算所400登记一个对象，就要以Ginter等人的说明书中所描述的格式登记两个控制集：

●一个控制集规定包括给零售消费者的价格在内的默认控制，以及

●第二个控制集传递零售消费者很少感兴趣的权利和价格，例如选编权。

律师通讯的出版者从专利法专题论文中选取了一章，并想在其它文章之外在通讯中包括一个1000字的摘录。该通讯出版者已经得到了专题论文的这一章及其零售控制集，它利用Internet MIME兼容的电子邮件，在VDE安全容器中向权利及许可结算所400发出一个询问，要求得到由所附的统一对象标识符标识的那一章的摘录权和选编权。该律师发现正在使用安全目录服务600的权利及许可结算所400（或者，

可以在律师收到的最初的零售版本中包含权利及许可结算所400的站点）.

权利及许可结算所400检验对象数据库，找到以该统一对象标识符命名的对象的控制集信息，并确定可以与各自的价格一起利用摘录和选编权．摘录权并不传递修改摘录部分的权利．选编权与将价格定为零售价打折30%的控制一起传递，如果没有选编整章，就按照摘录的长度按比例计算价格．

利用VDE知道的排版应用程序，该通讯出版者综合了几部作品，包括将1000字的摘录作为新作品，并且将这个新的对象与其控制集一起，向权利及许可结算所登记．该通讯出版者还向版权登记职能部门，如美国专利及版权局，登记这个新的对象．该通讯发行者将新作品分布在VDE安全容器中，该容器还包括单独的选编作品、以及全部完整的通讯中每一个的控制集．用户电器中的本地VDE受保护的处理环境根据适用于该复合对象的控制及其有单独规则的每一部分的控制记录使用情况．有的时候，VDE向使用结算所300和金融结算所200发送审核记录．

实例：分布式商务公共事业75可支持电子权利协商

分布式商务公共事业75可支持电子权利协商．在一个实例中，假设一名教授正在创建“课程包”：在该实例中，为供具体某一课程的学生使用的许多不同作品的汇编，该课程只有一个学期．在该实例中，该教授向适当的权利及许可结算所400发出一个带有查询的VDE安全容器，并收回查询所列出的数字财产的控制集．在查看了许可和价格之后，该教授注意到书中有一章的价格过高，使得课程包的总价格高于她/他希望的最高价．

该教授使用Ginter等人公开的协商机制（如参见图75A－76B），与权利及许可结算所400协商．权利及许可结算所400又自动发现它自己缺乏这种协商的权力，于是就将协商重新定向到发行者．

在通过提供证明，表明在“高等教育”这一类别中具有成员资格，而从认证机构500获得适当的凭证504之后，出版者Web服务器的受保护的处理环境就为面向该教授的财产提供一个新的、修改过的控制集．这些控制提供折扣价，要求在具有VDE能力的、授权过的打印机上打印副本，该打印机将记录打印副本的份数，这些控制还使用VDE

技术向交易各方汇报。该教授仍然对价格不满意，于是就在安全容器中给发行者发了一个VDE协商还价。发行者的VDE与该教授的协商还价控制集协商并达成协议，向该教授提供带有双方同意的新的价格、期限和条件的新控制集，然后，该教授继续制作课程包。权利及许可结算所400之所以愿意批准降低了的价格，部分是因为在该实例中，该教授能够提供数字凭证，表明她在加州大学洛杉矶分校供全职并且有一定的最低数量的学生将要利用这些材料这一事实。这种验证符合出版者向权利及许可结算所400说明的要求。

实例：可执行模块的认证

认证机构500的一个有价值的用处就是代表政府颁发数字凭证。除了颁发表明身份、法律状况等的凭证外，政府认证机构500可以颁发证实可执行模块如装载模块的凭证。例如，各级政府认证机构500可以认证代表他们行政区域的法律和贸易惯例的可执行模块的集合。例如，沙特阿拉伯可能会要求，在其管理控制下的所有电器都要有装载模块，并且这些模块已通过检查容器的属性以保证只发布合适内容的政府部门的认证。加利福利亚州可能会认证计算州税收的安装模块。

实例：娱乐的分布

分布式商务公共事业75可用于高效灵活地支持向消费市场发行电影的模式。例如，假设电影和娱乐公司如迪思尼想提供电子分布式商务公共事业75，以支持向消费者95发行其电影。迪思尼可以自己打开商务公共事业系统90，或者与中立的第三方联系，代表它自己提供商务公共事业系统90。在该实例中，商务公共事业系统90的目的，是支持向消费者提供安全的按观看次数付费/按使用次数付费、租赁、租借和其它电影发行交易。

电影本身可以以数字化的线性形式发行－例如，数字多用光盘（DVD）或其它高容量的媒介。除了电影本身以外，这些媒介还储存包括控制这些电影的使用的控制集在内的一个或多个安全容器。消费者95可以利用具有网络150联接或其它“背后通道”（如读写智能卡等的能力）的媒体播放机104（参见图1）播放这些电影。

媒体播放机104有一受保护的处理环境154，如用于管理权利和操纵安全容器的安全处理装置。还可以用配备受保护的处理环境和网络联接的个人计算机来播放存储媒介。

机顶盒104可由分布在媒介上的电子控制和/或通过背后通道来控制。这些控制要求机顶盒104记录消费者决定观看的每个财产的消费者使用和支付信息。例如消费者95可将媒介如DVD光盘放入媒体播放机104，点击“播放（play）”按钮。消费者的媒体播放机104接下来会显示（如在电视机102上）一则消息，告诉消费者观看这部电影要花多少钱（如2.95美元），并询问消费者她是否想继续。如果消费者回答“是”，媒体播放机104就在消费者的电视机102上播放这部电影－同时记录使用和支付信息，报告给商务公共事业系统90。在交付给它的一个或多个相关电子控制集的控制下，媒体播放机104内受保护的处理环境154可以监视和收集能够最终用于确保消费者为观看电影付费并提供安全的使用审核的信息。例如，安全的使用审核可用于允许迪思尼、电影的演员和导演、以及其它参与这部电影制作的其它人，安全地核实有多少人观看了这部电影（并且有可能提供人口统计信息，以便于广告的定位等）。例如，媒体播放机104受保护的处理环境可以安全地收集记录与特定控制有关的计量、记帐和/或预算查账索引中的以下信息：

- ●电影的名称，
- ●电影的数字标识符，
- ●播放财产的时间和日期，
- ●播放财产的次数，
- ●播放财产的人是谁。

在一个实例中，消费者95必须拥有由适当认证机构颁发的表明一定事实的数字凭证122。这样的数字凭证122可用于为交付给媒体播放机104的电子控制集提供环境。在允许消费者播放电影和/或在一定条件下禁止播放电影和/或使在播放电影时应用的控制生效之前，可能要有这样的凭证。

例如，父母可以获得数字凭证122，表明家中有儿童。这个“有儿童”的数字凭证122可用于防止媒体播放机104播放“G”级、“GP”

级以外的其它任何电影。如果需要的话，这些凭证122可由与本发明一起提供其它管理和支持服务的同一组织颁发。

与媒介如光盘中的特定电影一起提供的电子控制还可规定特定的价值链分解与支付安排一起实施。例如，媒体播放机104会从交付给它的电子规则和控制“知道”电影发行商、工作室和分布式商务公共事业75将得到2.95美元使用费的具体百分比，并且州政府部门必须得到销售税或VAT形式的一定税收。因为该信息是在媒体播放机104内受保护的处理环境154中维护的，消费者95永远不会知道支付分解的计划和/或其细节。（通常，消费者并不关心发行商“份额”与工作室的收入之比。媒体播放机104内受保护的处理环境可以在本地或者如上所述通过分布式或集中式的金融结算功能200，提供这个支付分解）。

媒体播放机104可以实时（在线）和/或在周期性事件驱动的基础上报告它所收集的使用规模信息。在一个实例中，媒体播放机可以在每个月的月底报告它在前面这个月收集的信息。它可以向迪思尼运营的金融结算所200（或者，可直接向结算所200直接报告此信息）报告收集的支付信息（包括控制集提供的分解数据）。金融结算所200确保将消费者的帐户适当地计入借方，并且各受款人（如迪思尼、电影发行商、以及价值链中的其它各方）获得消费者支付中的适当“份额”。金融结算所200还可提供消费者的信用调查和授权，协助确保消费者不会累积到她无法支付的大帐单。

媒体播放机104可以向由独立审核者（电影制片商和演员可以坚持由独立的第三方审核者－而不是迪思尼－来执行此项功能）运作的使用结算所300报告它所收集的使用信息，或者，例如，向迪思尼和/或结算所200报告该信息－如果规则和控制要求，可以向迪思尼隐藏某些信息，以保证价值链其它方面的权利，而且，由于如VDE的保护机制，迪思尼无法识别、变更和/或去除这些信息。使用结算所300可以分析使用数据并发布表明观众的总数、市场份额等的报告。使用结算所300还可以进一步分析该信息，以提供人口统计和/或其它市场研究信息。这类信息对广告客户和销售人员来说非常有用。

迪思尼还可以运营权利及许可结算所400。在该实例中，即使许可被分布在光学媒介中，权利及许可结算所也能出于各种原因，提供

附加的控制集。例如，分布在媒介中的控制集在某一天会到期。权利及许可结算所400可以发布新控制集来替代过期的控制集。权利及许可结算所400还可颁发许可，以提供“销售”和/或改变价格（如降低老电影的价格）。权利及许可结算所400还能颁发特殊的许可（如摘录或选编权利，即多媒体开发人员或广告客户可以请求获得权利和/或向某些画面如获得批准的米老鼠图案重新分布权利以便打印）。迪思尼可以“预先批准”一些这样的特殊许可，使权利及许可结算所能自动根据要求提供它们。数字凭证122可用于和许可交互－从而保证获得控制集的用户有权利用它。

实例：分布式商务公共事业75可支持使用信息的收集、分析和再定向

在Ginter等人的说明书公开的发明之前，电子社区缺乏能够在本地计算机或受保护的处理环境中高效率、有实效地监视和衡量使用情况的通用的、可重复利用的、分布式的、对等的技术。收集、分析和报告使用数据为权利拥有者和分布链的其它参与者、基础架构的分布式商务公共事业75、消费者、以及其它感兴趣的各方，提供了重要的价值。知道发生了什么常常可能对可能或应当发生什么有决定性作用或贡献。另外，可以再定向使用信息，以支持其它广泛的商业活动，包括广告和经销模式。

假设几家公司中每一家的一个或多个消费者有信息电器100，在该实例中为个人计算机，该电器带有Ginter等人所述的VDE受保护的处理环境（PPE）154。进一步假设在一段时间当中，在该实例中或许为一个月，VDE一直在记录详细的使用信息并将这些信息储存在每台计算机的每个硬盘中的加密数据库中，计算机是消费者PPE的逻辑扩展并受其控制。这些消费者每个人都从通常不同的来源，购买了不同的信息和娱乐组合。VDE的每个示例都根据与购买或使用的内容和/或服务相关的控制记录使用信息。

每月和/或其它要求（或者，如果支持、允许的话）的报告间隔的第一天或第一天刚过，VDE的每个事例都根据与它们在上个月使用的每个数字财产相关的控制，将使用记录发送给使用结算所300。使用结算所300又向每个权利拥有者提供关于上个月或其它任何报告间隔（每天、每周、每个季度、每年等）内使用财产的报告。

在一个实例中，这些报告含有识别个人消费者和雇佣他们的公司的信息。在另一个实例中，报告含有详细的使用信息，但个人消费者的身份被使用结算所300去除。或者，可以将个人消费者和公司的身份都去掉。可以该按任意一个或多个一定的分类，如行业、地理位置、和/或国家、和/或其它任何有用的分类，汇总使用信息。

在另一个有用的实例中，某个特定的公司或个人消费者可能并未允许VDE（当然，受通过现场规则和控制而得到的权利的管辖）从他们在第一位置的信息电器向使用结算所300传送身份信息。用户可能已经建立了VDE控制，禁止公开这些身份识别信息。在另一个实例中，用户可能使用了Ginter等人申请中公开的协商机制，协商与每个消费者购买或使用的信息有关的各个控制集中要求以外的另外各级隐私和秘密，就是说电子协商过程生成经过修改的或新的规则和控制集，反映另外各级的隐私或机密性。在又一个实例中，权利拥有者、权利及许可结算所400或使用结算所300或其它方，可以通过利用VDE规则和控制集的各级隐私和秘密，使用相同的协商机制。

如图11和图33－39所示，使用结算所的功能，即可以去除识别信息、汇总数据、分析数据、生成报告、和/或向权利拥有者和其它感兴趣的各方发送这些报告，可以存在于一个或多个逻辑或物理位置。例如，在本地计算机（或其它信息电器）上执行的分布式使用结算所300可以执行这些使用结算所功能中的任一项或所有项。一个或多个使用结算所可以存在于一指定的公司或指定的公司集合中，这些公司包括产供销行业、保健、贸易组织、公司家族（“keiretsu”）。类似地，这些使用结算所的功能由每个国家或其它辖区内或其它任何分类和/或地理变量规定的使用结算所来完成。

使用结算所300还可向权利拥有者、分布链参与者和/或其它感兴趣的各方，提供原始数据、汇总数据和/或定制的报告。这些各方包括：例如，内容创建者、发行者、再打包者、再定向者、广告代理机构和它们的客户、贸易协会、市场研究和咨询公司、发行量审核和观众调查机构、对一个或多个市场有兴趣的销售、市场营销、广告功能的公司以及政府机构。

在另一个实例中，使用结算所300还可向广告客户出售信息，表明特定广告和/或类型的广告对个人、公司和/或一组公司内的客户、市场和/或其它分析组合和分类公司的曝光率。

实例：安全目录服务保护秘密和隐私

个人和商业秘密和隐私常常是现代生活的及其重要的一个方面。个人不想让其它人知道他们在跟谁交往。在商业中的许多个参与方面，企业不希望披露它们对与其它各方联系、接洽或做生意感兴趣。在今天的Internet上，例如，有些访问Internet的人能够确定给定的个人和目录服务之间的查询的情况。这种信息可以提供有关尚未公开的现有或未决商业安排、合并或购并等的重要线索。

VDE安全容器为安全目录服务600提供了一个基础，秘密和隐私就保存在其中。在一个实例中，一家排名幸福100家之列的公司Corporation Counsel在想获得投资银行家在处理拟议中购并的这家企业内的email地址－但不将她的想法透露给其它任何人。代理人在VDE安全容器中给安全目录服务600发送一个附有她想接洽的个人和公司名称的查询。接着，安全目录服务就在另一个VDE安全容器中将回答返回给代理人。查询和回答都可以利用认证机构500颁发的凭证，证实代理人和安全目录服务600。查询的支付可以由金融结算所200处理，将支付存入提供者在安全目录服务600中的帐户，同时将雇佣该代理人的公司的帐户计入借方。

由于这些交易是利用VDE和VDE安全容器进行的，监测通信的人除了知道各方正在通信以外，其它一无所知。安全分析家已经开发了“通信量分析”的技术，其中监测双方或多个参与方之间的通信频率，并且将通信频率的变化与其它信息关联，从而形成有关这些通信的内容和/或目的的参考。

使用VDE和VDE安全容器，有可能挫败通信量分析，但代价是成本上升。在这一个实例中，公司可以向安全目录服务600发送一个附有空的查询的VDE容器，该查询在平均的经过时间内，在附有空的响应的VDE容器中，生成返回消息。代理人计算机中的VDE事例将生成送往金融结算所的支付交易，但会将这些支付记录与其它的一起汇总，以便消除查询和支付模式之间的关联。尽管从商业立场上看这是不充分的，这种使用VDE和VDE安全容器挫败通信量分析攻击的方法，原则上

可在利用Ginter等人的申请书所公开的安全、可信、有效的分布式交易能力的同时，在隐藏它们之间的通信模式的多个参与方之中使用。

实例：组织内部和外部的结算所之间的合作

各商务公共事业系统90可以按不同程度和不同组合分布（如图2A－2E和图3A－3C）所示。在图65所示的一个实例中，美国一家排名幸福100大公司之列的公司1070在多个国家（如美国、日本和欧洲）开展业务，并且在这些国家中，该公司在许多国家都分别在多个地点开展业务，该公司发现有必要跨国分布VDE分布式商务公共事业75。为了提高购买外来信息的效率和充分利用信息提供者的作用，公司1070选择与多个提供者商讨协议，该协议就象是在美国国内制造和以美元支付一样处理所有购买。在该实例中，公司1070维护着它自己的全球Intranet 1072。Intranet 1072将公司总部1074HQ（此处示为位于美国）与公司美国员工的电器1074US（1），…，1074US（N）、公司日本员工的电器1074JP（1），…，1074（N）、和公司欧洲员工的电器1074EU（1），…，1074EU（N）联接在一起。Intranet 1072还允许每个员工1074相互通信。公司1070及其信息提供者之间基于VDE的交易还可以通过公司在美国的某个或其它网关路由到Internet。

为提供高效的管理和支持服务，公司1070在每个国家都部署了至少一个分布式的金融结算所200和至少一个分布式的使用结算所300。例如，公司1070可以在美国运作金融结算所200A和使用结算所300A，在日本运作金融结算所200B和使用结算所300B，在西欧运作金融结算所200C和使用结算所300C。在有多个地址的国家和美国国内，可以存在几个这样的分布式结算所。除了与信息提供者商讨协议，公司1070还可以与大型商业性的使用结算所300和主要的金融结算所200商讨协议。这些集中式的结算所可以位于任何地方，并且可通过Internet和公司的Intranet 1072与公司通信。这些结算所200、300都不是公司1070的附属机构，只不过是利用这种业务安排。公司1070内的每个分布式的结算所都同时在公司和公司与之有业务安排的外部结算所的管理之下运作。

在这一个实例中，公司1070在日本录用的产品销售经理1074JP（1）从美国的分布者1076得到一份市场研究报告166。该报告和有关的控制在VDE安全容器152a中被美国的分布者1076发送给员工1074JP

（1）. 该经理1074JP（1）的电器中VDE记录了使用情况和信息提供者应得的支付. 这些审核记录302（1）、302（2）在VDE安全容器1052b、1052c中，被周期性地传送给分布式的使用结算所（专用使用结算所）300B和内部金融结算所200B－两者都位于日本公司内部的公司私有网络（或Intranet）1072中. 在该实例中，根据与购买内容相关的VDE控制，专用使用结算所300B时常根据管理受保护的处理环境的处理的VDE规则和控制，去除个人的识别信息，并在VDE安全容器中将审核记录302（3）发送给外部商业性的使用结算所300. 公司内部所有分布式的使用结算所300A、300B、300C都在VDE安全容器152中向商业性的使用结算所300发送周期性的通讯信息。主使用结算所300回过来又创建、出售、许可和/或向权利拥有者和其它各方（如对获得这些信息有商业兴趣的第三方）发布报告，其中个人的身份被去除，而且在很多情况下，根据VDE规则和控制，公司的名称也被去掉。

根据与购买的内容166相关的VDE控制188a，完整的使用记录（带有员工的身份识别信息）副本时常还被发送到公司的主使用结算所300HQ（可以位于公司总部），作为来自公司所有分布式的使用结算所300A、300B、300C的审核记录。然后将这些记录汇总合并，供进一步分析、报告和审核。

内部分布式的金融结算所200A、200B、200C也根据所购信息的VDE控制集，在VDE安全容器152中，从向它们报告的每个VDE受保护的处理环境1074收取审核记录302. 每个内部金融结算所200A、200B、200C都汇总支付，并时常发送带有审核记录302的VDE安全容器152，审核记录表明即将划拨给信息提供者、作为交易结果的总金额。公司还可以提供关于即将划拨资金的公司帐户和/或收取这些资金的提供者帐户的更新信息。回过来，外部主金融结算所200完成这些支付交易之后，又给公司1070和信息提供者发回确认支付交易的审核记录。在优选实施方案中，这些活动在分布式VDE节点的控制之下安全的发生，并通过使用VDE容器和管理多节点、多个参与方、顺序处理的处理链以及控制，使活动至少部分自动化。有一个备选的实例，支付金额的计算和支付交易的完成是在外部主金融结算所200进行，并从收自使用结算所300的使用信息得出的。（当然，如果使用结算所300和金融

结算所200为同一方，金融结算所就已经收到了这种信息）．在该实例中，外部和内部金融结算所接下来会比较支付信息．

该实例并不取决于管理和支持服务以什么样的程度分布．在一个相关的实例中，使用和金融结算所的功能可能已经分布到了每个VDE受保护的处理环境1074，如图2A－2E和图3A－3C所示．在该实例中，每个受保护的处理环境1074都能向主结算所200和300、分布式的外部结算所、和/或按不同于上述方式，如按洲组织（北美洲、中南美洲、澳大利亚、欧洲等），而不是按国家和公司1070的位置组织的内部结算所直接报告．

在又一个实例中，公司总部1074HQ及以总部为基地的有关结算所200HQ、300HQ提供了集中式的结算系统，所有的使用和金融信息都必须流经该系统．在这个具体的、更加集中的实例中，所有的用户电器1074都通过Intranet，在安全容器152中，向以总部为基地的结算所200HQ、300HQ报告它们的使用和金融交易．公司总部的金融结算所200HQ可以直接介入VDE兼容的通用支付系统，该系统直接支持VDE处理链和控制的使用，以确保按照管理与支付有关的变量，如支付金额、各方、地点、定时和/或其它条件的规则和控制，自动、安全地履行金融交易．这些以总部为基地的结算所200HQ、300HQ（可以作为单个、集成的商务公共事业系统起作用）又可以向每个国家内的各个结算所200A、200B、200C、300A、300B、300C传送适当的汇总和/或其它查账索引和/或支付信息．尽管比上述较少分级的实例的效率低，这种安排对于大公司来说还是有吸引力的，这些公司希望在向分布式内部金融结算所提供贷款和/或电子货币时扮演中央管理员的角色，并有效地管理内部收集的与交易有关的信息，从而对使用信息和金融信息进行集中控制．

实例：交易机构可用于组织内部和组织之间

图66示出了示例性地使用交易机构700跨组织和在组织内通信．图66示出了一个拥有“Intranet”（特定机构内的专用数据网络）5100（A）的组织A（图的左侧）．Intranet 5100（A）可以是局域网和/或广域网．用户电器100（A）（1），…，100（A）（N）（例如，组织A的员工）可以通过Intranet 5100（A）相互通信．

图66还示出了另一个组织B，该组织也可以拥有自己的Intranet 5100（B）、用户电器100（B）（1），…，100（B）（N）、以及专用交易机构700（B）。此外，图66示出了一个公用数据网5104（如Internet）和一个公用交易机构700（C）。图66显示，在该实例中，组织A和B与外部世界通过可信的交易机构700（A）、700（B）（如果需要的话，可以包括“网关”、“防火墙”和其它相关的安全通信组件）进行通信。在另一个实例中，可信交易机构700（A）、700（B）不需要实际的“网关”、“防火墙”来进出Internet5104，但却分别能够完全在组织A、B内部运作，同时可能生成电子容器302，以便在Internet5104上传输。

在该实例中，组织A的用户受保护的处理环境100（A）（1），…，100（A）（N）每个都有一虚拟分布环境受保护的处理环境，并能通过安全电子容器302，在Intranet 5100（A）上相互通信。类似地，组织B的用户受保护的处理环境100（B）（1），…，100（B）（N）每个都有一虚拟分布环境受保护的处理环境，并能通过安全电子容器302，在Intranet 5100（B）上相互通信。此外，组织A和组织B可以通过安全电子容器302，在Internet 5104上相互通信。

组织A专用的可信交易机构700（A）可用于为组织A的内部通信和处理提供便利。例如，专用的可信交易机构700（A）可用于详细记录组织A内一个用户发给另一个用户的消息。与此同时，公用交易机构700（C）可用于在组织A和组织B之间协调，并且不会将其中某个组织的机密信息透露给另一个组织。下面是怎样有利地利用图66的装置布置从事商业交易的更加详细的实例。

假设在将机密的备忘录分发给每个用户100（A）（2），100（A）（7）－100（A）（10）和100（A）（12）（他们当中每个人都不能修改备忘录）之前，首先必须征得用户100（A）（1）、100（A）（3）和100（A）（5）（每个人都可以修改备忘录）的批准，除了用户100（A）（1）、100（A）（3）和100（A）（5）（在三人都在上面签名之后，他们也不能再修改备忘录）得到备忘录的副本外，其它人都得不到。专用交易机构700（A）可以维护规定这些要求的规则集。交易机构700（A）可以：

●以“循环（round robin）”的方式向每个用户100（A）、100（A）（3）和100（A）（5）发送等待批准的备忘录（在安全容器中）。

●如果这些用户中有一个人修改了备忘录，交易机构700（A）就会将修改过的备忘录给另外两个用户传阅，让他们再作评论和修改。

●一旦三个用户100（A）（1）、100（A）（3）和100（A）（5）都批准了备忘录，交易机构700（A）就有权将他们每个人的数字和/或手写签名或签名缩写加在备忘录中，将它置于一个或多个带有控制集的安全容器中，控制集表明它是只读的，只有用户100（A）（2），100（A）（7）－100（A）（10）和100（A）（12）才能阅读它。

●接下来，交易机构700（A）就可以在容器中将备忘录的一份副本发送给这些用户中的每一个人，或者要求将同一个容器从一个人传阅到另一个人。

●交易机构700可能需要电子控制来维护安全的查账索引，该索引表明容器到过哪里、谁打开过它、谁访问了它所保护的备忘录、以及是什么时候访问的。这样，交易机构700（A）就可以通过证明特定的某个人是否访问过特定的文档、什么时候访问的、以及访问了多长时间，来提高个人的可统计性。

组织A的Intranet 5104还可用于交换和/或分布高度机密的设计说明书。例如，交易机构700（A）可以维护表示谁已经在设计说明书上签字的数字形式的详细记录－这样，确保个人的可统计性并提高高度的效率。

如上所述，专用交易机构700（A）、700（B）还可以提供“防火墙”功能，防止机密信息泄露到组织A、B的外部。例如，假设组织A是一家集成电路设计室，组织B是一家集成电路制造厂。组织A设计并规定芯片电路的布线图案，做成“磁带输出”并发送给组织B。组织B按照“磁带输出”制造集成电路，并向组织A交付芯片。

交易机构700可用于为上面的商业交易提供便利，同时保护每个组织A和B的机密。例如：

●组织A的专用交易机构700（A）可监管组织A的整个设计及规范开发的效果。为保守机密，所有通信都是通过组织A的Intranet 5100（A），在安全容器302中发生的。交易机构700（A）可以维护过去的设计文档、正在进行的工作、以及作为设计过程进展情况的规格版本的档案。

●组织A的专用交易机构700（A）可以管理最终设计规格的开发－确保完成设计规格所需的所有条件都得到遵守。

●一旦设计规格最终完成，交易机构700（A）就可以在安全容器152中将它传阅给组织A中需要在上面“签字”的那些人。各个电器100（AA）（1），…，100（A）（K）可以附加和/或嵌入上述的数字签名，手写签名、印章和/或指纹，表明特定的批准。

●组织B的专用交易机构700（B）可以通过组织B的Intranet 5100（B），自动地将设计规格的一份副本发给组织B内的适当用户100（B）（1），100（B）（N）。组织B外面的任何人都知道谁收到了的规格的副本。另一方面，如果需要的话，组织A的交易机构700（A）可以包括限制访问的电子控制集，只限于访问组织B内的某些工程师－这些安全控制将随电器100（B）（1），…，100（B）（N）一起带入组织B并有这些电器安全地执行。

组织B的交易机构700（B）可以管理芯片的制造过程，保证根据组织A的设计规格制造芯片所要求的所有步骤和条件都得到了遵守。

实例：交易机构可以推动国际贸易

图67示出了怎样利用交易机构700从事国际贸易的实例。在这个具体的实例中，交易机构700协调位于它们各自国家（如美国、澳大利亚和欧洲）的公司1106A、1106B和1106C之间复杂的多国交易。公司1106A有自己的银行1108A和律师1110A。类似地，公司1106B有自己的银行1108B和律师1110B，公司1106C有自己的银行1108C和律师1110C。

交易机构700通过在安全容器中来回传递出价和还价，并使用上述的合同形成技术制定部分或全部条款并提供不可否认性，协助在跨国的各方之间达成协议。一旦形成合同，交易机构700就可维护规则和控制的主集，规定完成交易所必须满足的全部条件－由此，必须为不同的事件提供结论。或者，合同一旦开始执行，交易机构就不起实际作用了，特别是在简单的模型中，也就是说，VDE容器可以携带价值链规则和控制，这些规则和控制从总体上规定了必须满足的过程和条件，包括它们的操作顺序。交易机构700提供的规则和控制可以将国际法考虑在内－不同的规则适用于不同的国家。这些规则可以将各种进出口要求和限制、国与国之间的国际税收协定考虑在内，包含与

提前支付和/或进行中的关税有关的路由和归档要求，识别规范的货币交易机构，协助相关的国家和国际机构将合同或某些合同条款归档，管理任何发货或其它运输要求，协助建立规范的合同条款翻译服务（特别是标准术语和条件），管理国际认证机构的要求和格式的差异，施加适用的管理团体要求的社会规范，以及收取适用的管理团体税收，如国家和地区政府实体的税收等。交易机构700可以利用安全电子容器在国际各方之间通信，并可安全地使国际各方提供的各种事件通知生效并加以验证。

实例：分布式的交易机构

交易机构700控制下的复杂的商业交易也可以分布在组织和/或辖区内部或它们之间。假设一个复杂的国际房地产交易要求买卖公司、数个金融机构、保险公司、法律事务所、或许还有几个国家的管理机关它们当中好几个职能部门的参与。进一步假设交易的各组织和个人方都有具备VDE功能的计算机，而且每个组织或机构中至少有一个分布式的交易机构，该交易机构在按主交易机构700批准的权力，为该房地产交易服务。

在这一个实例中，房地产交易的每一方都以VDE规则和控制的形式，提出了代表它们的商业关系的商业规则和参数，这些规则和控制规定了每一方在整个交易中所起的作用。例如，保险公司必须以购买者认为可以接受并且得到抵押贷款人同意的价值和费用给财产保险。此外，假设已经利用Ginter等人的申请书所描述的协商机制相互认可了这些交易的VDE规则和控制，并且协商的规则和控制已经与协商这些规则和控制的历史一起，被储存在该房地产交易的主交易机构中。最高级的交易机构可以是主交易机构700或任何相互认可的分布式交易机构。在这一个实例中，我们假设是前者。简而言之，所有各方都同意管理交易的规则和控制。因为交易机构700可能已经为国际房地产销售分布了分布式的模板应用程序，因此协商过程可能已经简化，该模板是以交易机构700过去的经验为基础，或者是交易机构700为该交易专门创建的，以此作为向其重要客户提供的增值服务。

按照规定该基本交易的VDE规则和控制，交易的每一方都有责任留意必须在终止和完成整个交易之前结束某段交易。在有些情况下，由多个参与方共同负责完成总交易的一部分。例如，买方和卖方必须

在购买价格上达成一致．在该实例中，它们提出了自己的商业要求，例如，包括它们的价格和其它变动，它们并且利用VDE协商机制，达成利益比较平衡的协议．如果电子协商不成功，各方可直接协商，或者将带有表明协商失败的审核记录的VDE安全容器发送给交易机构，由它通知授权参与整个交易的其它各方中的每一方。

在该实例中，如果买方和卖方真的达成了一致，完成协商（或通过使用VDE技术，收取有双方数字签名的协商完成指令）的VDE受保护的处理环境将通知发送给分布式的交易机构，由交易机构再通知包括其它参与的交易机构在内的其它方，已经在价格上达成了一致。根据子交易的VDE控制，VDE可以安全通知一方或多个参与方，其它某些交易现在已经完成了．在该实例中，标题搜索公司现在就可以执行它们的任务了；保险公司现在可以利用VDE协商机制，与买方协商承保范围。买方法律顾问办公室的律师可以和卖方公司的同行协商；在制定和协商完成部分或整个交易的各种文档的过程中，两家公司的律师都可以使用VDE和VDE安全容器和外面的法律顾问打交道。

在该实例中，每一方都有认证机构500颁发的一个或多个数字凭证，用来验证参与该交易及其子交易的每一方。金融结算所200为各个增值服务提供支付手段，在一个实例中，这些服务是由交易机构700提供的。使用结算所300收集每个参与的VDE受保护的处理环境在VDE安全容器中不时发出的审核记录，并为这些交易提供独立的第三方审核。安全目录服务600在保持机密和隐私的同时，帮助参与者寻找其它各个参与者的电子地址。

在每个子交易完成之后，子交易就在其中完成的组织内的一个分布式交易机构通知该交易的主交易机构700子任务已经完成。根据以前达成的VDE规则和控制，部分或所有参与此项交易的个人都会得到从至少一个参与者的VDE受保护处理环境发出和验证的审核记录和/或消息，例如，个人节点处的PPE、分布式商务公共事业系统、分布式交易机构、以及/或者该交易的主交易机构。

当总交易的所有组成单元都完成以后，一个交易机构，在该实例中就是房地产销售的主交易机构，会通知每个参与者和每个参与的分布式交易机构，前提条件已经全部满足，并清算整个交易。或者，交易机构可以给予卖方和买方最后一次机会，让它们决定是继续完成还

是搁置交易．这一个实例表明，包括交易机构700在内的商务公共事业系统90，可以被分布在支持一个或多个商务公共事业系统90的中间VDE受保护的处理环境中。

实例：数字广播网

让许多用户分期偿还架构和其它资源，比竞争者更快地建立临界批量、支持专业化以适应并向消费者交付最具吸引力的产品和服务、充分发挥购买协商的杠杆效力、以及建立最全面的架构，作为一定商业活动的最佳“一站”资源－这些全都是建立成功的现代商业的核心思想。VDE和分布式商务公共事业为创建极有竞争力和成功的电脑空间商业奠定了基石，这些商业体现了这些属性。这些商业中许多反映了Internet和WWW网的特点。象VDE和分布式商务公共事业一样，它们也包含分布式的社区，该社区通过支持电子商务的合作关系来充分发挥优势。它们将提供不同层次的服务和补充性的产品及服务，并在协调它们的活动使双方受益方面极具优势。

数字广播网（“DBN”）就是这样一个独创性的商业企业。DBN的参与者由基于WWW网（“Web”）的许多不同的站点和服务组成，它们通过共享资源、经历最大的购买力、生成营销和消费者的信息、以及支持将许多经常互补的活动捆绑在一起的合理的管理覆盖，获得更好的平衡和运作效率．与相容的规则非常相似（这些规则和控制使WWW网和VDE及分布式商务公共事业的设计成为可能并成为它们的基础），而且位于这两个架构的能力上层，数字广播网采用它们的发明来支持高效、高度自动化、和分布式的社区，充分发挥商业效率。其它实例以类似的方式包括其它实体的组合，共同实现虚拟企业（如公司或其它组织）的功能．VDE和商务公共事业系统的分布性的本质，对为这些现代的、潜在性大规模的、电脑空间的商业活动提供有效的架构来说非常重要。

数字广播网可以作为Web站点和服务提供者两者的综合，有一个中央、或许是地区性的逻辑（如以市场为依据）总部群体，或者，可作为一个盈利性股份制的公司，其商业模式使人联想到电视广播公司（如NBC），或者可作为合营的或虚拟的公司，该公司具有上述属性的某种混合或混合属性的综合，并采用分布式、对等、分级、以及集中式管理的商业关系和活动。在一个实例中，若干公司可以联合在一起

提供规模和配合的优势，各参与者提供一定程度的专业特长，实体组织则在“更高级”的合营或公司内以某种形式一起协调。

在一个实例中，数字广播网可以是一家有许多获得许可的联营单位的公司。得到许可的联营单位可包括WEB站点，专门为地理和/或逻辑上的市场区域服务，以及/或者在所述的分布式商务公共事业服务的分级和/或对等的环境中为其它Web站点服务。该公司可代表它自己及其联营单位:

●与广告客户和它们的广告代理协商播放时段的最合理的收费，

●以最低的成本获得第三方提供的内容，

●转售市场分析和用户群情况的信息，

●与它的联营单位分享收益，其联营单位又与DBN和/或其它联营单位分享收益，

●根据联营单位和/或联营单位用户的基本情况，向联营单位提供广告，

●保证有相当数量的人观看（曝光和/或其它交互）广告客户的材料，

●提供采用VDE和分布式商务公共事业能力的安全虚拟网络，包括使用公共的用户应用工具、界面以及管理操作，使整个组织能够安全高效地运作。

●为网络提供对网络和联营单位有利的广告，

●根据联营单位的请求和/或使用情况表明的需要，向联营单位购买和/或提供内容，

●按照它与联营单位的协议，收集分析内容的使用情况、电脑空间的购买以及其它数据，

●允许联营单位在本地执行许多网络功能－就是说，获得和利用地理上和/或逻辑上位于本地（与那里的目标一致）的内容（和/或其用户群特别感兴趣的其它内容），

●协商关于广告材料的协议，这些材料对联营单位物理和/或逻辑市场的目标有商业价值，

●按照协议，用其余的控制至少控制它的部分Web“广播”空间－就是说至少对部分内容加以控制－并且在DBN和/或其它某个或某几个参与者的控制下，由规则和控制执行，

●代表和/或为网络执行其它管理、支持和/或服务功能.

例如，DBN可以利用VDE的许多安全和管理能力以及本发明所提供的服务功能，管理并使作为DBN商业模式核心的分布式的关系和活动自动化．例如：

●交易机构700可以为网络社区的管理提供整个管理环境．例如，交易机构700可以管理（通过使用优选实施方案中的VDE规则和控制）发给适当联营单位的内容的路由．它还可以管理与报告使用信息有关的处理链和控制．交易机构700可从DBN与其联营单位之间的协议关系获得和/或得到其电子控制集。可以使用电子协商来创建这些协议关系。交易机构700还可以接收直接反映联营单位和其它参与者中间的双边或其它联网关系的控制。

●权利及许可结算所400可以将与内容有关的商业权利扩展到网络联营单位。它起着与网络实体向消费者提供的内容有关的权利储存库的作用－包括网络实体自身持有的内容权利，并使之为其它网络实体所利用。这样的内容权利可包括，例如，显示、出售、再分布、再定向、以及做广告。它可以根据请求和/或以使用为依据的自动形成的情况信息提供另外的权利（如再分布权利或专门的再定向权利）。

●使用结算所300可以收集使用信息，以支持市场分析、用户情况、以及广告。它还可以分析信息并得出报告。它可以将这些内部分布给适当的DBN，并按照商业机会向外销售报告和/或其它基于使用的信息。

●金融结算所200可保证在整个网络中履行合理的补偿.它可以收取联营单位因内容而欠DBN的支付。它可以向联营单位分布它们做广告和销售使用信息应得的支付。它可以从联营单位收取支付，以支持DBN架构和网络广告等服务。它联在通用金融结算所的架构上，以便收发与支付有关的信息。

●安全目录服务600可以维护以唯一身份和/或类别属性为基础的目录服务。在全球可能会有数量庞大的联营单位。目录服务600还可以维护消费者的目录信息，包括唯一的标识符和情况信息．安全目录服务600可以维护网络所拥有、管理和/或利用的内容的目录架构．

●认证机构500可以证明网络中所有参与者的作用．例如，它将给每个联营单位颁发一个凭证。它还可以颁发证实分组网络实体的商业

关系的凭证，以便为安全、高效地与第三方打交道提供便利．它还可以向消费者颁发证书，代表关于消费者与外界各方之间商业活动的一定的专门的消费者权利（例如，折扣、或成为更大的“DBN”社区的一员）．

部分或全部服务功能（例如上面所述的）可以是高度分布的，并且可以主要地、基本地甚至完全只在联营单位和服务网络的Web服务器上运行．

尽管结合目前认为是最实际、最优选的实施方案对本发明进行了说明，应当懂得，本发明并不限于已公开的实施方案，相反，应扩展为涵盖所附权利要求的思想和范围内所包括的各种修改和相应的安排。

说 明 书 附 图

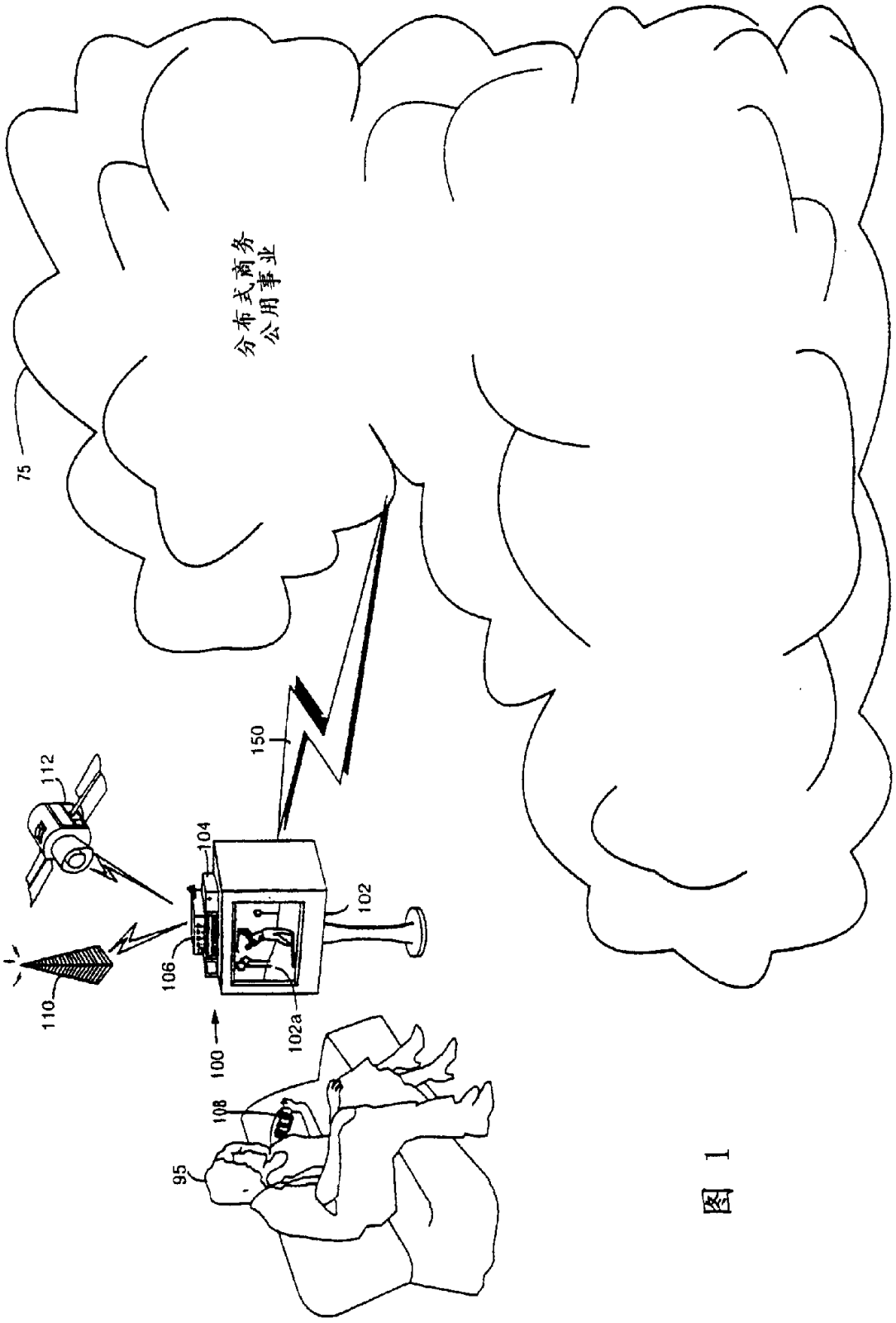


图 1

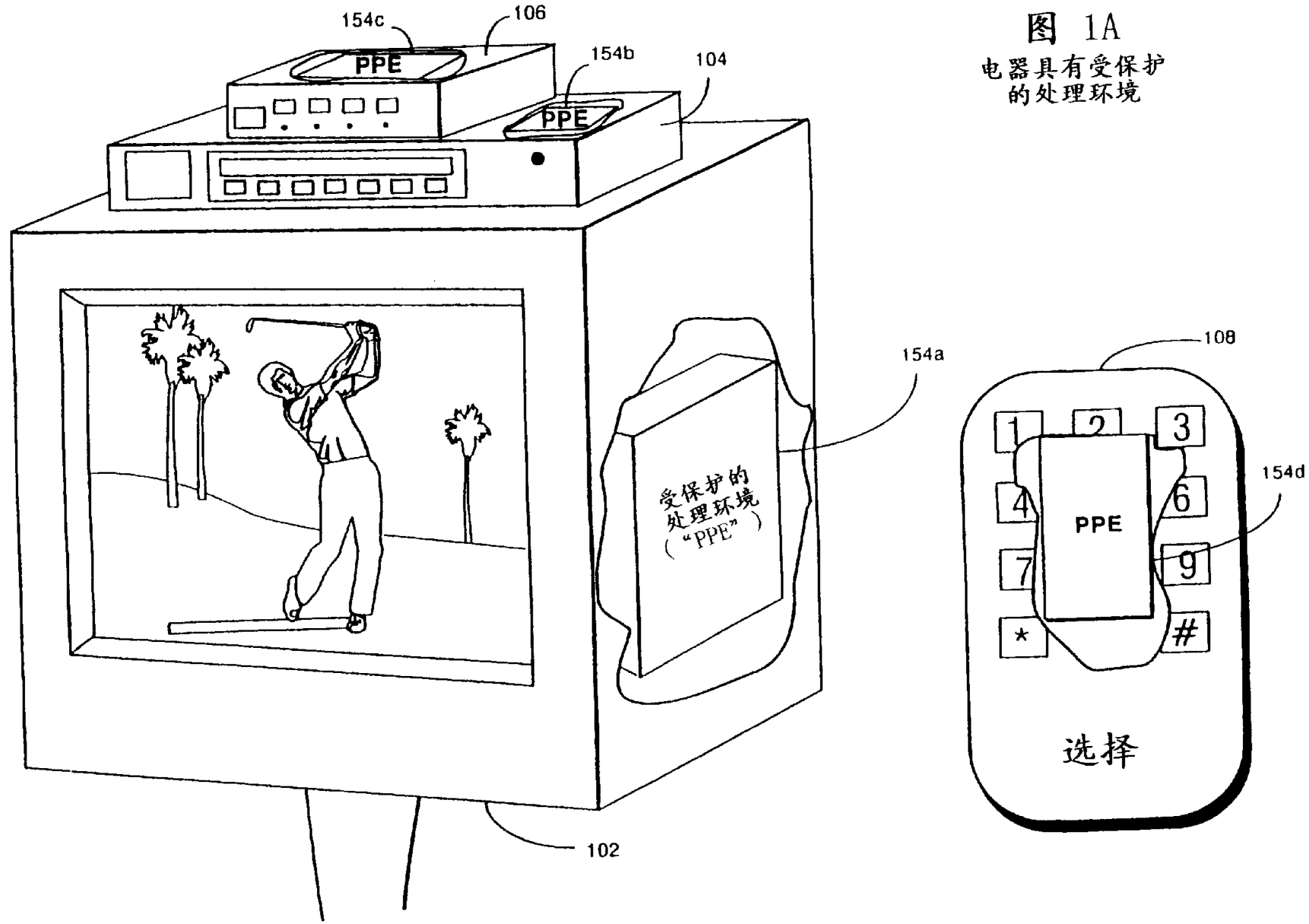


图 1A

电器具有受保护的处理环境

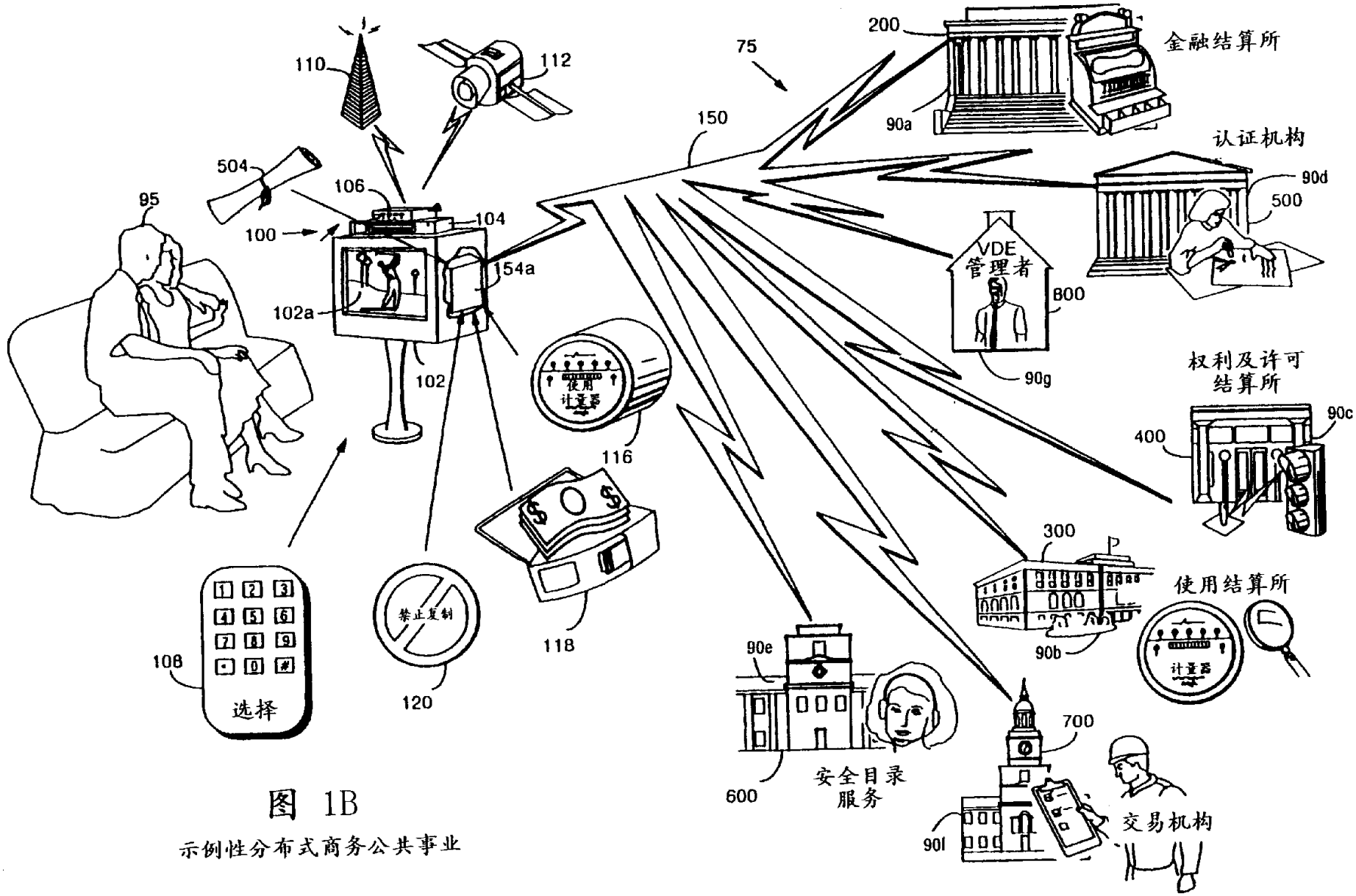


图 1B

示例性分布式商务公共事业

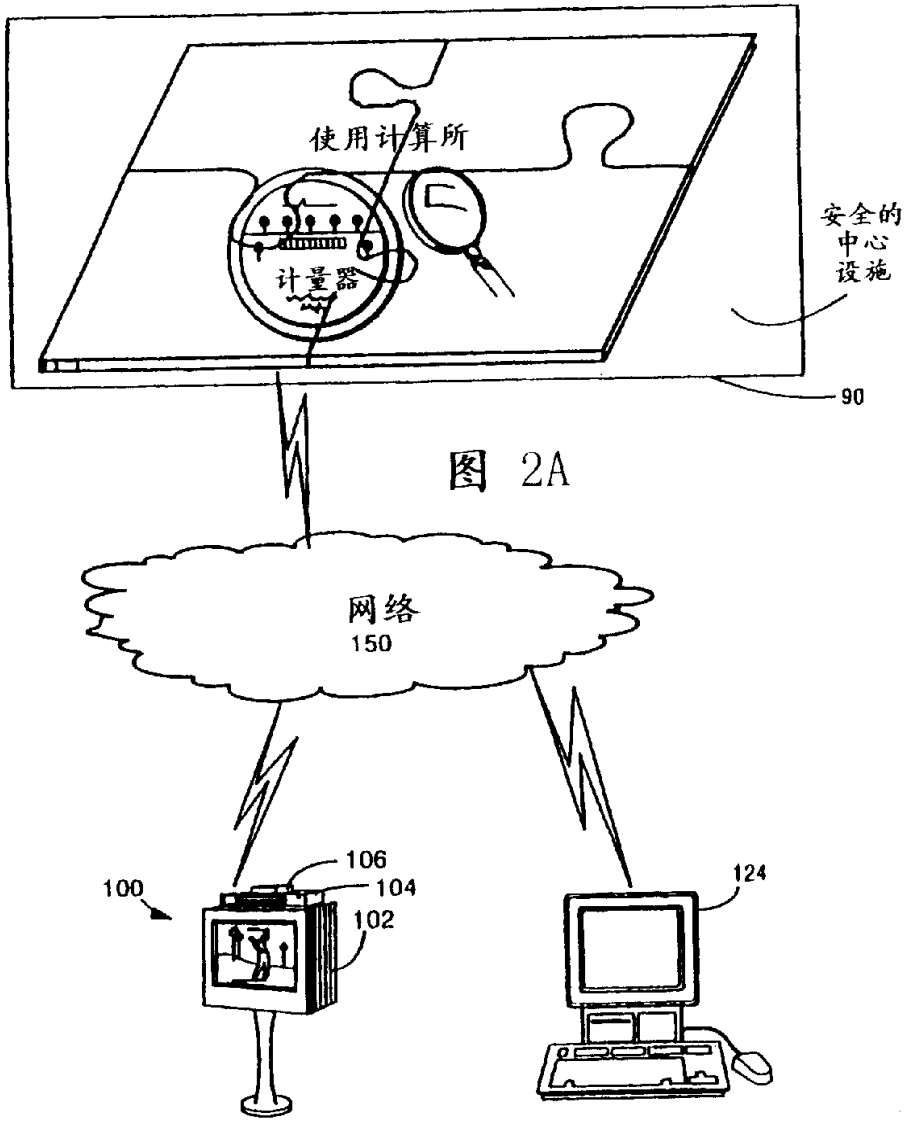

使用计算所
计量器
安全的
中心
设施
90
网络
150
100
106
104
102
124

图 2A

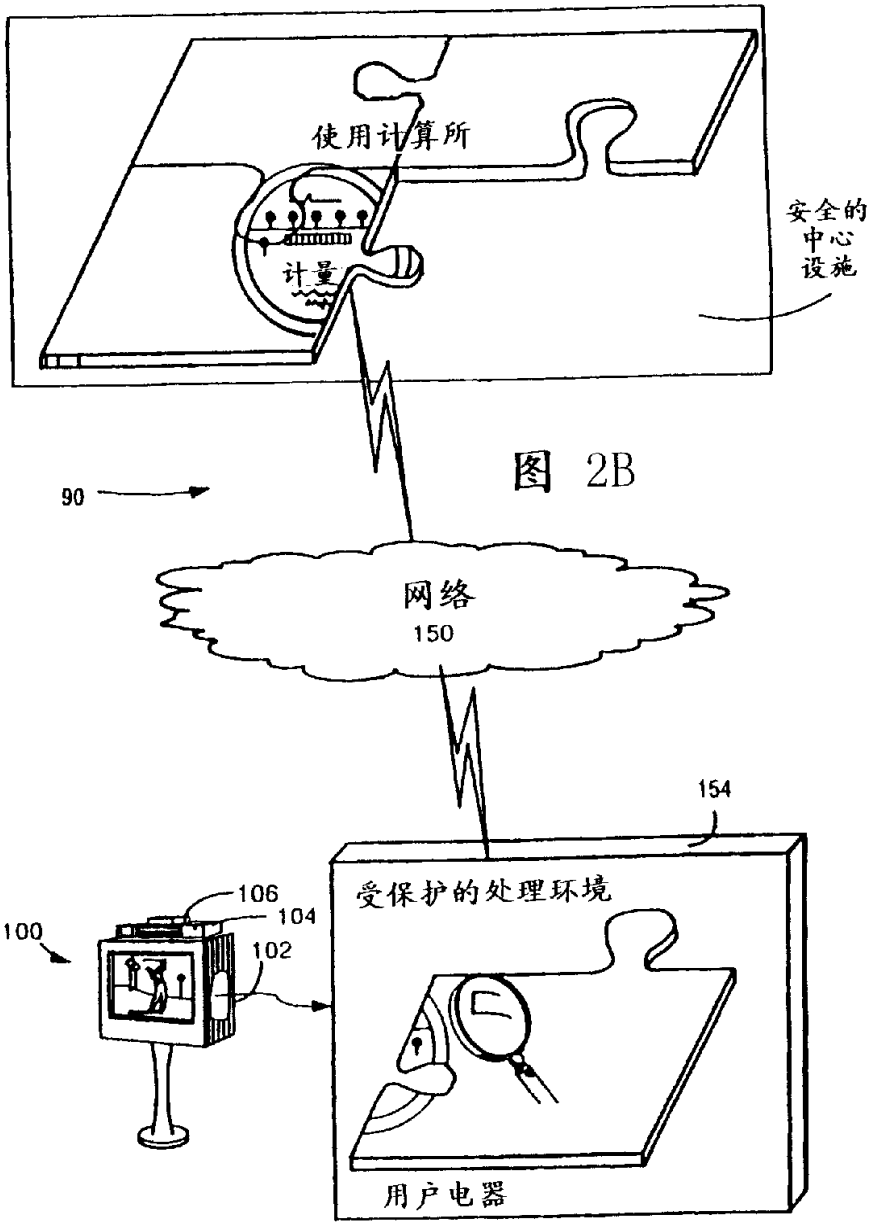

使用计算所
计量
安全的
中心
设施
90
网络
150
154
受保护的处理环境
100
106
104
102
用户电器

图 2B

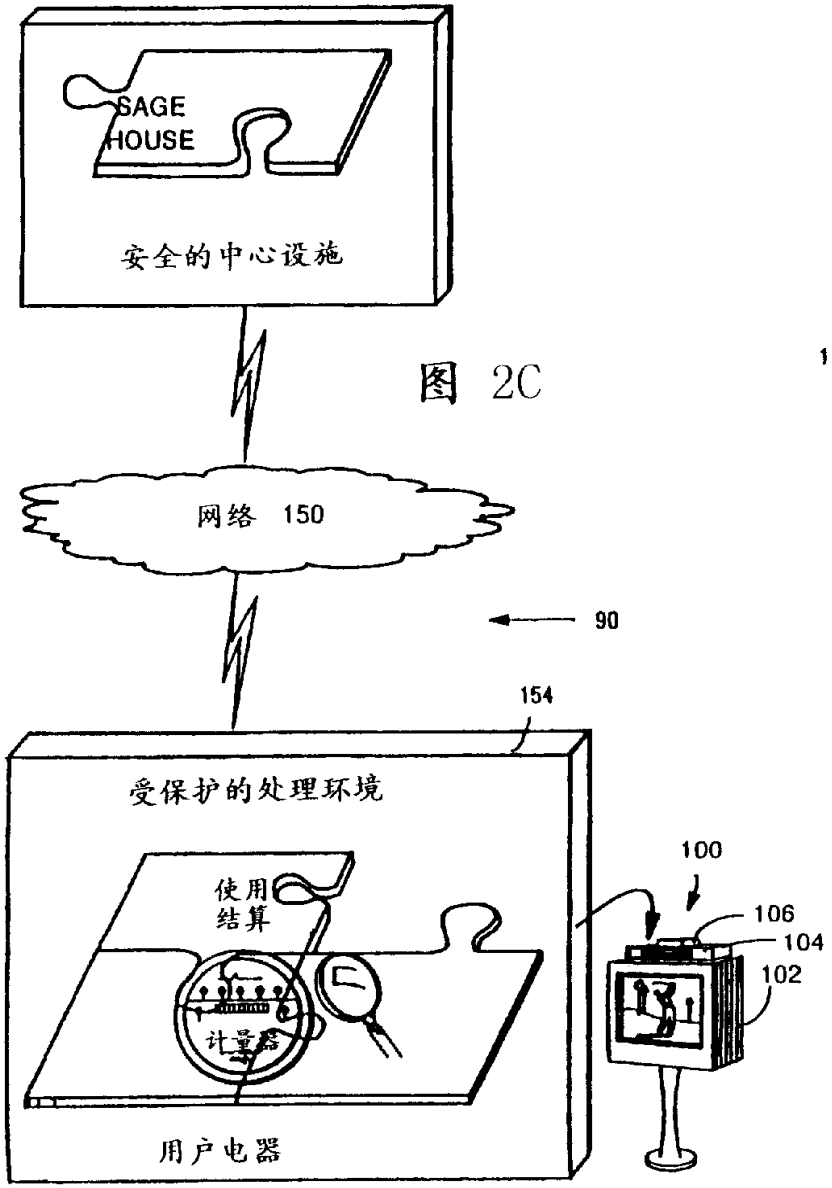

SAGE
HOUSE
安全的中心设施
网络 150
90
154
受保护的处理环境
使用
结算
计量器
用户电器
100
106
104
102

图 2C

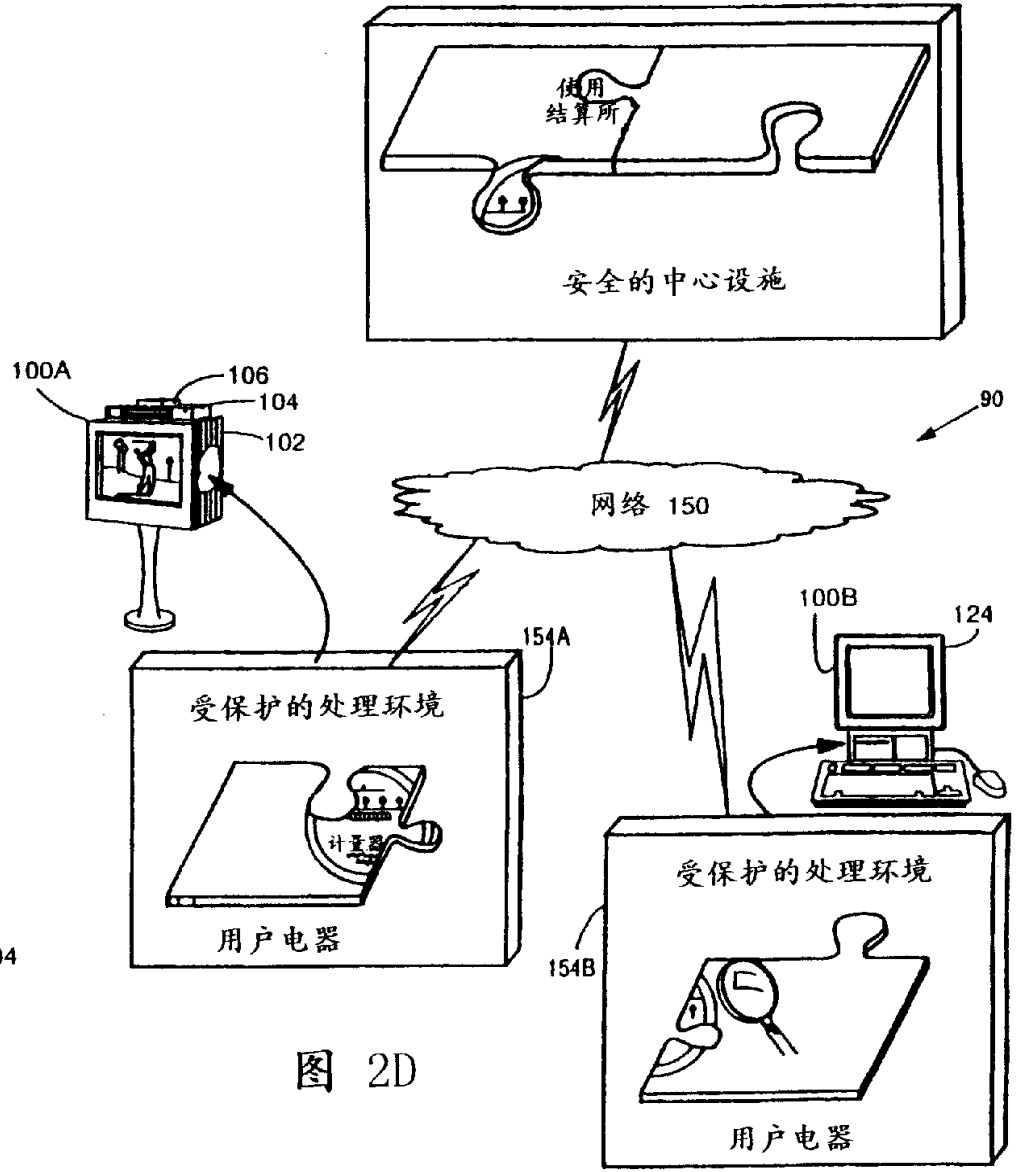

使用
结算所
安全的中心设施
100A
106
104
102
90
网络 150
154A
受保护的处理环境
计量器
用户电器
100B
124
受保护的处理环境
154B
用户电器

图 2D

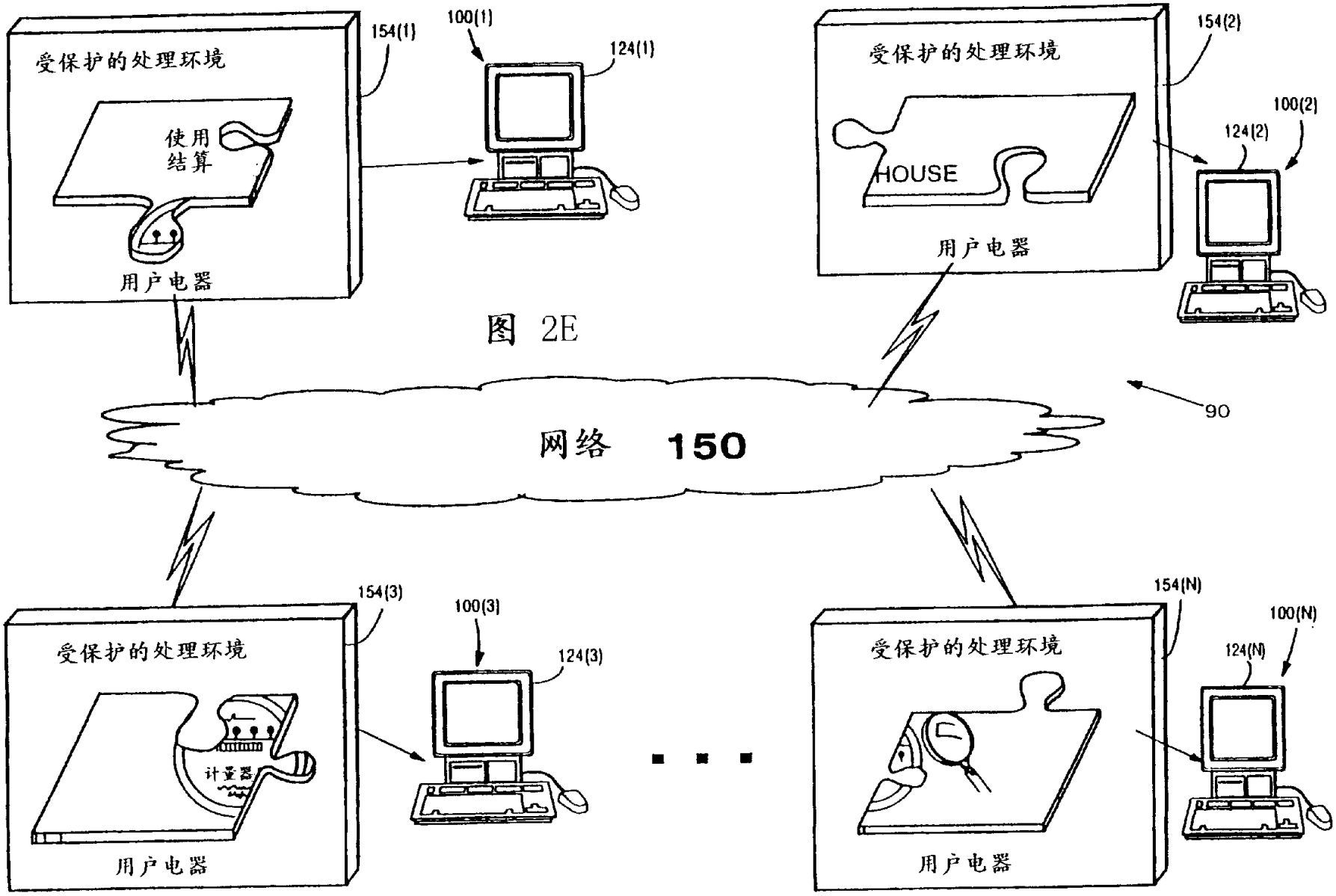

受保护的处理环境
使用
结算
用户电器
154(1)
100(1)
124(1)
受保护的处理环境
HOUSE
用户电器
154(2)
100(2)
124(2)
网络 150
90
受保护的处理环境
计量器
用户电器
154(3)
100(3)
124(3)
受保护的处理环境
用户电器
154(N)
100(N)
124(N)

图 2E

图 3A

分布式商务公共事业系统

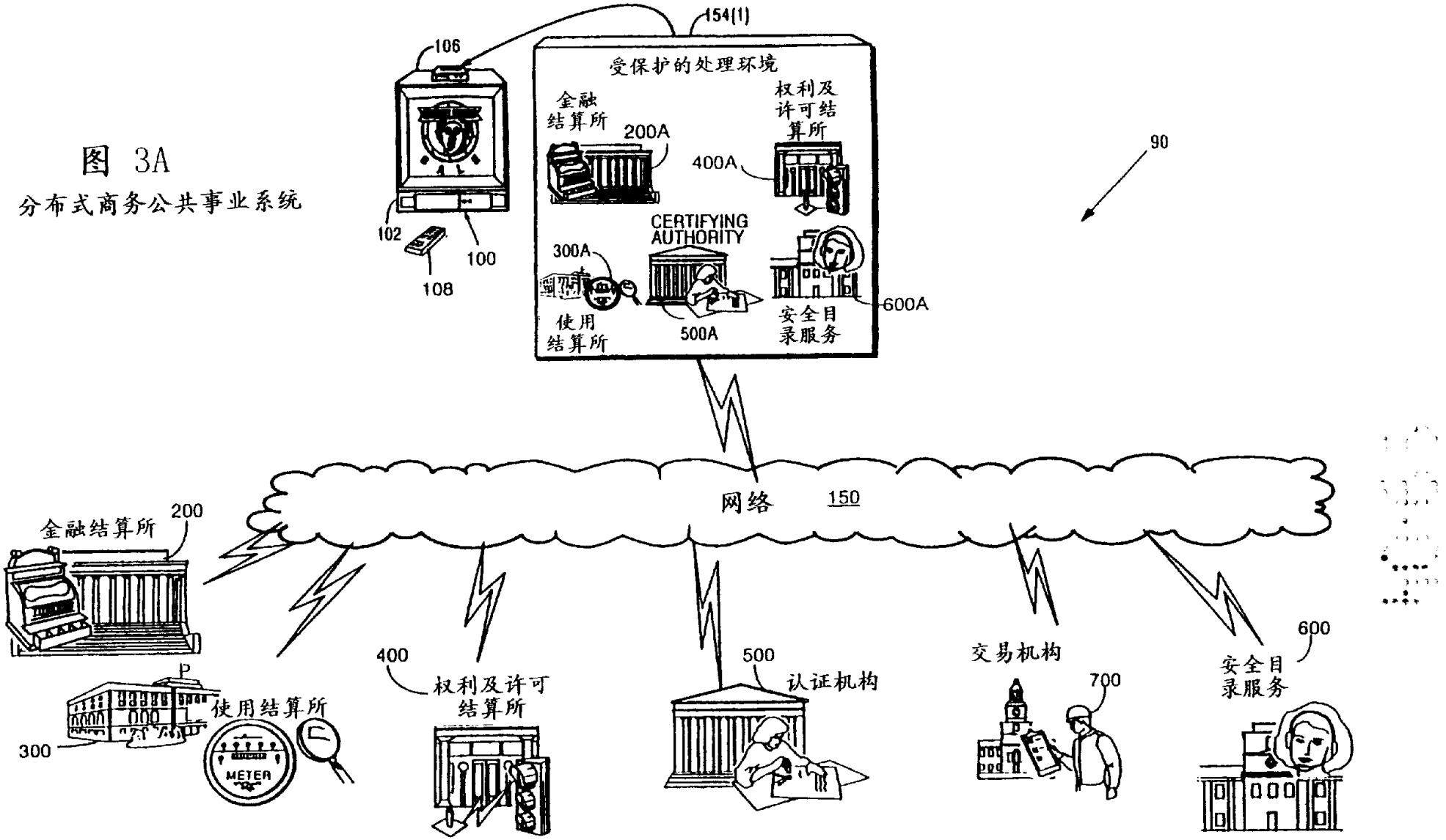


图 3B

分布式商务公共事业系统

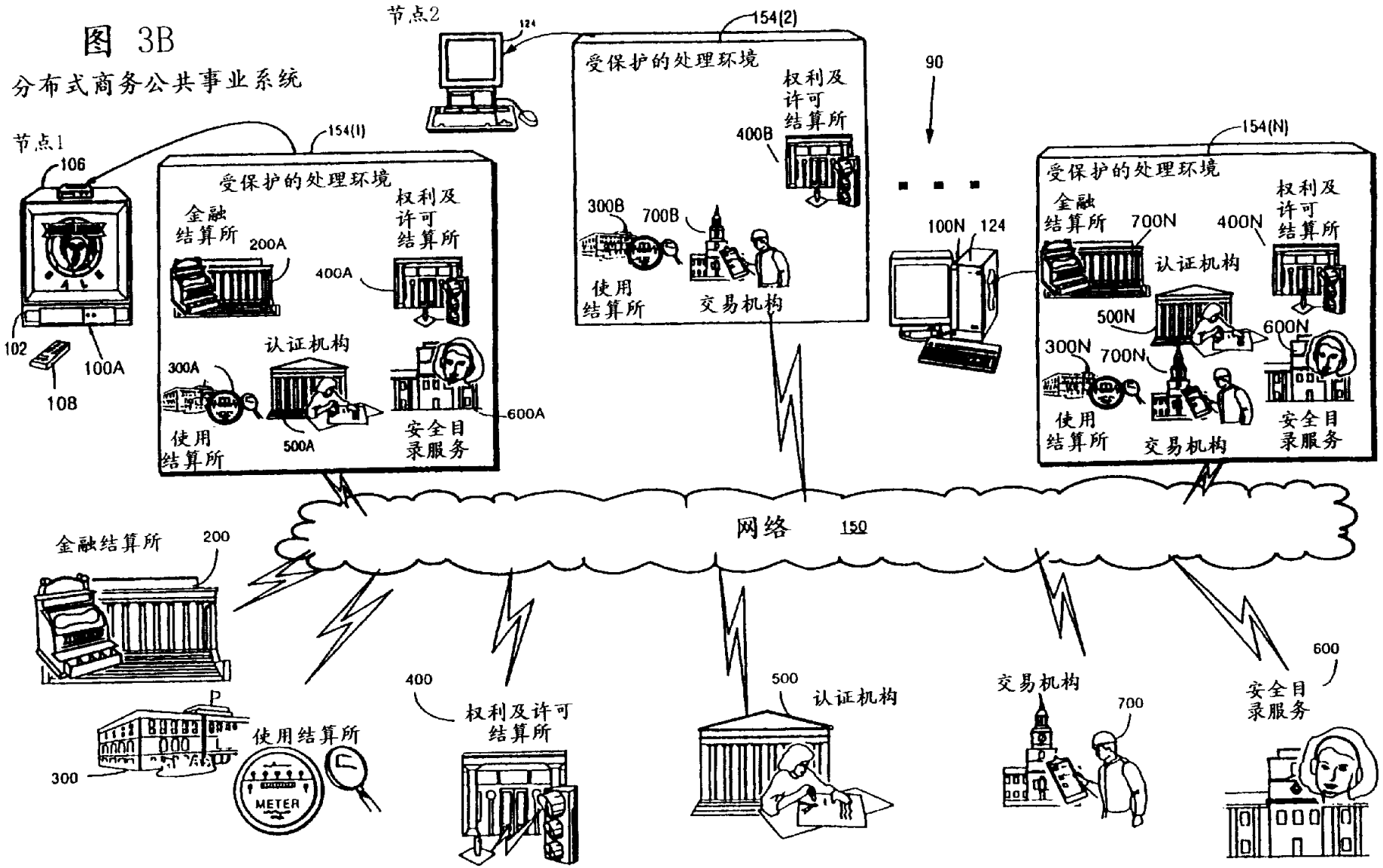


图 3C

分布式商务公共事业系统

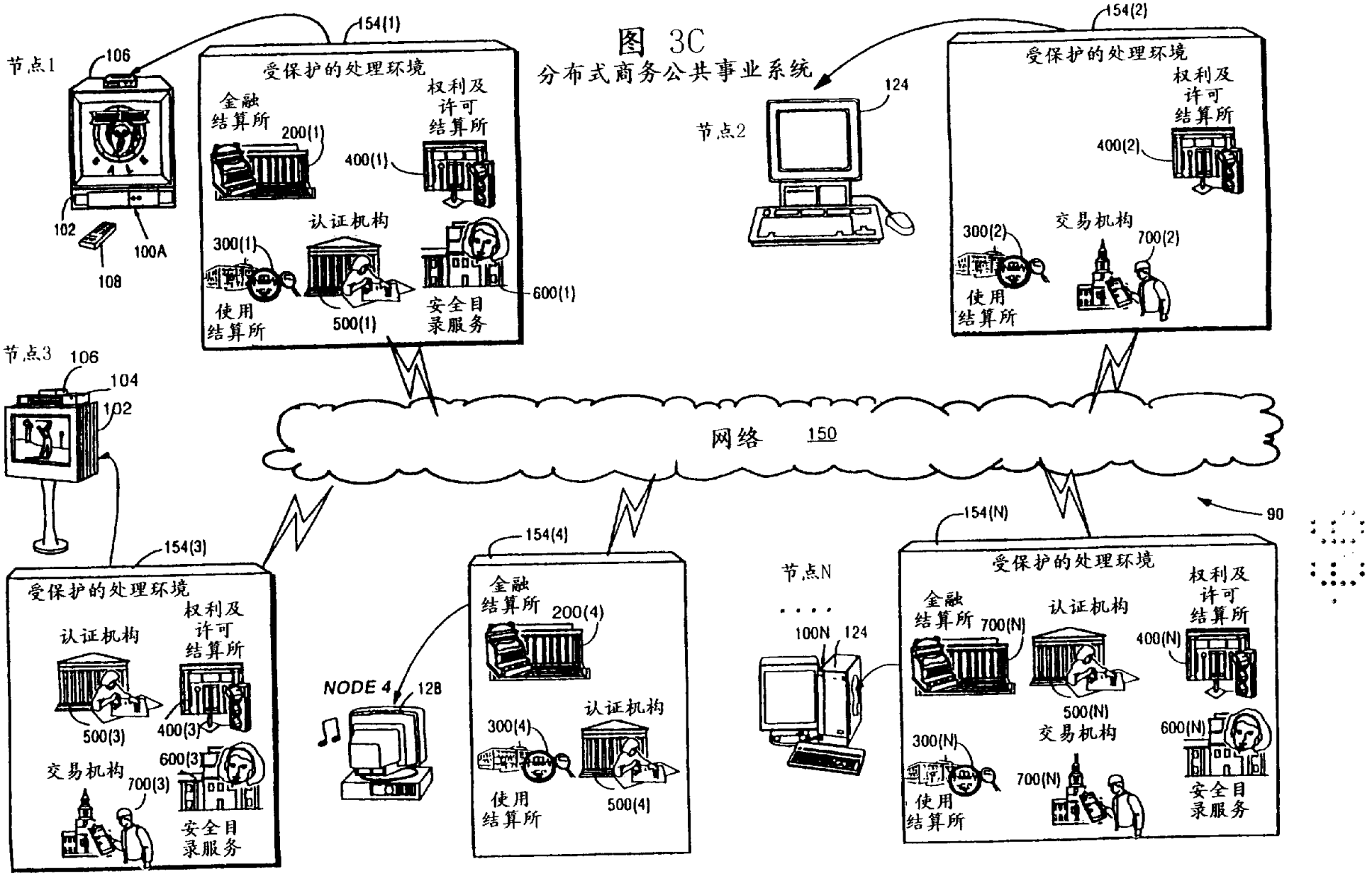
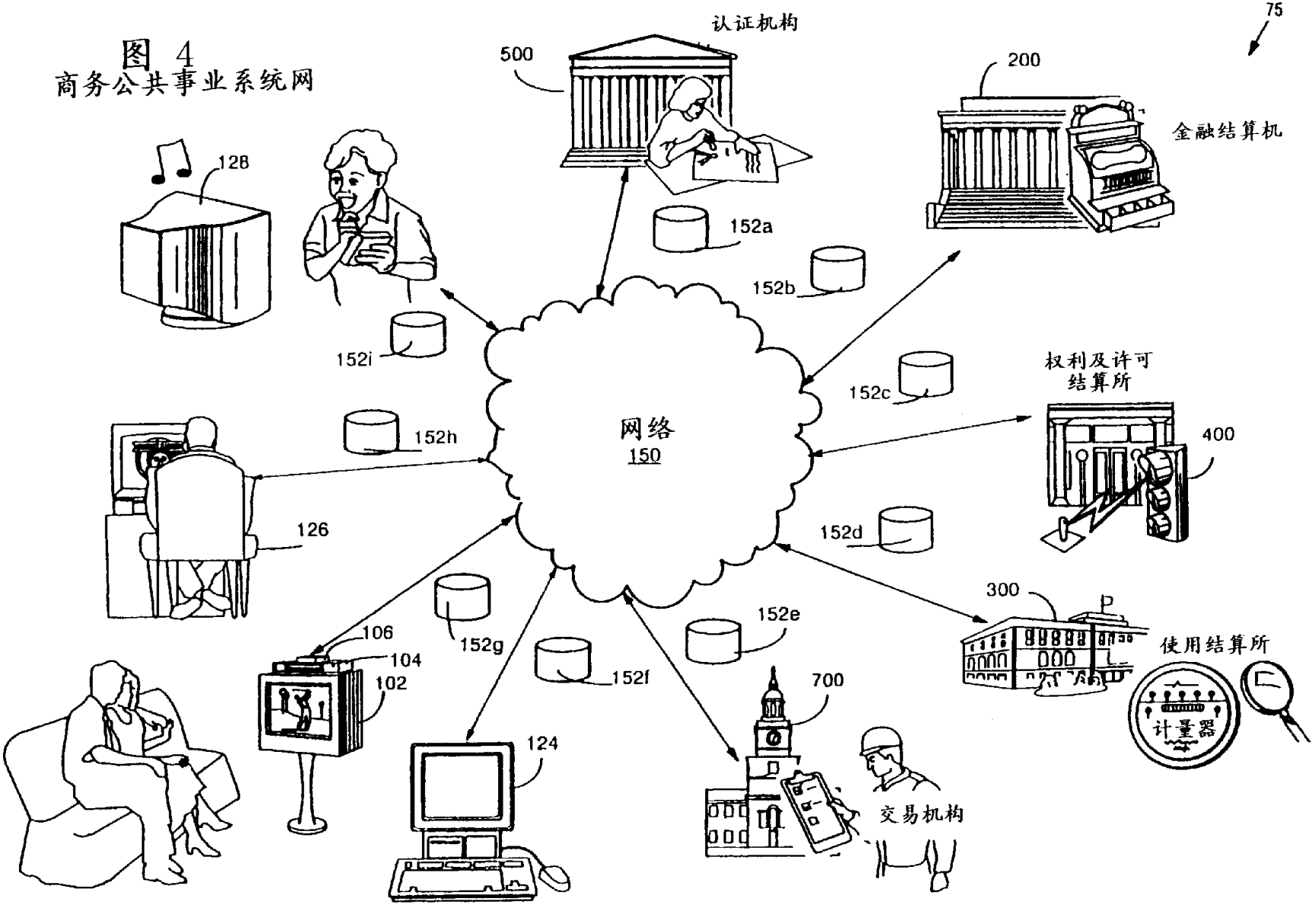


图 4
商务公共事业系统网



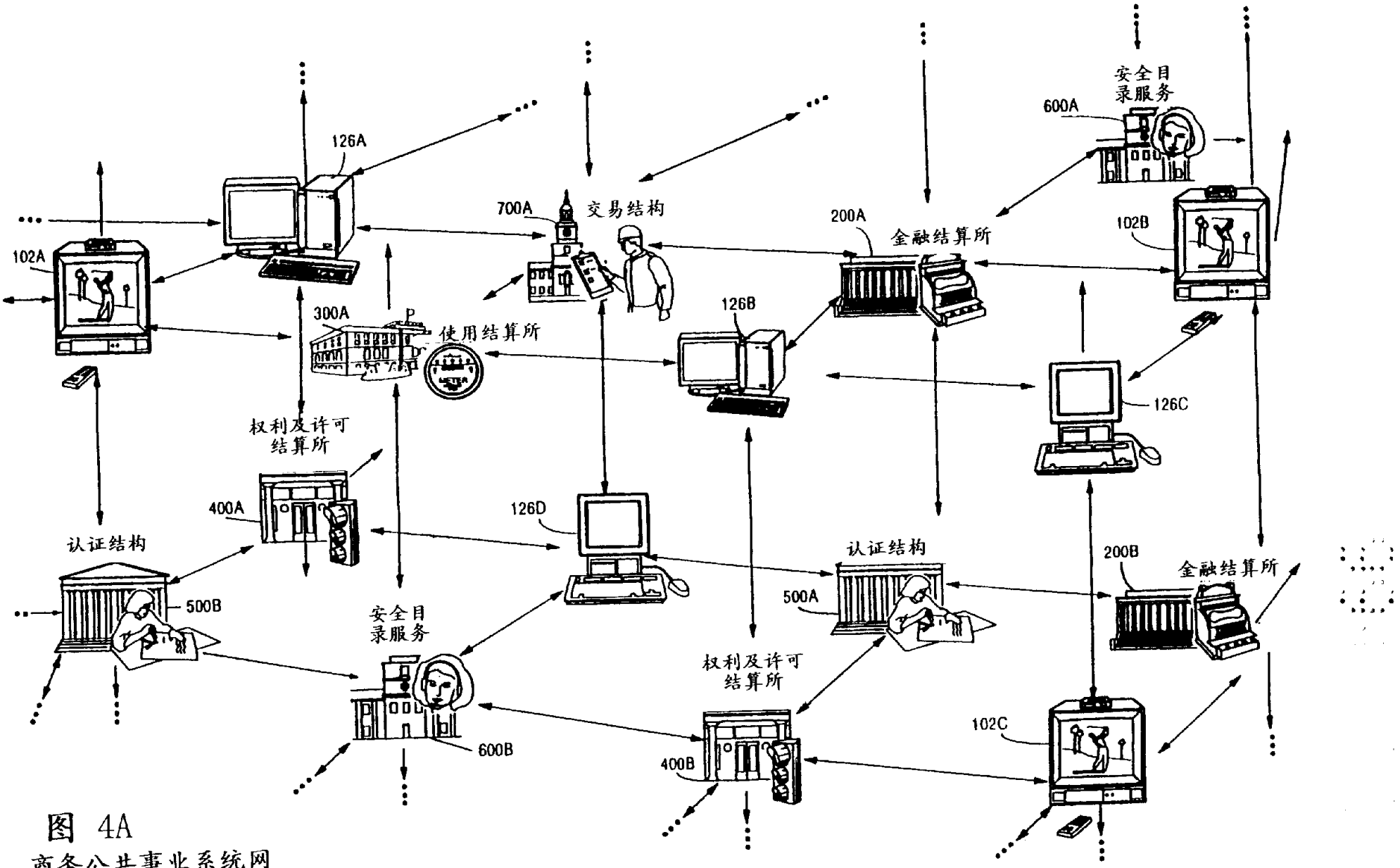


图 4A

商务公共事业系统网

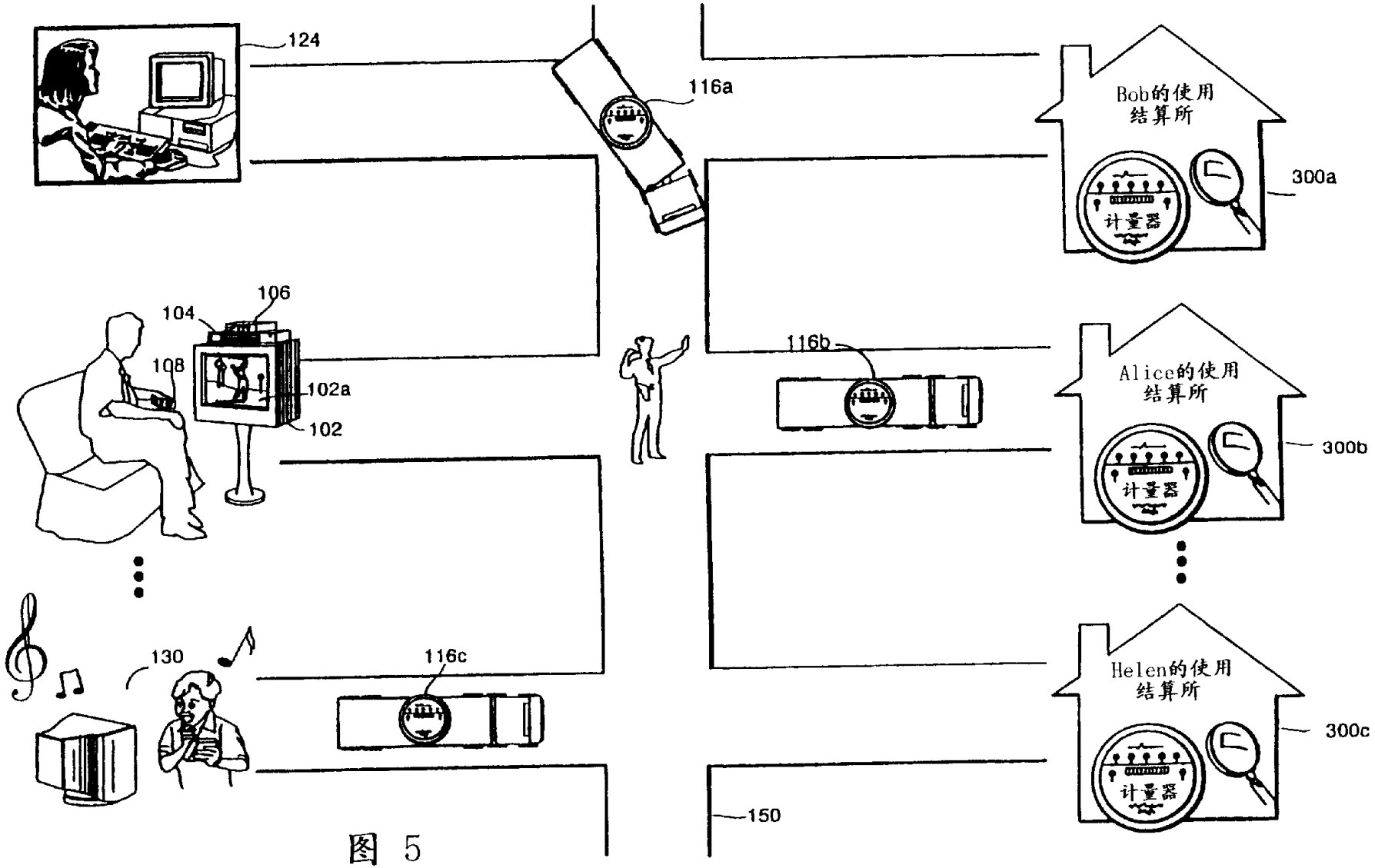
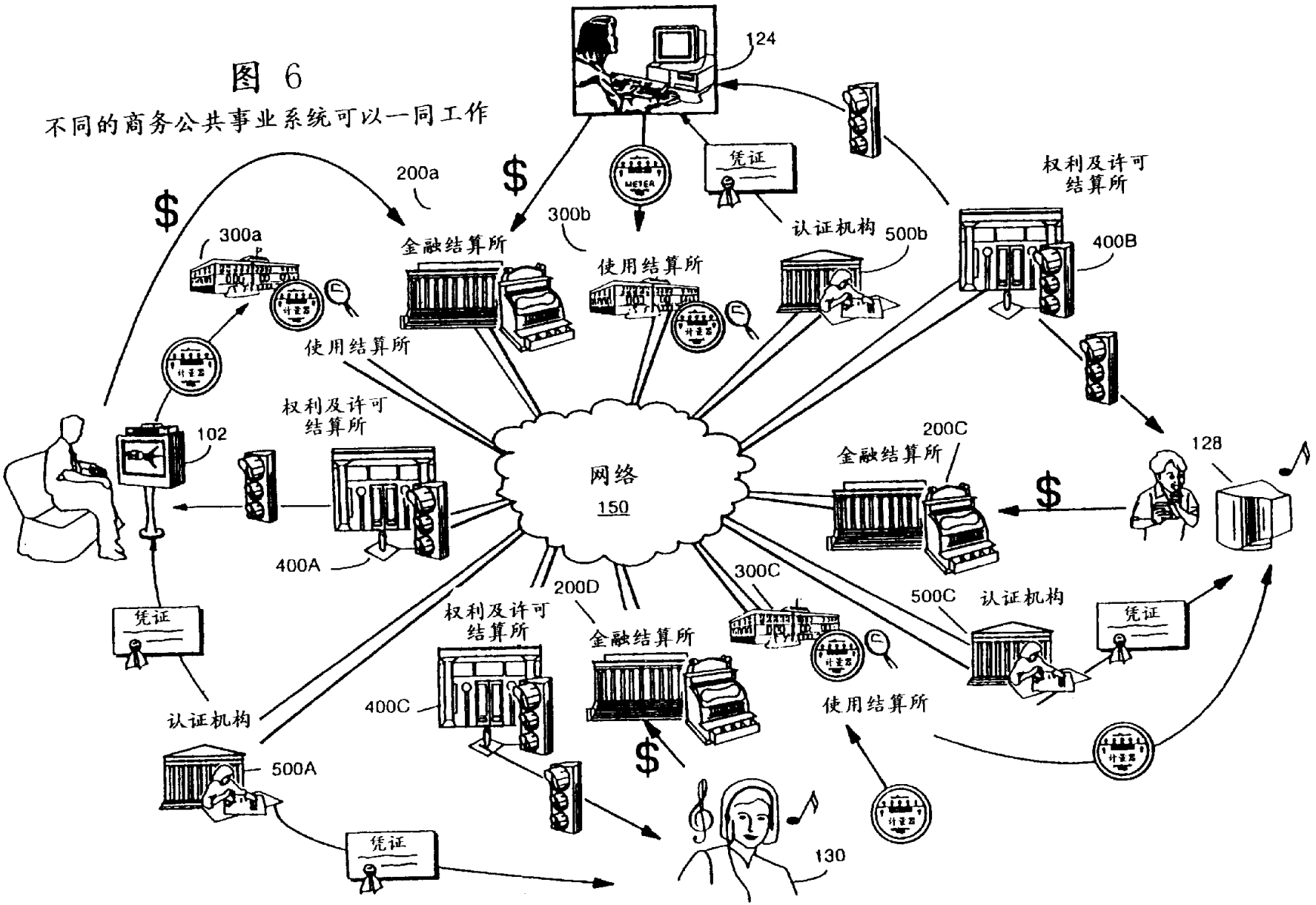


图 5

权利拥有者可以在商务公共事业系统之间选择

图 6

不同的商务公共事业系统可以一同工作



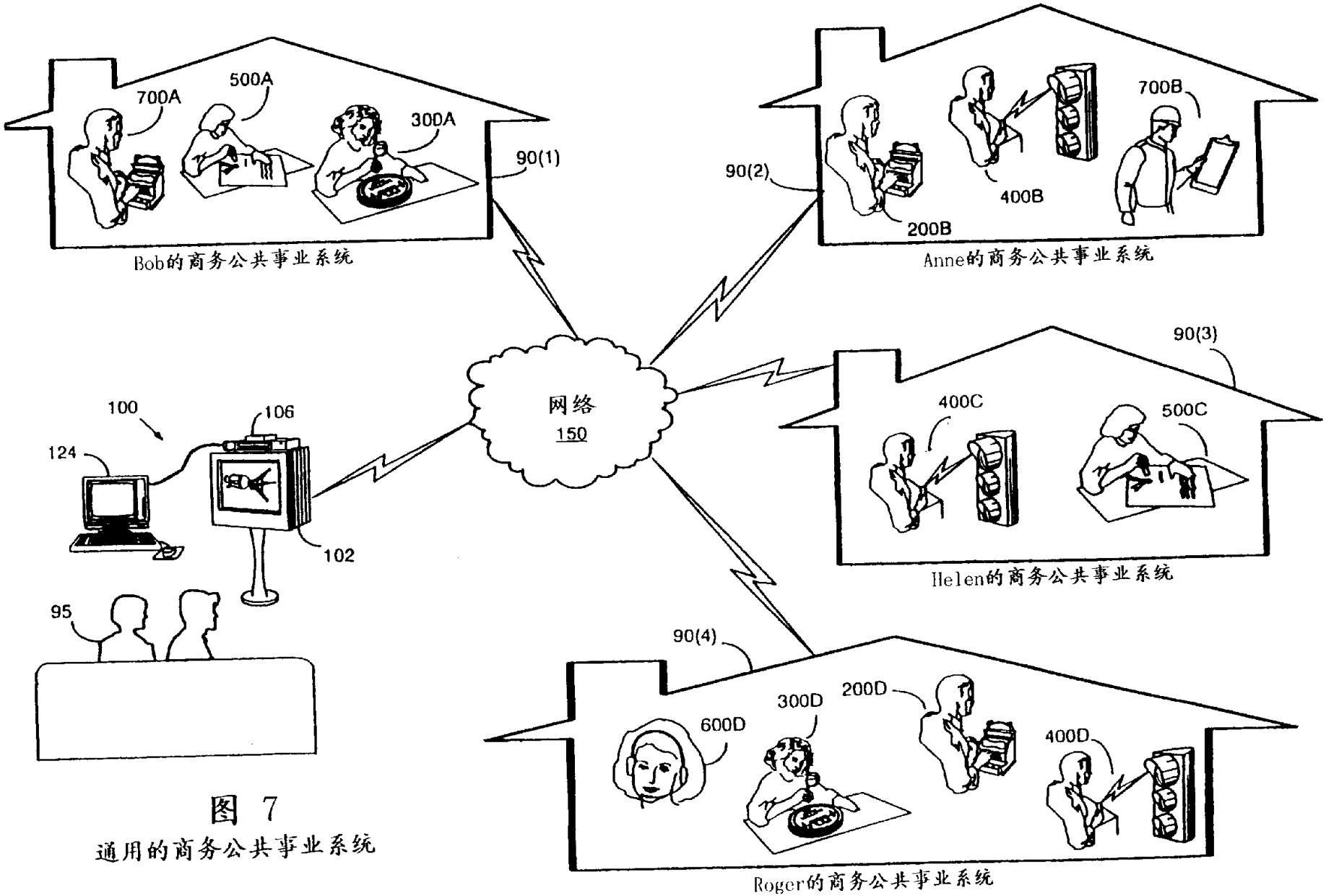


图 7

通用的商务公共事业系统

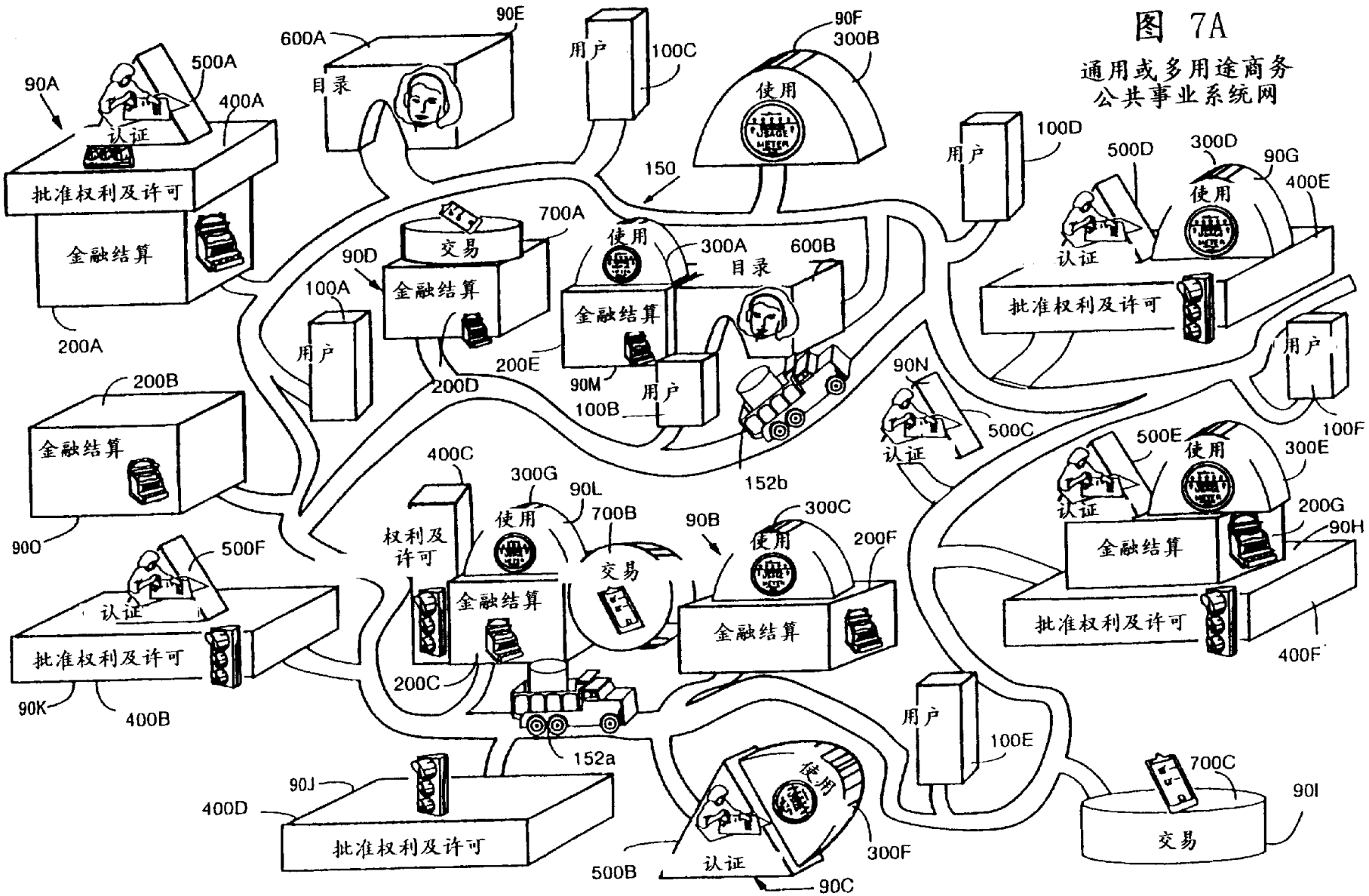


图 7A

通用或多用途商务
公共事业系统网

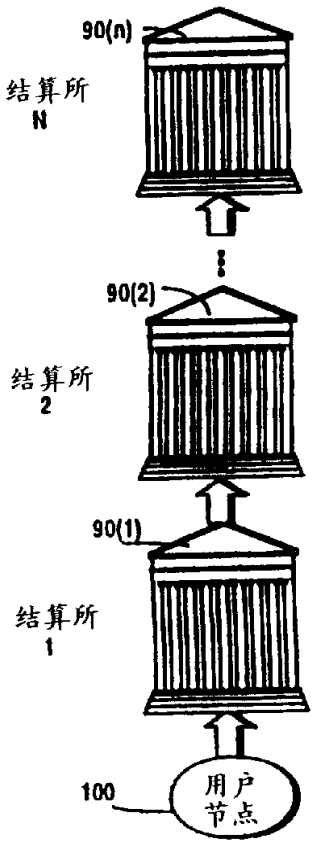


图 8A

图 8B

商务公共事业系统的分级结构

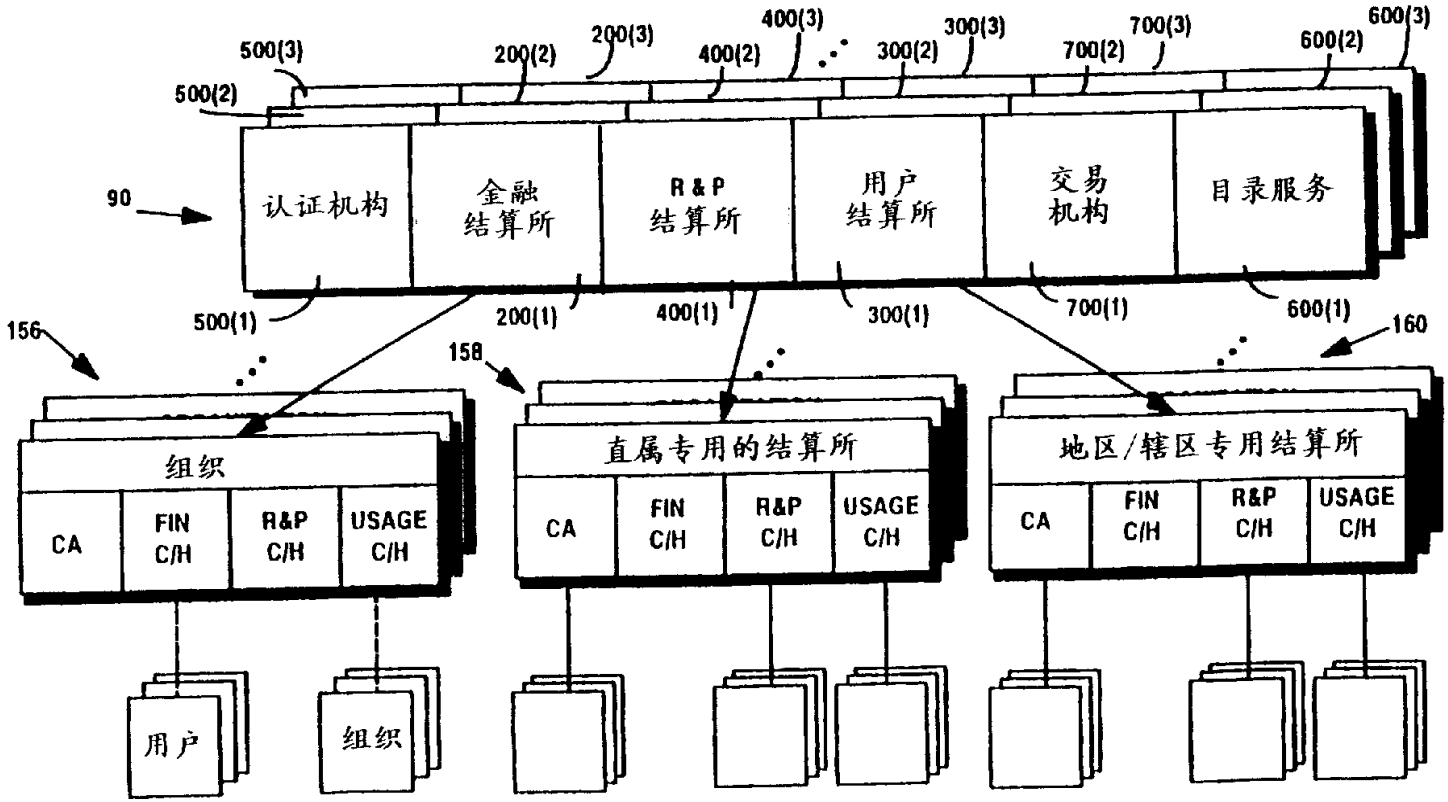


图 9

分级和/或网状（对等）
商务公共事业系统

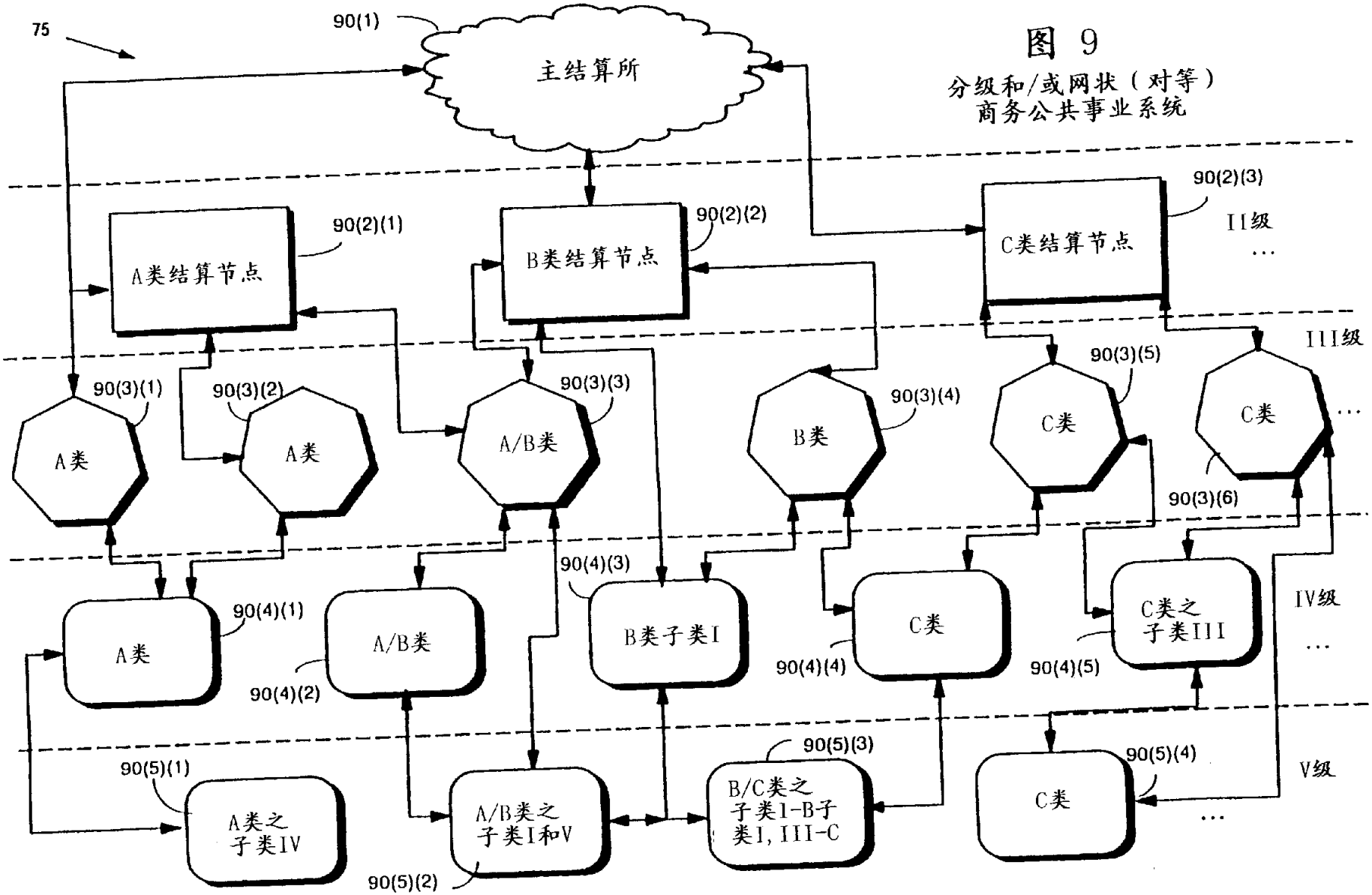


图 10
金融结算所

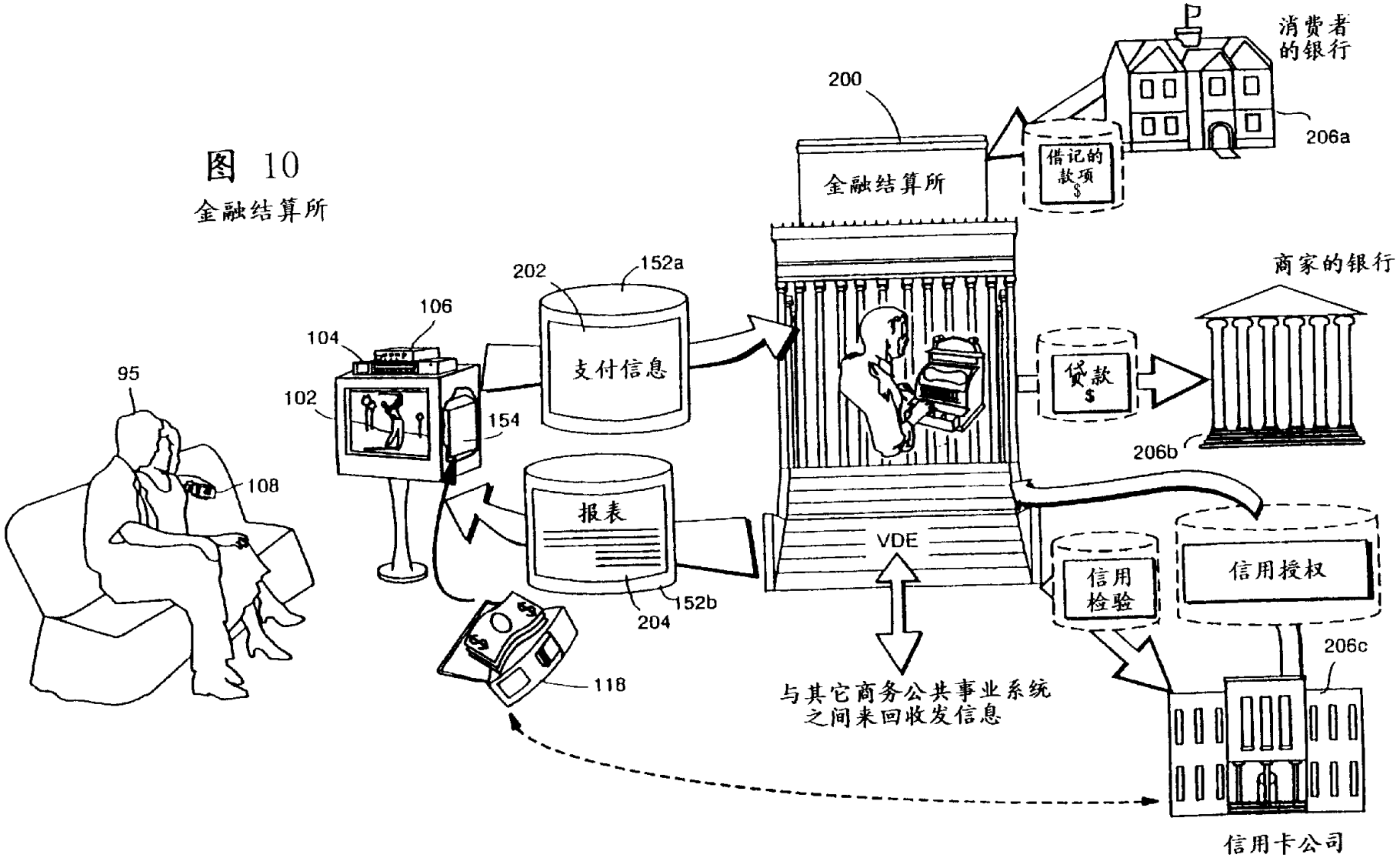

消费者
的银行
206a
200
金融结算所
借记的
款项
$
商家的银行
202
152a
106
104
支付信息
贷款
$
102
154
95
206b
108
报表
VDE
信用
检验
信用授权
152b
204
206c
118
与其它商务公共事业系统
之间来回收发信息
信用卡公司

图 11
使用结算所

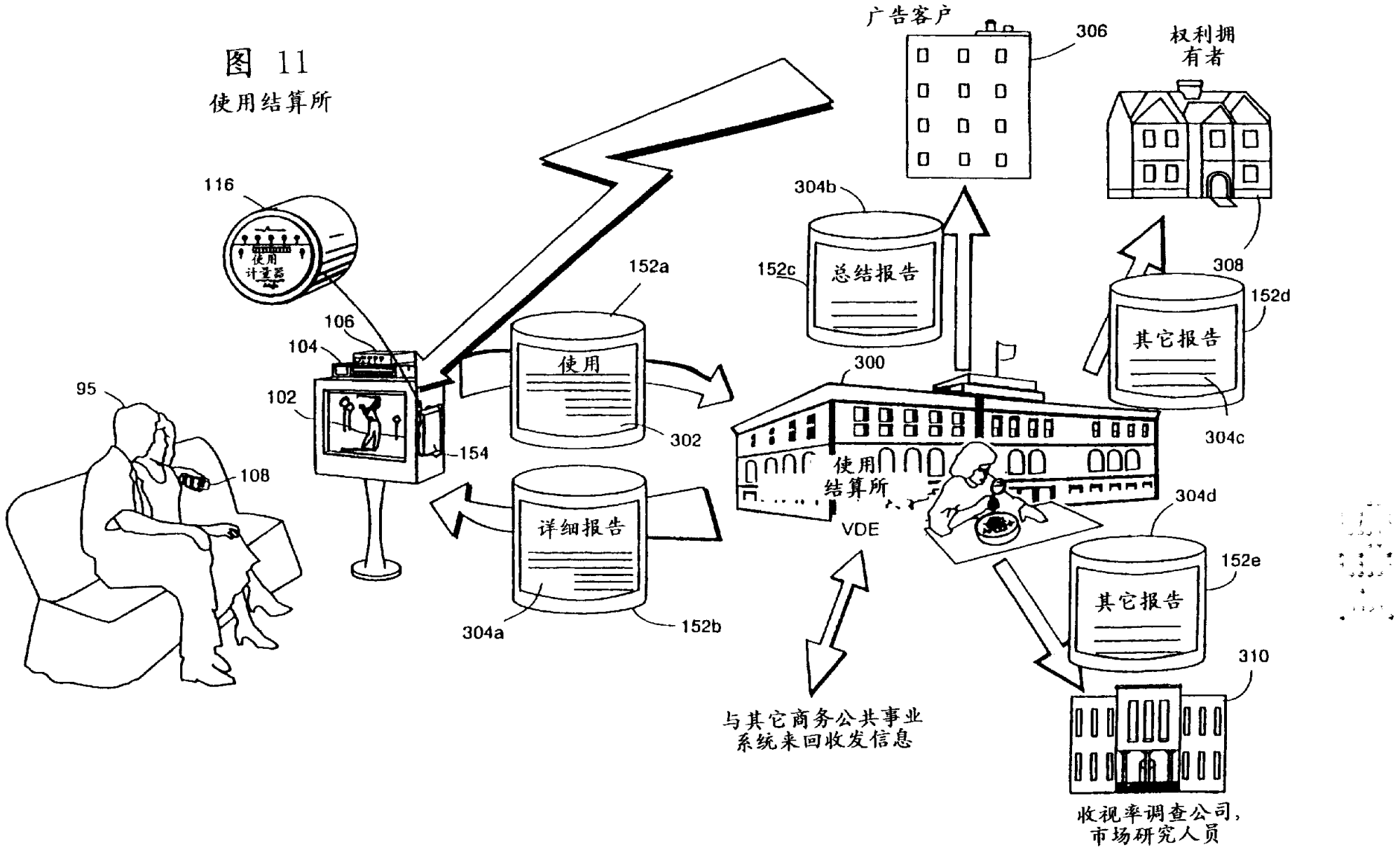

广告客户
306
权利拥有者
116
使用计量器
304b
总结报告
152c
152a
106
104
102
154
使用
302
308
152d
其它报告
304c
300
95
108
使用结算所
VDE
304d
详细报告
304a
152b
152e
其它报告
310
与其它商务公共事业系统来回收发信息
收视率调查公司，市场研究人员

图 12

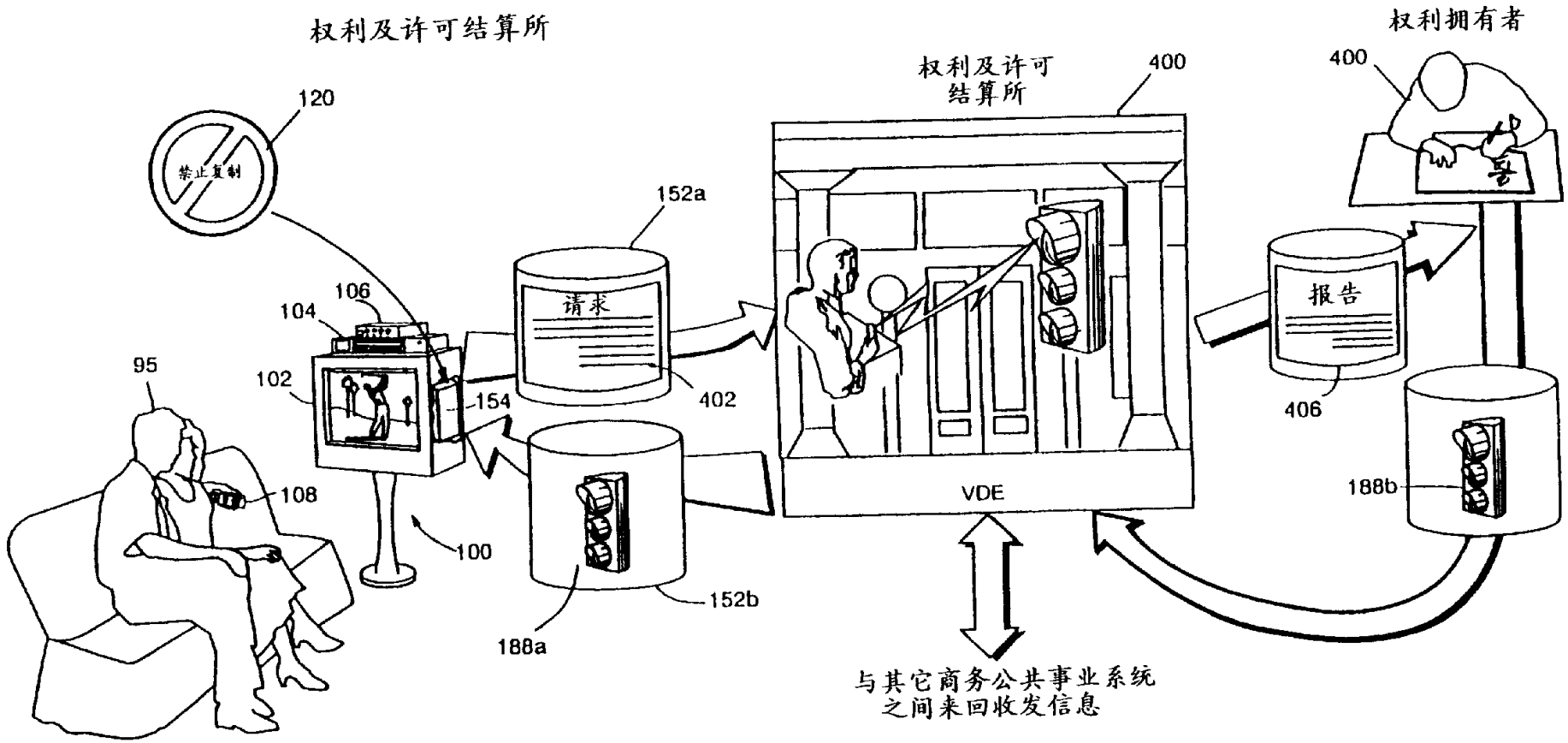

权利及许可结算所
权利拥有者
权利及许可
结算所
400
400
120
禁止复制
152a
请求
106
104
102
154
402
95
108
100
188a
152b
VDE
报告
406
188b
与其它商务公共事业系统
之间来回收发信息

图 13

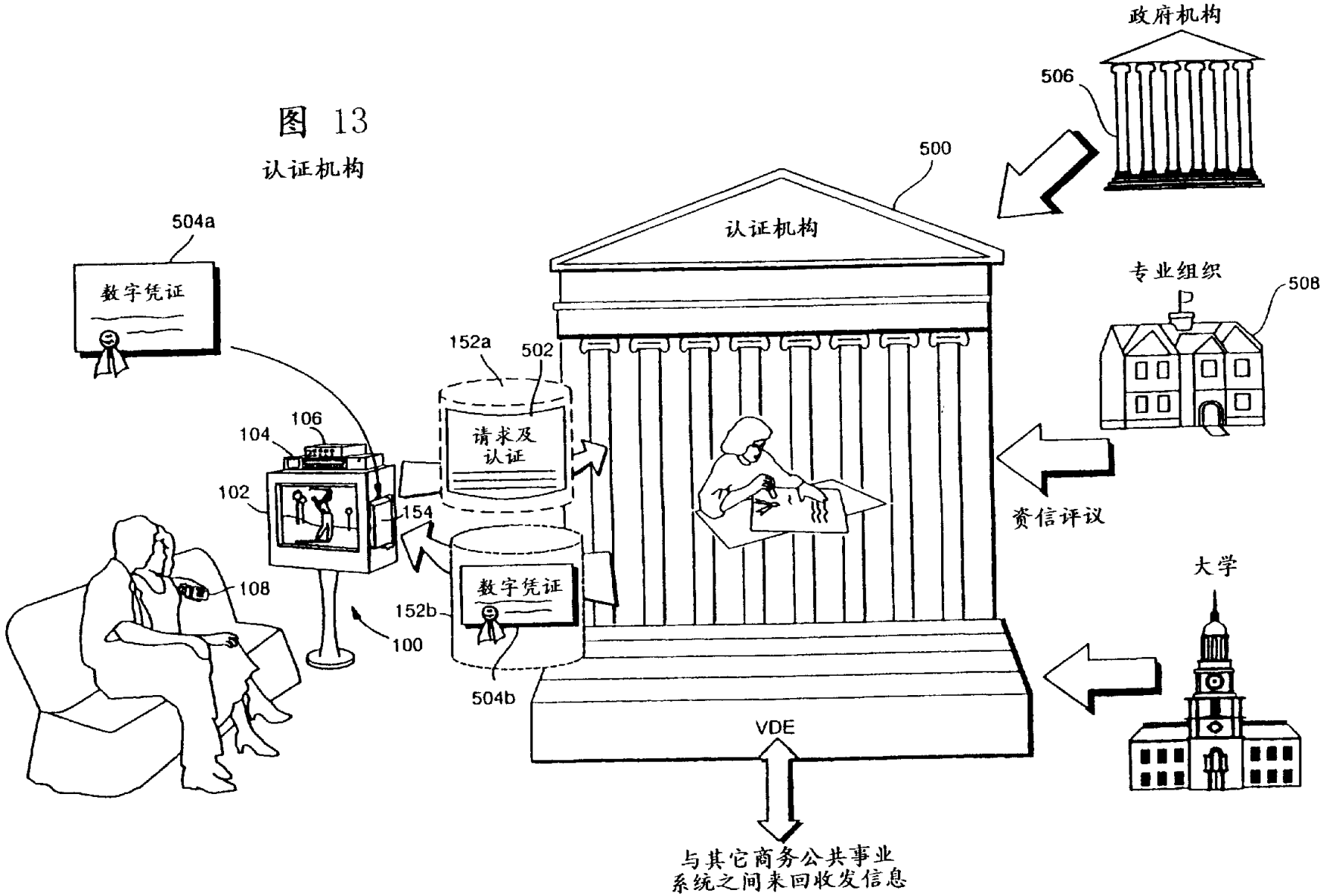

认证机构
政府机构
506
500
认证机构
504a
数字凭证
专业组织
508
152a
502
106
104
请求及
认证
102
154
资信评议
数字凭证
大学
108
152b
100
504b
VDE
与其它商务公共事业
系统之间来回收发信息

图 14
安全目录服务

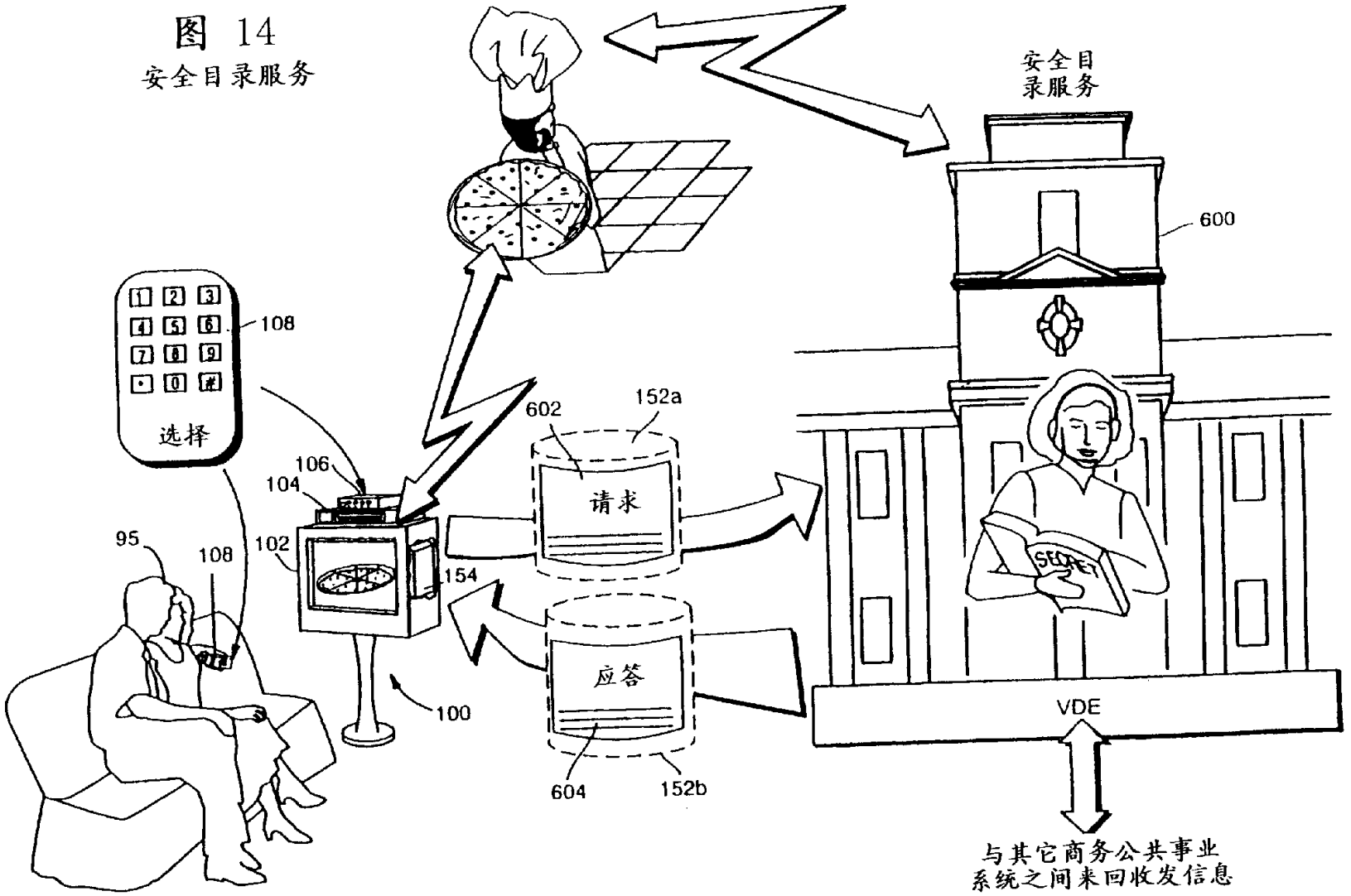
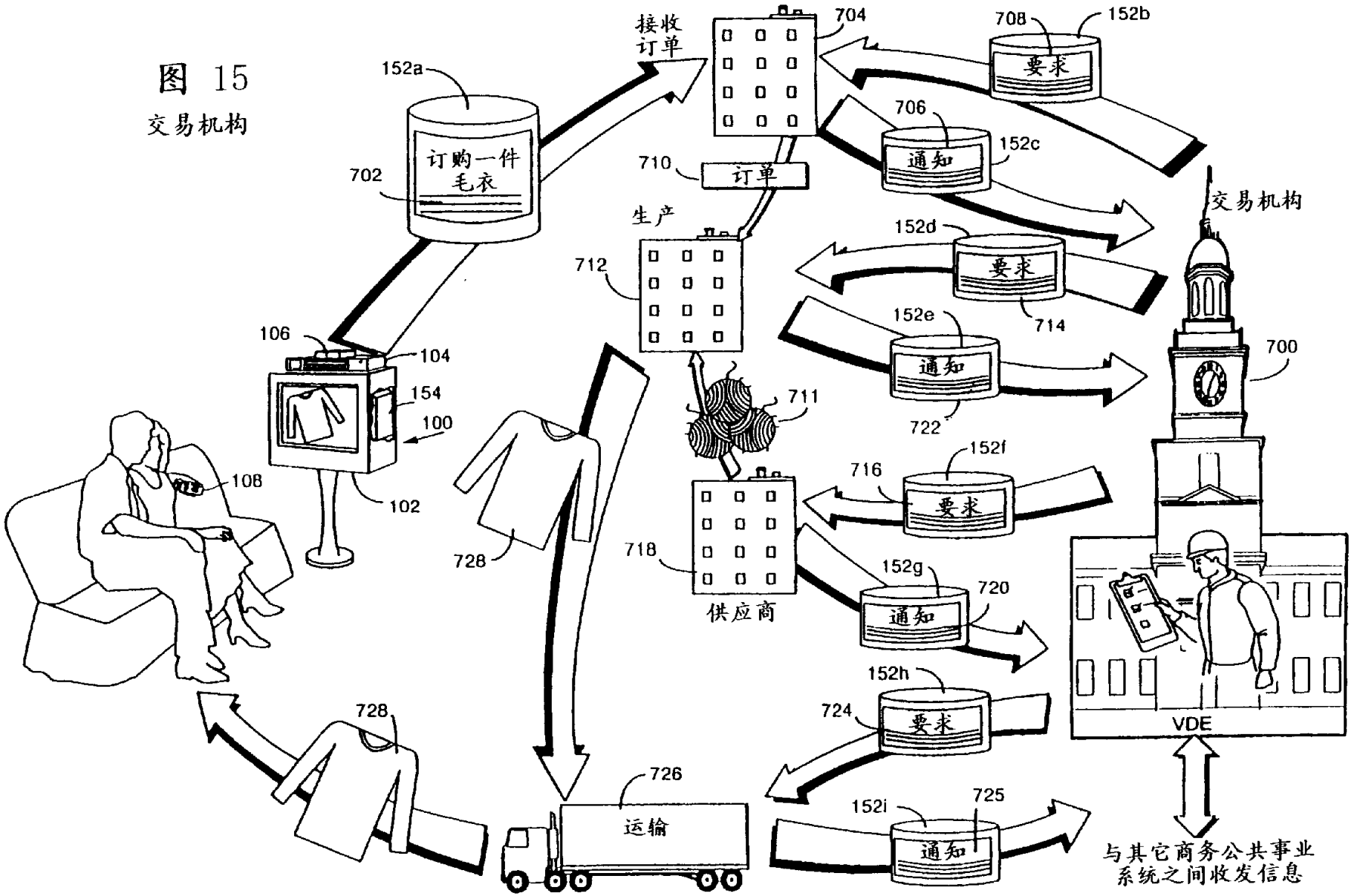

安全目
录服务
600
108
选择
602
152a
请求
106
104
102
154
95
108
应答
100
604
152b
VDE
与其它商务公共事业
系统之间来回收发信息

图 15
交易机构


接收
订单
704
708
152b
要求
152a
订购一件
毛衣
702
706
通知
152c
710
订单
交易机构
生产
152d
要求
712
714
152e
通知
700
722
106
104
154
100
711
108
102
716
152f
要求
728
718
152g
720
通知
供应商
VDE
152h
724
要求
728
726
725
152i
运输
通知
与其它商务公共事业
系统之间收发信息

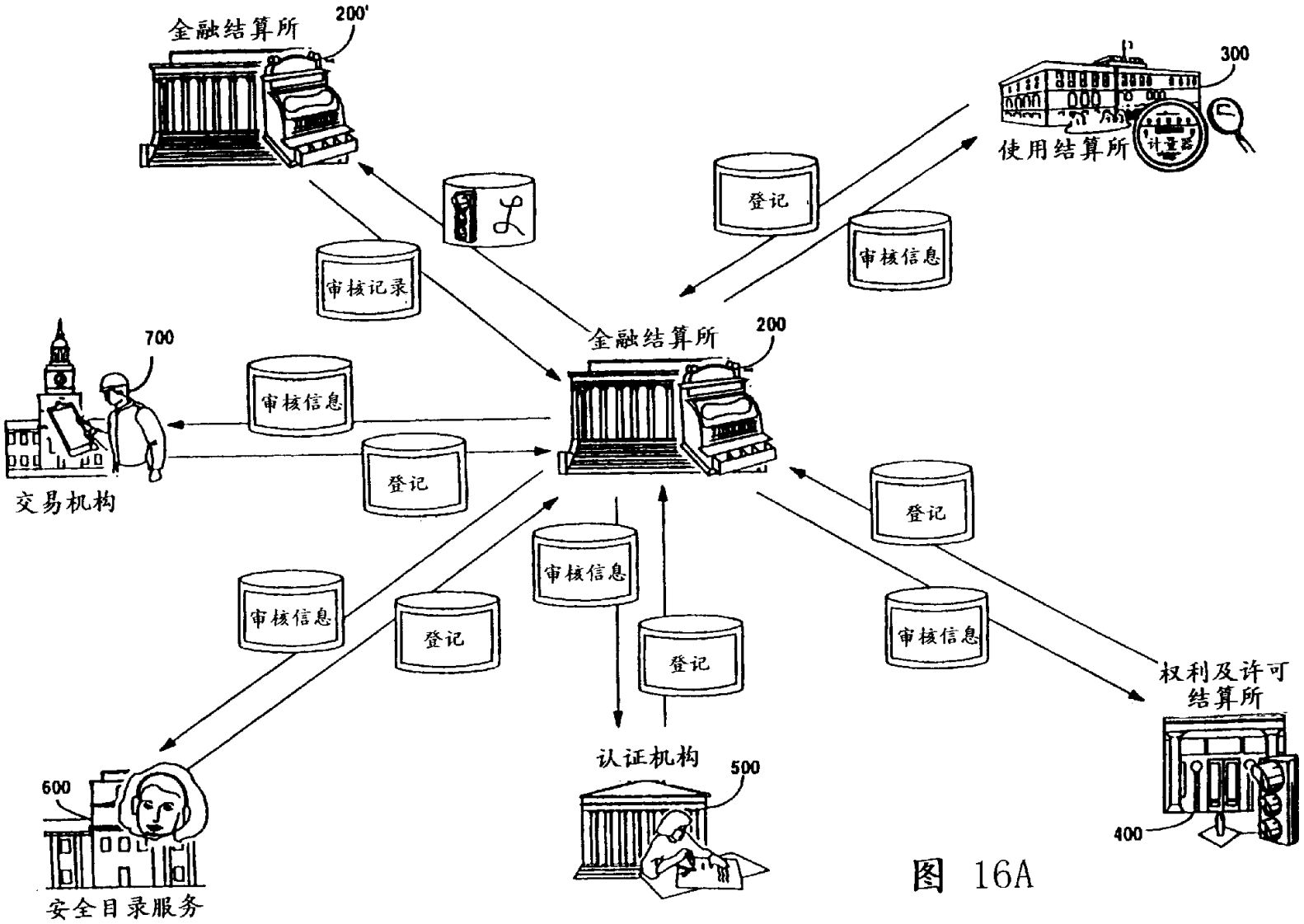

金融结算所
200'
300
使用结算所
登记
审核信息
审核记录
金融结算所
200
700
审核信息
登记
交易机构
审核信息
登记
审核信息
登记
登记
审核信息
权利及许可
结算所
认证机构
500
600
400
安全目录服务

图 16A

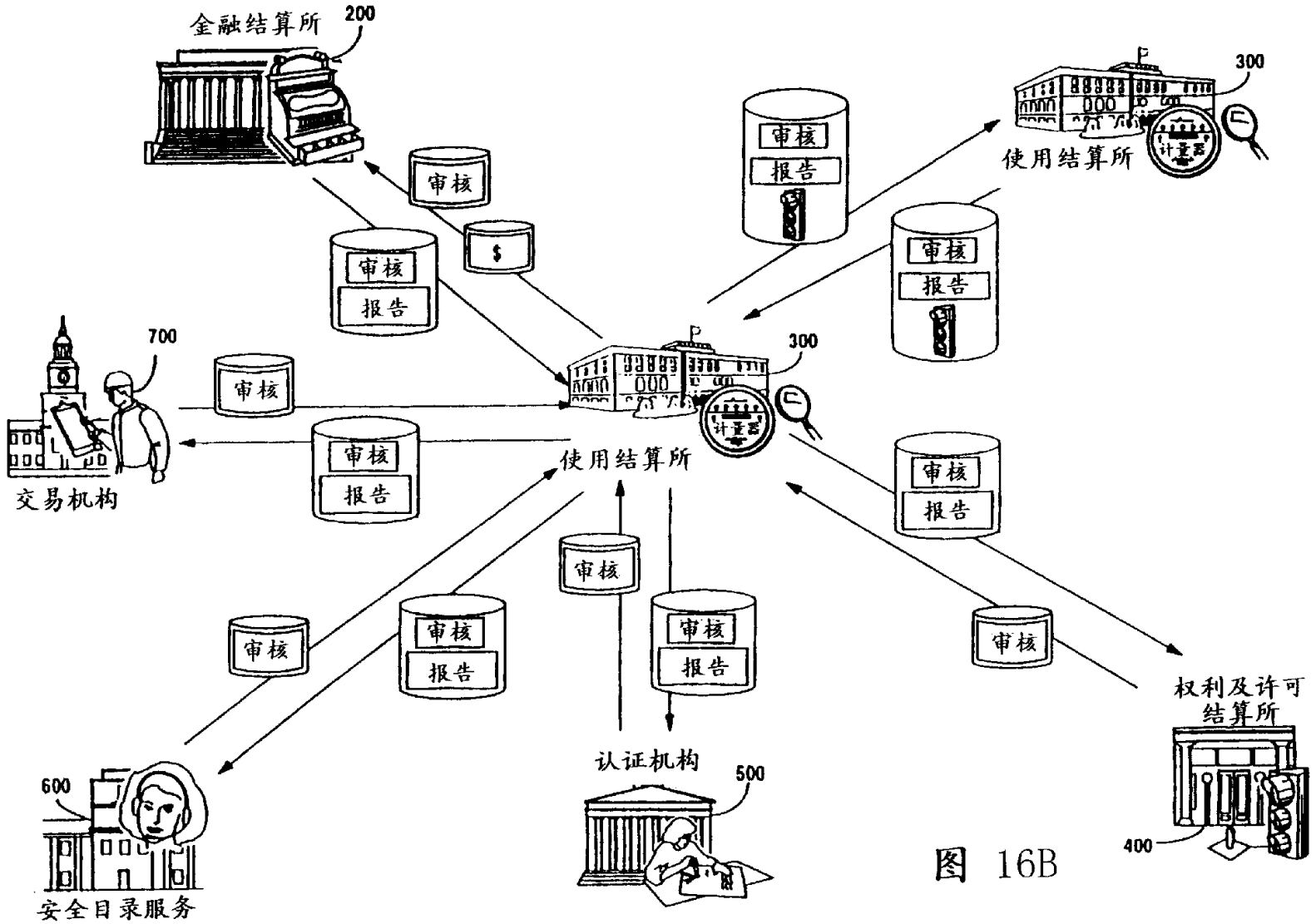

金融结算所
200
审核
报告
$
300
使用结算所
700
交易机构
使用结算所
认证机构
500
600
安全目录服务
权利及许可
结算所
400

图 16B

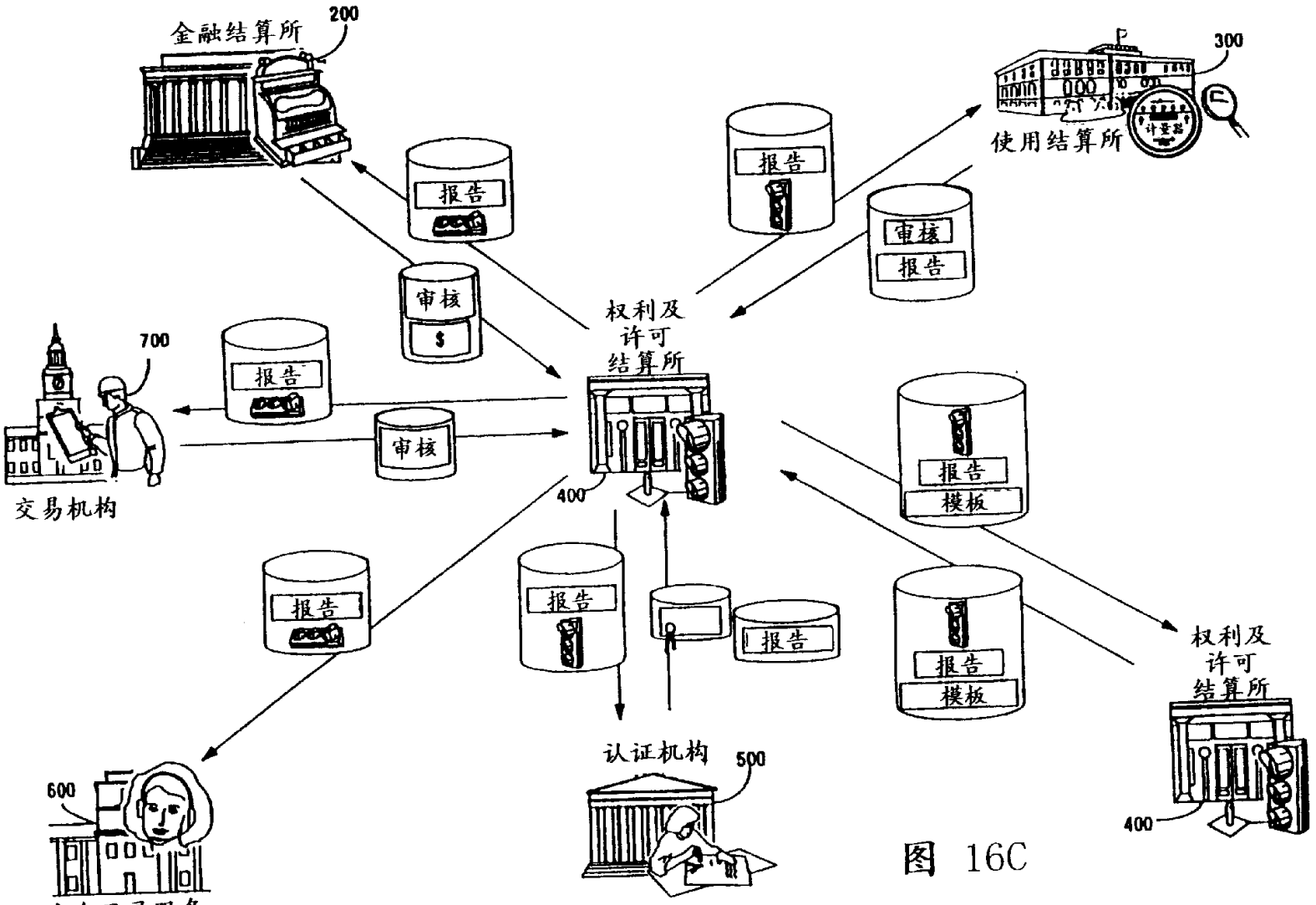

金融结算所
200
报告
审核
$
300
使用结算所
计量器
报告
审核
报告
权利及
许可
结算所
400
700
报告
审核
交易机构
报告
模板
报告
模板
报告
报告
权利及
许可
结算所
400
认证机构
500
600
安全目录服务

图 16C

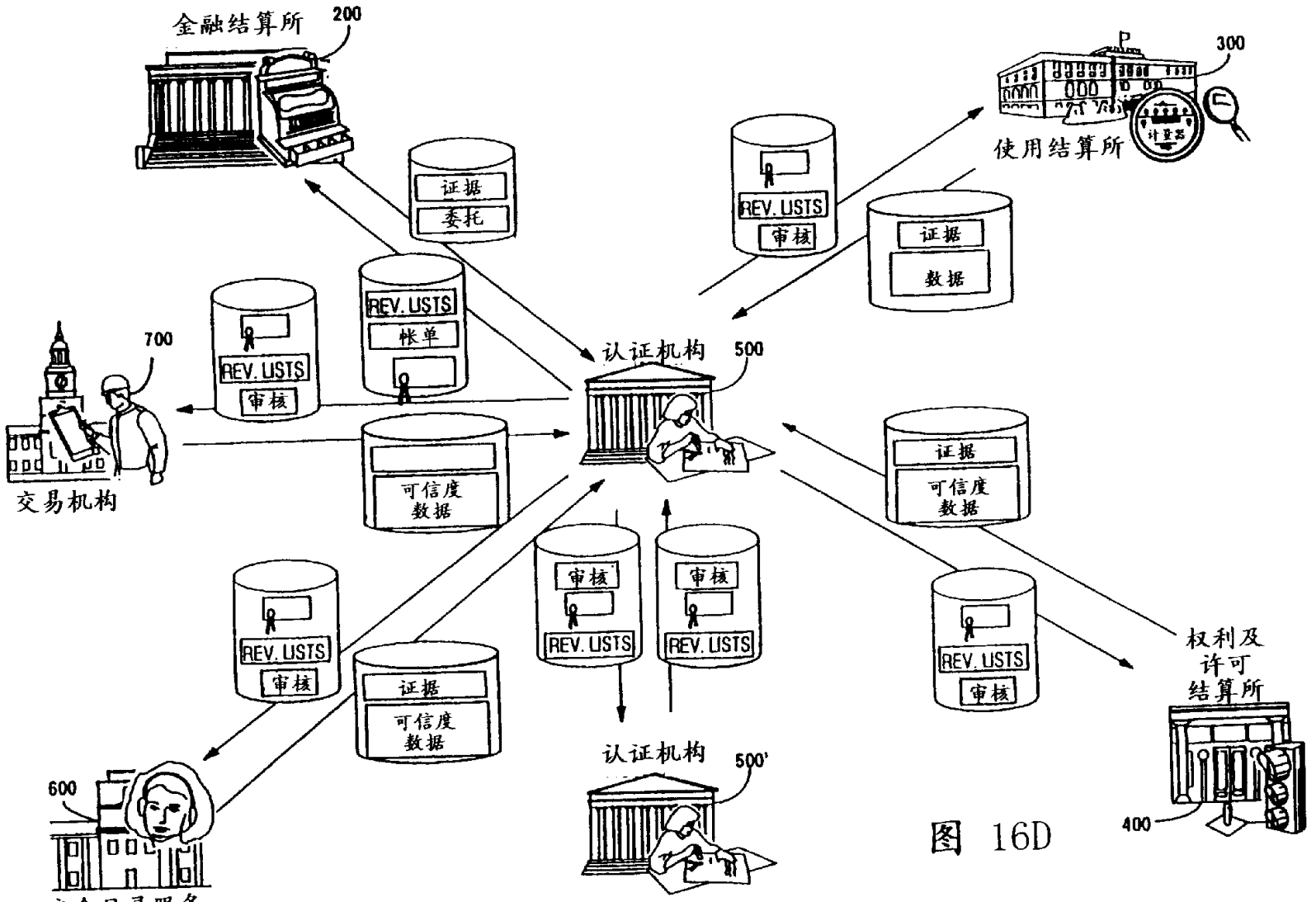

金融结算所
200
证据
委托
REV. USTS
帐单
REV. USTS
审核
700
交易机构
REV. USTS
审核
证据
数据
使用结算所
300
认证机构
500
证据
可信度
数据
REV. USTS
审核
REV. USTS
审核
REV. USTS
审核
证据
可信度
数据
600
安全目录服务
认证机构
500'
REV. USTS
审核
证据
可信度
数据
权利及
许可
结算所
400

图 16D

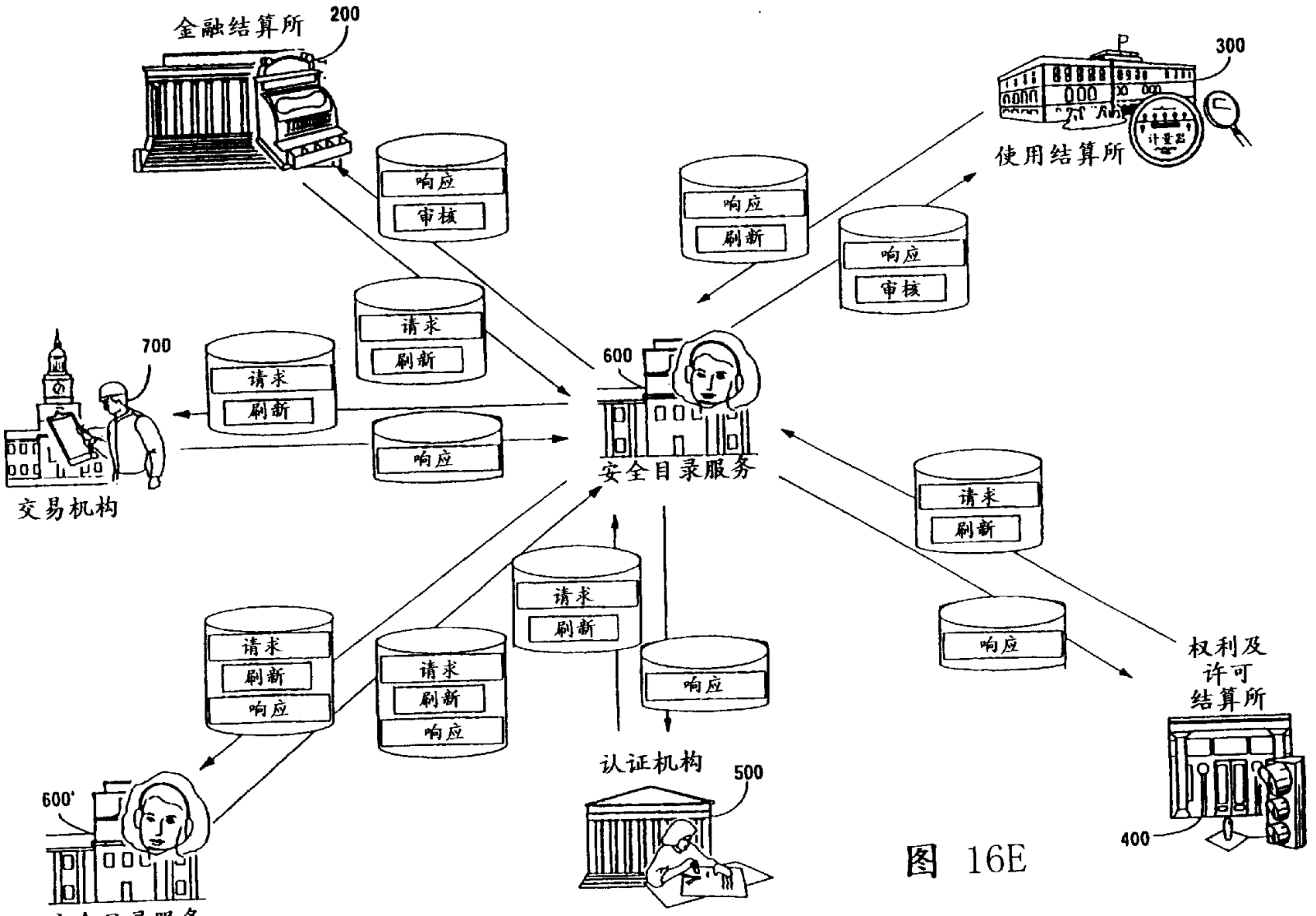

金融结算所
200
响应
审核
请求
刷新
700
交易机构
600
安全目录服务
响应
刷新
300
使用结算所
响应
审核
请求
刷新
响应
请求
刷新
响应
请求
刷新
响应
600'
安全目录服务
认证机构
500
请求
刷新
响应
权利及
许可
结算所
400

图 16E

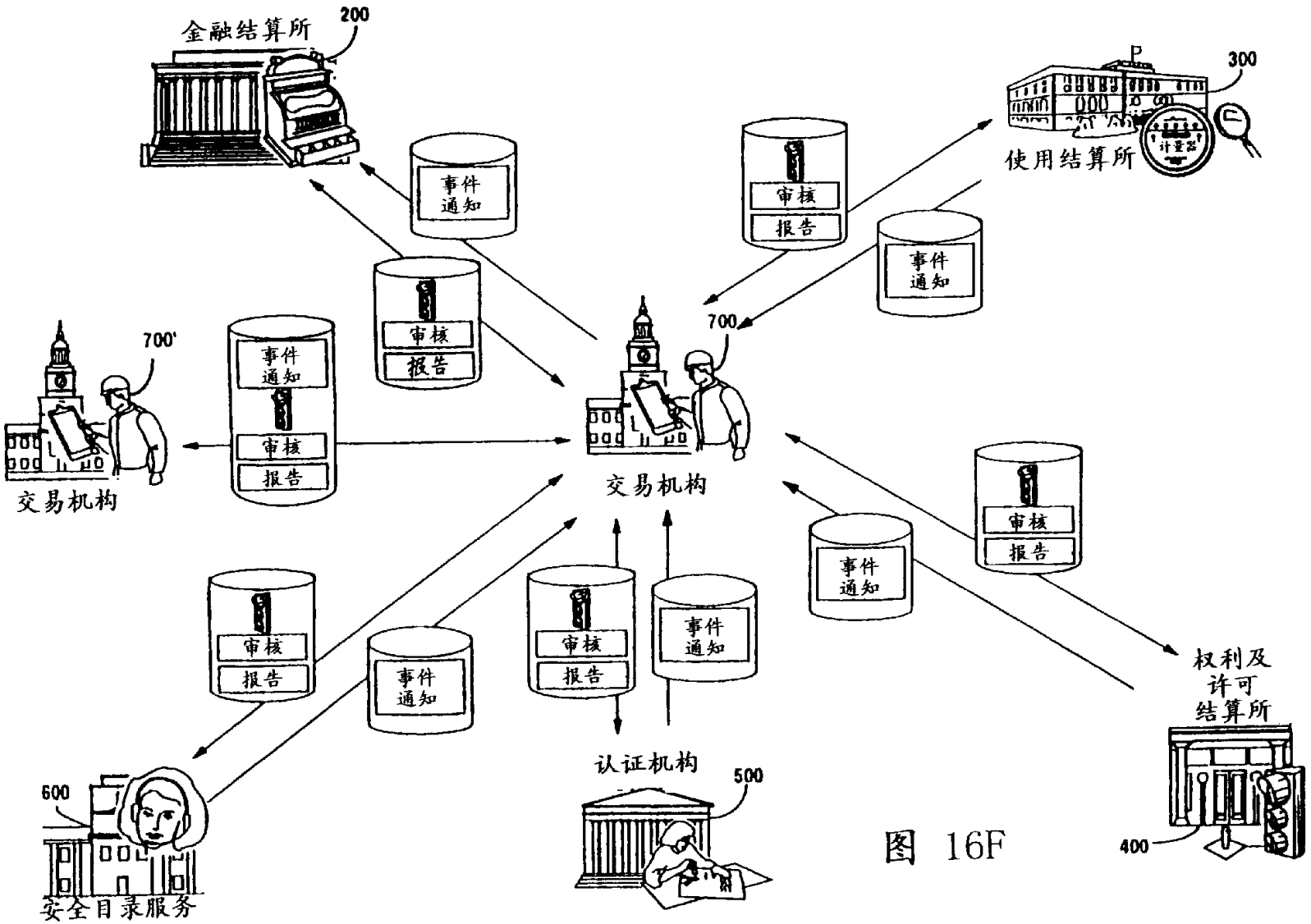

金融结算所
200
事件通知
审核
报告
使用结算所
300
700'
交易机构
700
交易机构
权利及许可结算所
400
认证机构
500
600
安全目录服务

图 16F

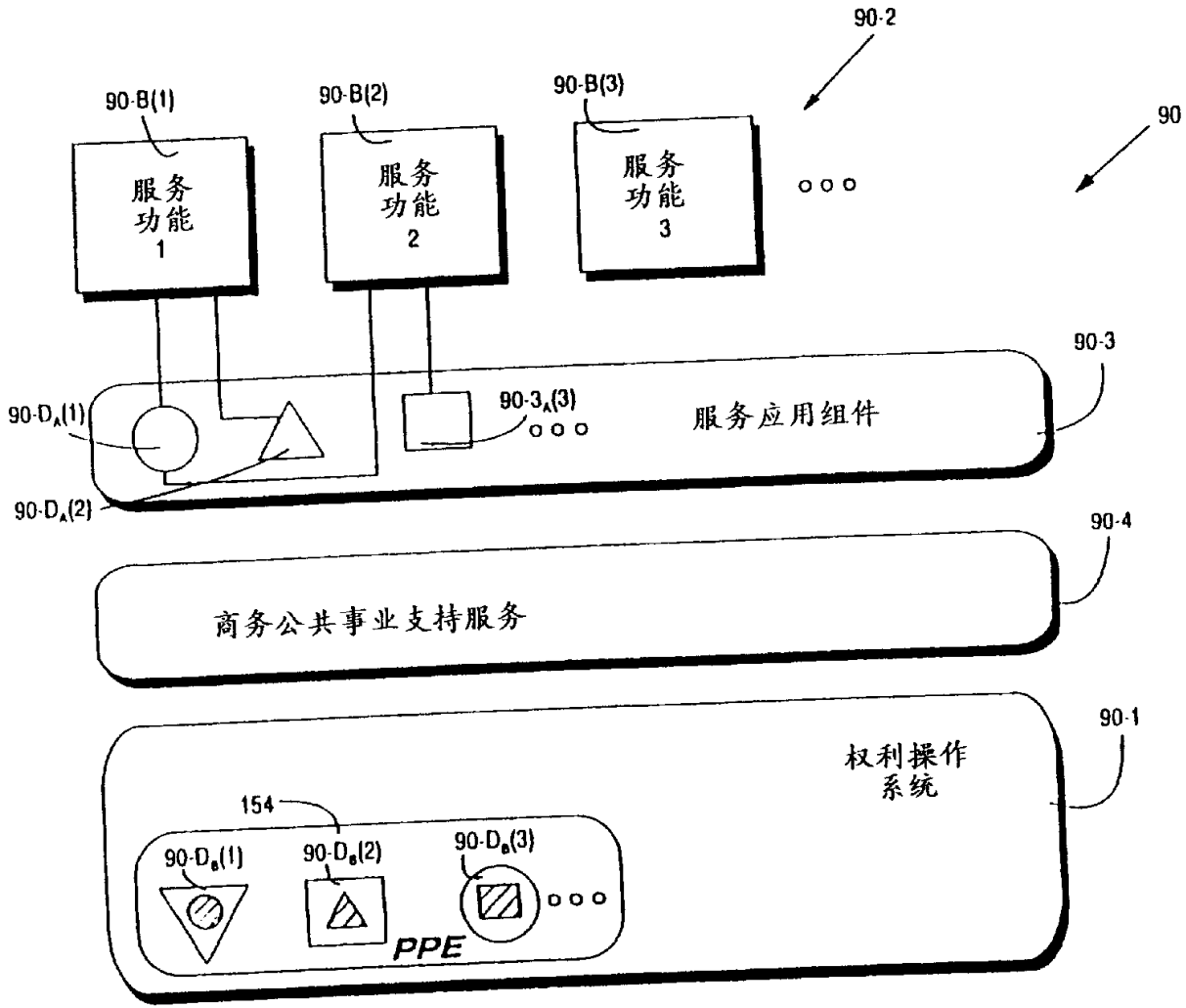


图 17A

商务公共事业系统90

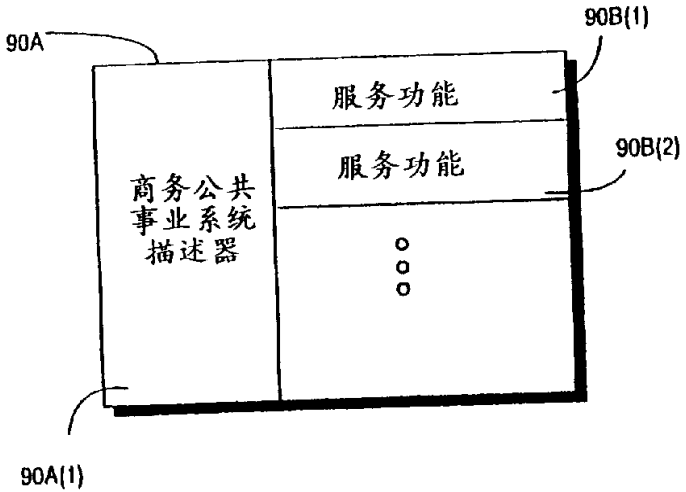

90A
90B(1)
服务功能
服务功能
90B(2)
商务公共事业系统描述器
90A(1)

图 17B

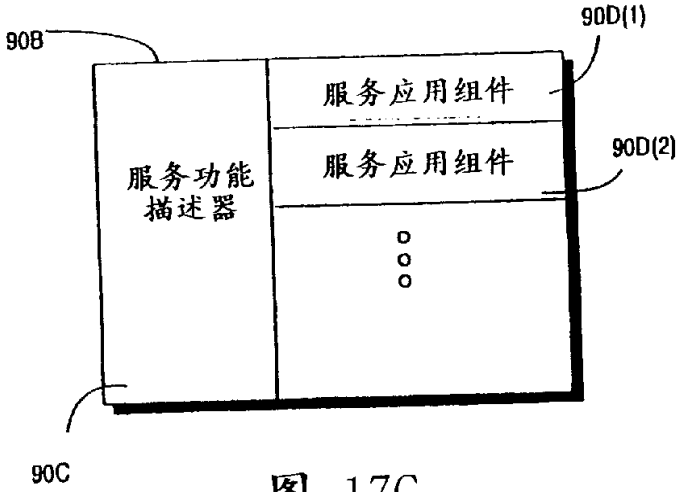

90B
90D(1)
服务应用组件
服务应用组件
90D(2)
服务功能描述器
90C

图 17C

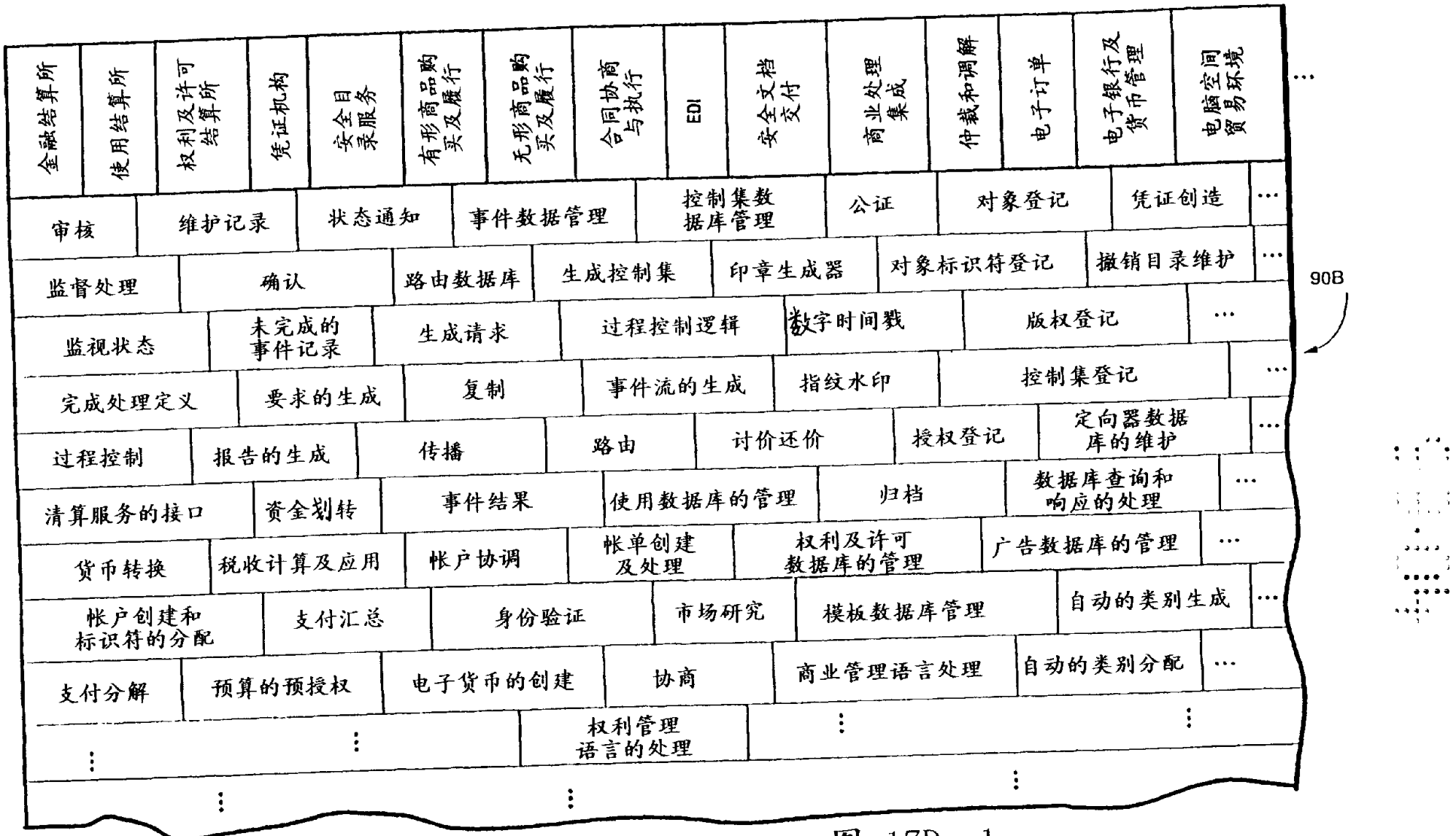

金融结算所
使用结算所
权利及许可结算所
凭证机构
安全目录服务
有形商品购买及履行
无形商品购买及履行
合同协商与执行
EDI
安全文档交付
商业处理集成
仲裁和调解
电子订单
电子银行及货币管理
电脑空间贸易环境
审核
维护记录
状态通知
事件数据管理
控制集数据库管理
公证
对象登记
凭证创造
监督处理
确认
路由数据库
生成控制集
印章生成器
对象标识符登记
撤销目录维护
监视状态
未完成的事件记录
生成请求
过程控制逻辑
数字时间戳
版权登记
完成处理定义
要求的生成
复制
事件流的生成
指纹水印
控制集登记
过程控制
报告的生成
传播
路由
讨价还价
授权登记
定向器数据库的维护
清算服务的接口
资金划转
事件结果
使用数据库的管理
归档
数据库查询和响应的处理
货币转换
税收计算及应用
帐户协调
帐单创建及处理
权利及许可数据库的管理
广告数据库的管理
帐户创建和标识符的分配
支付汇总
身份验证
市场研究
模板数据库管理
自动的类别生成
支付分解
预算的预授权
电子货币的创建
协商
商业管理语言处理
自动的类别分配
权利管理语言的处理
908

图 17D－1

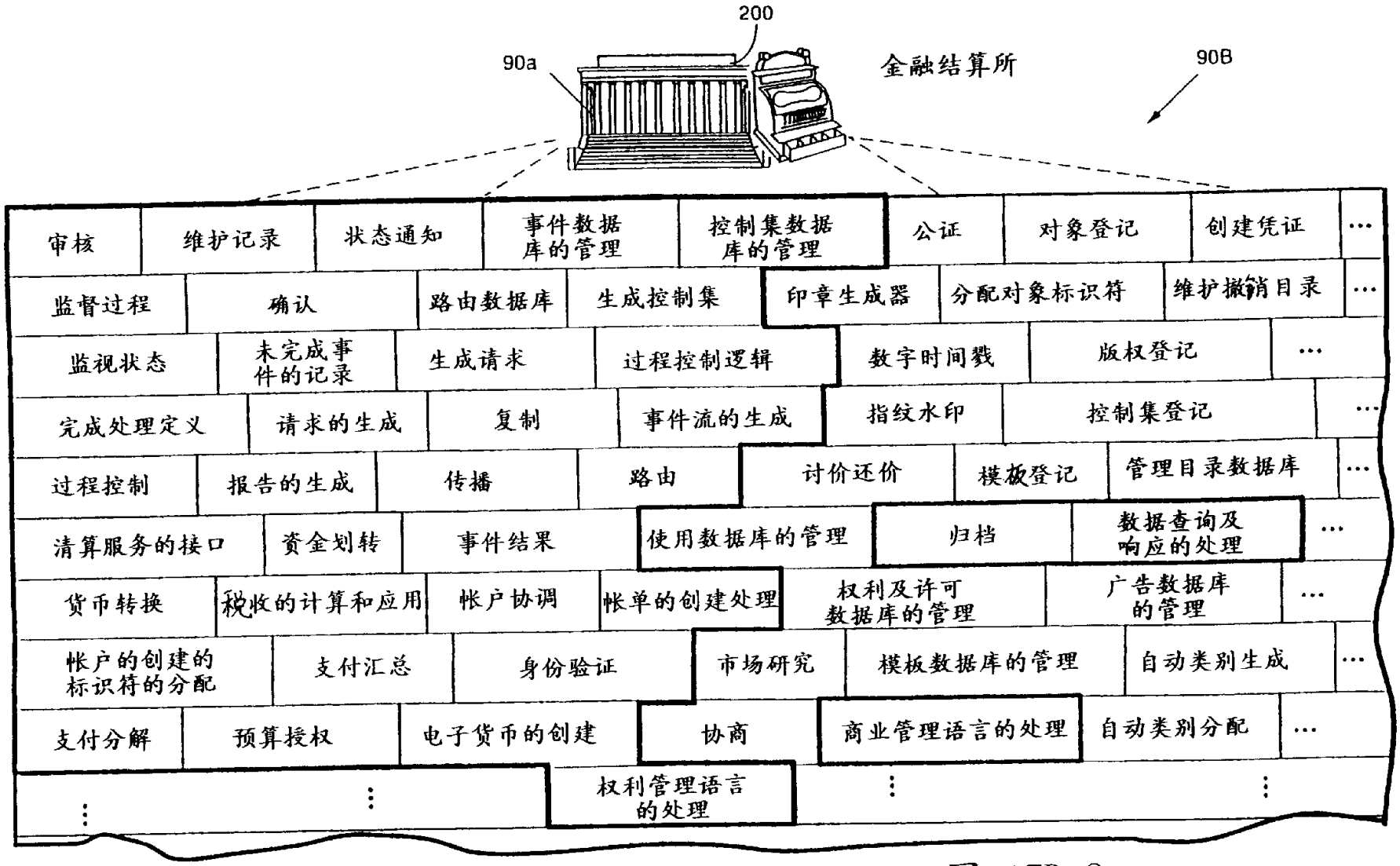

200
90a
金融结算所
90B
审核
维护记录
状态通知
事件数据库的管理
控制集数据库的管理
公证
对象登记
创建凭证
…
监督过程
确认
路由数据库
生成控制集
印章生成器
分配对象标识符
维护撤销目录
…
监视状态
未完成事件的记录
生成请求
过程控制逻辑
数字时间戳
版权登记
…
完成处理定义
请求的生成
复制
事件流的生成
指纹水印
控制集登记
…
过程控制
报告的生成
传播
路由
讨价还价
模板登记
管理目录数据库
…
清算服务的接口
资金划转
事件结果
使用数据库的管理
归档
数据查询及响应的处理
…
货币转换
税收的计算和应用
帐户协调
帐单的创建处理
权利及许可数据库的管理
广告数据库的管理
…
帐户的创建的标识符的分配
支付汇总
身份验证
市场研究
模板数据库的管理
自动类别生成
…
支付分解
预算授权
电子货币的创建
协商
商业管理语言的处理
自动类别分配
…
权利管理语言的处理

图 17D-2

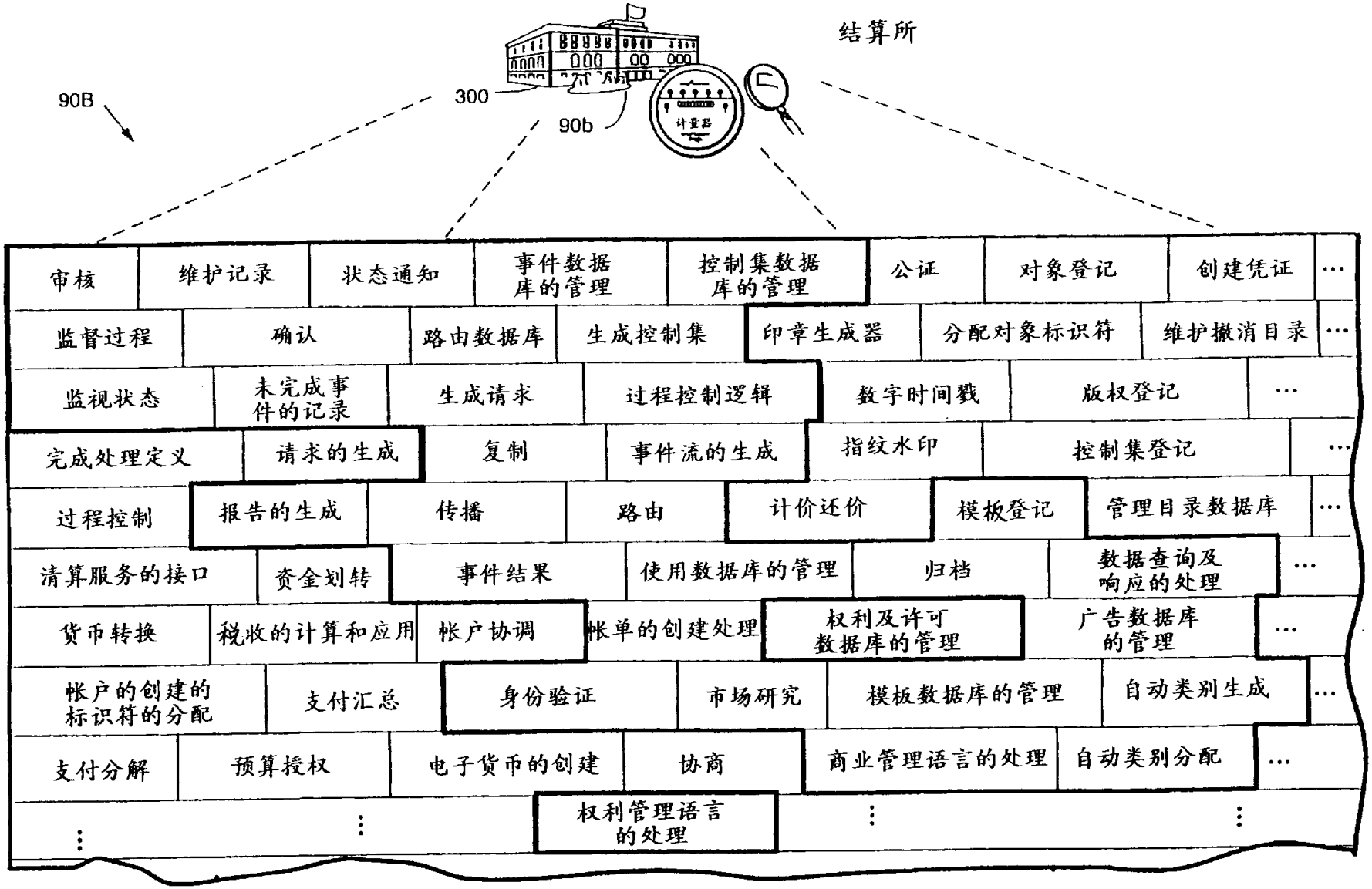

结算所
90B
300
90b
审核
维护记录
状态通知
事件数据库的管理
控制集数据库的管理
公证
对象登记
创建凭证
监督过程
确认
路由数据库
生成控制集
印章生成器
分配对象标识符
维护撤消目录
监视状态
未完成事件的记录
生成请求
过程控制逻辑
数字时间戳
版权登记
完成处理定义
请求的生成
复制
事件流的生成
指纹水印
控制集登记
过程控制
报告的生成
传播
路由
计价还价
模板登记
管理目录数据库
清算服务的接口
资金划转
事件结果
使用数据库的管理
归档
数据查询及响应的处理
货币转换
税收的计算和应用
帐户协调
帐单的创建处理
权利及许可数据库的管理
广告数据库的管理
帐户的创建的标识符的分配
支付汇总
身份验证
市场研究
模板数据库的管理
自动类别生成
支付分解
预算授权
电子货币的创建
协商
商业管理语言的处理
自动类别分配
权利管理语言的处理

图 17D-3

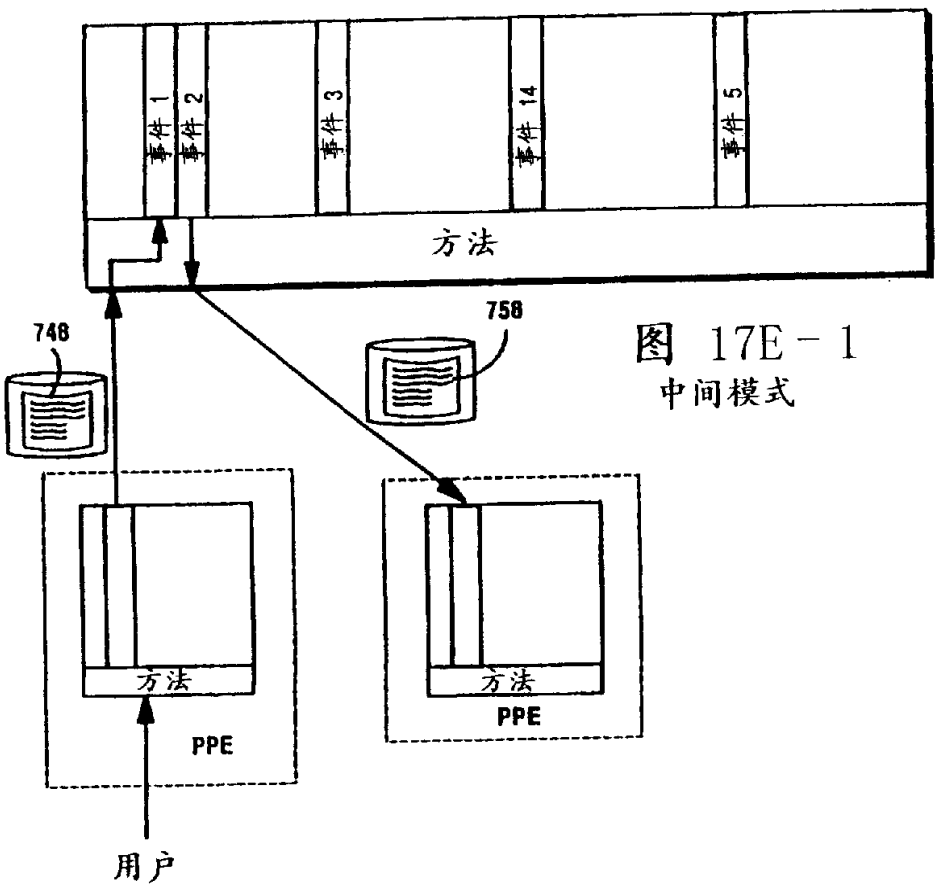


图 17E－1
中间模式

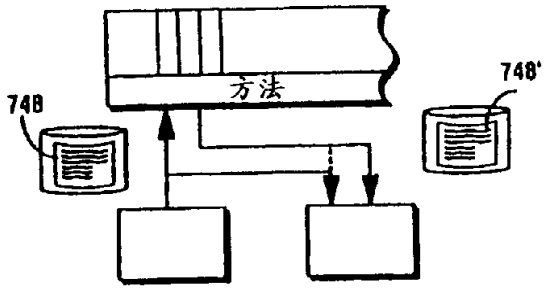


图 17E－2
授权继续进行

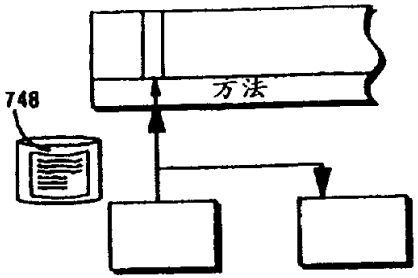


图 17E－3
通知模式

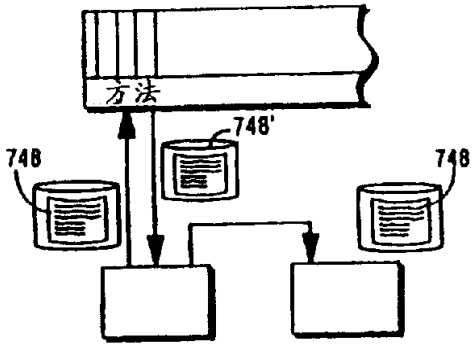


图 17E－4
以前的授权模式

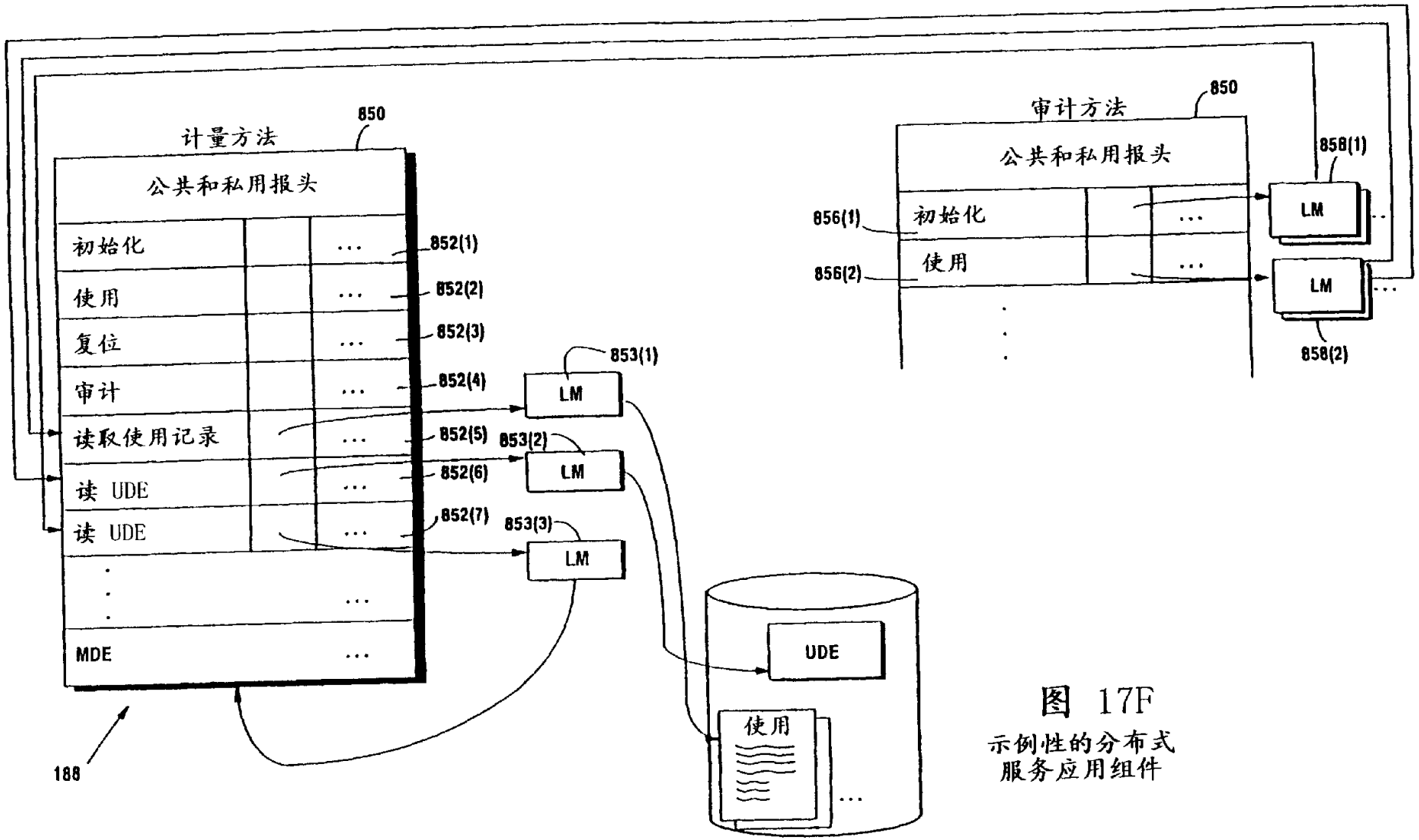


图 17F
示例性的分布式
服务应用组件

图 18

示例性的金融结算所

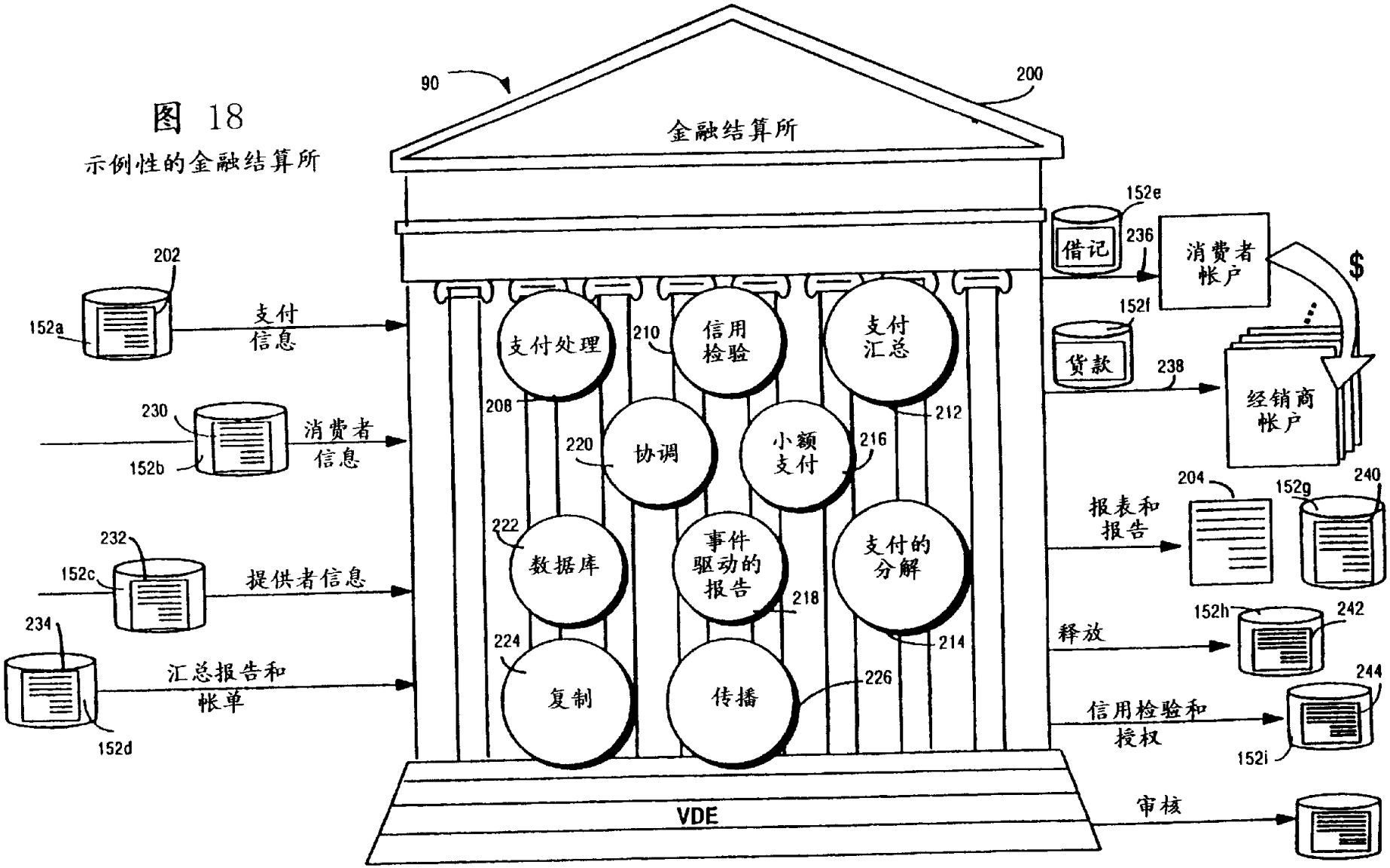


图 19
示例性的金融结算所安排

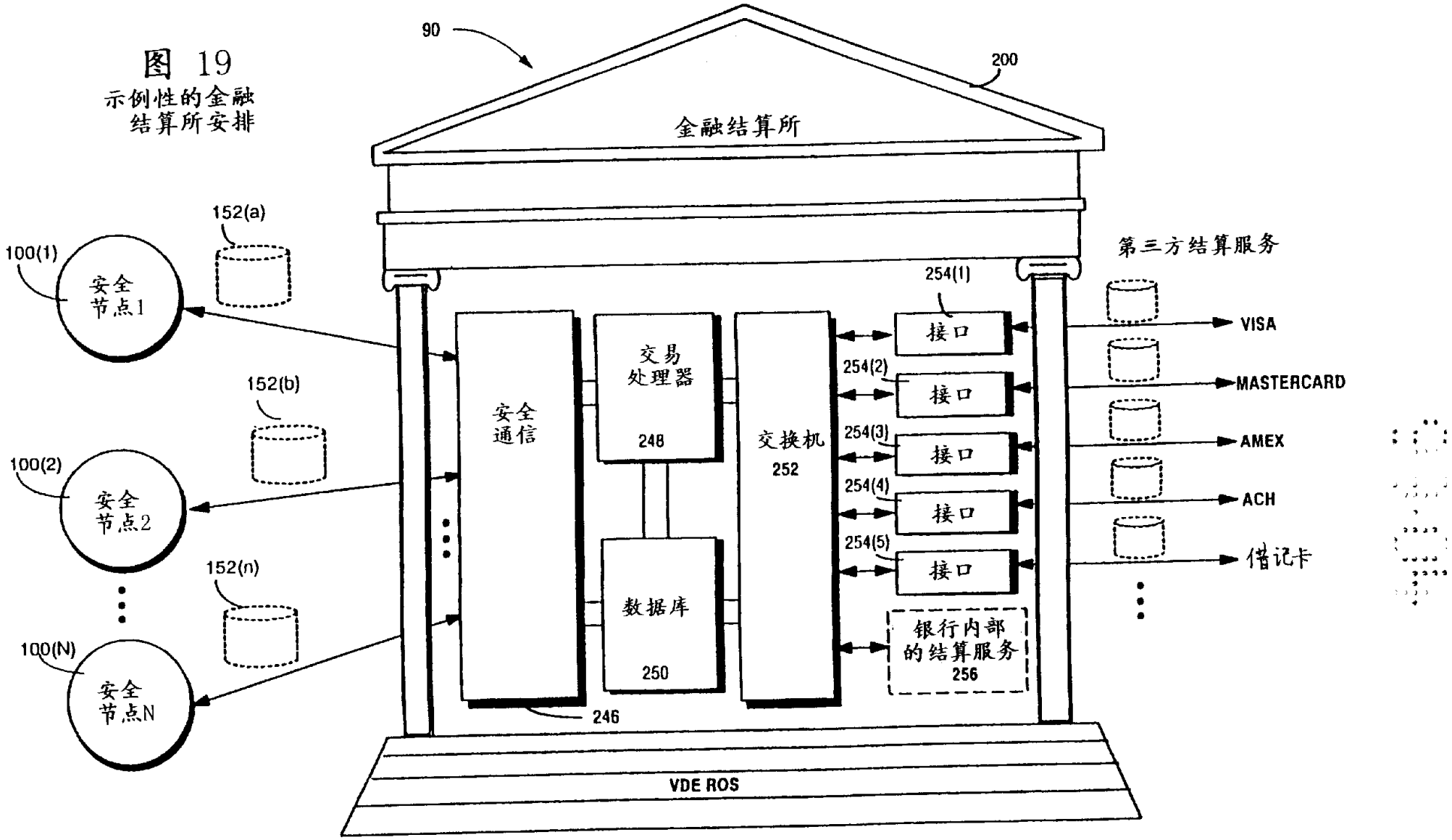
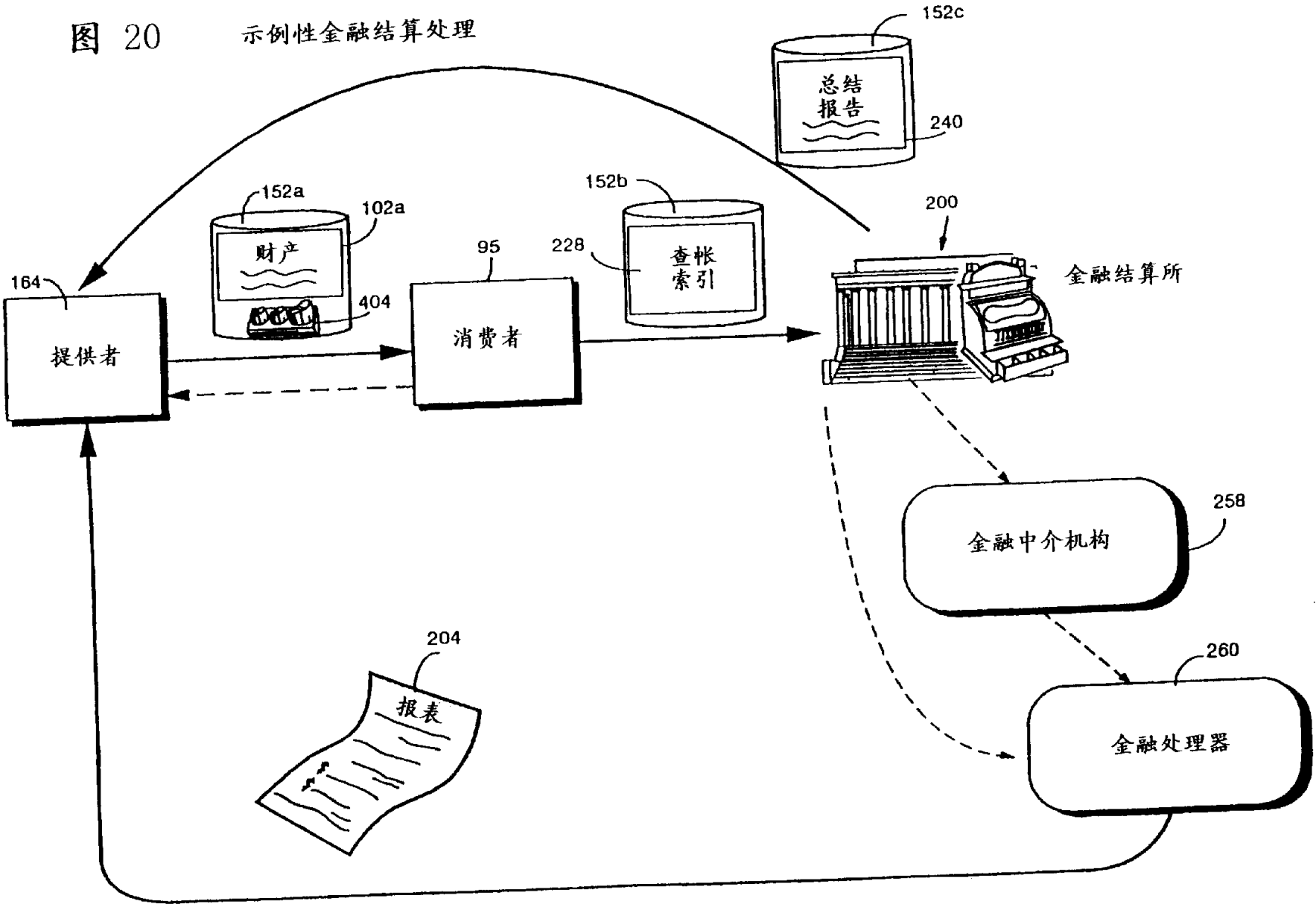
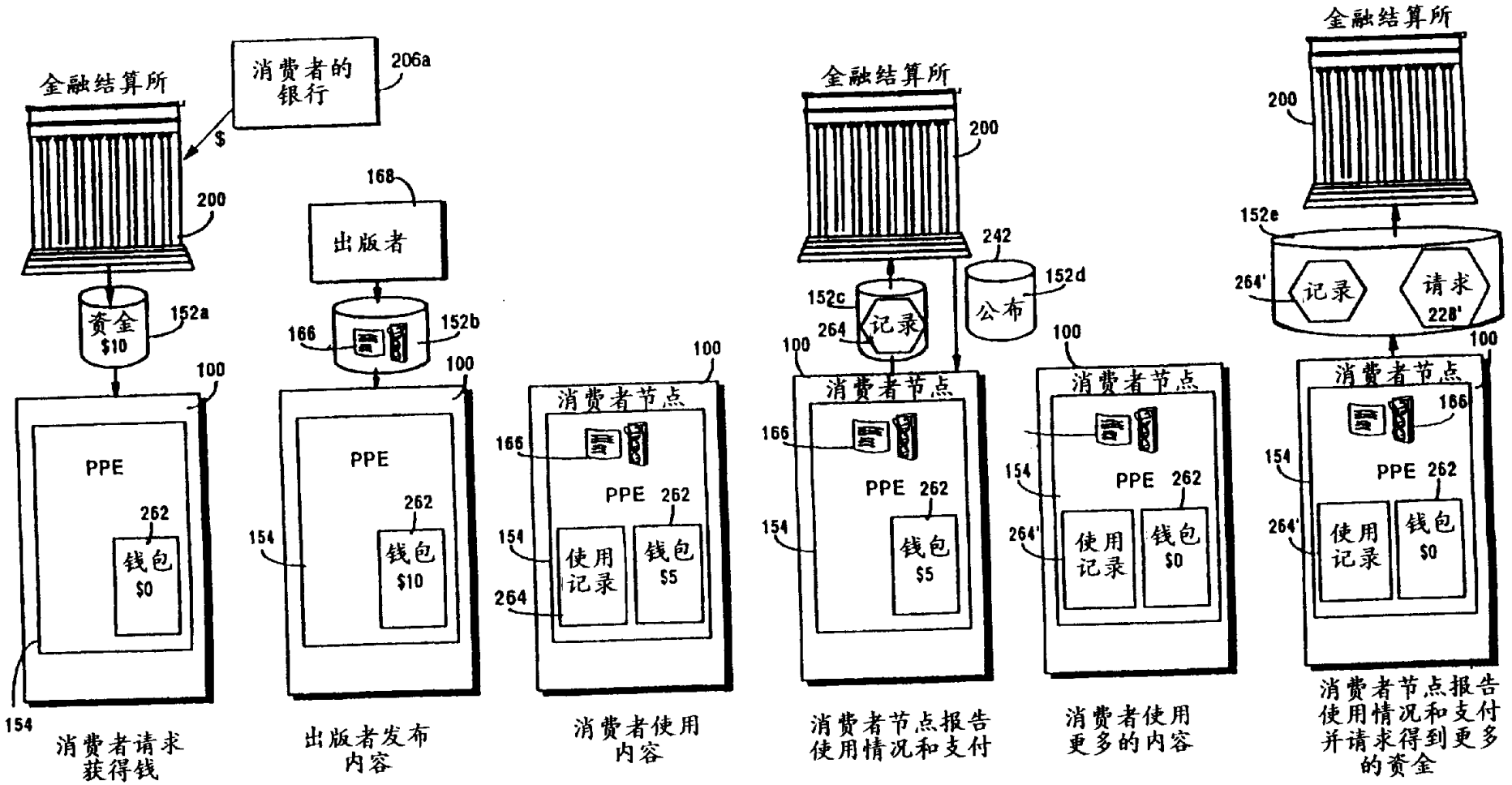


图 20　　示例性金融结算处理




金融结算所
消费者的银行
206a
$
200
资金 $10
152a
100
PPE
262
钱包 $0
154
消费者请求获得钱
图 20A
168
出版者
166
152b
100
PPE
262
钱包 $10
154
出版者发布内容
图 20B
100
消费者节点
166
PPE 262
154
使用记录
钱包 $5
264
消费者使用内容
图 20C
金融结算所
200
242
152c
记录
264
公布
152d
100
消费者节点
166
PPE 262
154
钱包 $5
消费者节点报告使用情况和支付
图 20D
100
消费者节点
PPE 262
154
264'
使用记录
钱包 $0
消费者使用更多的内容
图20E
金融结算所
200
152e
264'
记录
请求 228'
100
消费者节点
166
PPE 262
154
264'
使用记录
钱包 $0
消费者节点报告使用情况和支付并请求得到更多的资金
图 20F

示例性金融结算活动

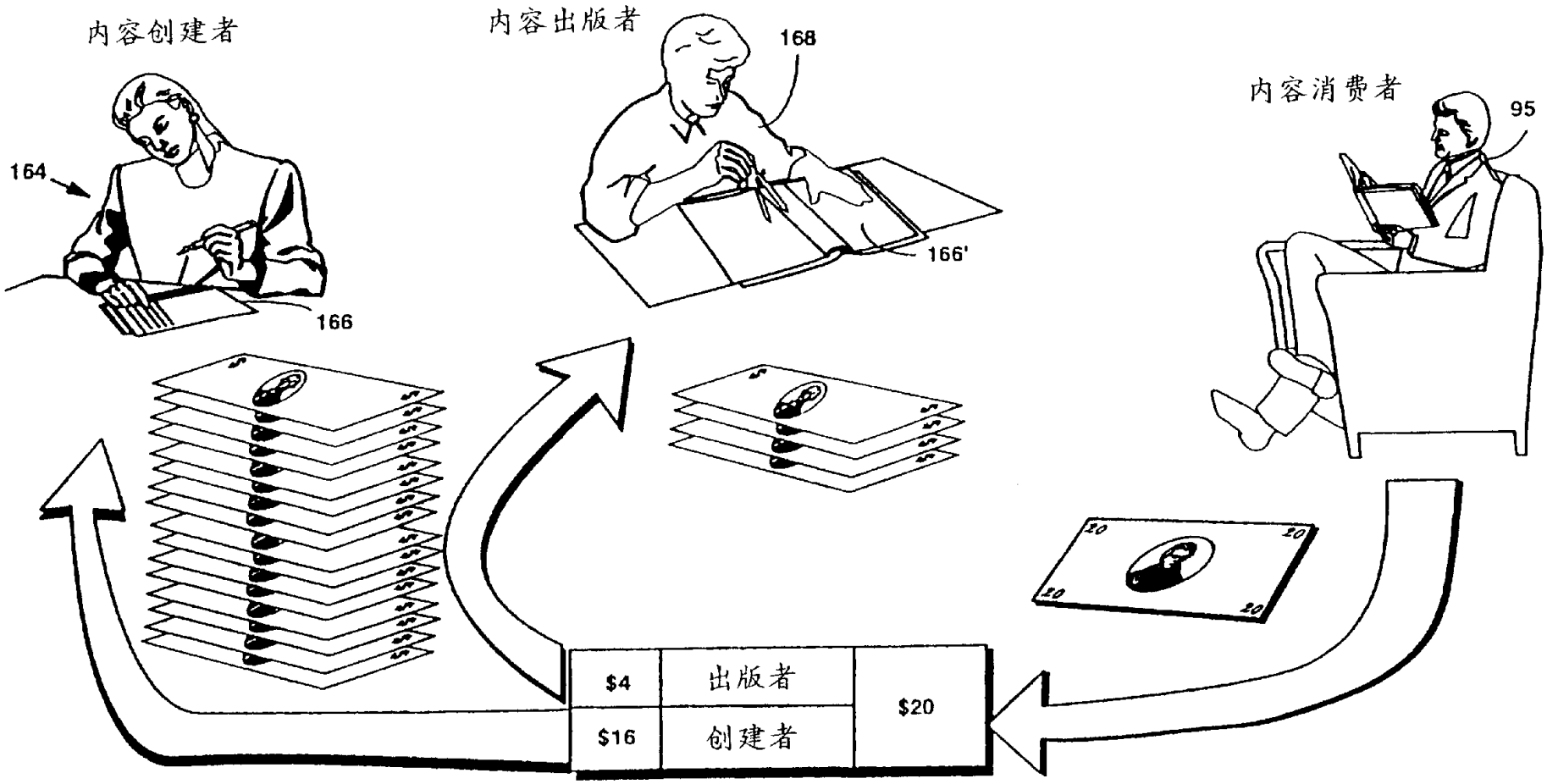


图 21 示例性支付分解

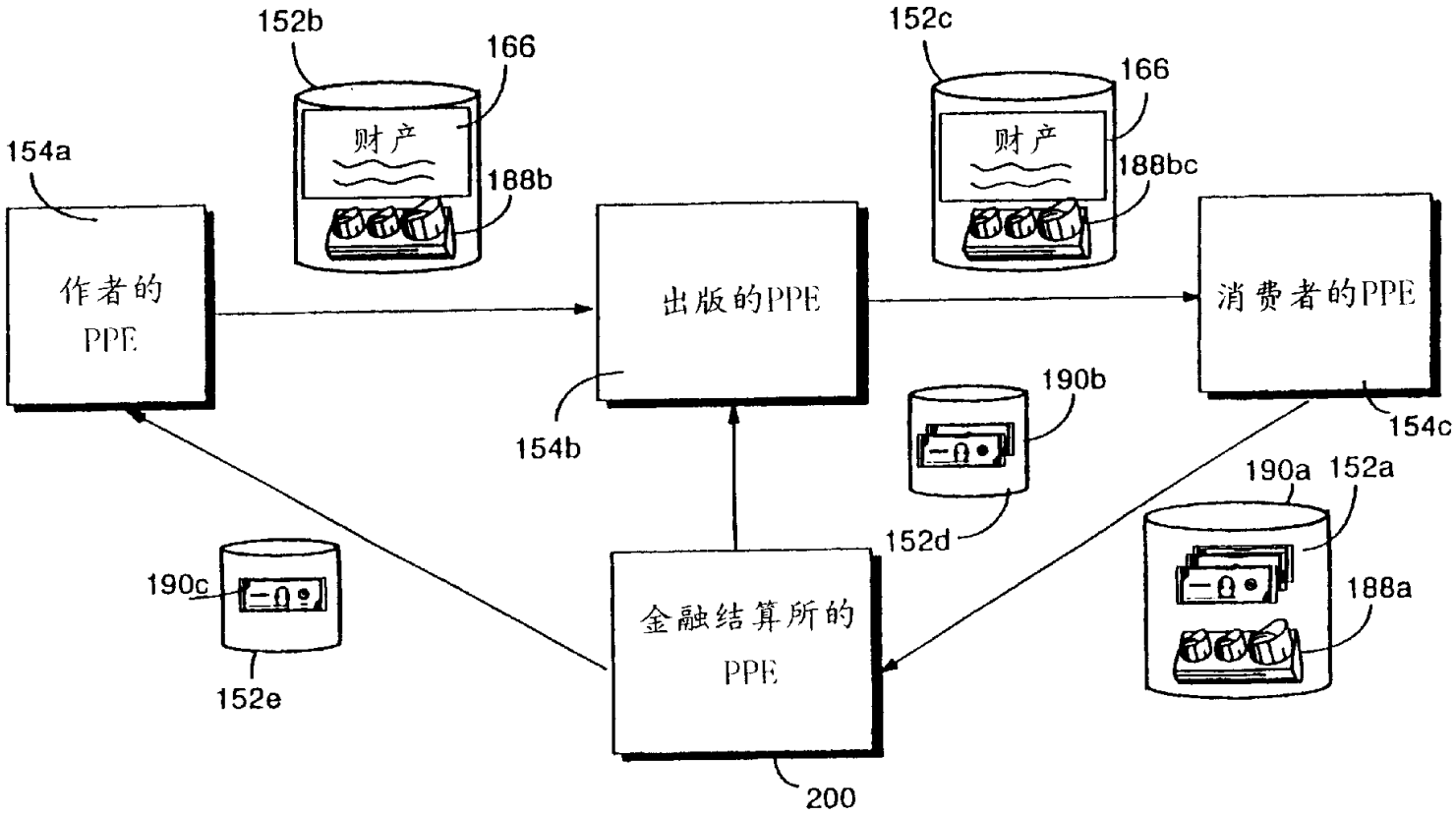


图 22 支付和再分布的实例

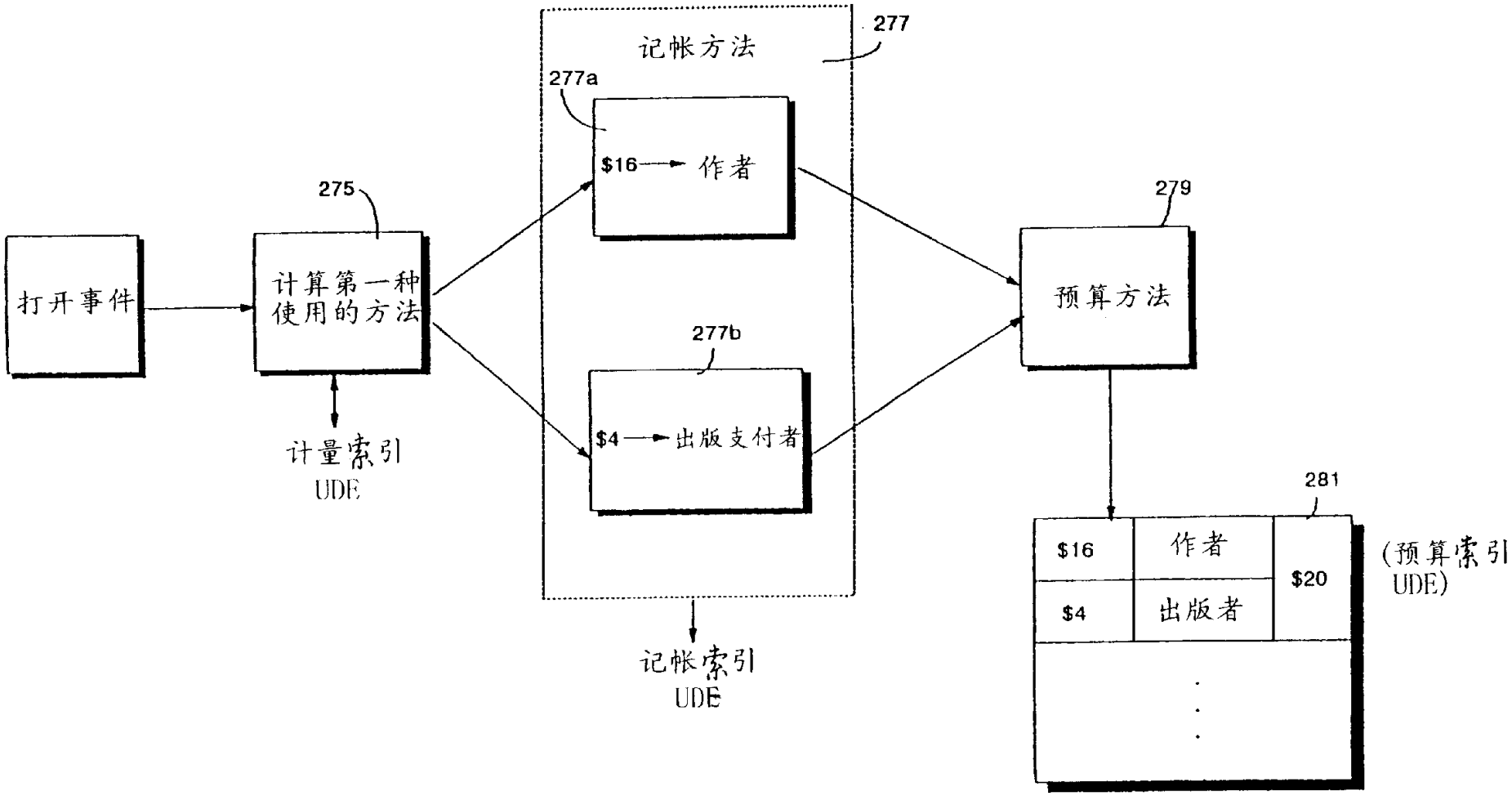


图 22A 用户节点分解实例

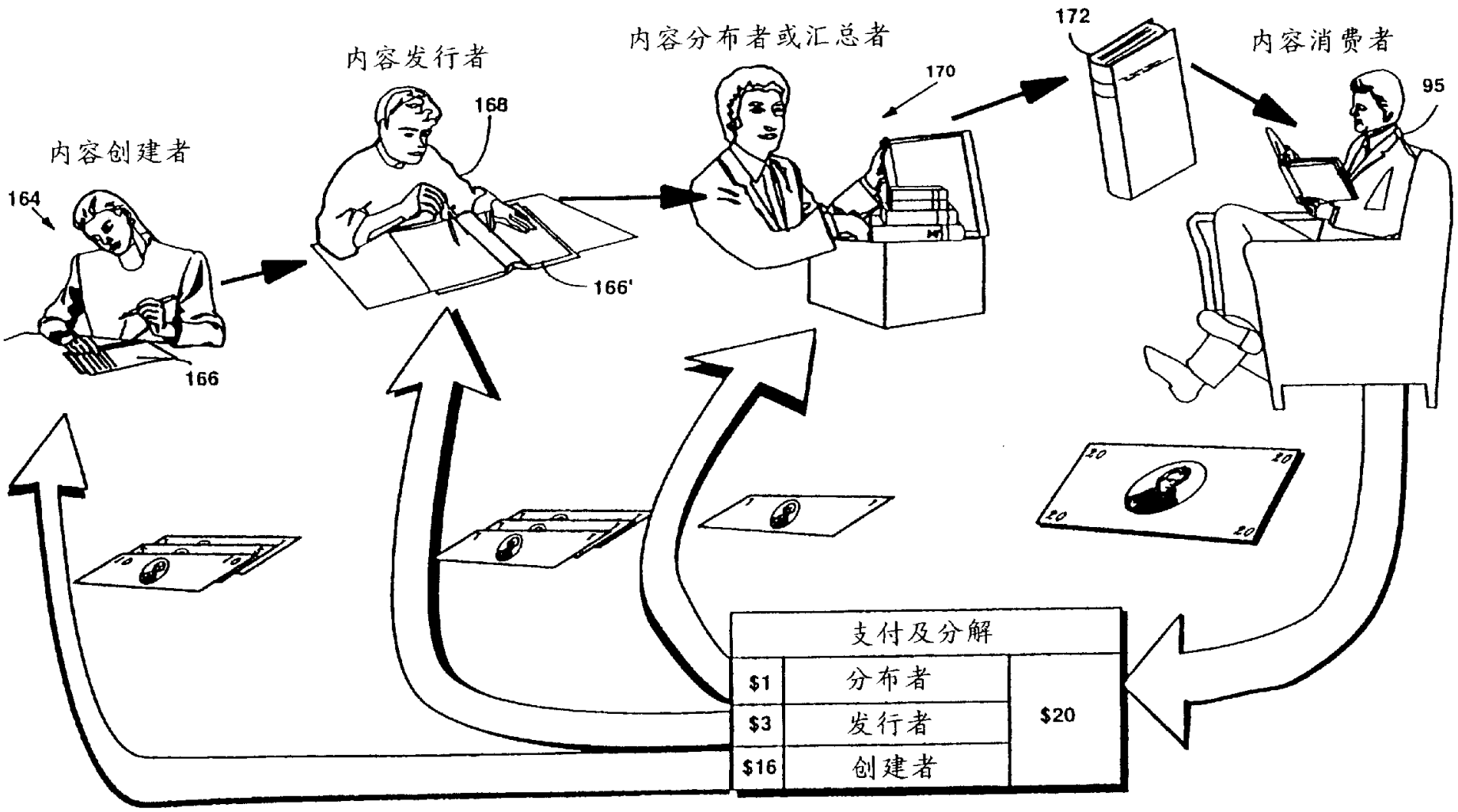

内容创建者
164
166
内容发行者
168
166'
内容分布者或汇总者
170
172
内容消费者
95
支付及分解
$1
分布者
$3
发行者
$16
创建者
$20

图 23 支付的分解

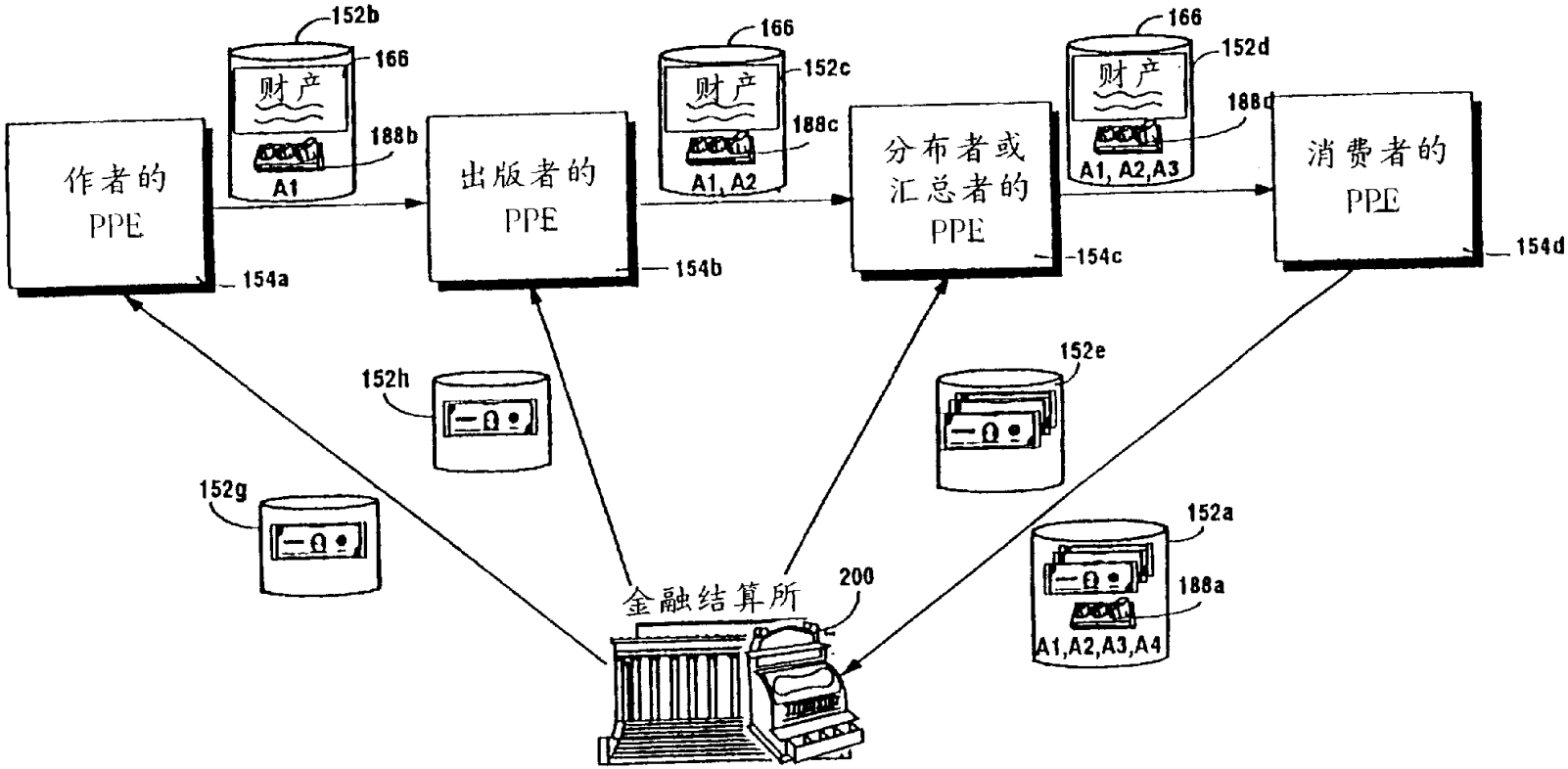


图 24 示例性支付和再分布方案

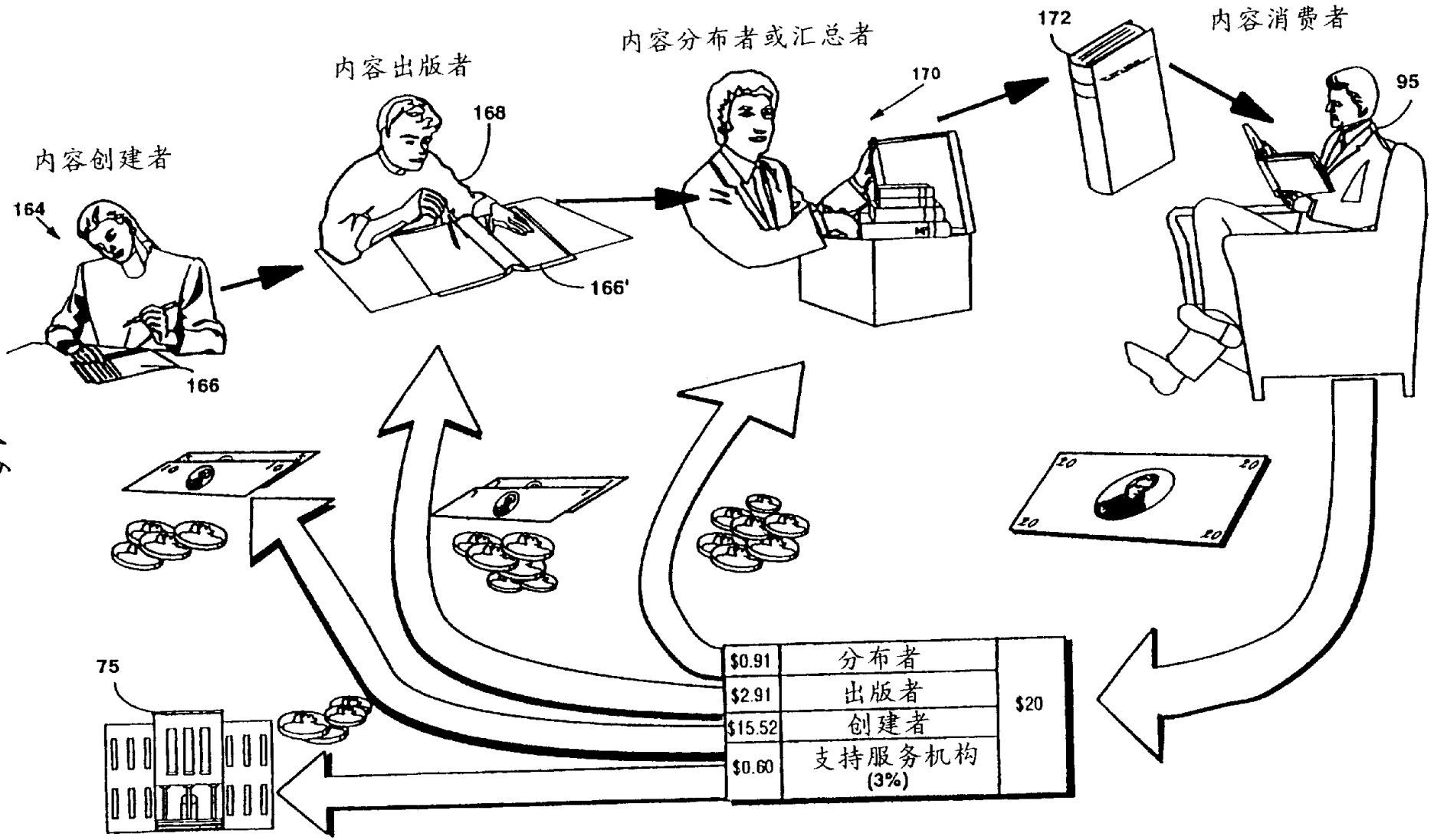

内容创建者
164
166
内容出版者
168
166'
内容分布者或汇总者
170
172
内容消费者
95
75
$0.91
分布者
$2.91
出版者
$15.52
创建者
$0.60
支持服务机构
(3%)
$20

图 25 示例性支付分解

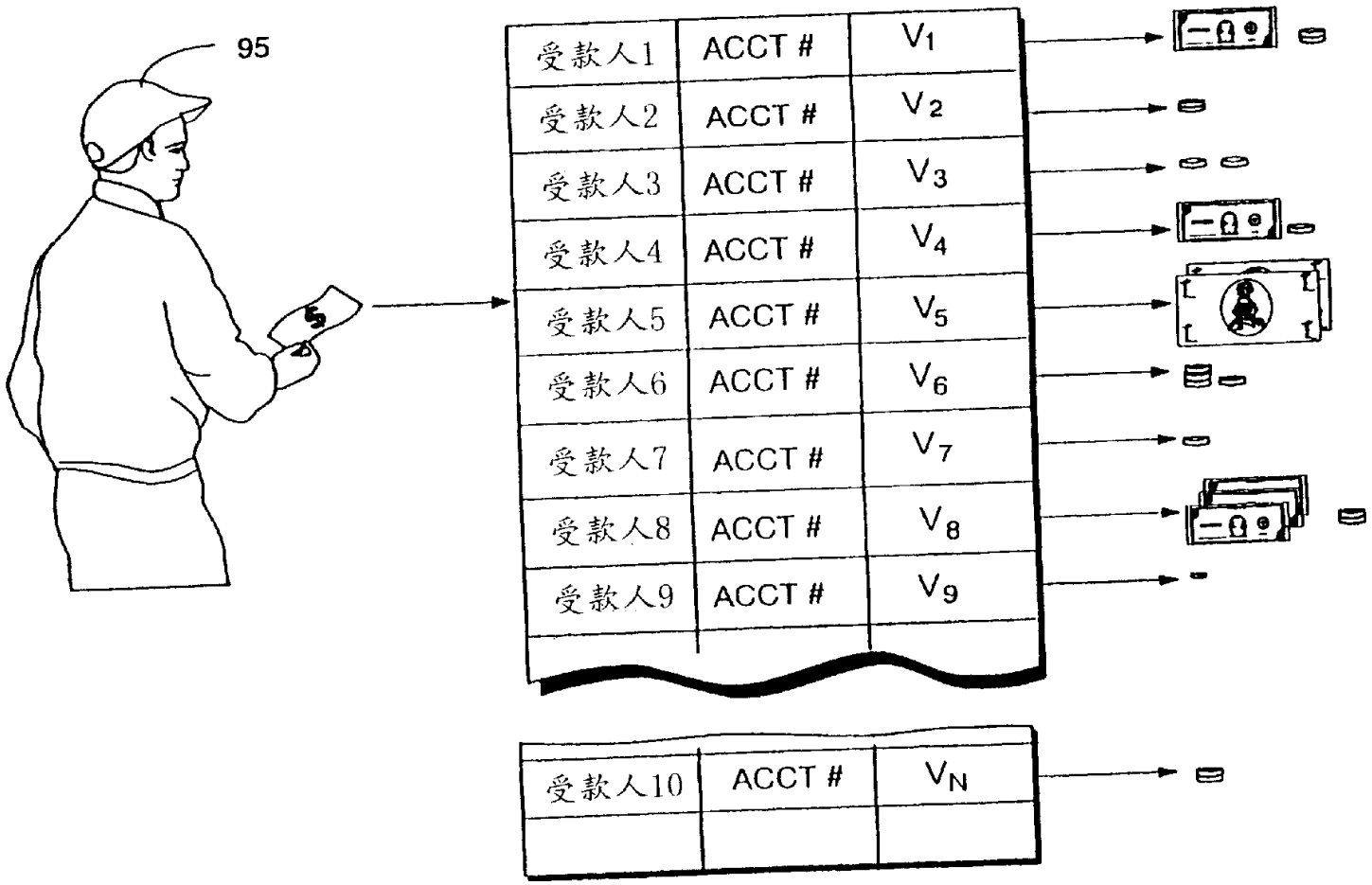

95
受款人1
ACCT #
V1
受款人2
ACCT #
V2
受款人3
ACCT #
V3
受款人4
ACCT #
V4
受款人5
ACCT #
V5
受款人6
ACCT #
V6
受款人7
ACCT #
V7
受款人8
ACCT #
V8
受款人9
ACCT #
V9
受款人10
ACCT #
VN

图 26 支付分解

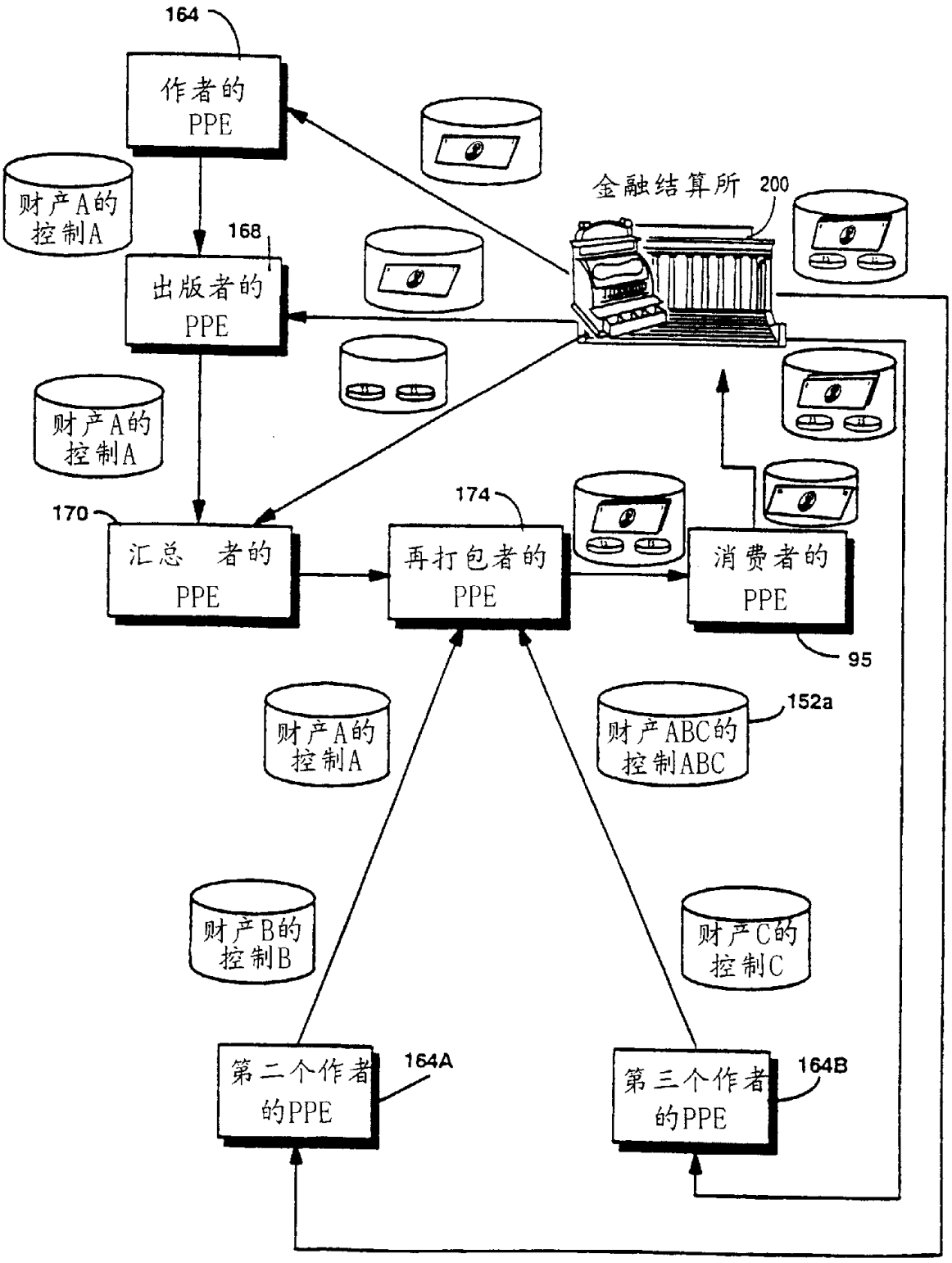
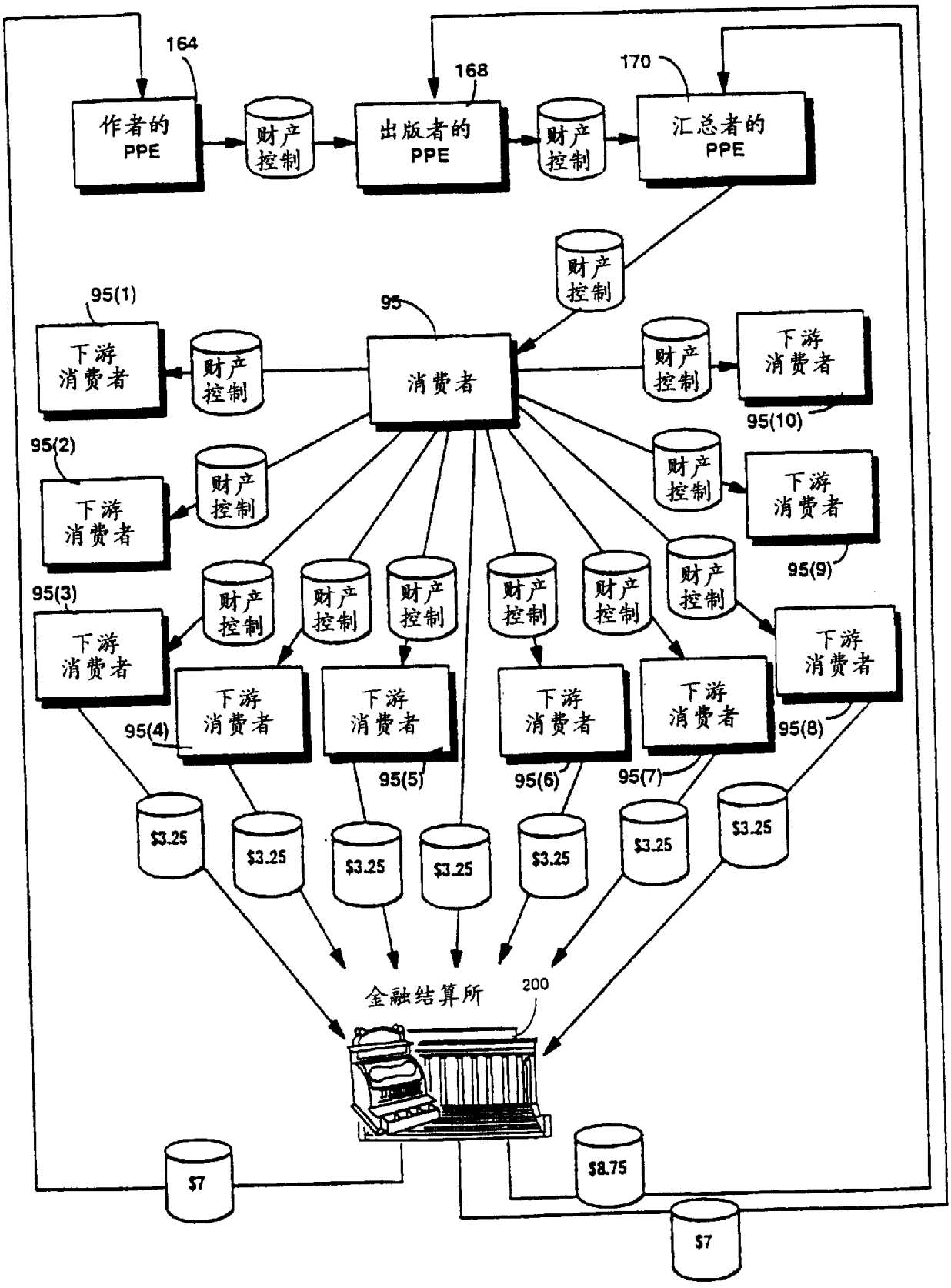


图 27

示例性支付和再分布方案

图 28 示例性超级分布


164
168
170
作者的 PPE
财产控制
出版者的 PPE
财产控制
汇总者的 PPE
财产控制
95(1)
95
下游消费者
财产控制
消费者
财产控制
下游消费者
95(10)
95(2)
下游消费者
财产控制
财产控制
下游消费者
95(9)
95(3)
下游消费者
财产控制
财产控制
财产控制
财产控制
财产控制
财产控制
下游消费者
下游消费者
下游消费者
下游消费者
下游消费者
95(4)
95(5)
95(6)
95(7)
95(8)
$3.25
$3.25
$3.25
$3.25
$3.25
$3.25
$3.25
金融结算所
200
$7
$8.75
$7

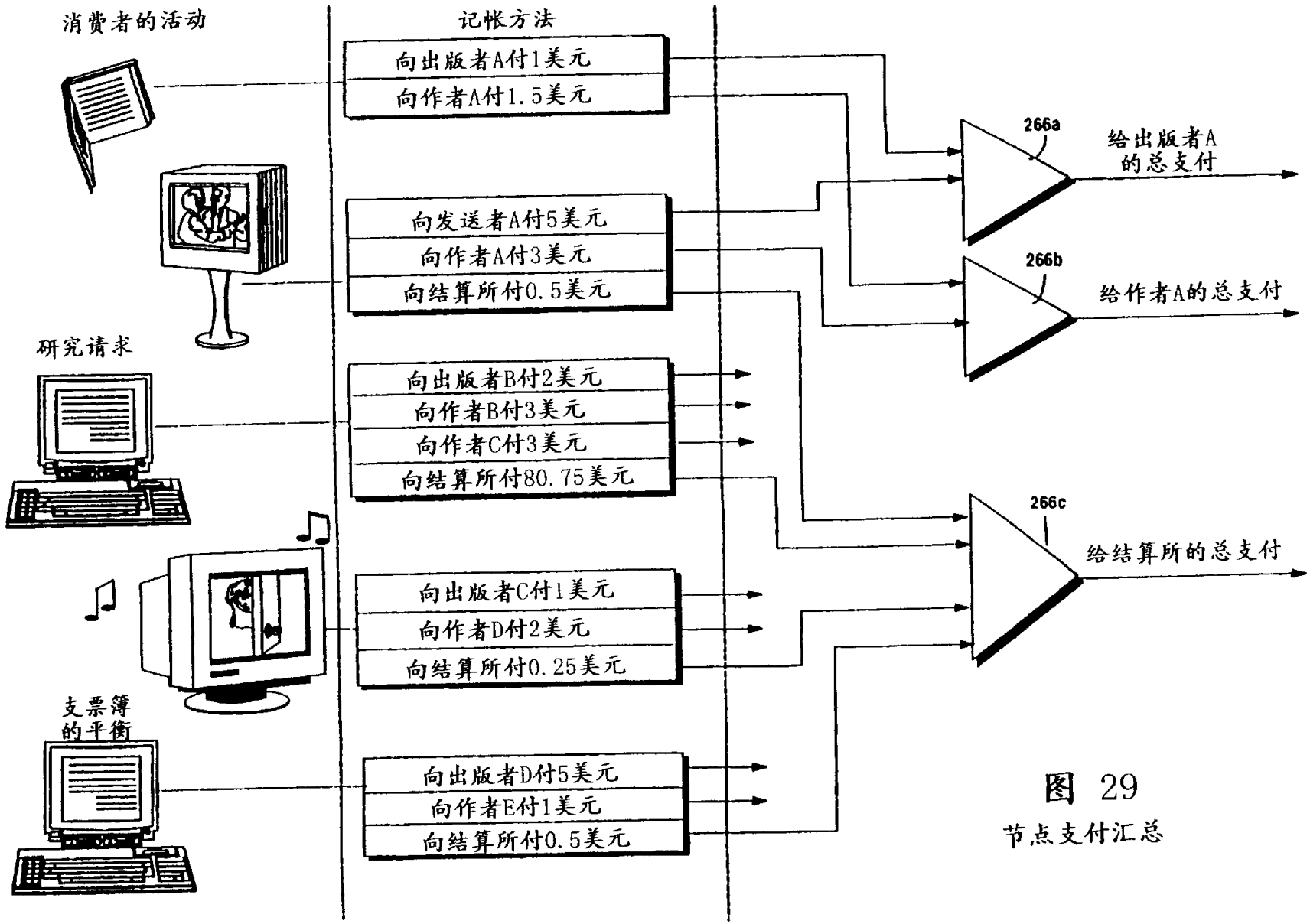

消费者的活动
记帐方法
向出版者A付1美元
向作者A付1.5美元
向发送者A付5美元
向作者A付3美元
向结算所付0.5美元
研究请求
向出版者B付2美元
向作者B付3美元
向作者C付3美元
向结算所付80.75美元
向出版者C付1美元
向作者D付2美元
向结算所付0.25美元
支票簿
的平衡
向出版者D付5美元
向作者E付1美元
向结算所付0.5美元
266a
给出版者A
的总支付
266b
给作者A的总支付
266c
给结算所的总支付

图 29

节点支付汇总

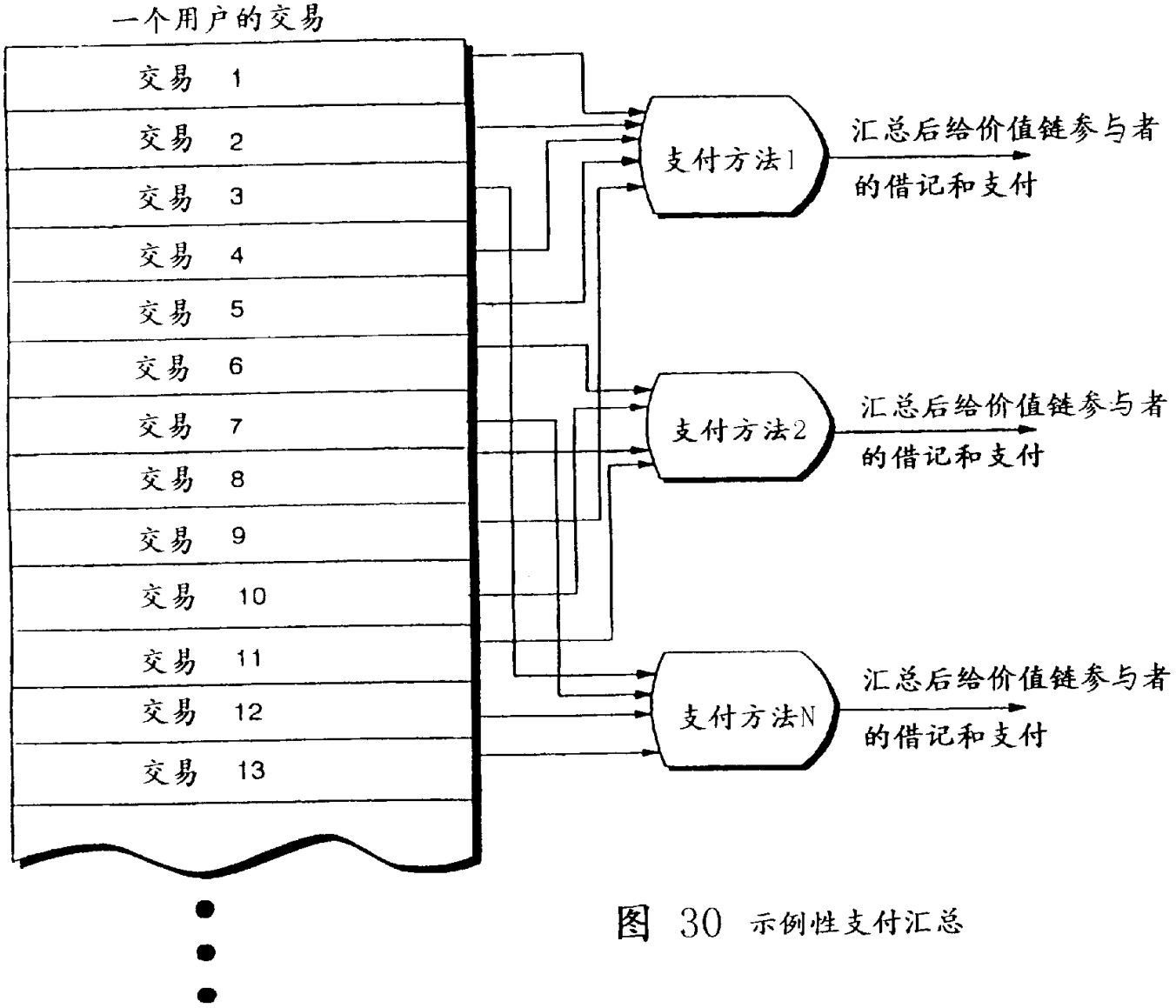

一个用户的交易
交易 1
交易 2
交易 3
交易 4
交易 5
交易 6
交易 7
交易 8
交易 9
交易 10
交易 11
交易 12
交易 13
支付方法1
汇总后给价值链参与者的借记和支付
支付方法2
汇总后给价值链参与者的借记和支付
支付方法N
汇总后给价值链参与者的借记和支付

图 30 示例性支付汇总

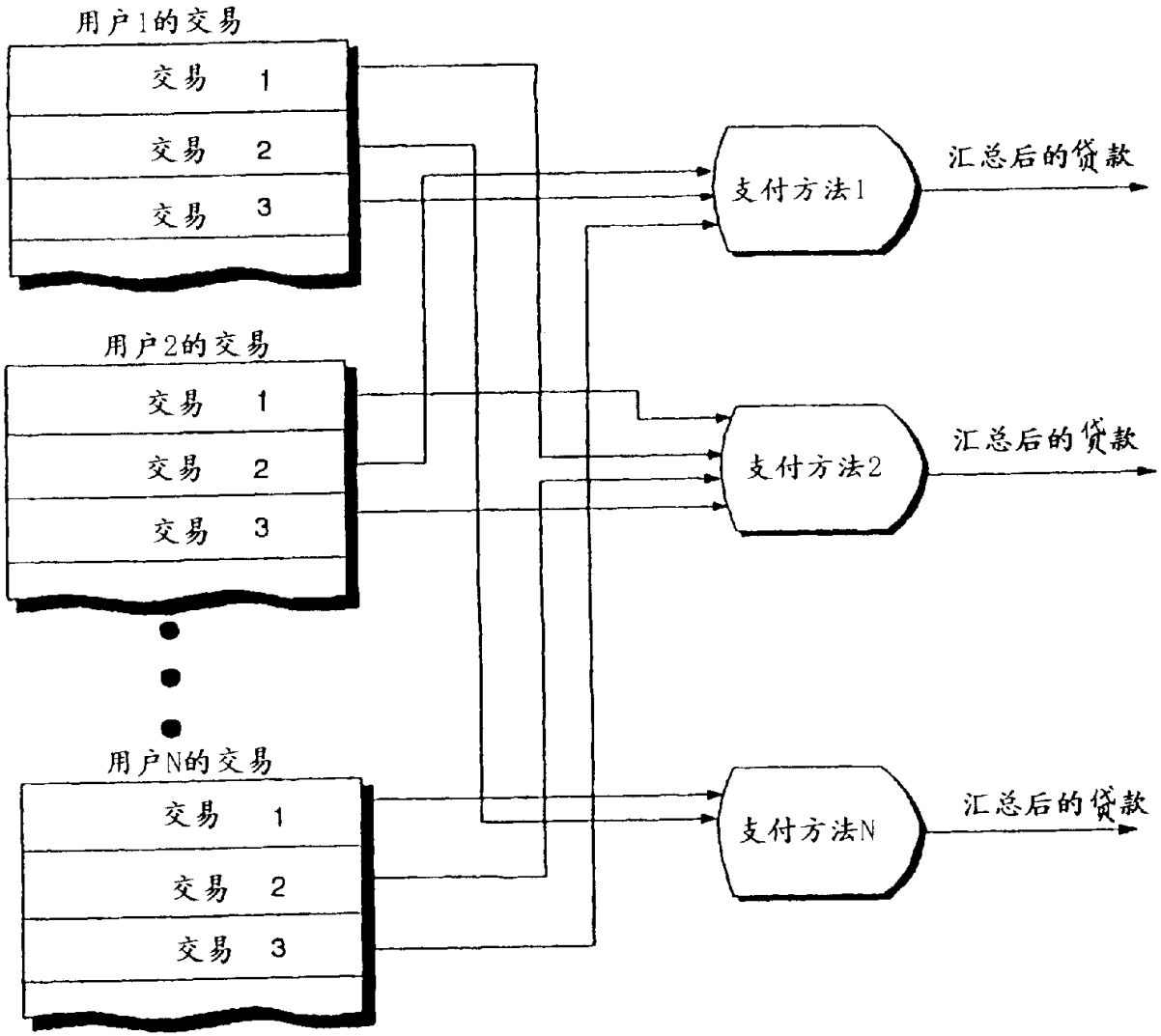


图 31 金融结算所的示例性支付汇总

图 32 示例性的金融结算所安排

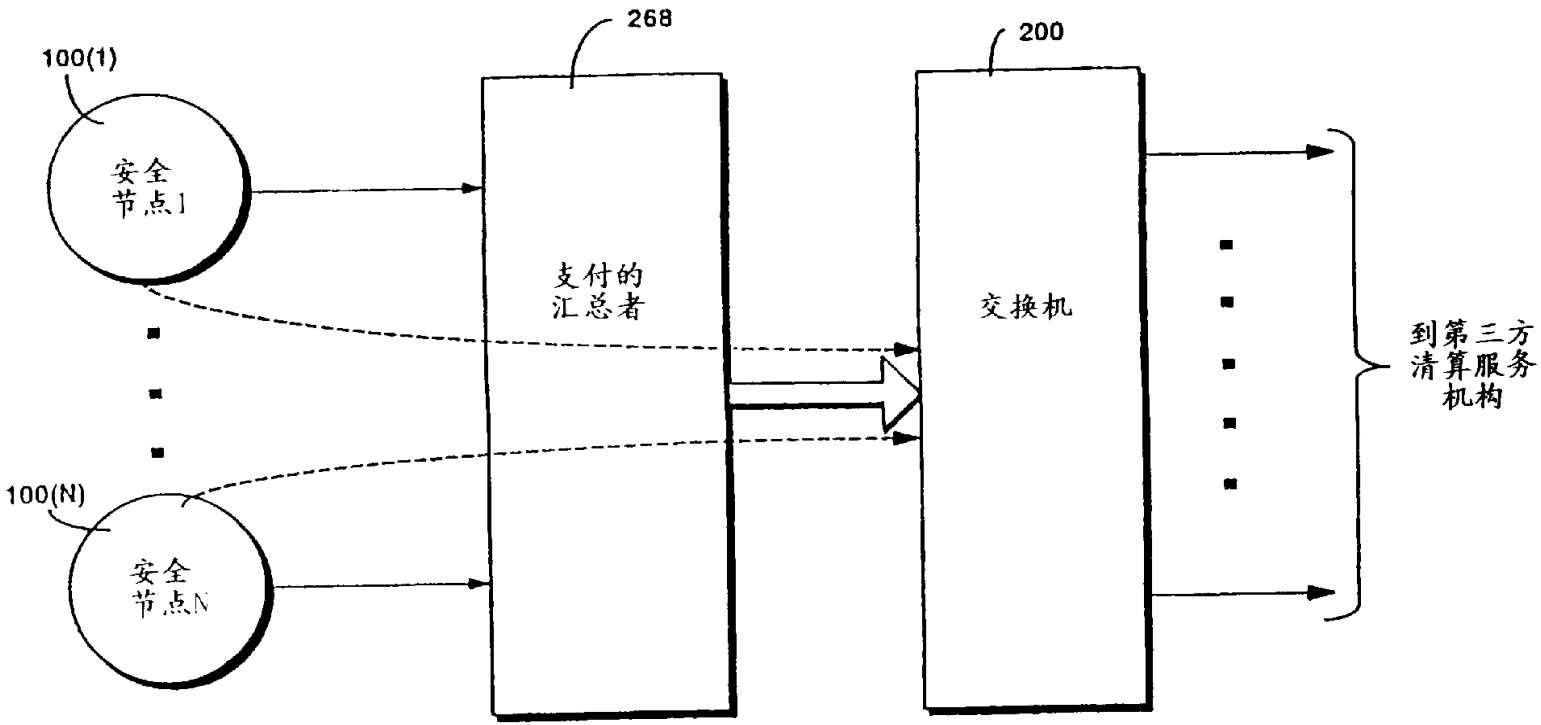


图 33
使用结算所实例

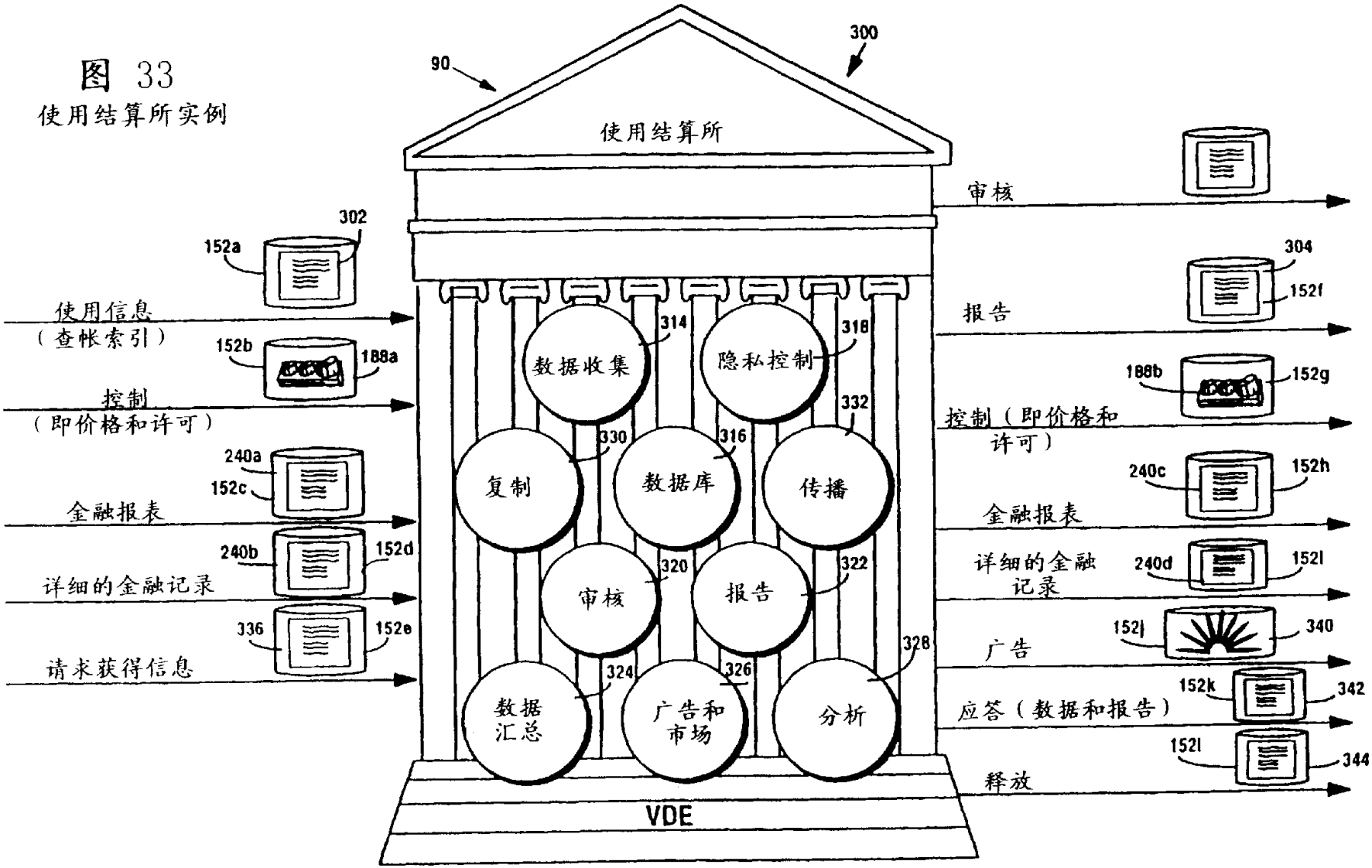

90
300
使用结算所
302
152a
使用信息
（查帐索引）
152b
188a
控制
（即价格和许可）
240a
152c
金融报表
240b
152d
详细的金融记录
336
152e
请求获得信息
数据收集
314
隐私控制
318
复制
330
数据库
316
传播
332
审核
320
报告
322
数据汇总
324
广告和市场
326
分析
328
VDE
审核
304
152f
报告
188b
152g
控制（即价格和许可）
240c
152h
金融报表
240d
152i
详细的金融记录
152j
340
广告
152k
342
应答（数据和报告）
152l
344
释放

图 34

示例性使用结算所

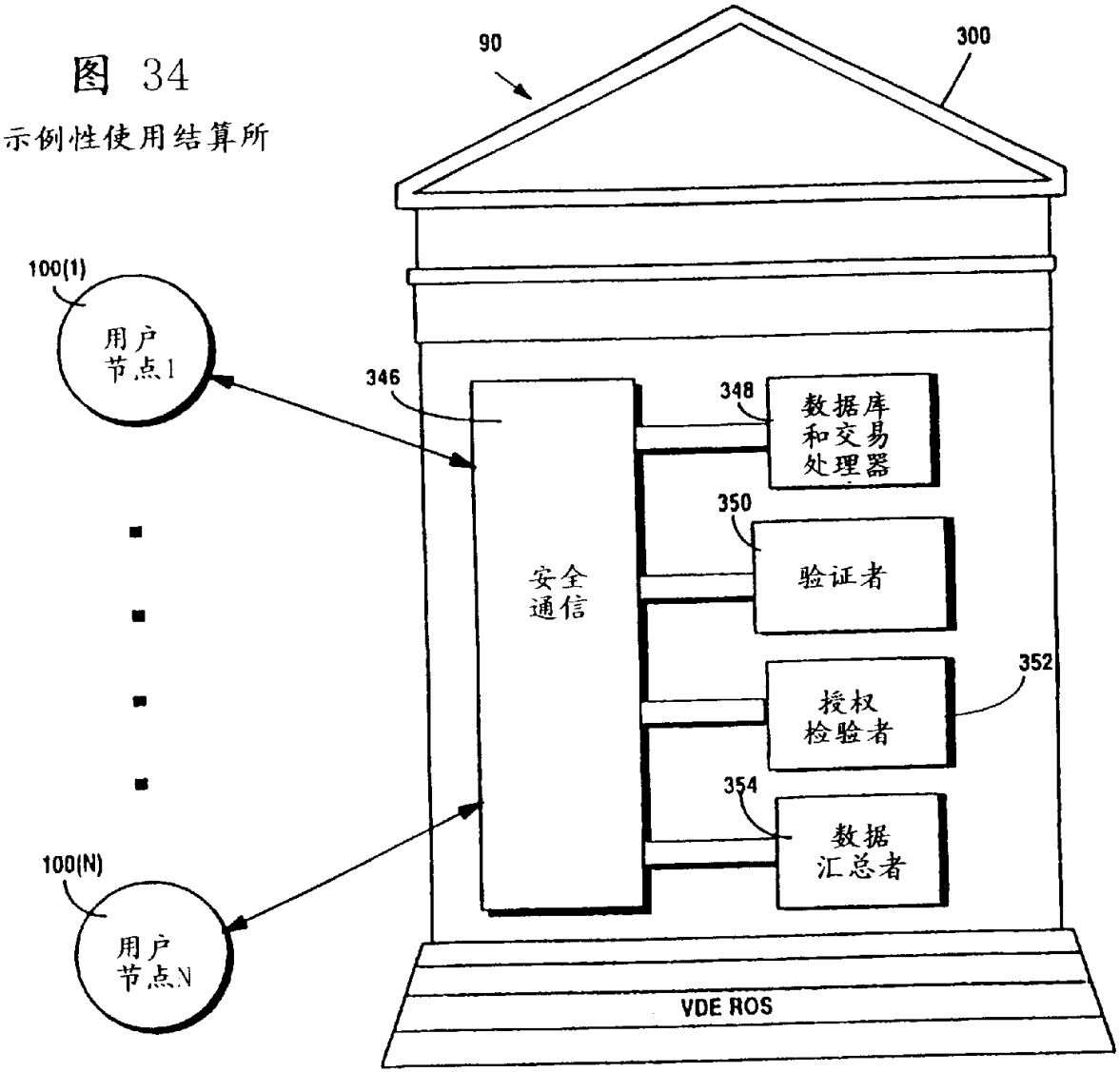


图 35 示例性使用结算过程

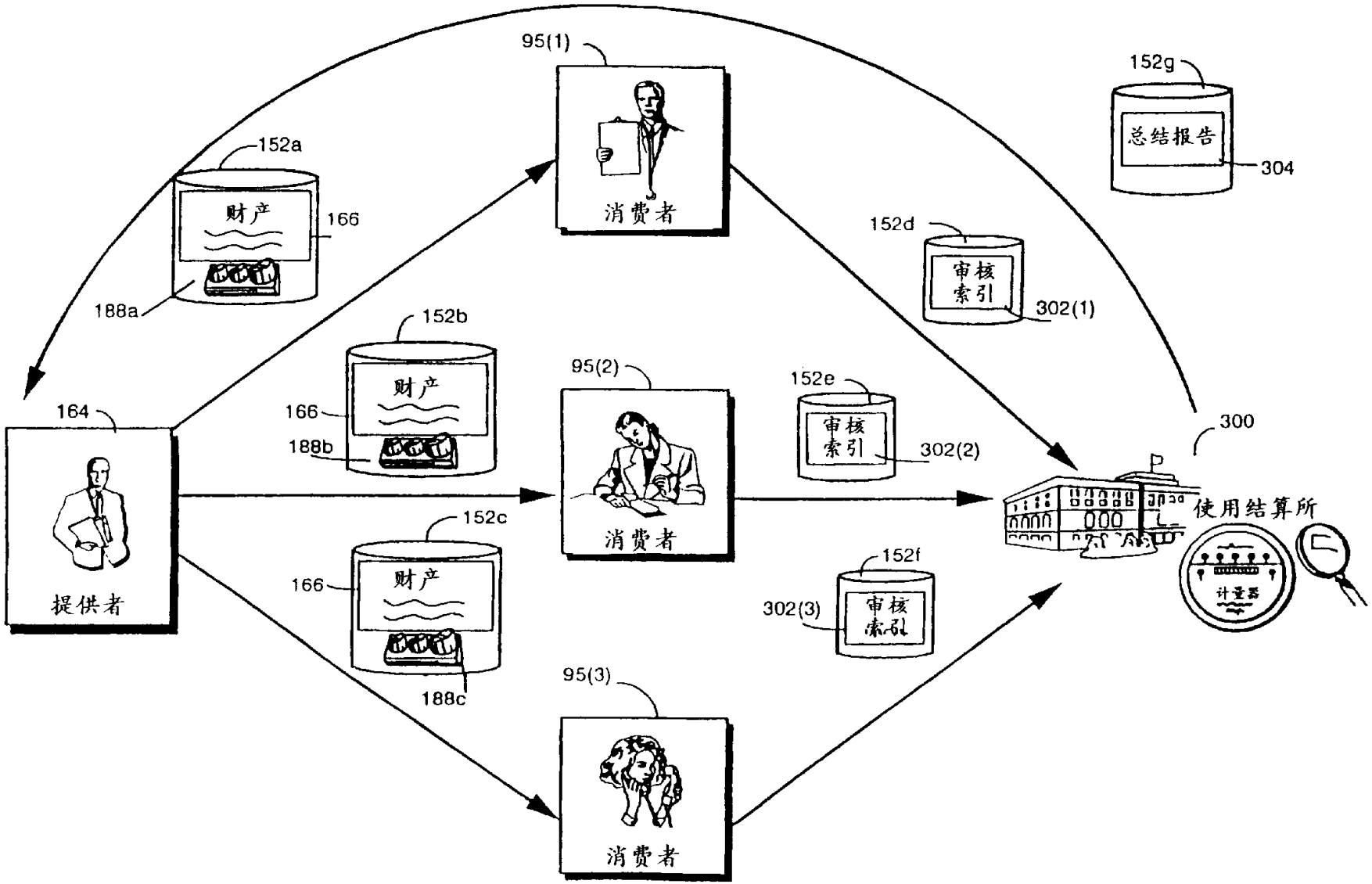


图 36 使用结算过程实例

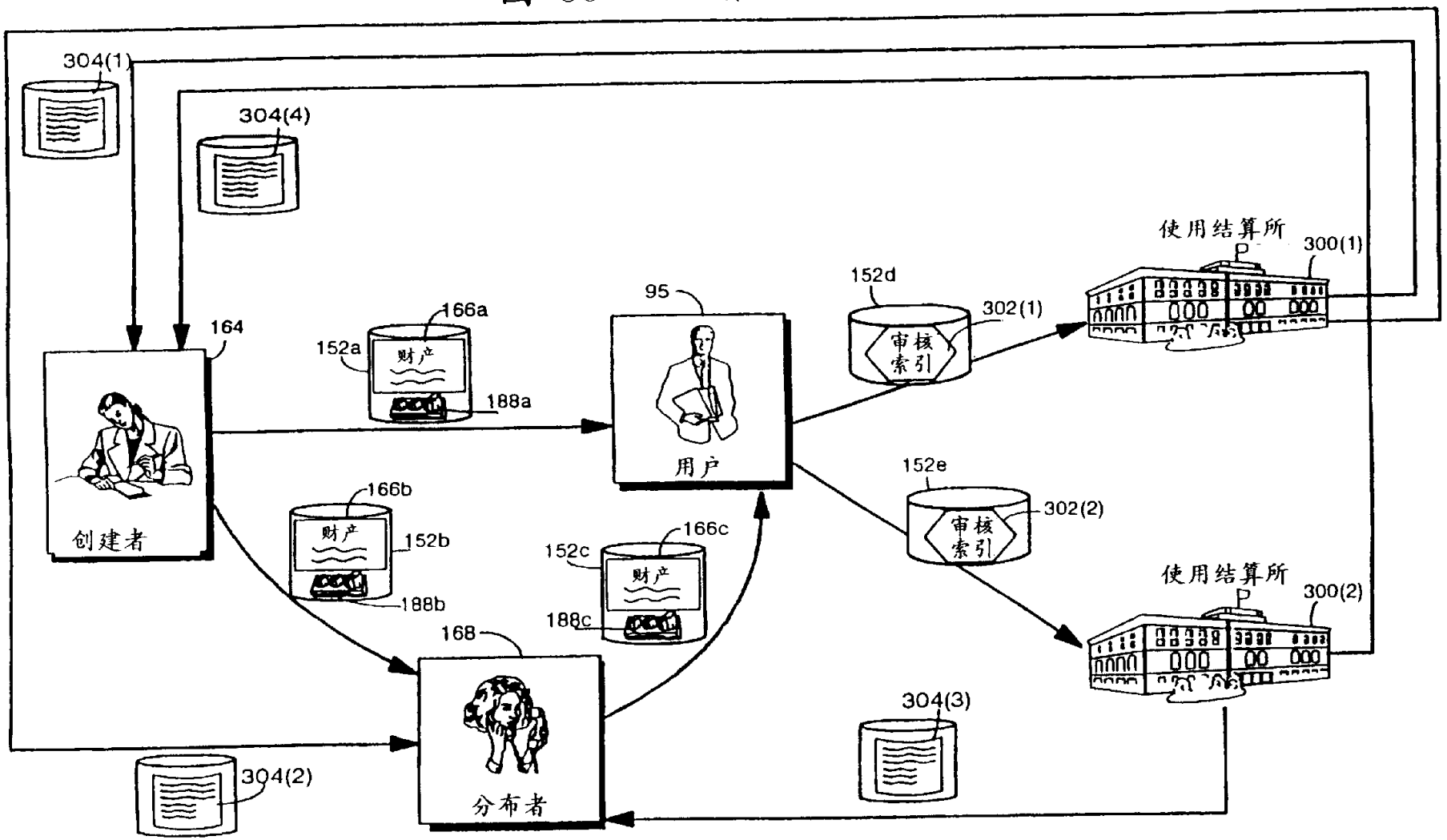


图 37 示例性金融和使用结算过程

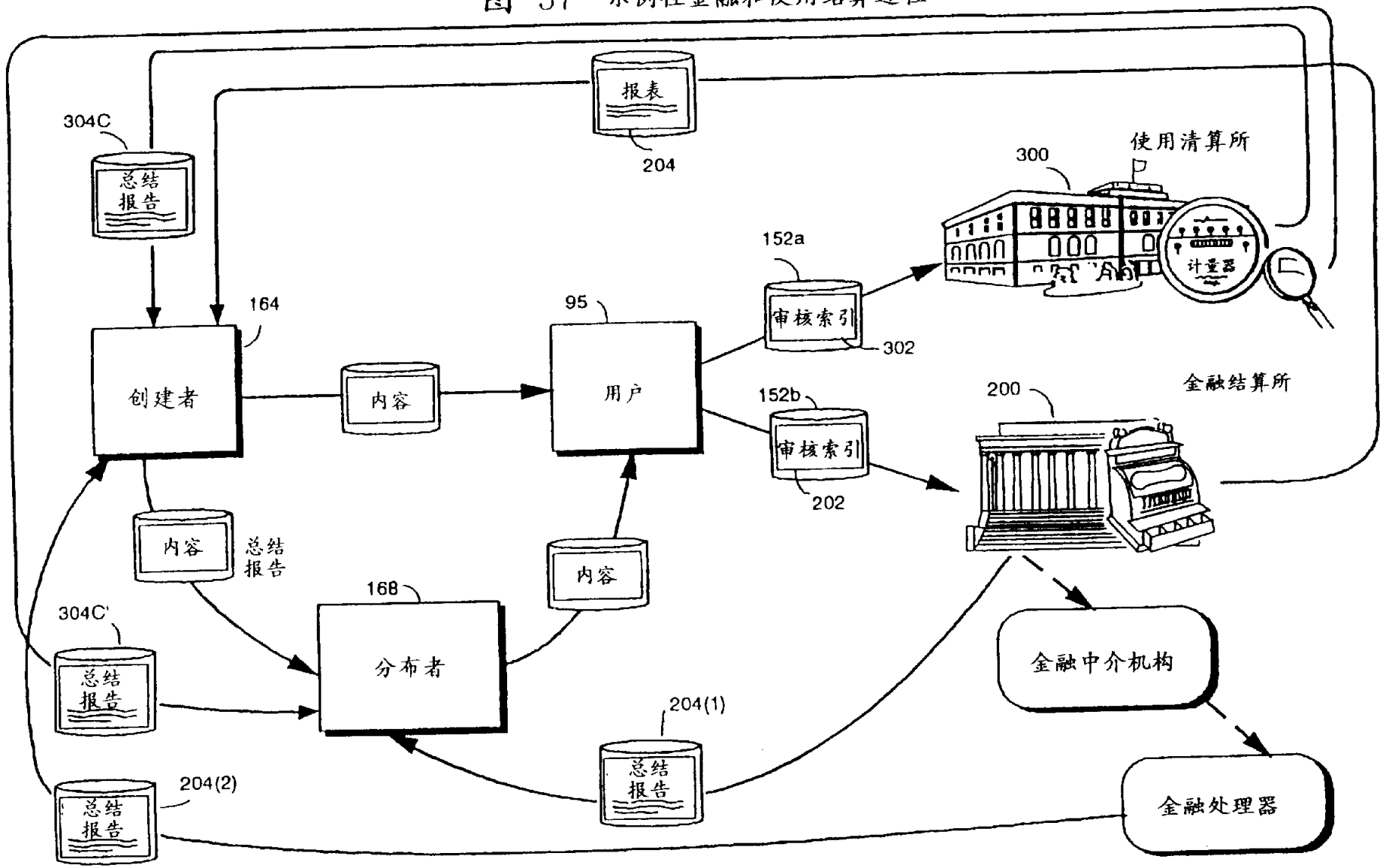


图 38 示例性使用结算所媒介定位

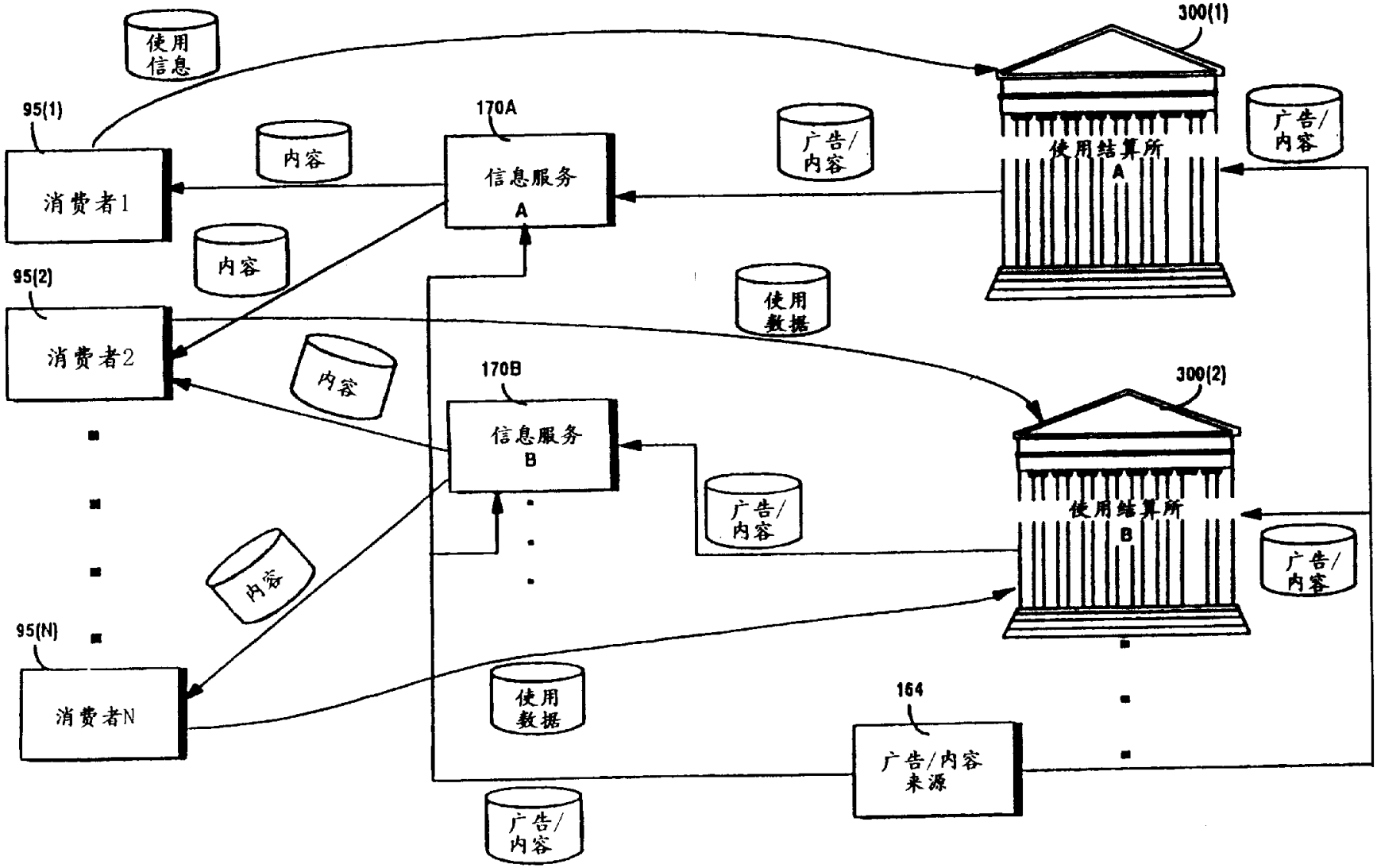


图 39 示例性使用清算所以公开为依据的折扣

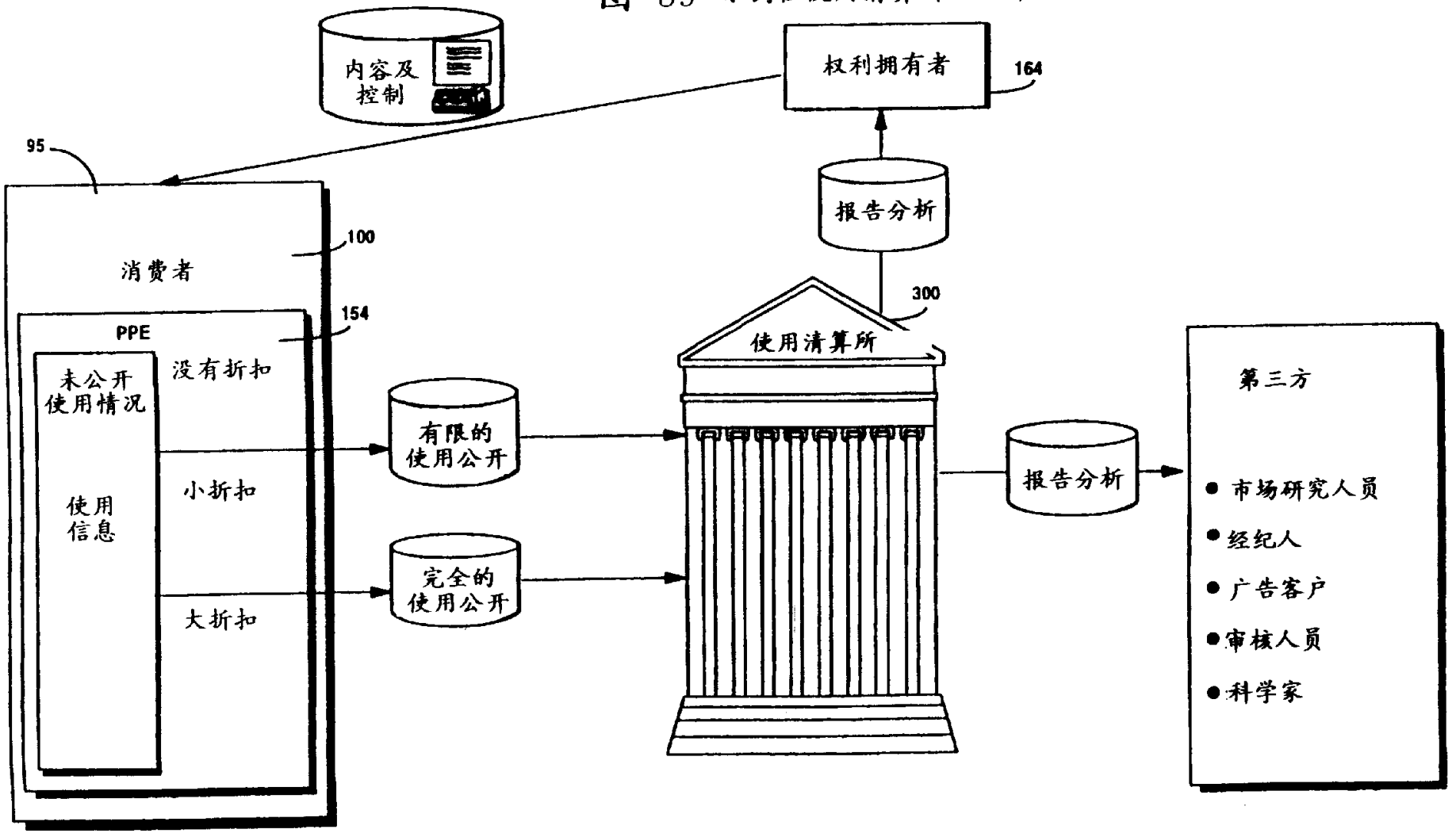


图 40

示例性权利及许可结算所

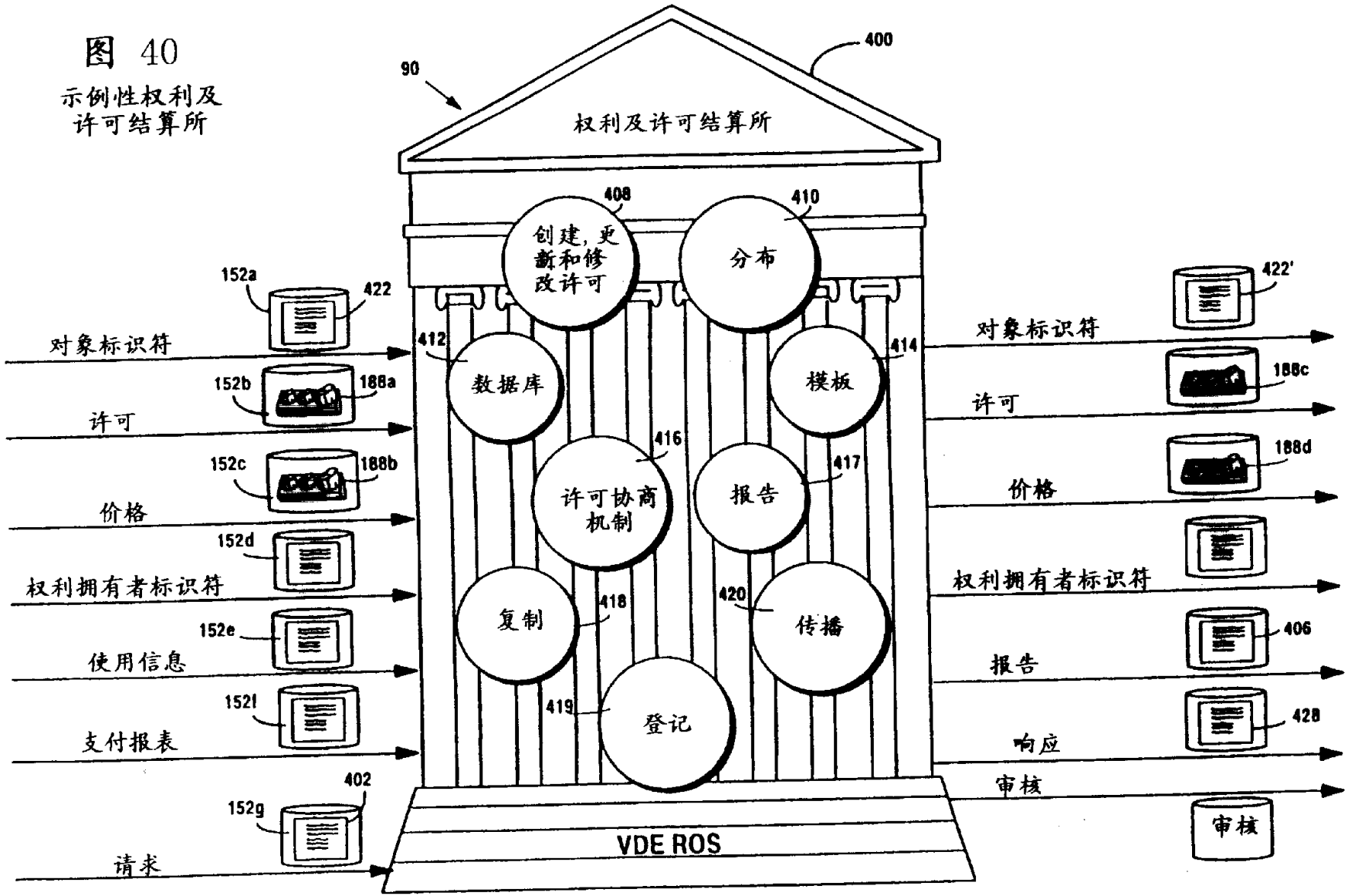
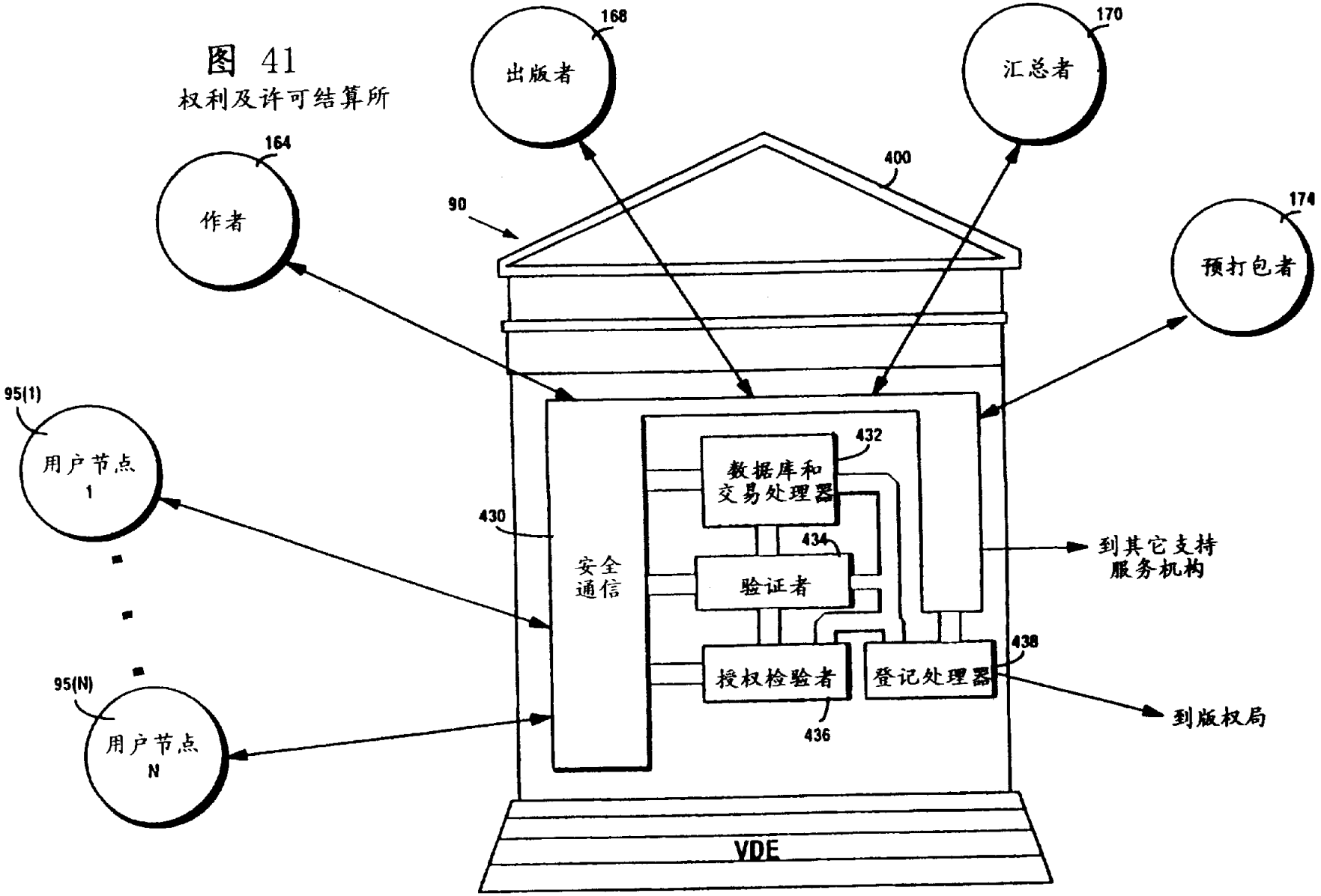


图 41
权利及许可结算所



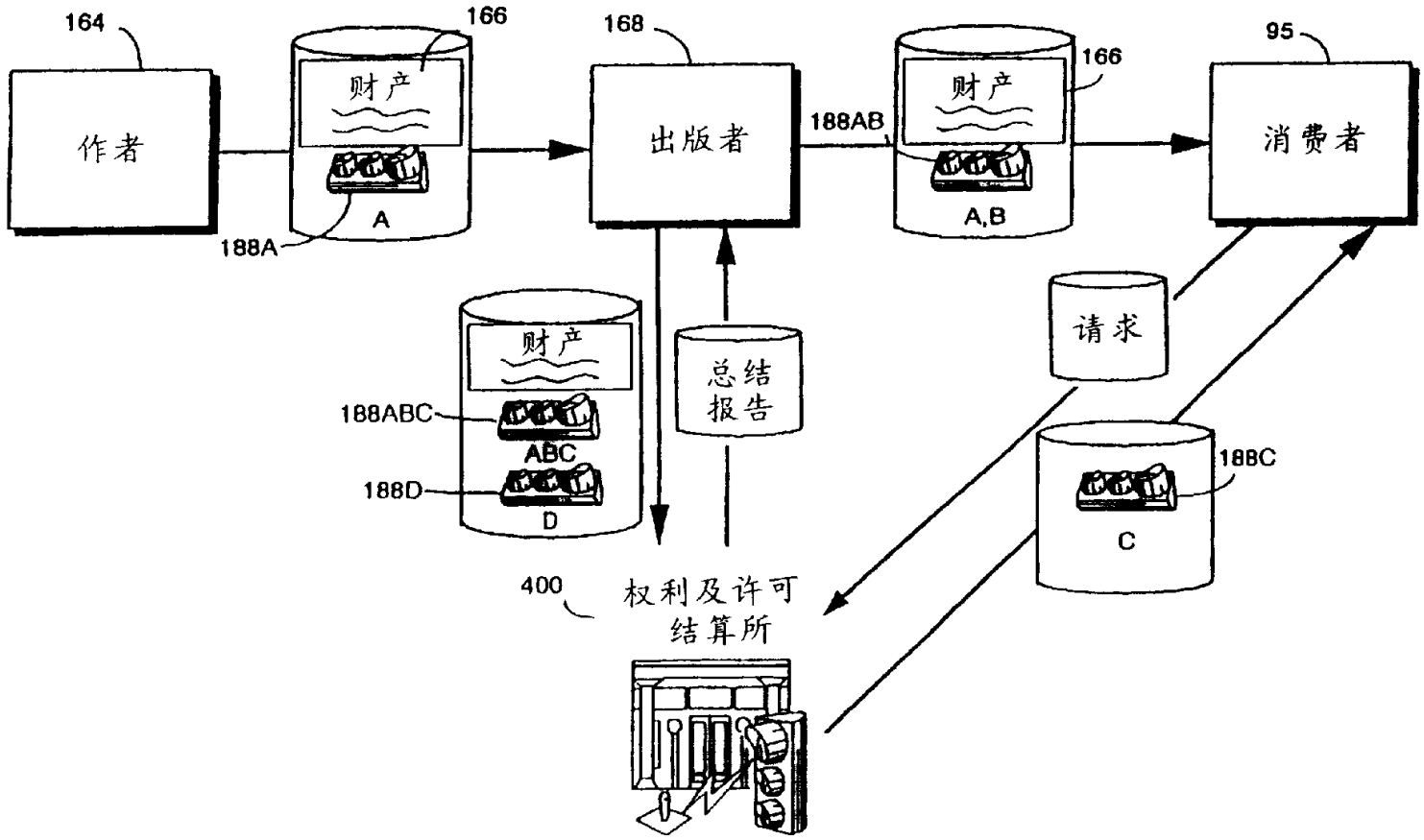


图 42 示例性权利及许可结算所处理

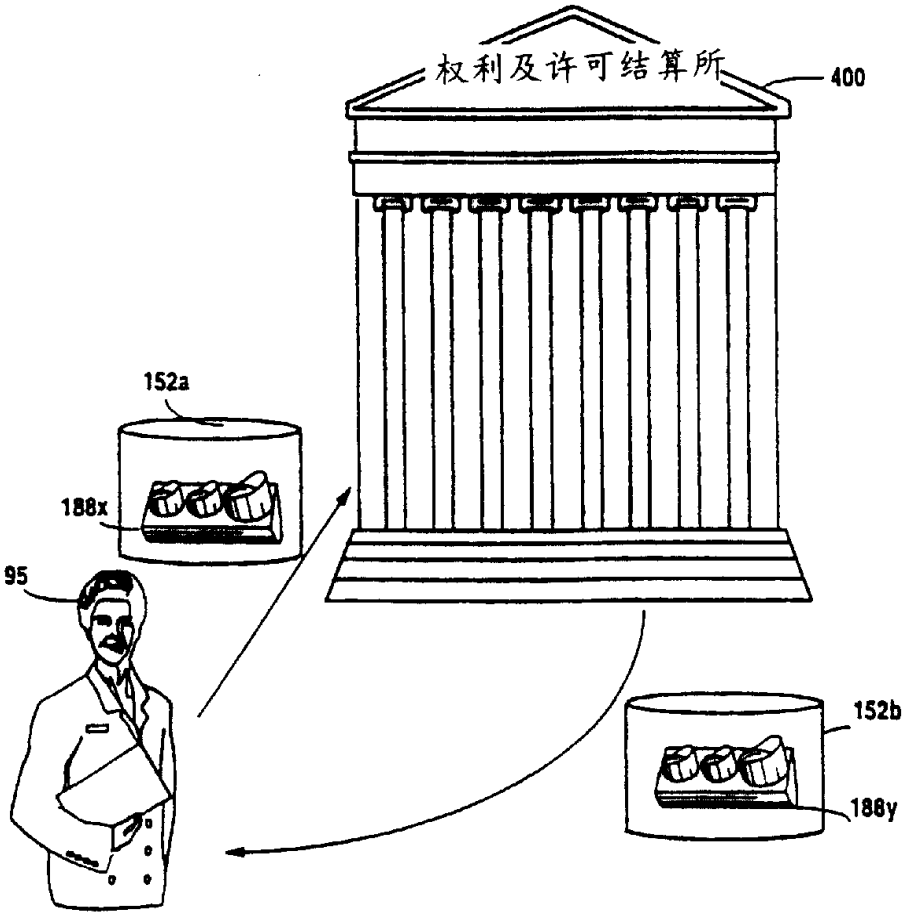


图 42A

消费者登记控制集请求更新

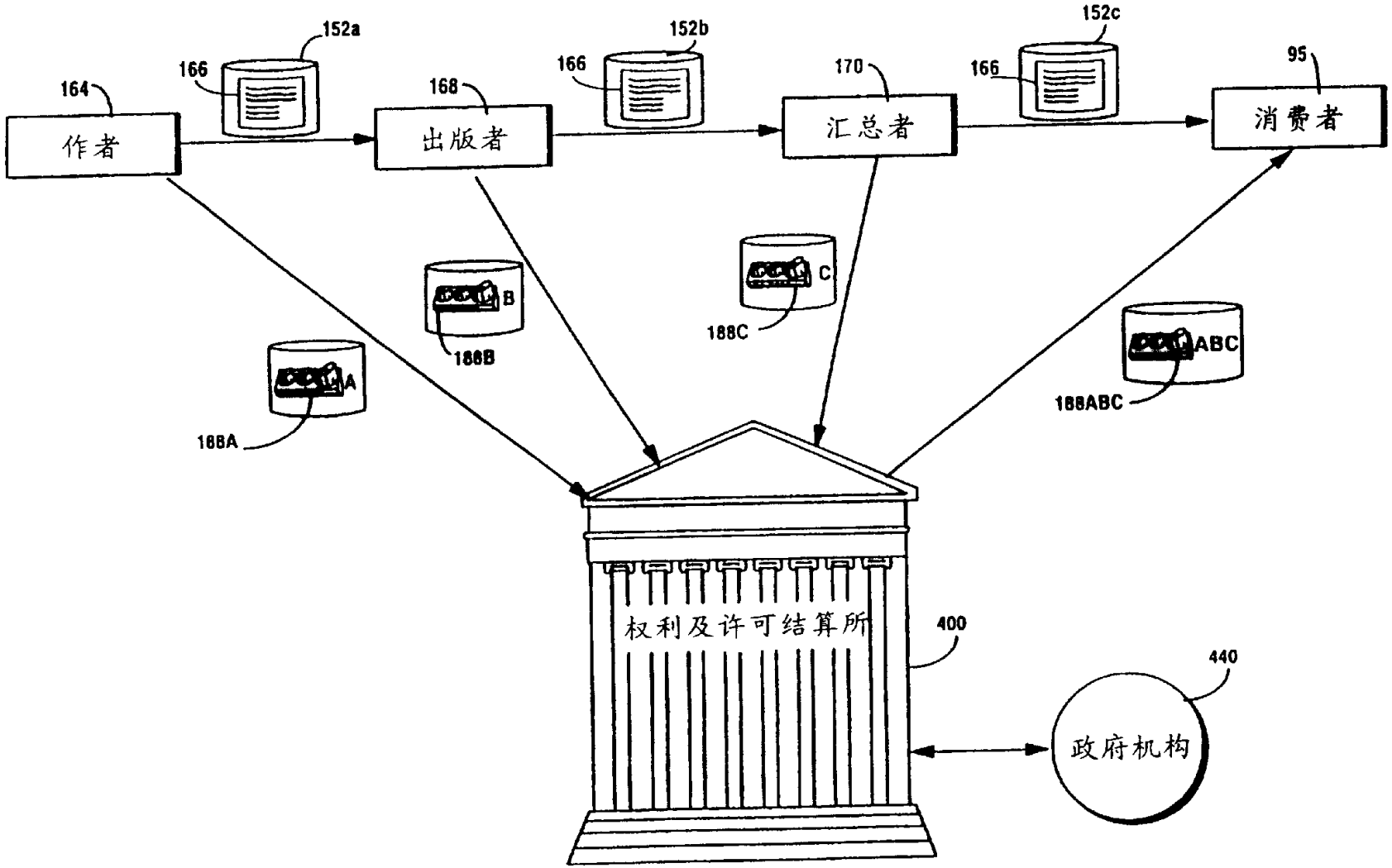


图 43　示例性权利及许可价值链

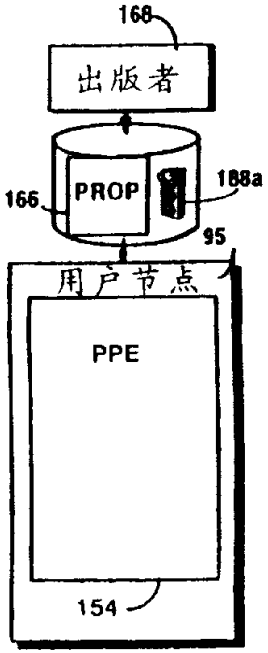


图 44A
消费者收取财产

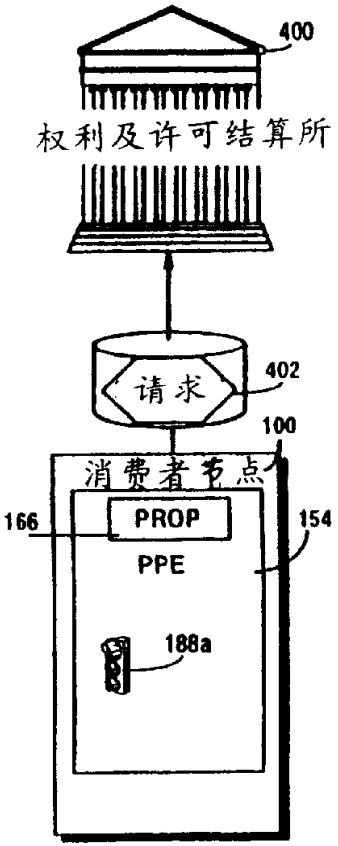


图 44B
消费者请求使用
财产的权利

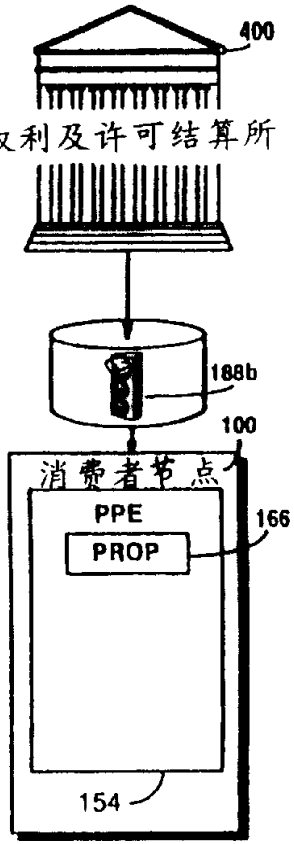


图 44C
权利及许可结算所
向消费者提供1权利

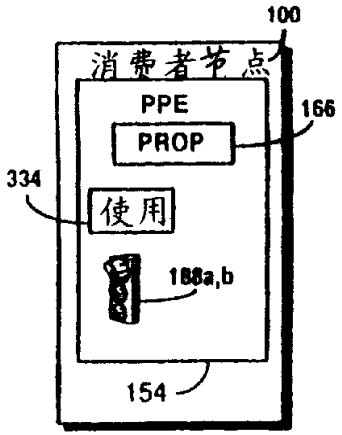


图 44D
消费者按照权利
使用财产

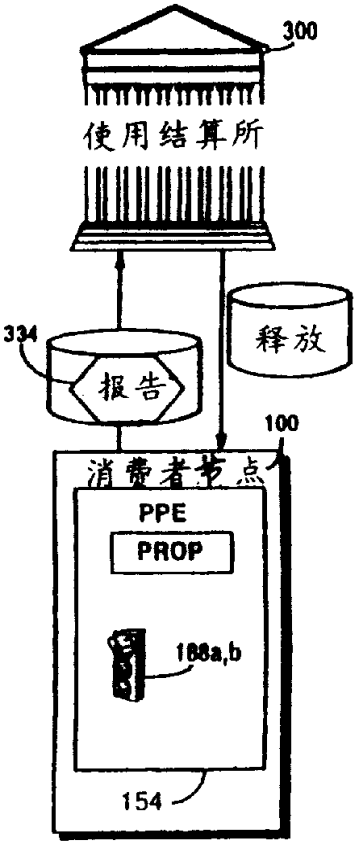


图 44E
消费者节点报告
使用情况

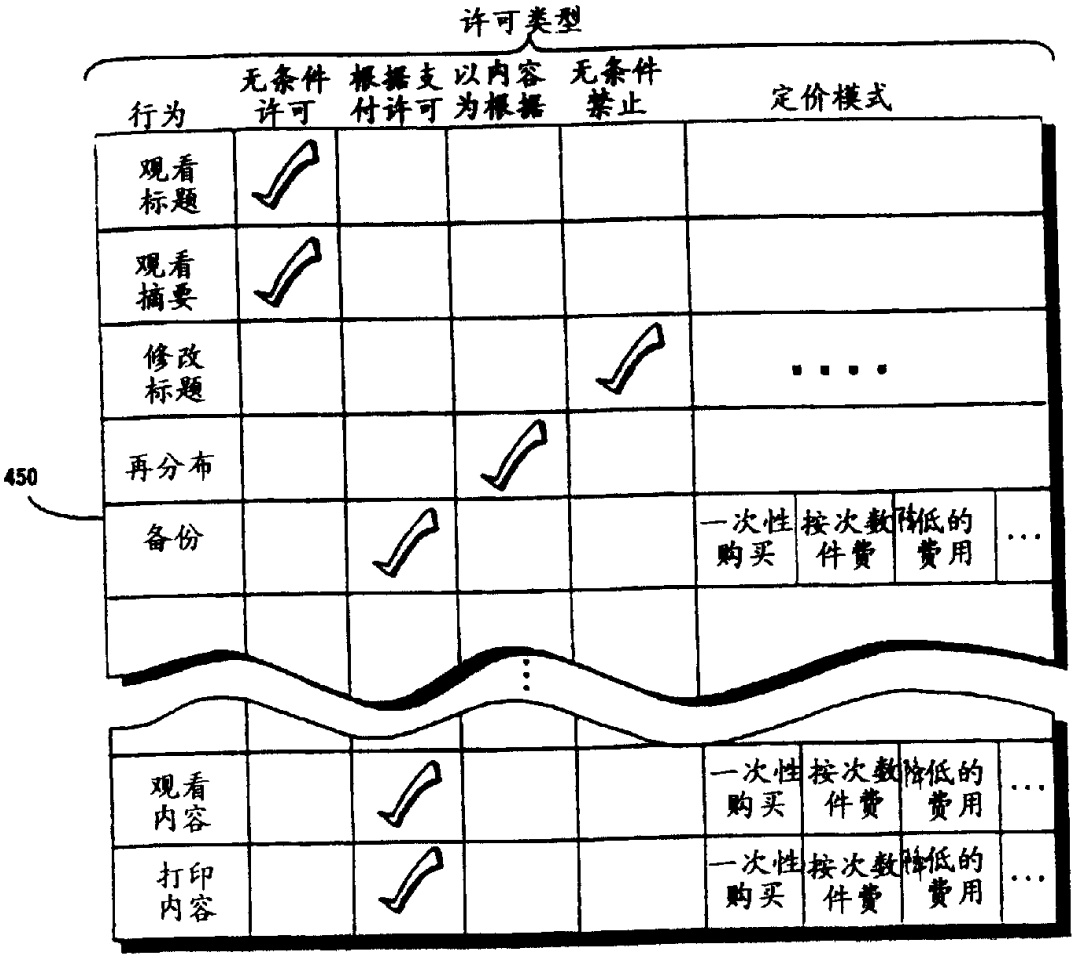


图 45A 示例性权利模板

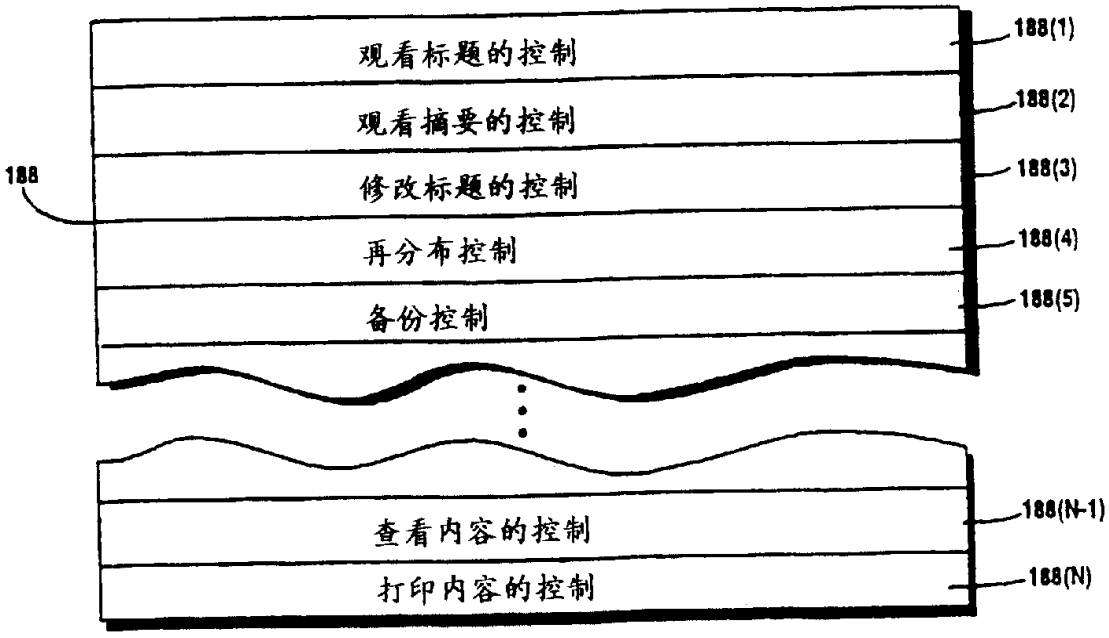


图 45C 示例性控制集

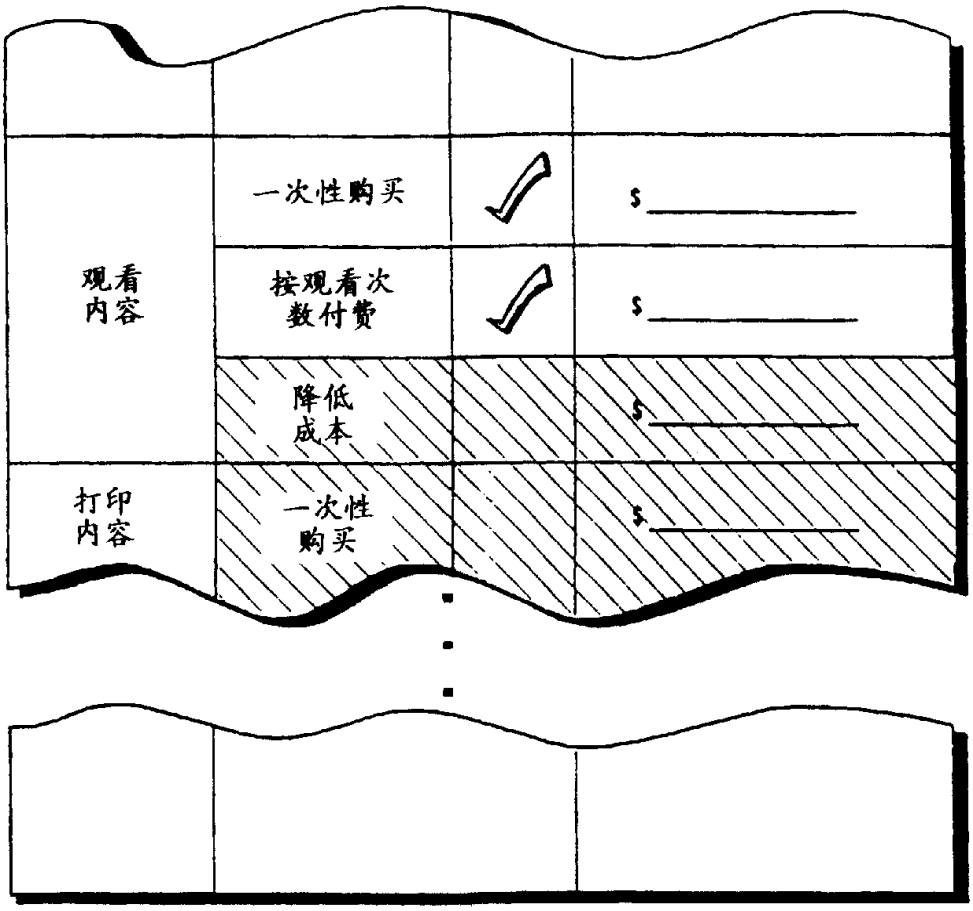


图 45B 定价模式和等级

图 46 示例性权利及许可结算过程

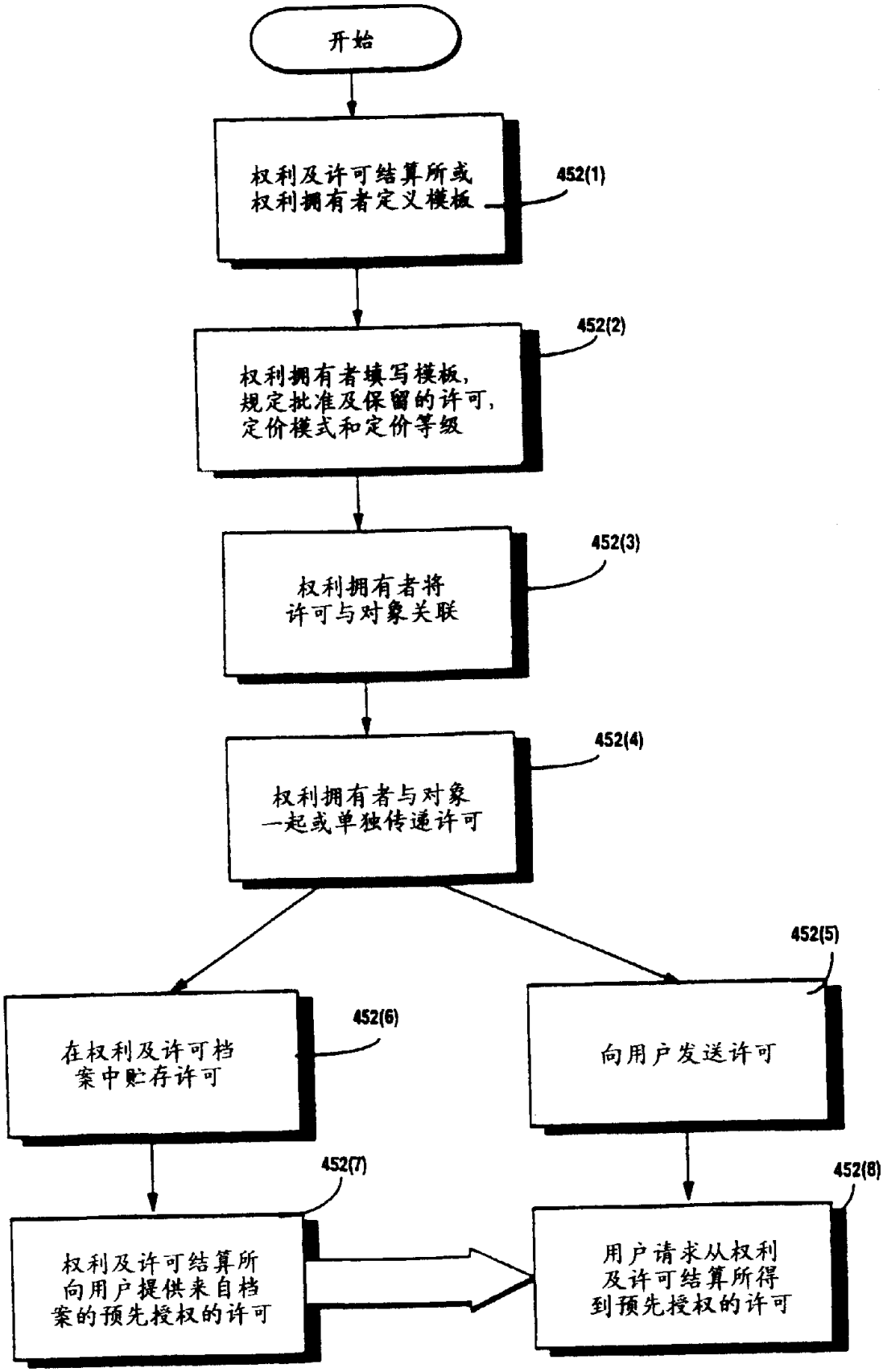


图 47

示例性认证机构

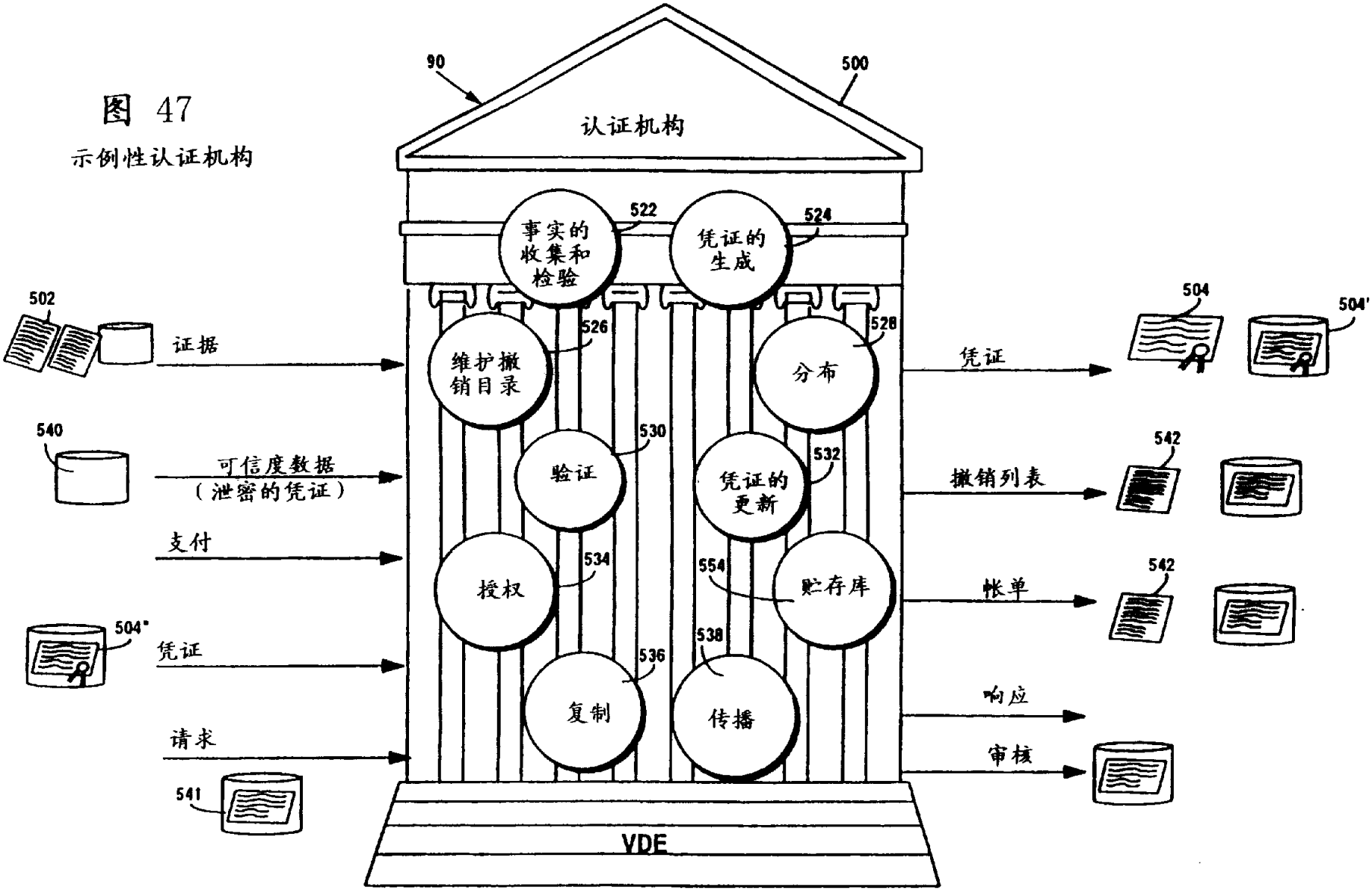

90
500
认证机构
事实的收集和检验
522
凭证的生成
524
502
证据
526
维护撤销目录
528
分布
504
504'
凭证
540
可信度数据
（泄密的凭证）
530
验证
532
凭证的更新
撤销列表
542
支付
534
授权
554
贮存库
帐单
542
504"
凭证
536
复制
538
传播
响应
请求
审核
541
VDE

图 48

示例性认证机构

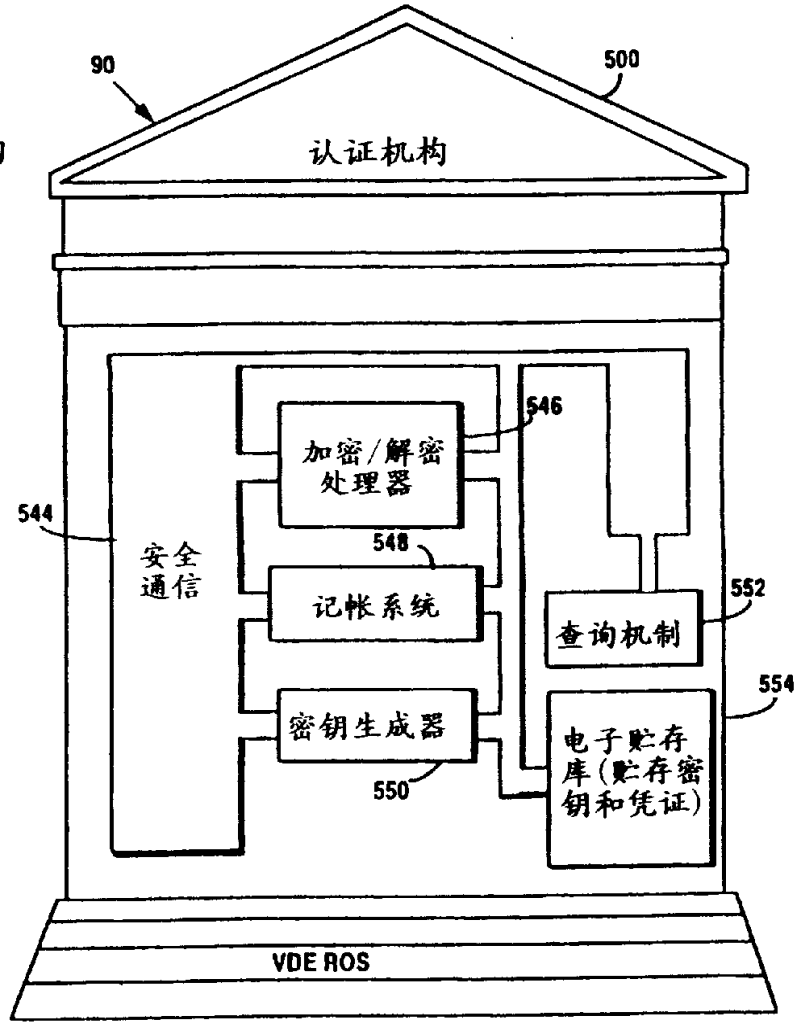
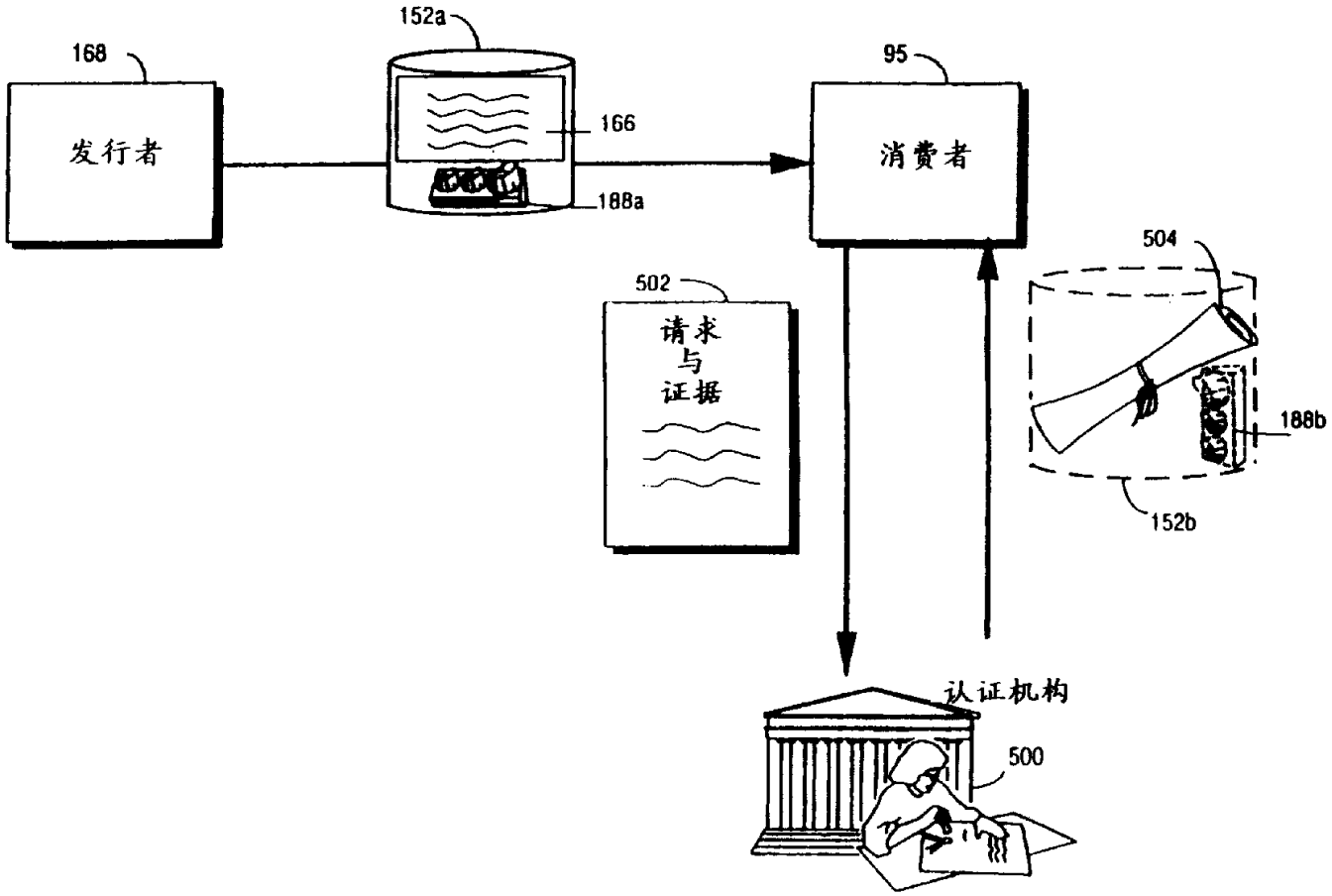

90
500
认证机构
546
加密/解密处理器
544
安全通信
548
记帐系统
552
查询机制
554
密钥生成器
电子贮存库(贮存密钥和凭证)
550
VDE ROS

图 49 示例性认证过程



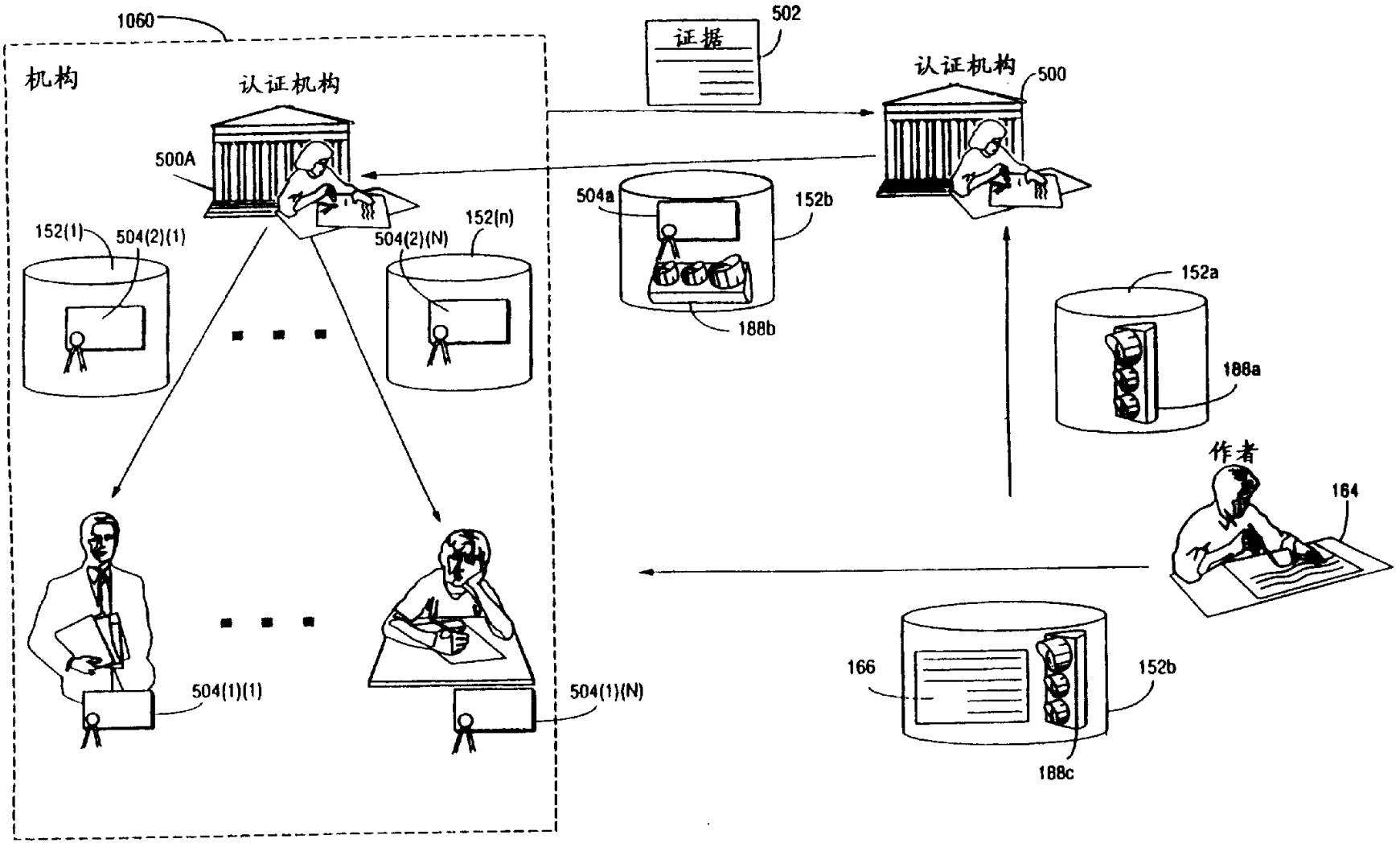
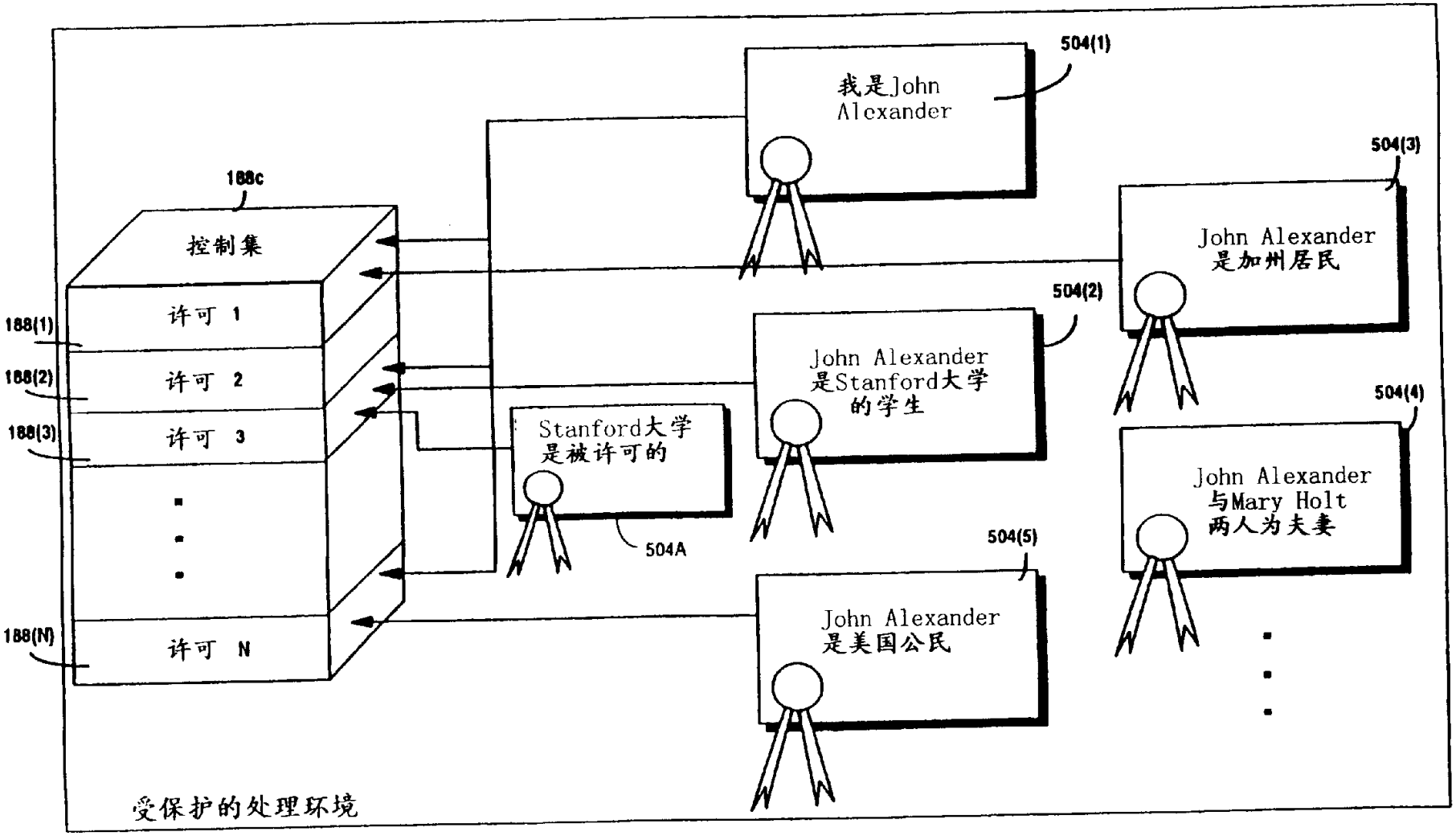


图 50 分布式的凭证颁发

图 50A 示例性的使用凭证的控制集



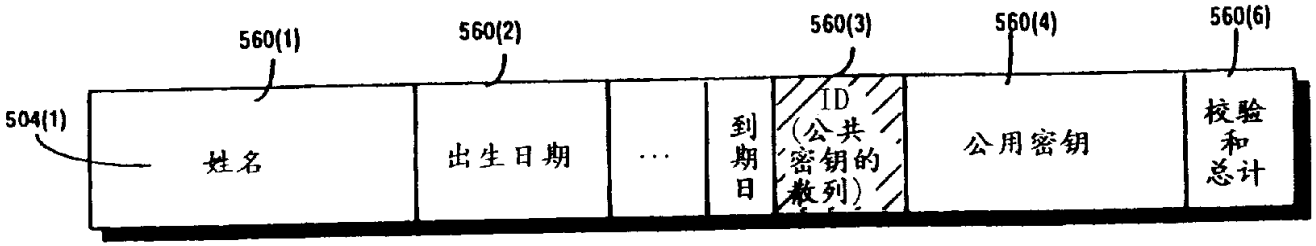


图 51A

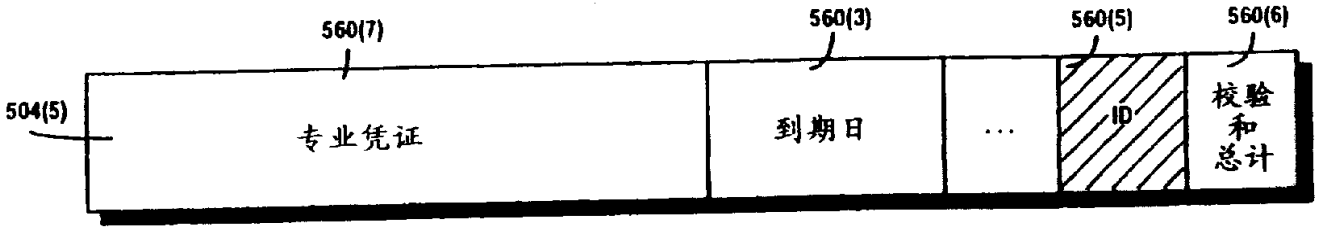


图 51B

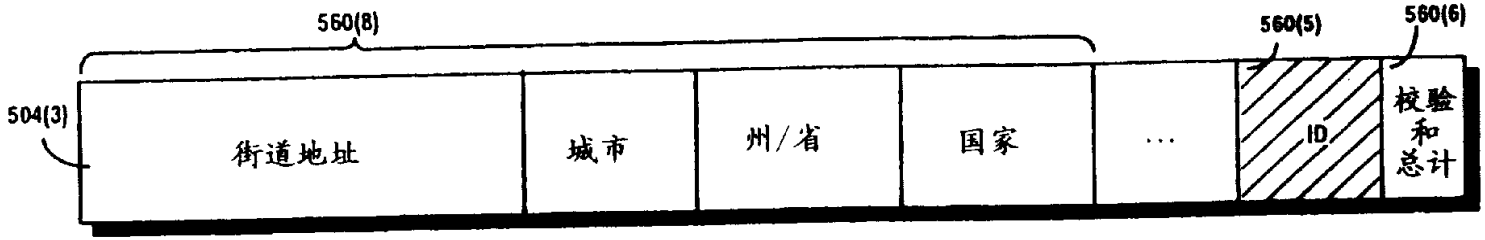


图 51C

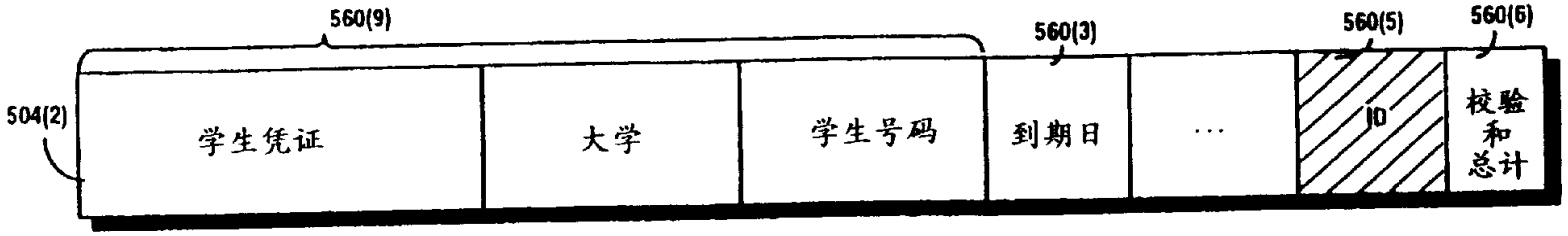


图 51D

示例性数字凭证

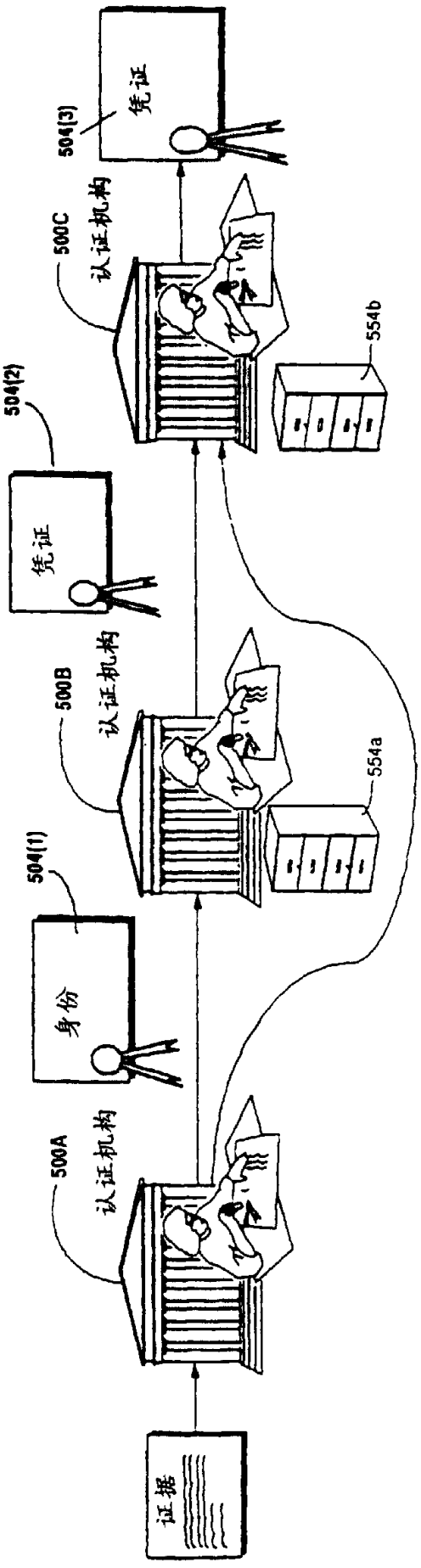


图 51E 根据其它凭证生成凭证

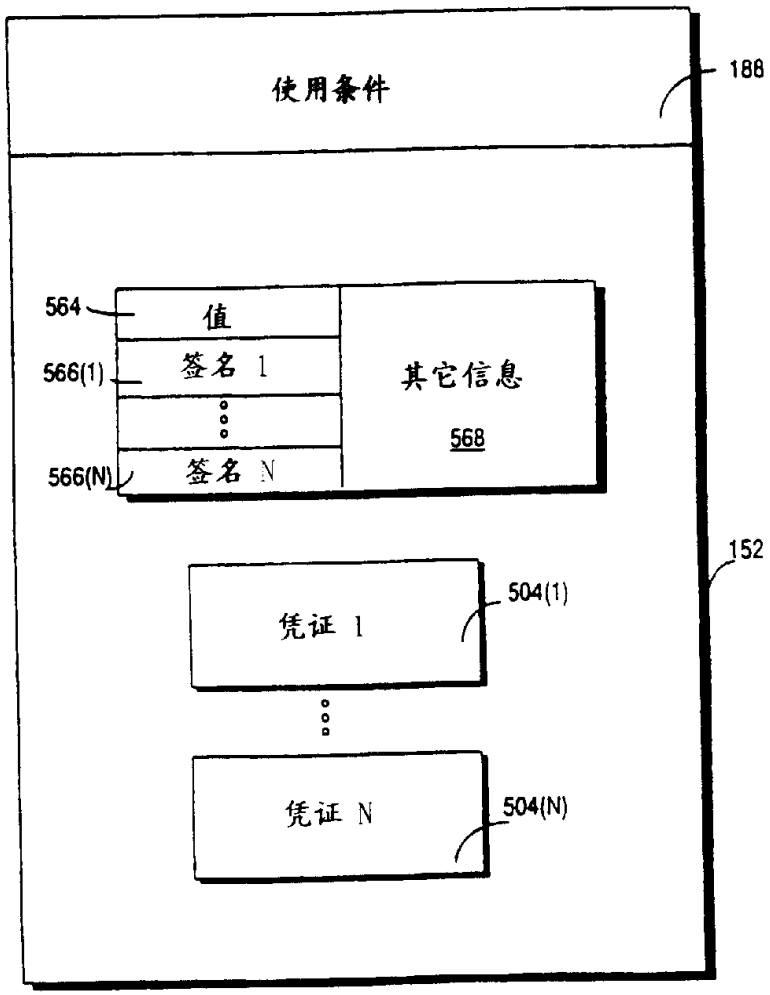


图 51F

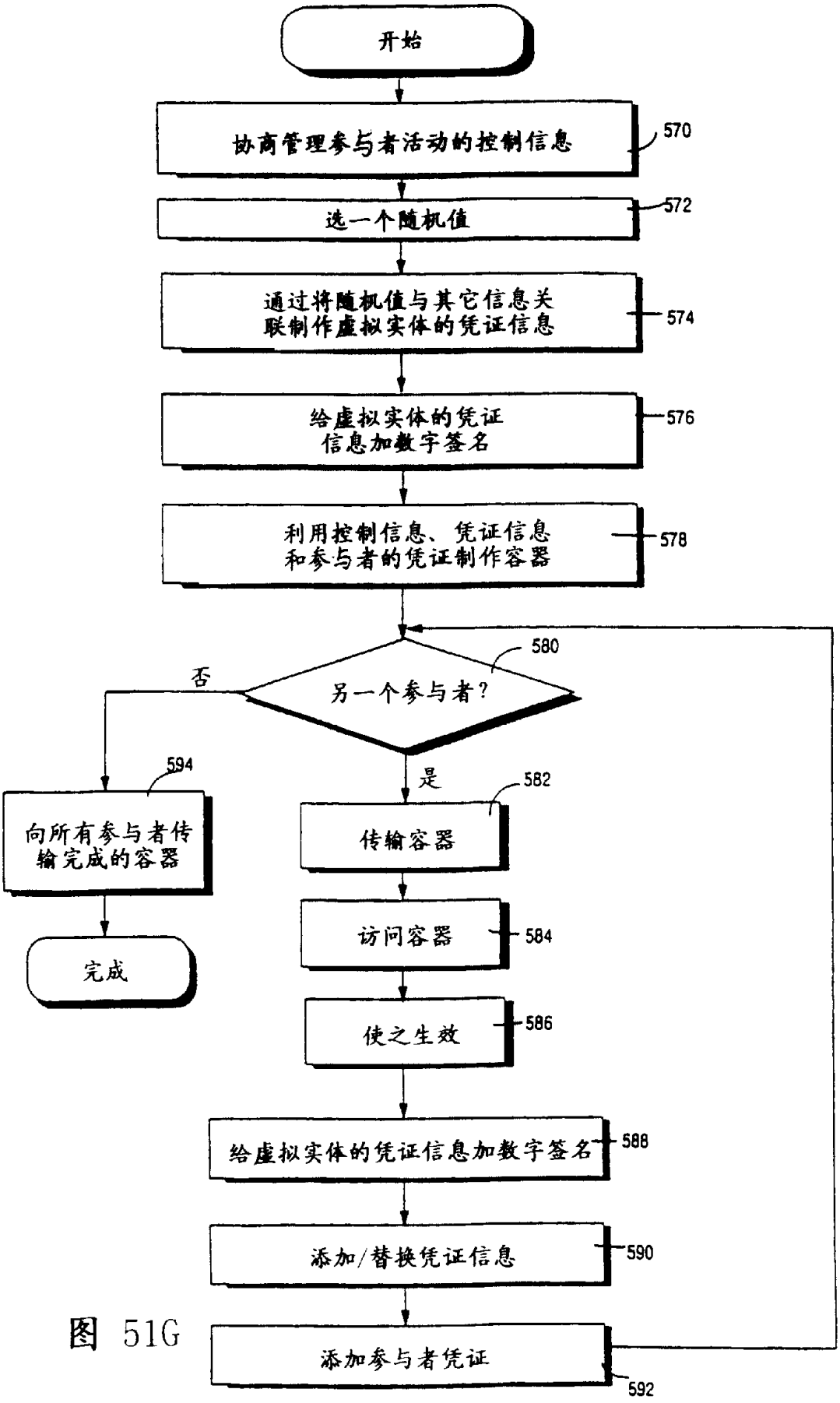

开始
协商管理参与者活动的控制信息
570
选一个随机值
572
通过将随机值与其它信息关联制作虚拟实体的凭证信息
574
给虚拟实体的凭证信息加数字签名
576
利用控制信息、凭证信息和参与者的凭证制作容器
578
另一个参与者?
580
否
是
向所有参与者传输完成的容器
594
完成
传输容器
582
访问容器
584
使之生效
586
给虚拟实体的凭证信息加数字签名
588
添加/替换凭证信息
590
添加参与者凭证
592

图 51G

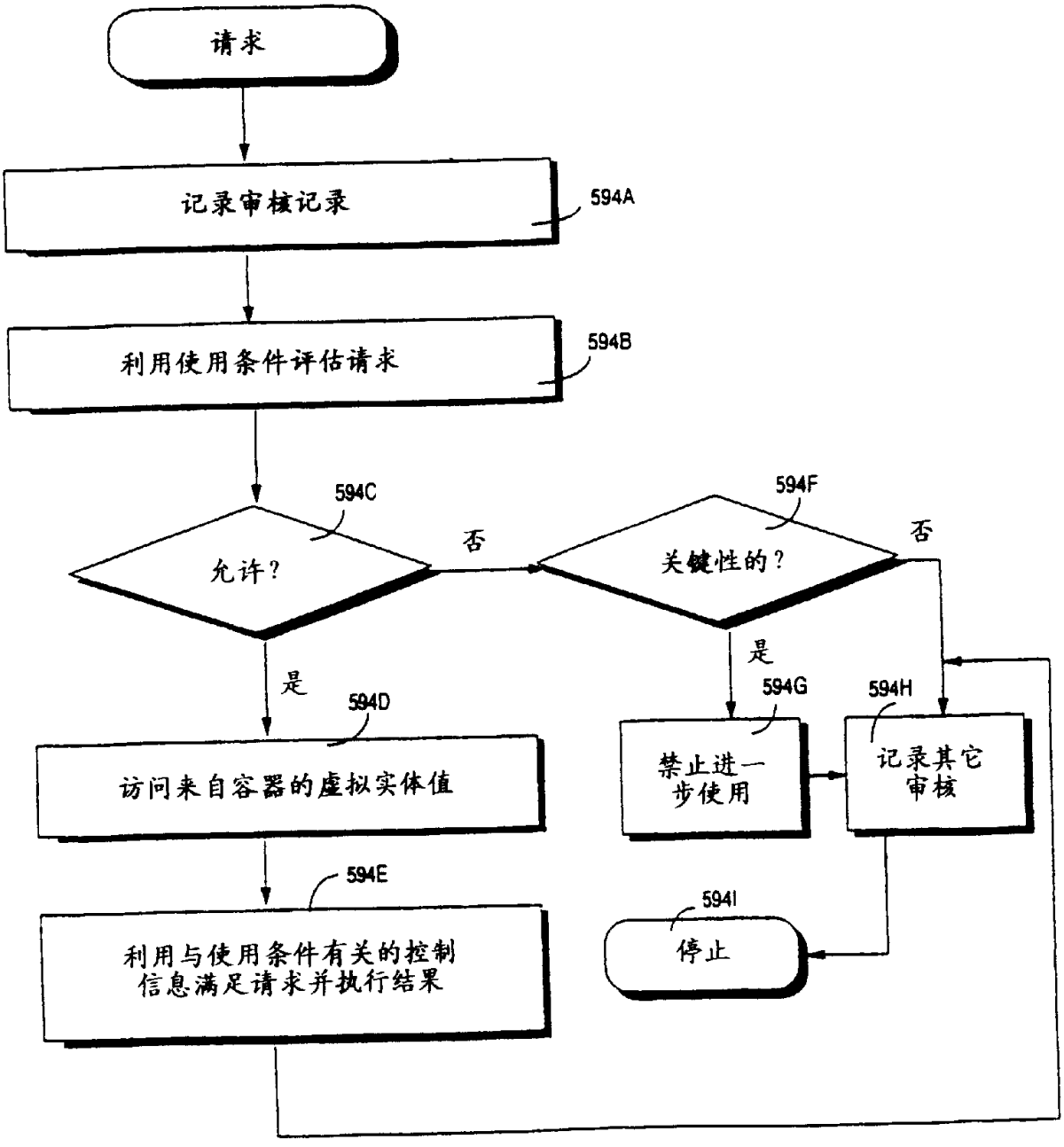
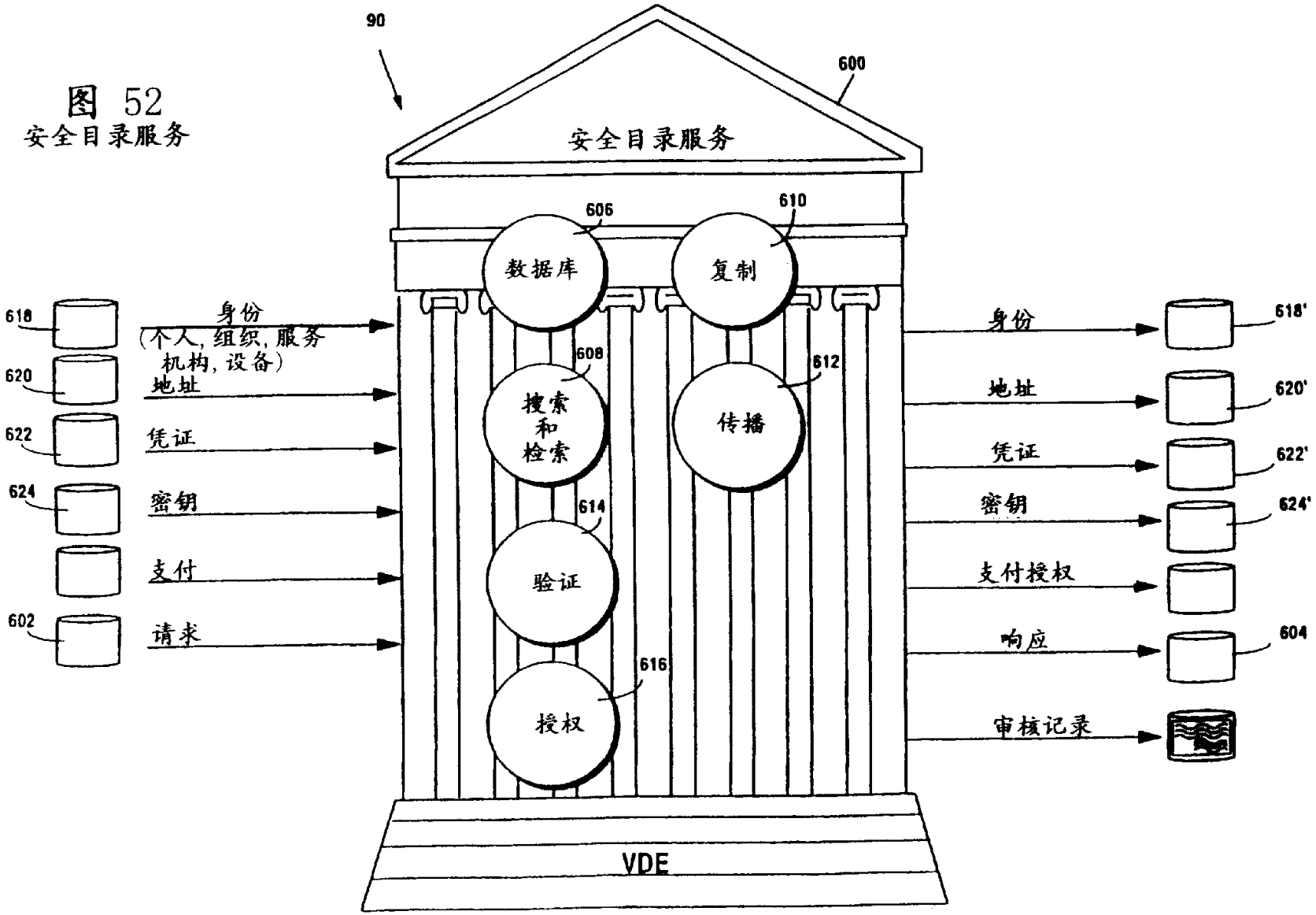

请求
记录审核记录
594A
利用使用条件评估请求
594B
594C
允许?
否
594F
关键性的?
否
是
是
594D
访问来自容器的虚拟实体值
594G
禁止进一步使用
594H
记录其它审核
594E
利用与使用条件有关的控制信息满足请求并执行结果
594I
停止

图 51H

图 52
安全目录服务


90
600
安全目录服务
606
数据库
610
复制
608
搜索
和
检索
612
传播
614
验证
616
授权
VDE
618
身份
(个人,组织,服务
机构,设备)
620
地址
622
凭证
624
密钥
支付
602
请求
身份
618'
地址
620'
凭证
622'
密钥
624'
支付授权
响应
604
审核记录

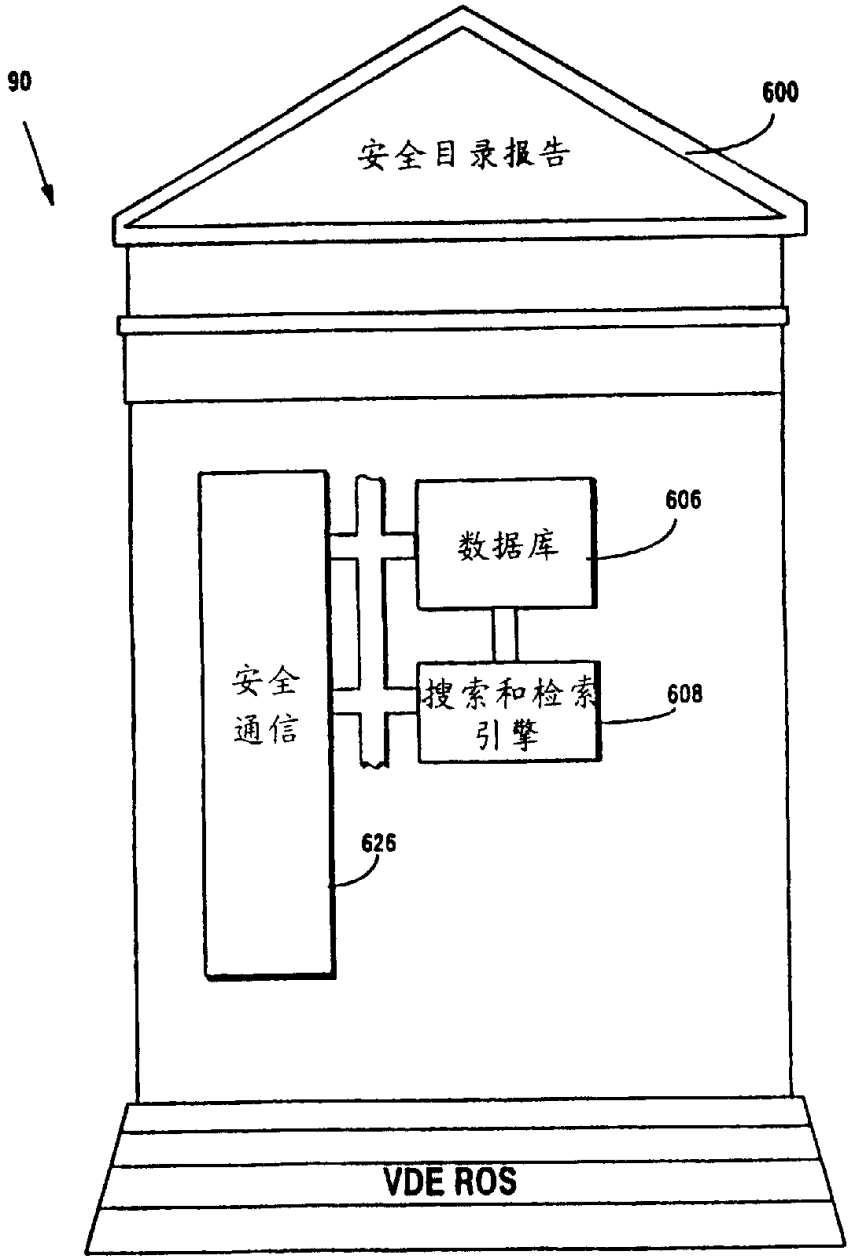


图 53

示例性安全目录服务

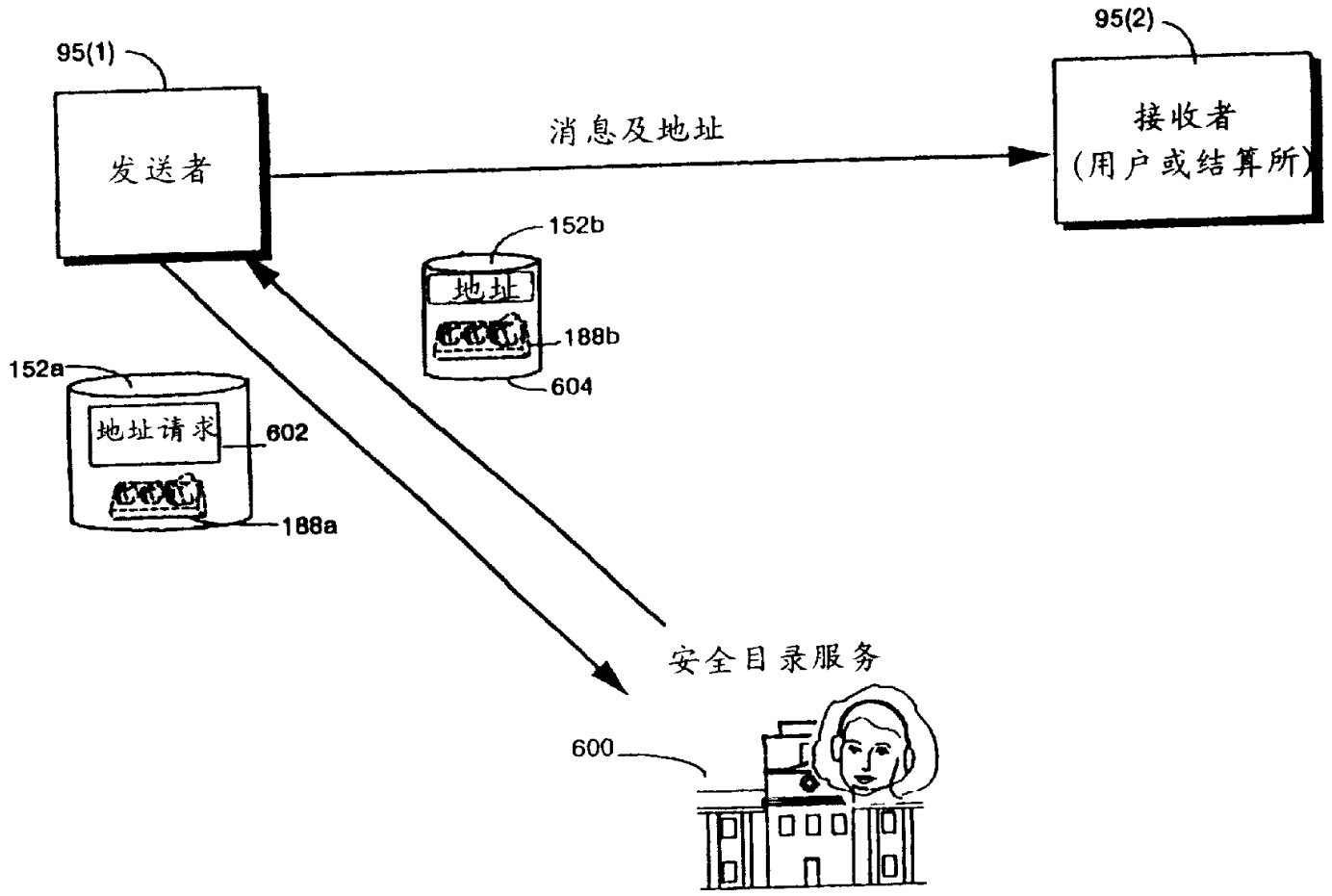


图 54 示例性安全目录服务过程

图 55
示例性认证机构

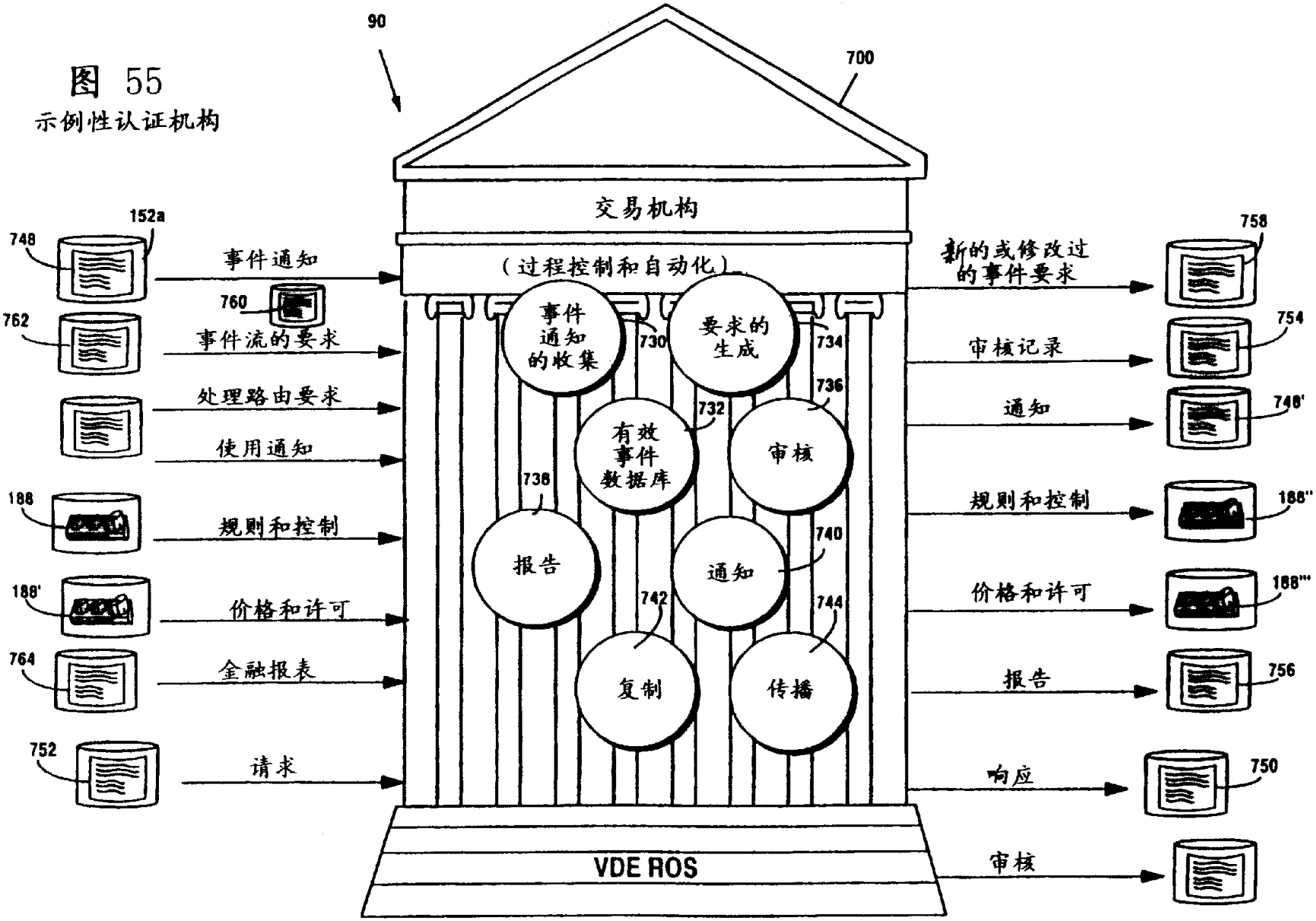
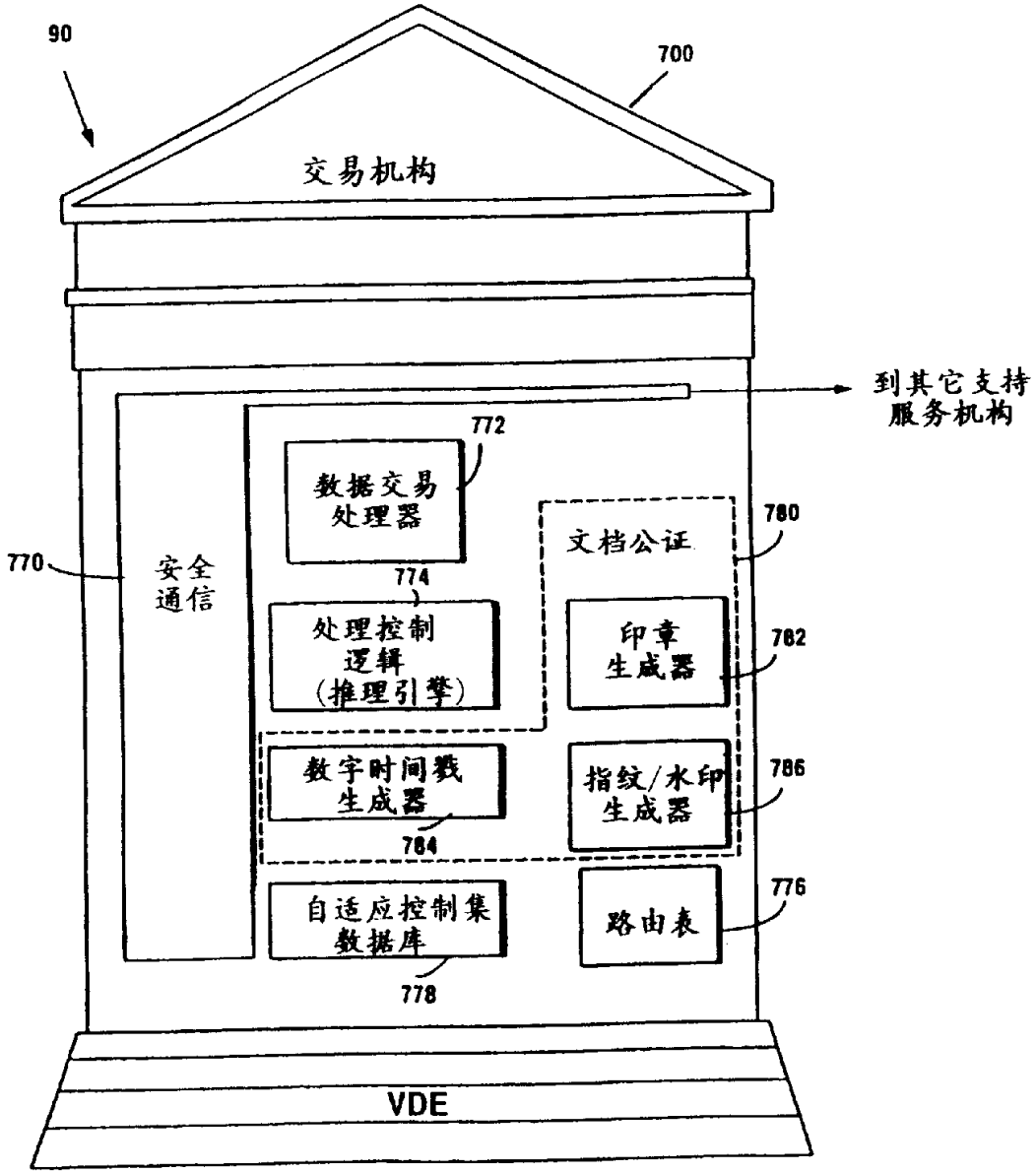

90
700
交易机构
（过程控制和自动化）
VDE ROS
152a
748
事件通知
760
762
事件流的要求
处理路由要求
使用通知
188
规则和控制
188'
价格和许可
764
金融报表
752
请求
事件通知的收集
730
要求的生成
734
有效事件数据库
732
736
审核
738
报告
740
通知
742
复制
744
传播
新的或修改过的事件要求
758
审核记录
754
通知
748'
规则和控制
188''
价格和许可
188'''
报告
756
响应
750
审核

图 56
示例性交易机构


90
700
交易机构
到其它支持
服务机构
772
数据交易
处理器
780
文档公证
770
安全
通信
774
处理控制
逻辑
(推理引擎)
印章
生成器
782
数字时间戳
生成器
784
指纹/水印
生成器
786
自适应控制集
数据库
778
路由表
776
VDE

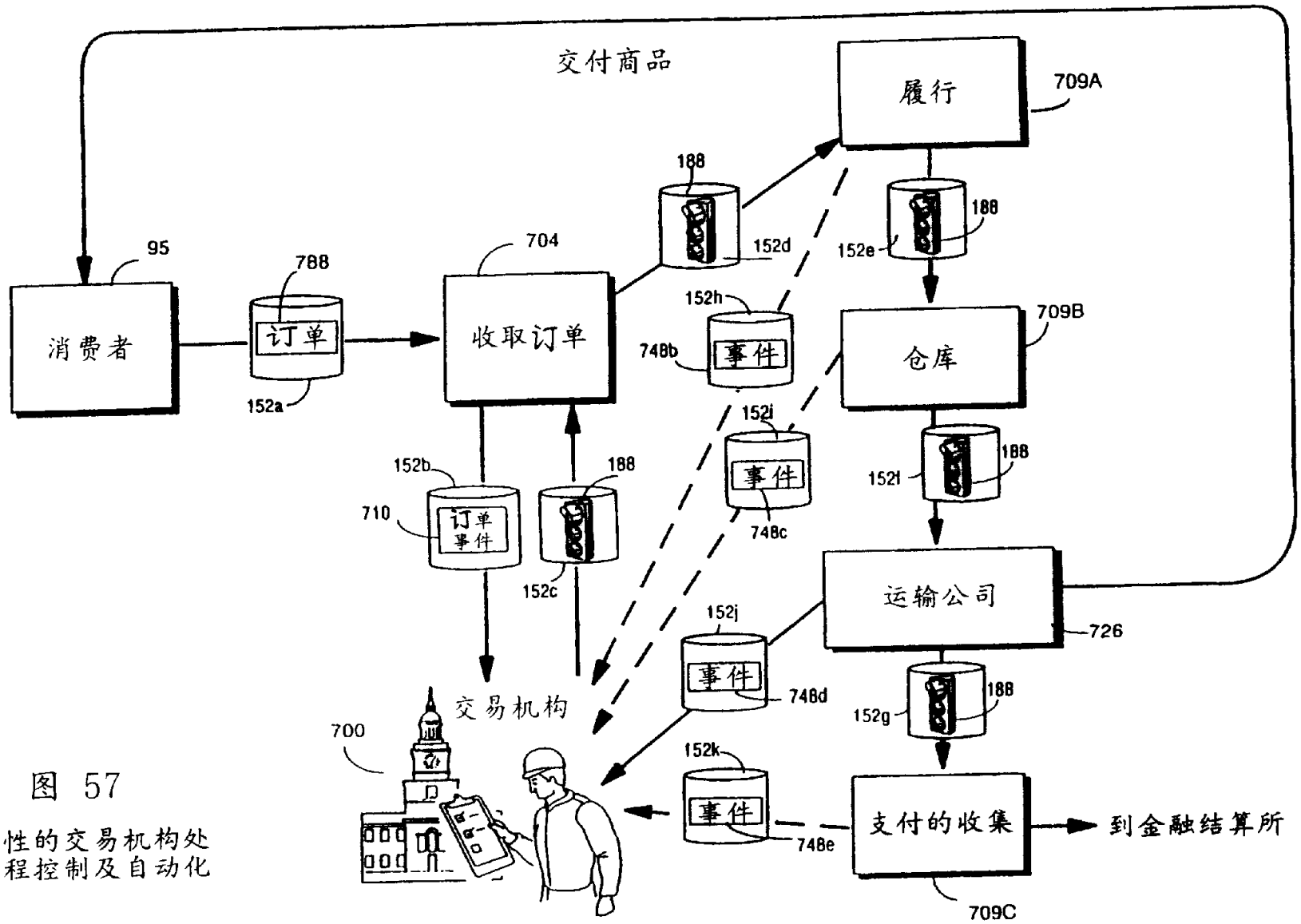


图 57

示例性的交易机构处理过程控制及自动化

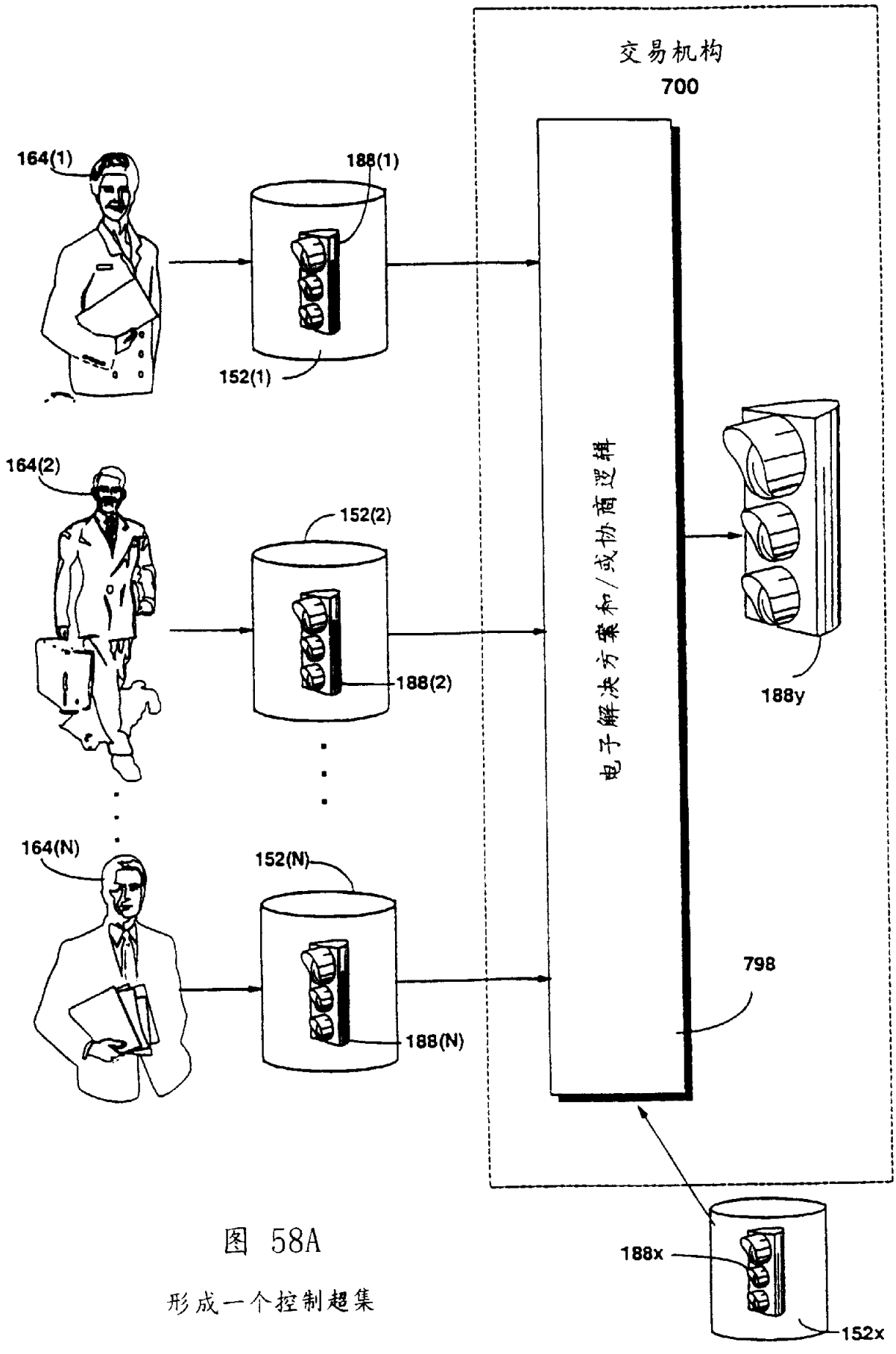
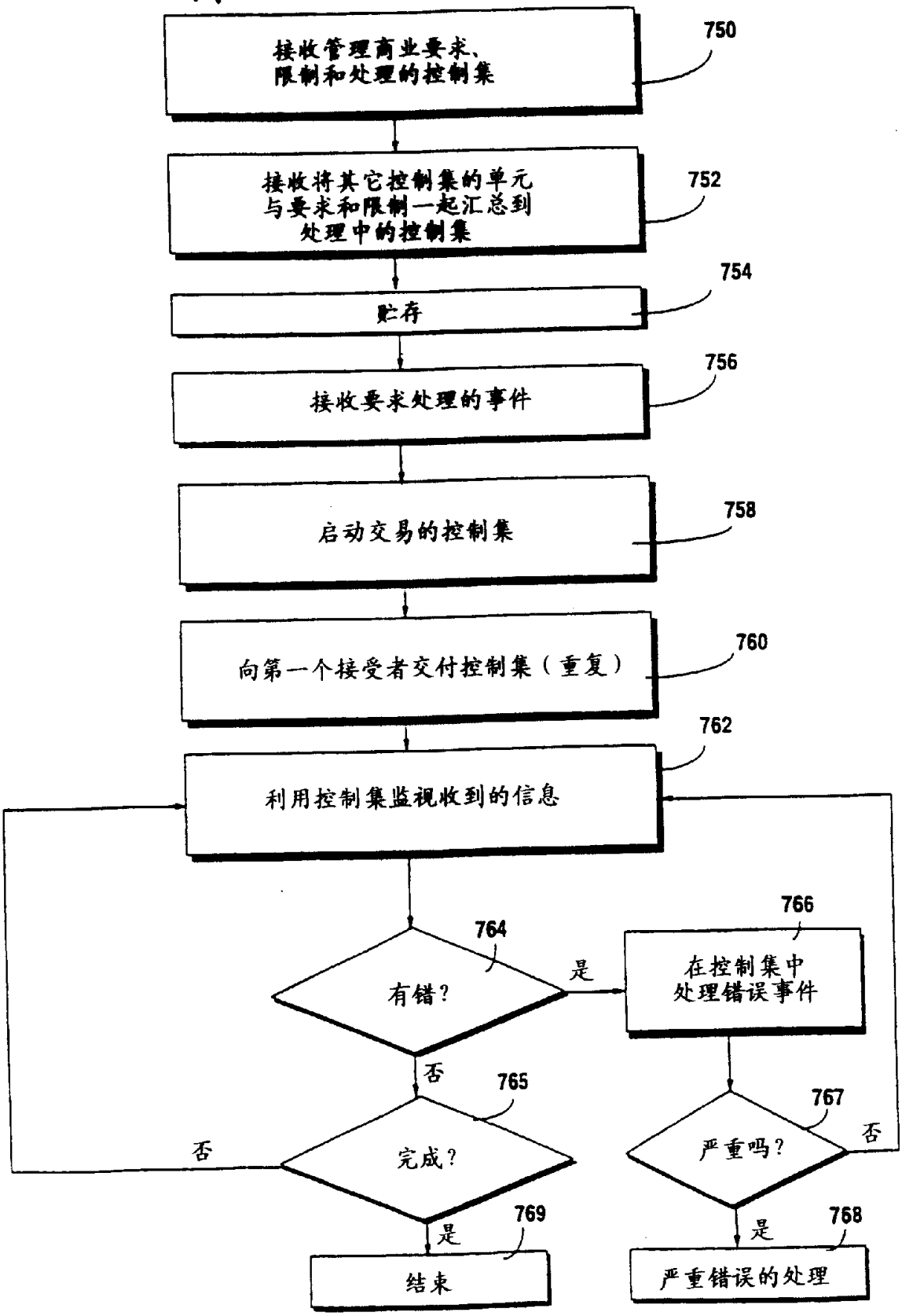


图 58A

形成一个控制超集

图 58B 交易机构的示例性步骤



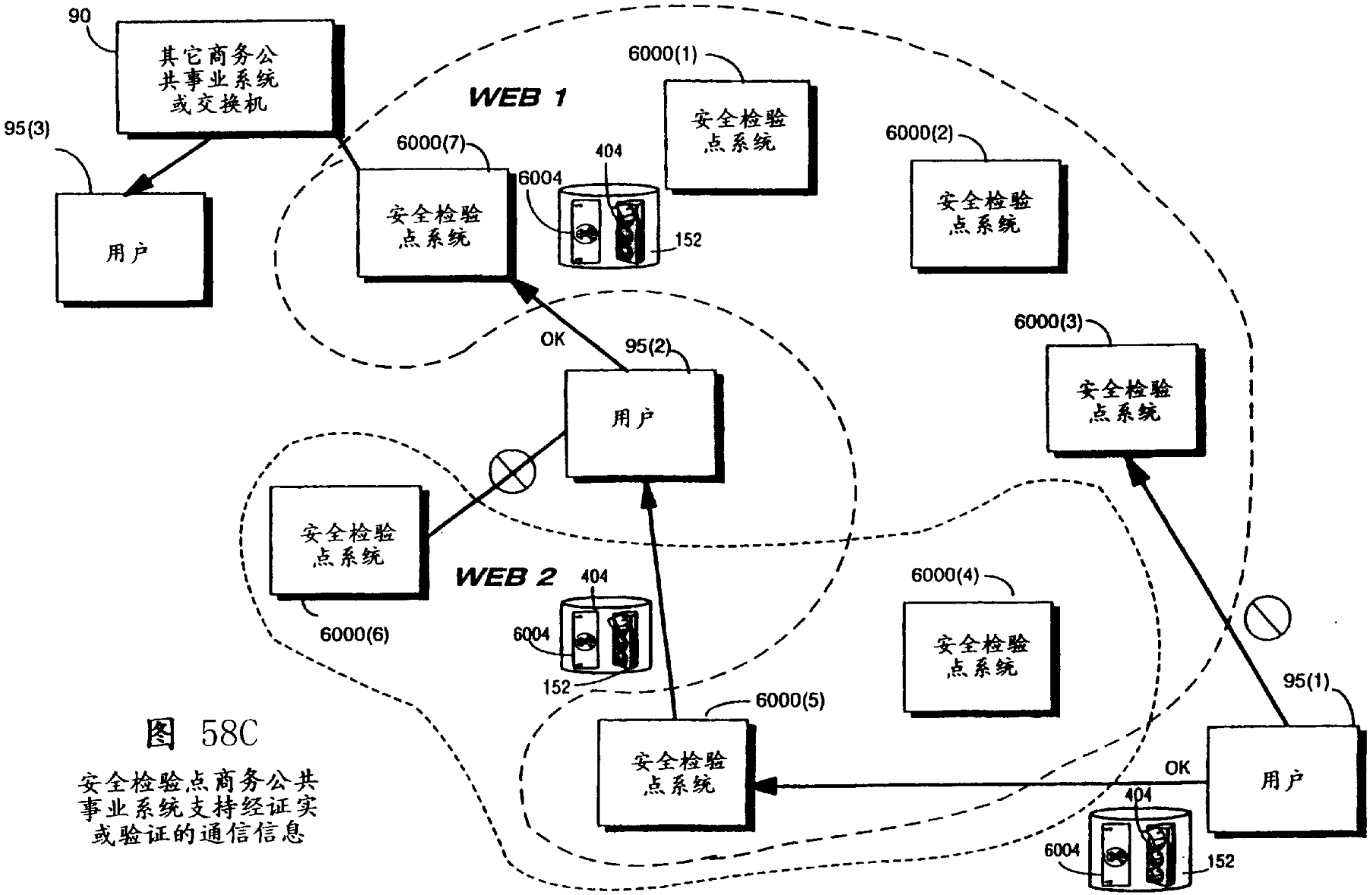


图 58C

安全检验点商务公共事业系统支持经证实或验证的通信信息

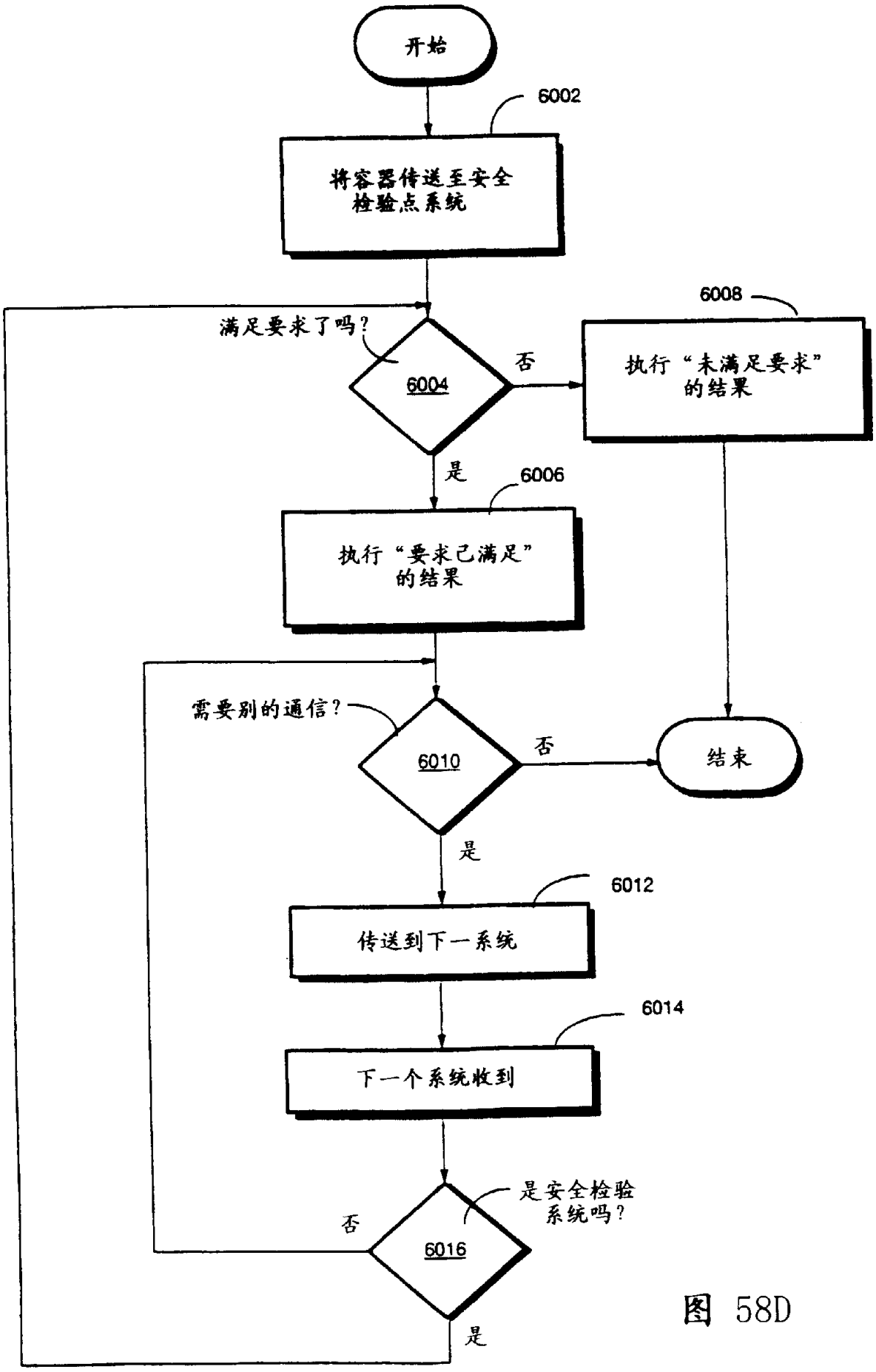

开始
6002
将容器传送至安全检验点系统
满足要求了吗?
6004
否
6008
执行“未满足要求”的结果
是
6006
执行“要求已满足”的结果
需要别的通信?
6010
否
结束
是
6012
传送到下一系统
6014
下一个系统收到
是安全检验系统吗?
否
6016
是

图 58D

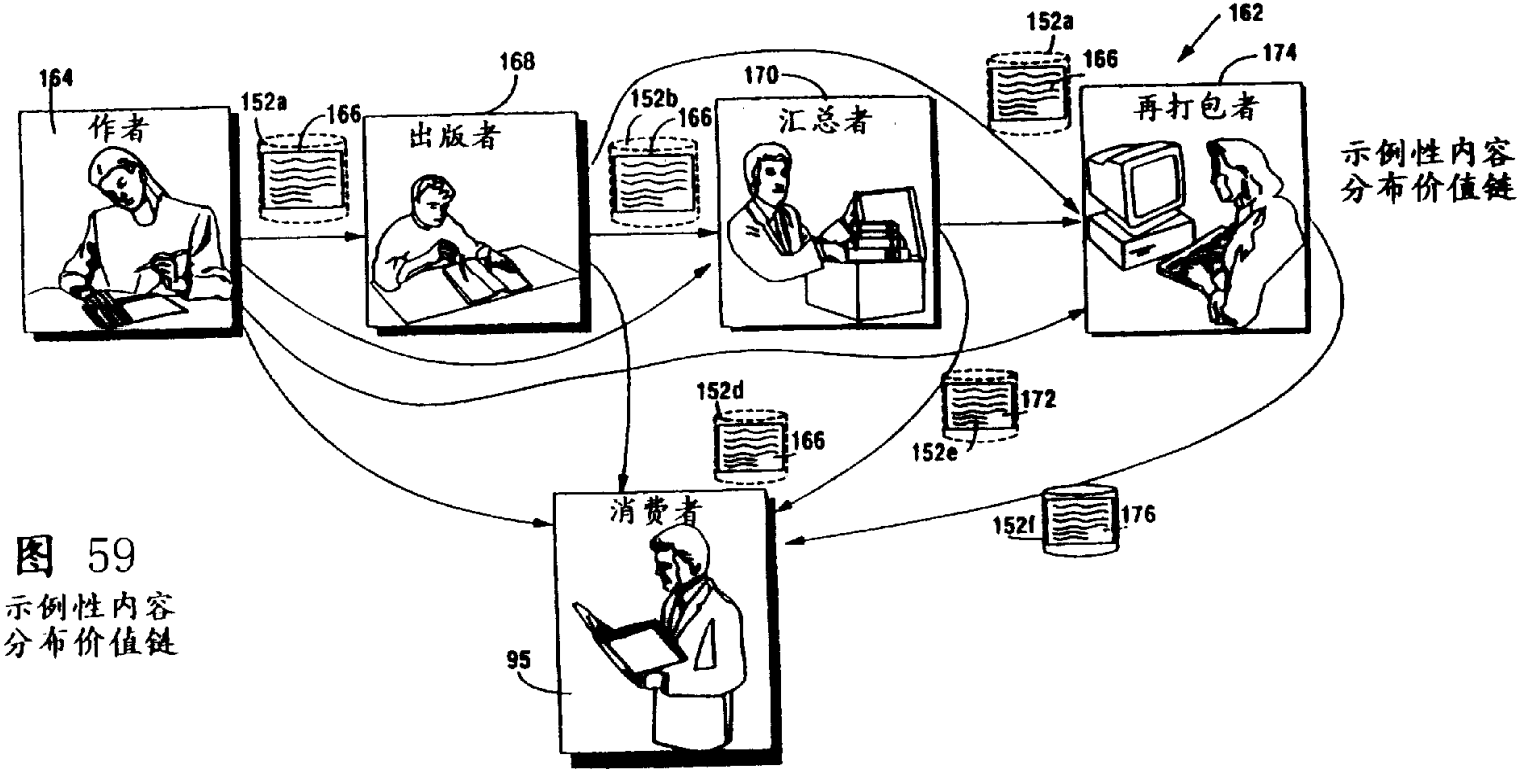
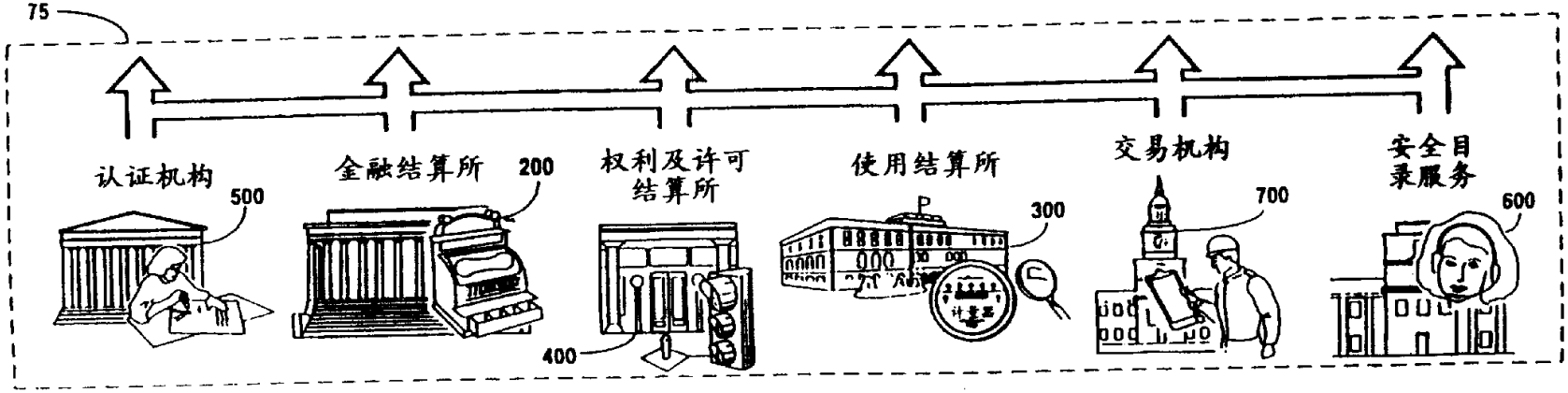


图 59
示例性内容
分布价值链



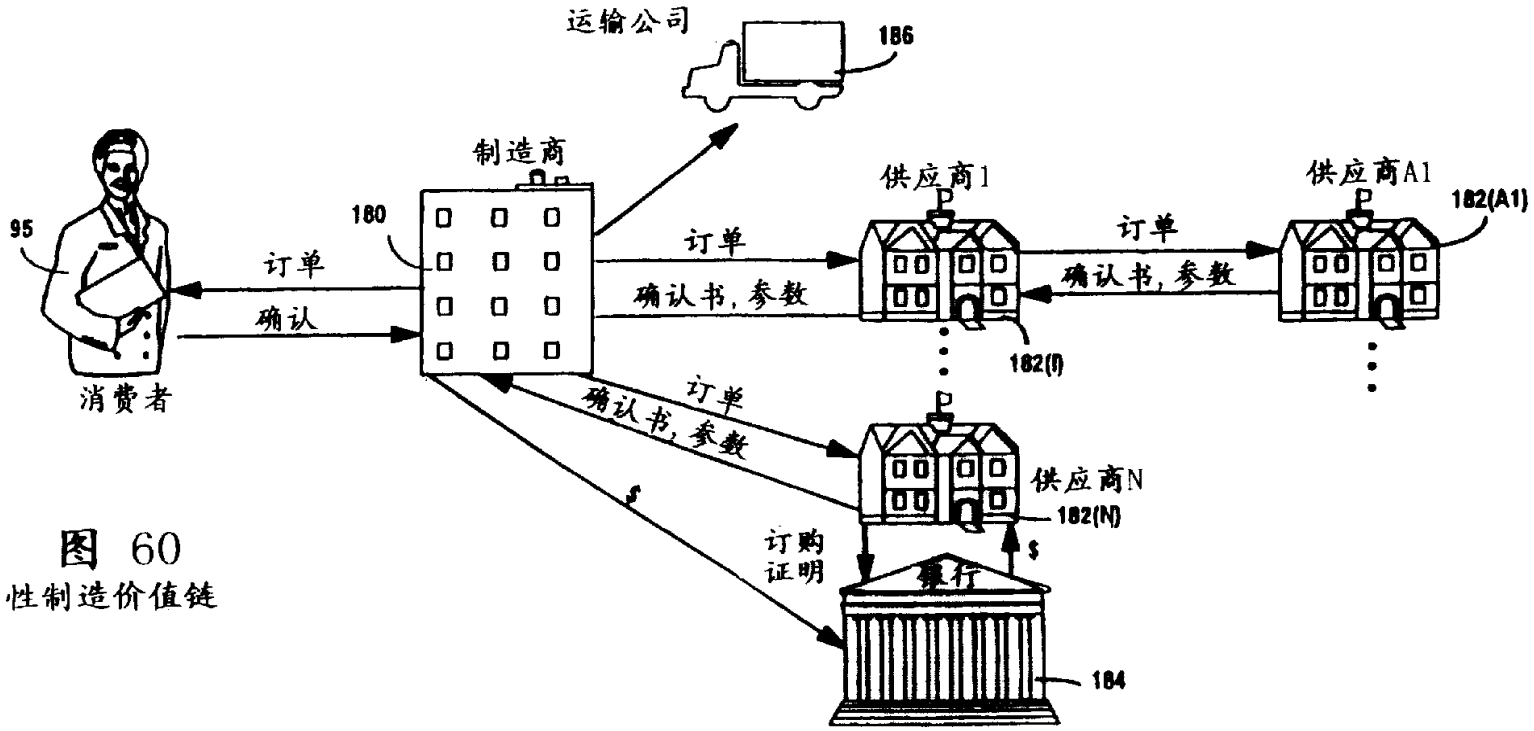
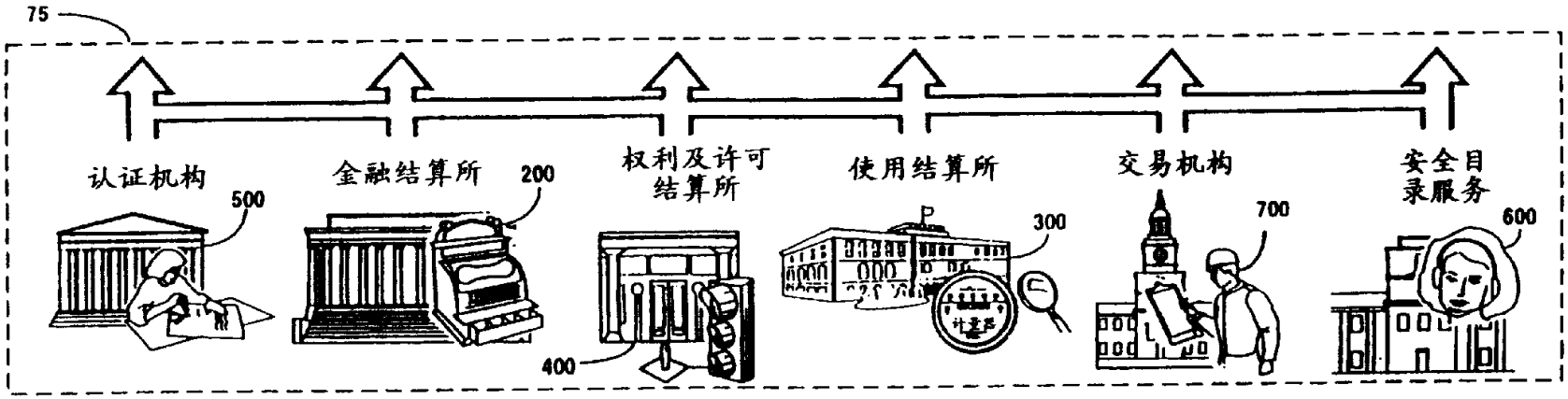


图 60
示例性制造价值链



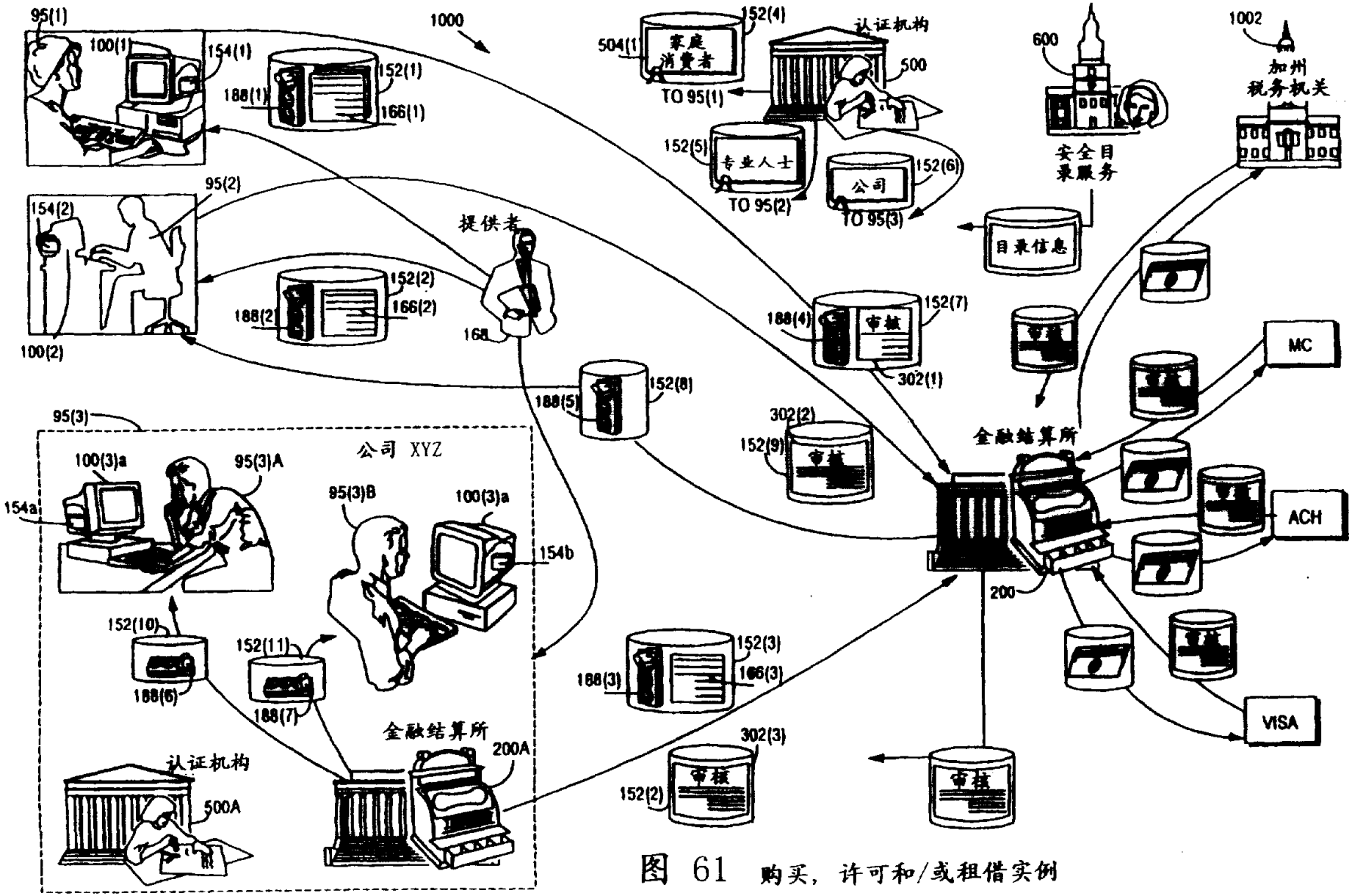
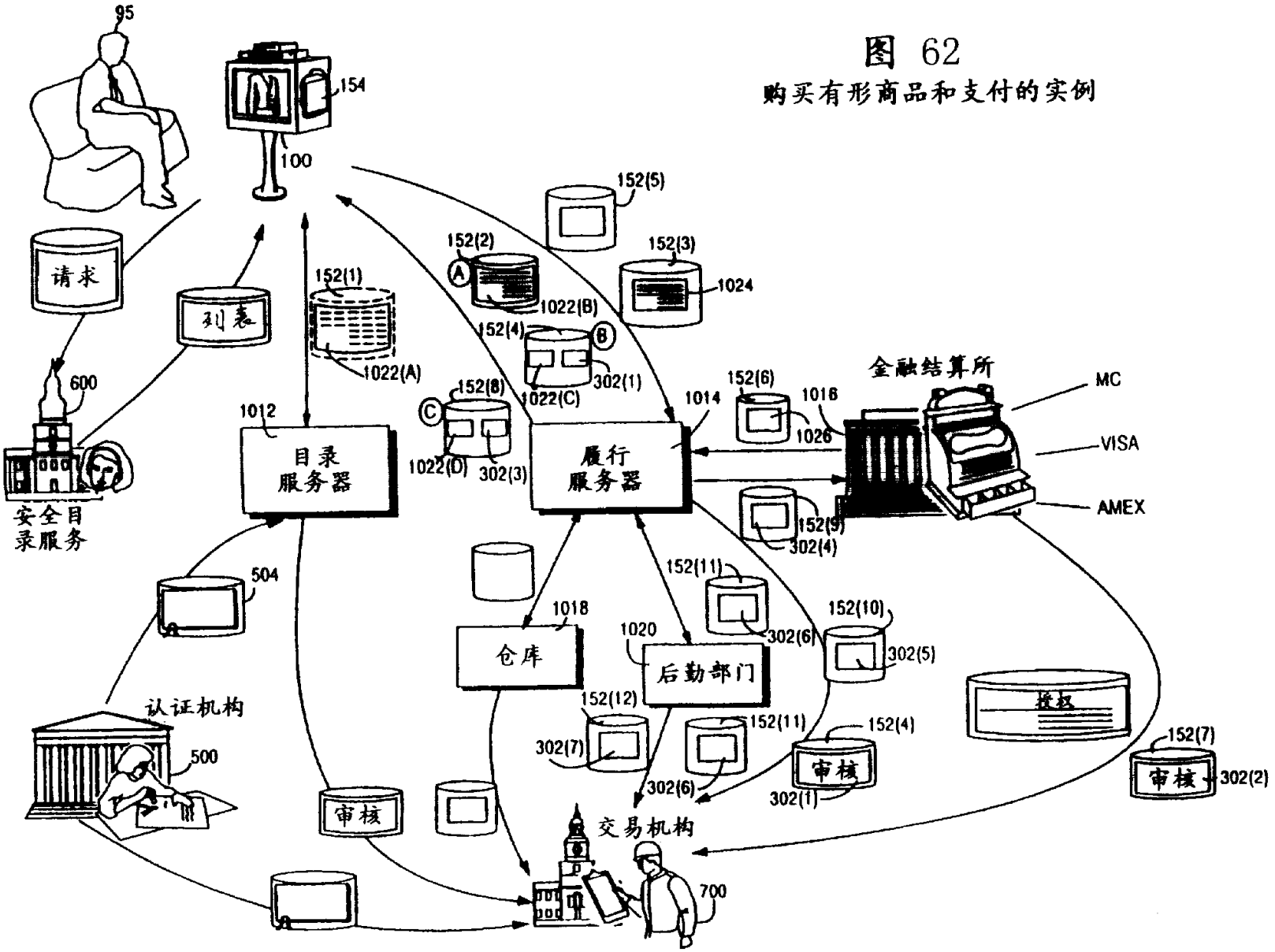


图 61 购买，许可和/或租借实例

图 62

购买有形商品和支付的实例



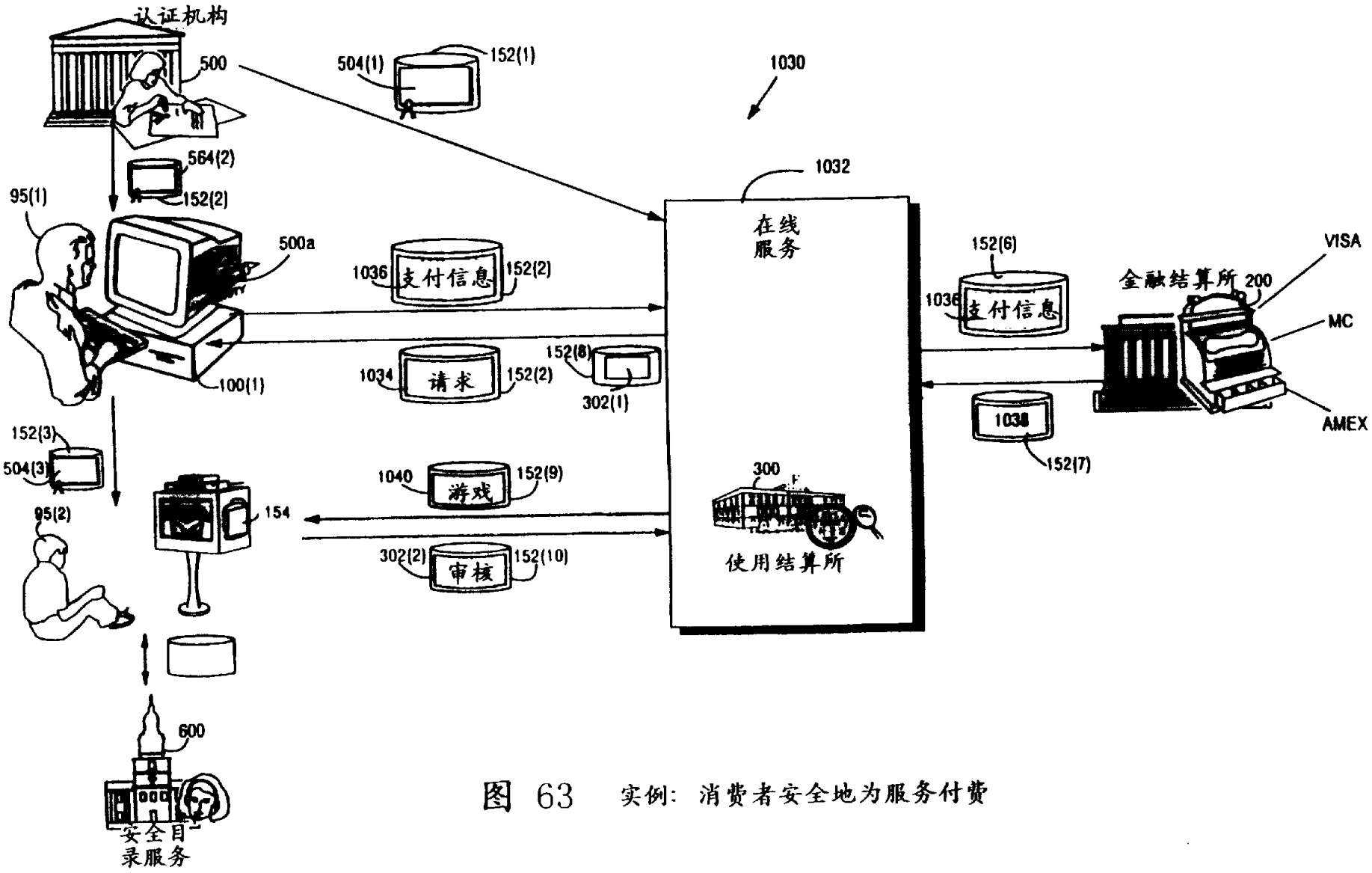
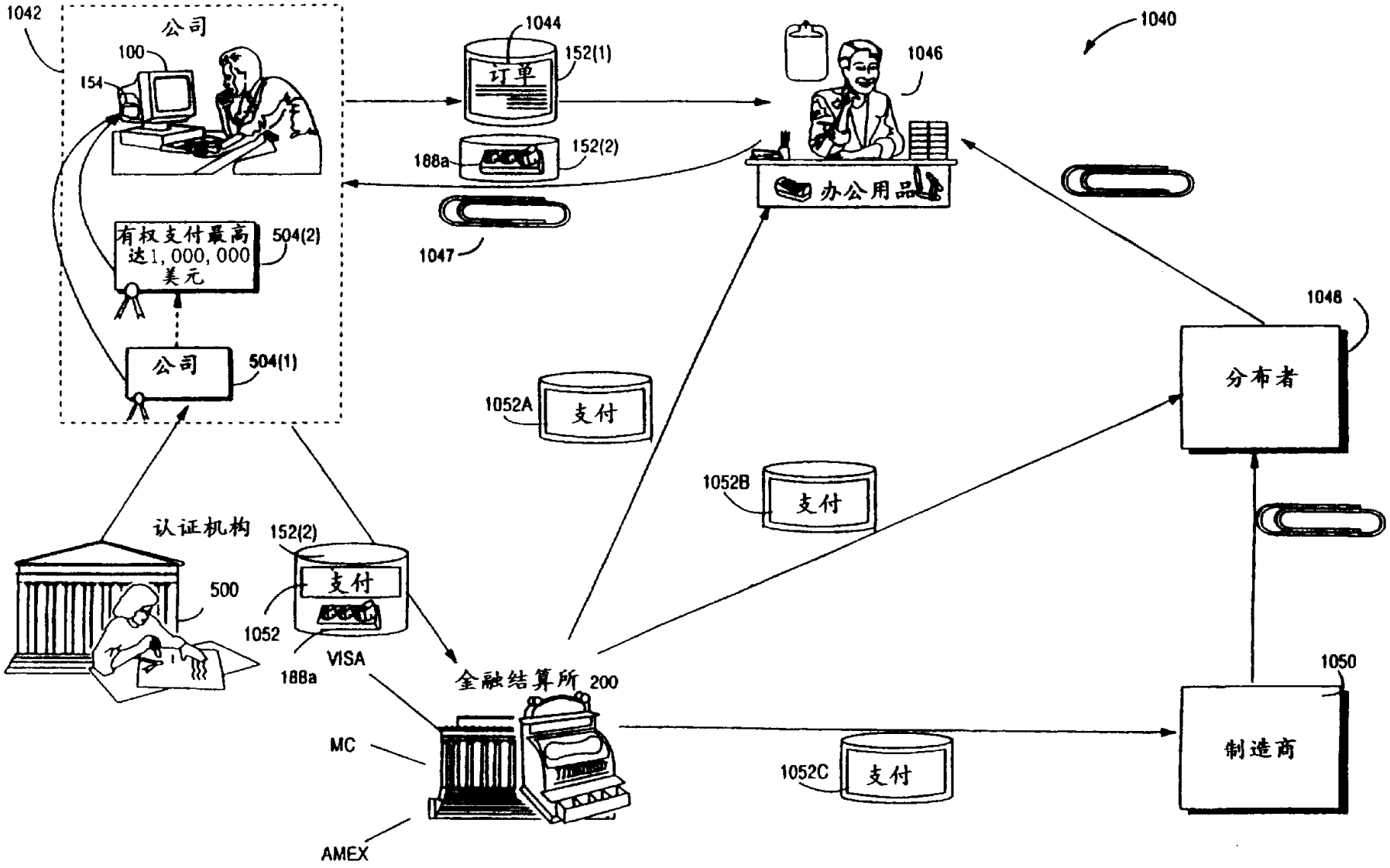


图 63　实例：消费者安全地为服务付费

图 64　购买有形商品的示例性价值链分解



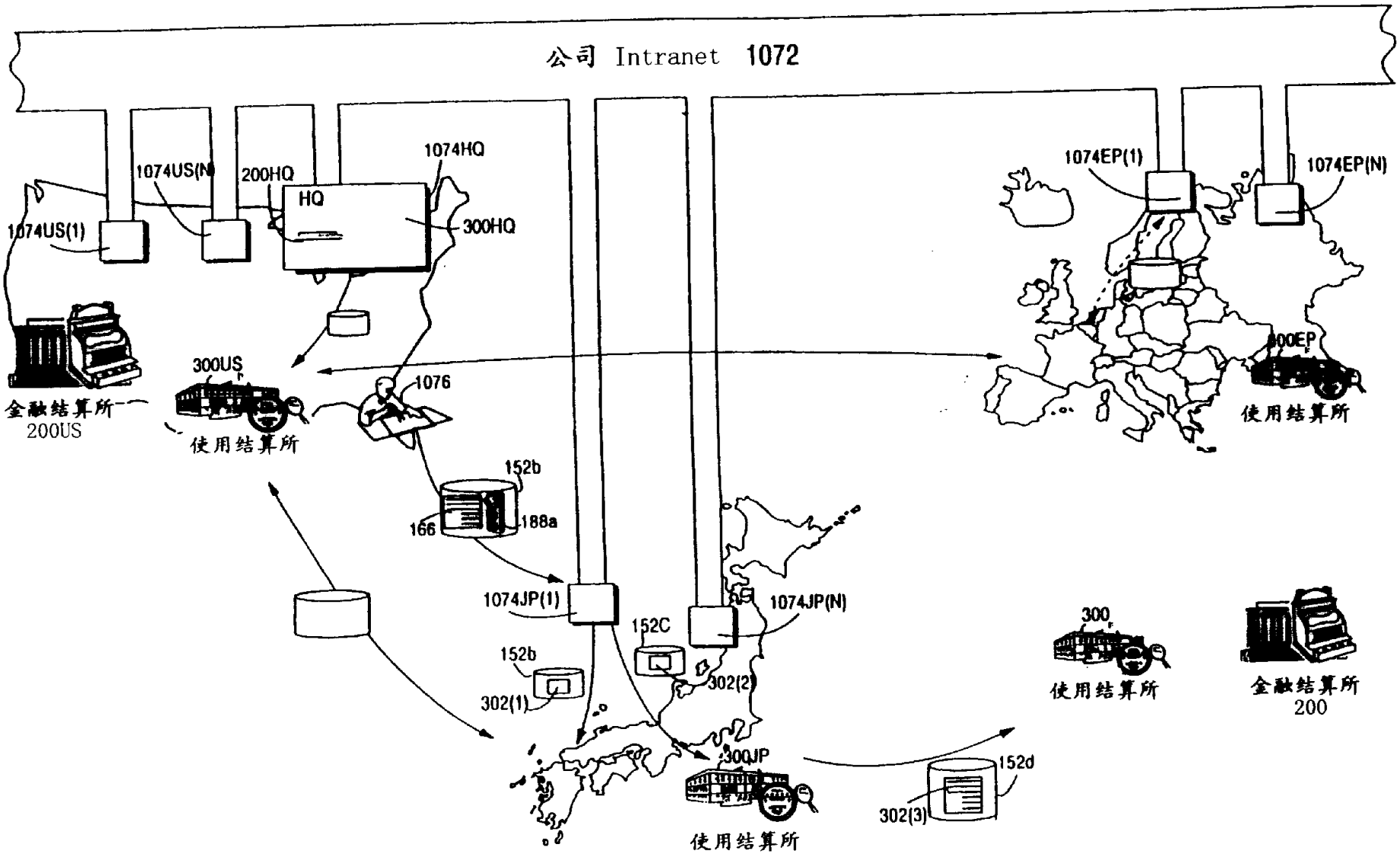


图 65 组织内外的商务公共事业系统间的合作

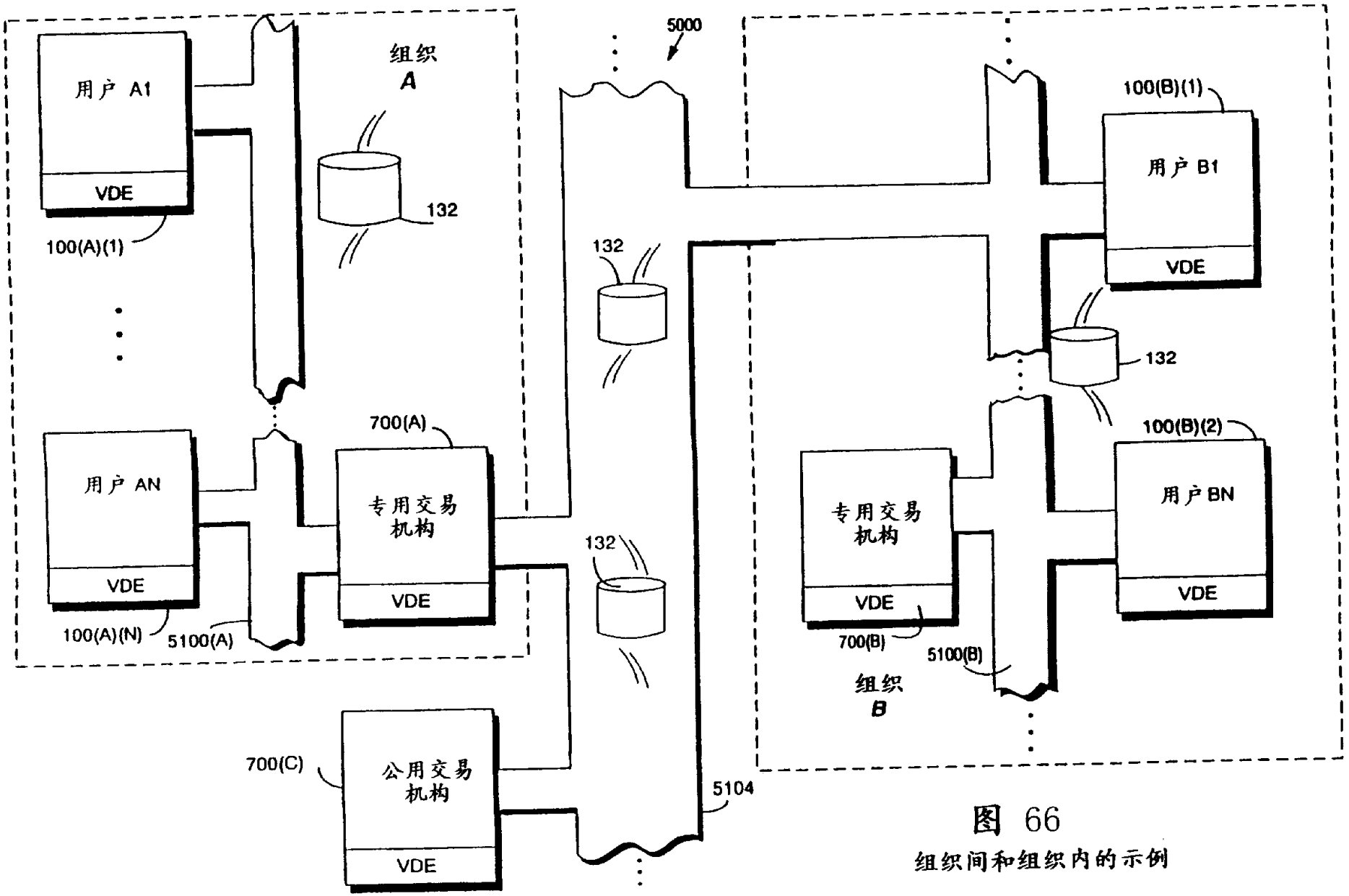


图 66

组织间和组织内的示例

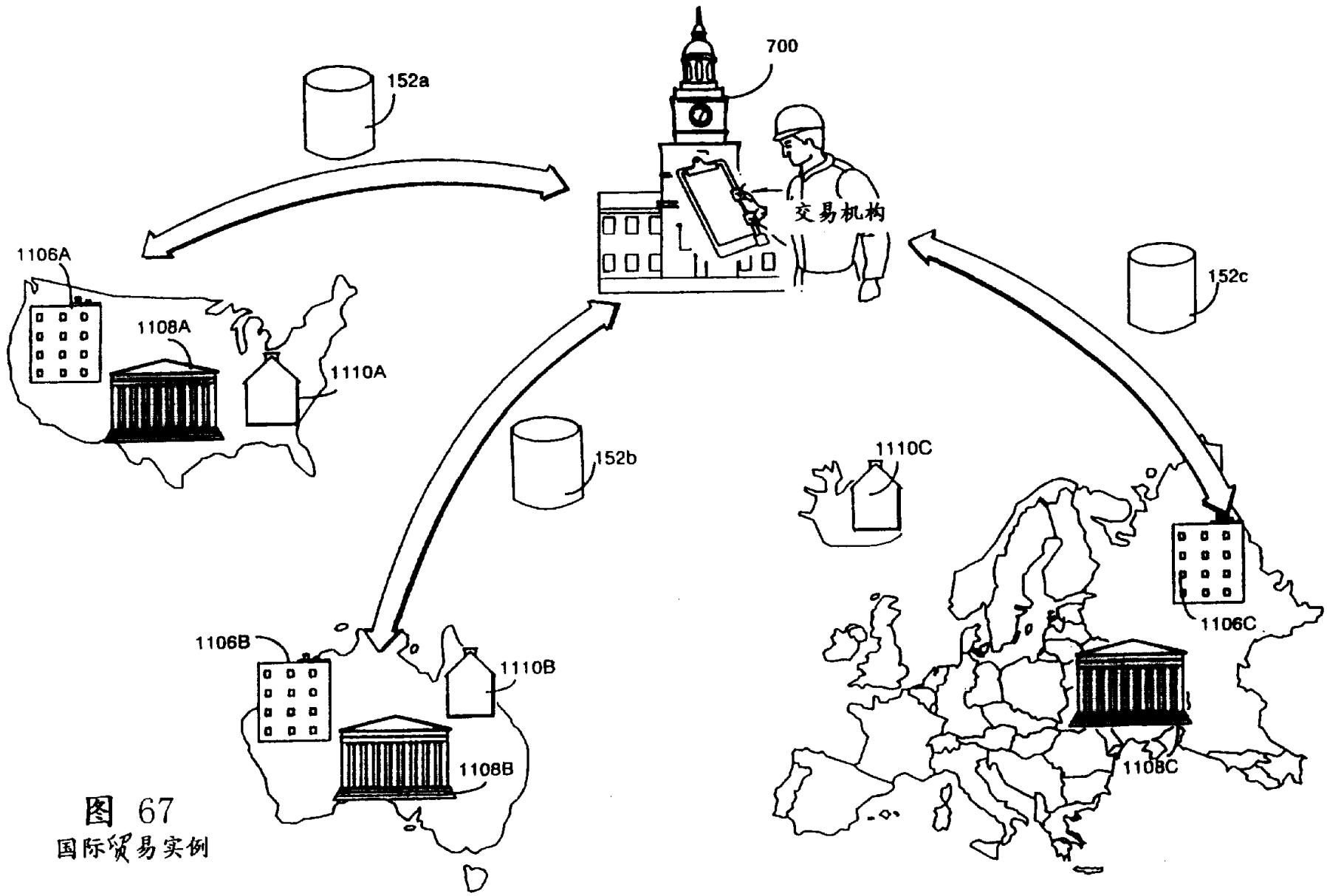

700
152a
交易机构
1106A
1108A
1110A
152c
152b
1110C
1106C
1106B
1110B
1108B
1108C

图 67
国际贸易实例