[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07F 7/08 (2006.01)
G06Q 20/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200610064899.9

[43] 公开日 2006 年 9 月 20 日

[11] 公开号 CN 1835030A

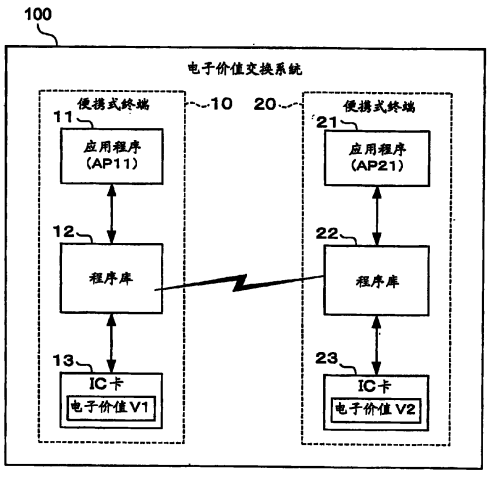
[22] 申请日 2006.3.20
[21] 申请号 200610064899.9
[30] 优先权
[32] 2005. 3.18 [33] JP [31] 2005 - 080443
[71] 申请人 株式会社 NTT 都科摩
地址 日本东京
共同申请人 国立大学法人东京大学
[72] 发明人 坂村健 越塚登 森谦作 寺田雅之
石井一彦 本乡节之
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 黄纶伟
权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称

电子价值交换系统及电子价值交换方法

[57] 摘要

电子价值交换系统及电子价值交换方法。 当在 IC 卡间交换电子价值时，能够避免伴随着应用程序不能识别在 IC 卡侧执行的处理或 IC 卡间的通信的切断等产生的不良情形。 便携式终端(20)在从便携式终端(10)接收到电子价值的交换提案消息时，将基于与该消息对应的侦听程序的交换提案内容通知给应用程序(21)。 当应用程序(21)承诺该提案内容并决定交换对象的电子价值(V1、V2)时，返回该电子价值的交换确定消息。 便携式终端(10)在接收到交换确定消息时，将基于与该消息对应的侦听程序的交换内容通知给应用程序(11)。 如果应用程序(11)承诺交换内容，则开始电子价值(V1、V2)的交换处理。



1、一种电子价值交换系统，在发送人侧终端和接收人侧终端之间进行保持于各终端的 IC 卡中的电子价值的交换，其特征在于，

所述发送人侧终端包括：

发送单元，其向所述接收人侧终端发送提出所述电子价值的交换的消息；

通知单元，其在接收到通过所述接收人侧终端的发送单元发送的用于确定交换的消息时，调出与该消息对应的侦听程序，将基于该侦听程序的交换内容通知给应用程序；以及，

交换单元，其在针对通过该通知单元通知的交换内容，得到来自所述应用程序的承诺时，在与所述接收人侧终端之间进行电子价值的交换，

所述接收人侧终端包括：

通知单元，其在接收到从所述发送人侧终端发送的交换提案消息时，调出与该消息对应的侦听程序，将基于该侦听程序的提案内容通知给应用程序；以及，

发送单元，其在针对通过该通知单元通知的提案内容，得到来自所述应用程序的承诺时，向所述发送人侧终端发送交换确定消息。

2、一种电子价值交换方法，其特征在于，包括：

发送人侧终端向接收人侧终端发送提出电子价值的交换的消息的发送步骤；

所述接收人侧终端

在接收到通过所述发送步骤发送的交换提案消息时，调出与该消息对应的侦听程序，将基于该侦听程序的提案内容通知给应用程序的通知步骤；

在针对通过该通知步骤通知的提案内容，得到来自所述应用程序的承诺时，向所述发送人侧终端发送用于确定交换的消息的发送步骤；

所述发送人侧终端

在接收到通过所述发送步骤发送的交换确定消息时，调出与该消息

对应的侦听程序，将基于该侦听程序的交换内容通知给应用程序的通知步骤；

在针对通过该通知步骤通知的交换内容，得到来自所述应用程序的承诺时，在与所述接收人侧终端之间进行电子价值的交换的交换步骤。

电子价值交换系统及电子价值交换方法

技术领域

本发明涉及在通信终端间交换电子价值的技术。

背景技术

近年来，作为实现普适计算环境的手段之一，正在进行 TRON(The Real-time Operating system Nucleus)的研究。其中，在内置有 e-TRON 卡等 IC(IntegratedCircuit)卡的便携式终端中，提出了如下的一种技术，当电子货币或电子优惠券(coupon)等电子价值在终端间授受时，不经由应用程序，而在双方的 IC 卡间直接地进行价值的收发。该技术作为应用于不足的电子价值的收费(charge)的系统，在专利文献 1（特开 2003-337887 号公报）中，公开了兼有高安全性和简便性的电子价值收费系统。

但是，所述现有技术在具有抗干扰性的 IC 卡间直接进行电子价值的交换。因此，能够确保高安全性，但另一方面产生不能够在应用程序侧随时把握 IC 卡侧的状态的问题。例如，由于 IC 卡是黑箱（black box），所以终端用户通过应用程序来把握处理内容。因此，只要不将处理状态通知该应用程序，IC 卡就不能对用户提示必要信息。

发明内容

因此，本发明的课题是，当 IC 卡的外部具有应用程序的终端装置，在 IC 卡间交换电子价值时，避免伴随着应用程序不能识别在 IC 卡侧执行的处理或 IC 卡间的通信的切断等产生的不良情形。

本发明提供了一种在发送人侧终端和接收人侧终端之间进行保持于各终端的 IC 卡中的电子价值的交换的电子价值交换系统，所述发送人侧终端包括：发送单元，其向所述接收人侧终端发送提出所述电子价值的交换的消息（交换提案消息）；通知单元，其在接收到通过所述接收人侧

终端的发送单元发送的用于确定交换的消息（交换确定消息）时，调出与该消息对应的侦听程序，将基于该侦听程序的交换内容通知给应用程序；以及交换单元，其在针对通过该通知单元通知的交换内容，得到来自所述应用程序的承诺时，在与所述接收人侧终端之间进行电子价值的交换，所述接收人侧终端包括：通知单元，其在接收到从所述发送人侧终端发送的交换提案消息时，调出与该消息对应的侦听程序，将基于该侦听程序的提案内容通知给应用程序；以及发送单元，其在针对通过该通知单元通知的提案内容，得到来自所述应用程序的承诺时，向所述发送人侧终端发送交换确定消息。

本发明提供了一种电子价值交换方法，包括：发送人侧终端向接收人侧终端发送提出电子价值的交换的消息的发送步骤；所述接收人侧终端，在接收到通过所述发送步骤发送的交换提案消息时，调出与该消息对应的侦听程序，将基于该侦听程序的提案内容通知给应用程序的通知步骤；在针对通过该通知步骤通知的提案内容，得到来自所述应用程序的承诺时，向所述发送人侧终端发送用于确定交换的消息的发送步骤；所述发送人侧终端，在接收到通过所述发送步骤发送的交换确定消息时，调出与该消息对应的侦听程序，将基于该侦听程序的交换内容通知给应用程序的通知步骤；在针对通过该通知步骤通知的交换内容，得到来自所述应用程序的承诺时，在与所述接收人侧终端之间进行电子价值的交换的交换步骤。

通过这些发明，接收人侧终端在从发送人侧终端接收到对保持于自终端的 IC 卡中的电子价值和发送人侧终端的 IC 卡内的电子价值进行交换的提案时，将该提案通知给自终端的应用程序。在通过由接收人侧终端的用户的操作等，使应用程序对该提案内容返回肯定的响应时，接收人侧终端委托发送人侧终端进行交换的确定。在发送人侧终端，与接收人侧终端同样地，向自终端的应用程序通知该委托。然后，当通过由发送人侧终端的用户的操作等，使应用程序对该委托内容返回肯定的响应时，发送人侧终端向接收人侧终端发送电子价值。同时，也从接收人侧终端发送电子价值，完成电子价值的交换。这样，等待通过双方终端存

储的应用程序的许可与否的判定来执行 IC 卡彼此直接的电子价值交换处理。即，在进行电子价值交换的双方终端的应用程序中，能够识别 IC 卡间执行的处理。

附图说明

图 1 是表示电子价值交换系统的结构的图。

图 2 是用于说明电子价值交换系统的动作的图的前半部分。

图 3 是用于说明电子价值交换系统的动作的图的后半部分。

具体实施方式

以下参照用于例示的附图，对本发明的一个实施方式进行说明。首先，说明本实施方式的电子价值交换系统 100 的结构。如图 1 所示，电子价值交换系统 100 具有便携式终端 10（与发送人侧终端对应）和便携式终端 20（与接收人侧终端对应）。便携式终端 10、20 例如是便携式电话或 PDA(Personal Digital Assistance)，如果是具有通信功能的终端装置，则不受其功能或用途的限制。便携式终端 10 和便携式终端 20 构成为能够使用各自具有的程序库，进行经由近距离无线通信线路的电子价值的收发。

接着，对便携式终端 10 的各构成要素进行说明。便携式终端 10 具有应用程序 11、程序库 12（与发送单元、通知单元对应）以及 IC 卡 13（与交换单元对应）。这些各构成要素通过总线连接为能够相互输入或输出信号。

应用程序 11（以下记为“AP 11”）在便携式终端 10 的用户指示电子价值的交换时，将该指示通知程序库 12。另外，AP 11 通过从程序库 12 输入“committed”，检测电子价值交换的完成。此时，根据需要将交换完成的意思通知便携式终端 10 的用户。

程序库 12 以从 AP 11 接收“exchange”为契机，作成对 IC 卡 13 指示交换的消息，并向 IC 卡 13 输出。另外，程序库 12 在取得消息时执行与此对应的侦听程序（listener）。例如，程序库 12 在接收从 IC 卡 23

发送的交换确定消息时，将基于与此对应的侦听程序的提案内容通知 AP 11。当得到对提案内容的承诺时，程序库 12 向 IC 卡 13 输出交换执行消息，指示电子价值的交换开始。另外，程序库 12 在随着电子价值的交换结束，从 IC 卡 13 中取得交换完成消息时，执行侦听程序“通知给 AP 11”。

在 IC 卡 13 中存储有作为交换对象的电子价值 V1。IC 卡 13 从防止电子价值 V1 的篡改或复制等确保安全性的角度出发，最好由抗干扰装置构成。电子价值 V1 通过电子化数据表现某种经济价值（表现体），例如，表现货币价值的电子货币，或者，以预付方式提供的电子票证（图书券、次券）等。

IC 卡 13 随着从程序库 12 输入交换指示消息，将该消息作为交换提案消息通过程序库 12 向便携式终端 20 发送。另外，IC 卡 13 在通过程序库 22、12 从 IC 卡 23 输入交换完成消息时，将该交换完成消息向便携式终端 10 的程序库 12 输出。

IC 卡 13 以从程序库 12 输入交换执行消息为契机，开始以 IC 卡 23 为通信对方的电子价值的交换处理。该交换处理不通过 AP 11、21 而在 IC 卡间直接地进行。即，IC 卡 13 将存储于其内部的电子价值 V1 经由程序库 12、22 以及无线网络向 IC 卡 23 发送。同样地，从 IC 卡 23 经由程序库 22、12 以及无线网络将电子价值 V2 向 IC 卡 13 发送。通过双方 IC 卡接收对方的电子价值来完成交换。

便携式终端 20 也具有与便携式终端 10 相同的结构。即，便携式终端 20 具有应用程序 21 和程序库 22（与通知单元、发送单元对应）以及 IC 卡 23。这些各构成要素通过总线连接为能够相互输入或输出信号。

应用程序 21（以下记为“AP 21”）根据从程序库 22 输入的“offered”，将其提案内容向便携式终端 20 的用户提示。AP 21 等待用户的指示操作，如果有承诺的指示，则在确定满足交换对象条件的电子价值 V1、V2 后，响应“agree”。如果没有，则对程序库 22 响应“NG”。另外，AP 21 通过从程序库 22 输入“committed”来检测电子价值的交换结束。此时，根据需要将交换完成的意思通知便携式终端 20 的用户。

程序库 22 在取得消息时，执行与其对应的侦听程序。例如，程序库

22 在接收从 IC 卡 13 发送的交换提案消息时，将基于与其对应的侦听程序的提案内容通知 AP 21。在得到对提案内容的承诺时，程序库 22 通过向 IC 卡 13 发送交换确定消息，敦促其用户确定开始执行交换处理。另外，程序库 22 在随着电子价值的交换结束，从 IC 卡 23 中取得交换完成消息时，执行对应的侦听程序“通知给 AP 21”。

IC 卡 23 以从程序库 22 输入交换确定消息为契机，向 IC 卡 13 传送该消息。另外，IC 卡 23 在电子价值交换时，经由程序库 22、12 和无线网络向 IC 卡 13 发送电子价值 V2。

下面，参照图 2、图 3 对本实施方式的电子价值交换系统 100 的动作以及构成本发明的电子价值交换方法的各步骤进行说明。作为说明的前提，在本实施方式中设定如下的状态：希望便携式终端 10 的用户 A 持有的电子价值 V1 和便携式终端 20 的用户 B 持有的电子价值 V2 进行交换。

首先，AP 11 在接收来自便携式终端 10 的用户 A 的指示时（图 2 中的 S1），使用 API（Application Program Interface），对程序库 12 指示电子价值的交换（S2）。作为指示交换开始的函数，例如可以使用“exchange（ICC13、ICC23、ConditionData)”。Exchange 函数具有（发送源 ID、发送目的地 ID、发送对象数据）的参数，在作为发送对象数据的“ConditionData”中至少包含能够成为交换对象的电子价值 V1、V2 的条件。

接受了交换指示的程序库 12 通过将所述 API 变换成消息，作成对 IC 卡 23 指示电子价值交换的消息[Start Exchange]（S3）。程序库 12 向被指定为目的地的 IC 卡 13 传送该交换指示消息（S4）。

IC 卡 13 在接收交换指示消息时，向作为通信对方的 IC 卡 23 的程序库 22 发送具有作为参数的要交换的电子价值条件“Condition”的交换提案消息（S5）。该交换提案消息经由程序库 12 发送，能够以“offer（Condition)”表现。

便携式终端 20 侧的程序库 22 在检测交换提案消息的接收时，取得作为与该消息对应的侦听程序的“通知给 AP 21”（S6）。在 S7 中程序库 22 按照在 S6 中读出的所述侦听程序的记述，向 AP 21 传递作为提案内容

的“offered (Condition)”。接受了提案内容的 AP 21 根据便携式终端 20 的用户 B 的指示，判断对提案内容是否进行了承诺（S8）。

在 S8 中，当用户 B 指示提案内容的承诺时（S8；是），AP 21 确定与所述 Condition 中的 V1、V2 条件符合的交换对象的电子价值 V1、V2。交换对象确定后，AP 21 将作为肯定响应的“agree”返回到程序库 22（S10）。在肯定响应中至少包含执行交换处理的 IC 卡 13、23 的 ID，以及作为交换对象的电子价值 V1、V2 的 ID。程序库 22 通过“agree”的返回，判断用户 B 承诺了提案内容，将用于确定电子价值交换的消息[AgreeExchange（V1、V2）]经由 IC 卡 23、13 向程序库 12 发送（S11）。

以下，在便携式终端 10 的程序库 12 中执行与所述 S6、S7 同样的处理。即，程序库 12 取得与从 IC 卡 13 输入的交换确定消息对应的侦听程序（S12）。另外，程序库 12 根据所述侦听程序的记述，将作为交换内容的“agreed”向 AP 11 传递（S13）。

转入图 3，接下来 AP 11 根据便携式终端 10 的用户 A 的指示，判定有无对交换内容的承诺（S14）。当用户 A 指示了承诺时（S14；是），AP 11 将肯定响应“confirm”返回到程序库 12（S15）。在该肯定响应中与 S10 同样地至少包含执行交换处理的 IC 卡 13、23 的 ID，以及被确定为交换对象的电子价值 V1、V2 的 ID。程序库 12 通过该“confirm”的返回，判断用户 A 承诺了提案内容，将交换执行消息[Confirm Exchange]向 IC 卡 13 输出（S16）。

以交换执行消息[Confirm Exchange]输入给 IC 卡 13 为契机，在 IC 卡 13 和 IC 卡 23 之间开始各自所有的电子价值的交换（S17）。S17 中的电子价值的收发处理经由程序库而不经由应用程序（可以说是直接地）来完成。由此防止电子价值的盗阅或篡改，以维持较高安全水平。

另外，在 S8 中，当用户 B 拒绝交换时（S9；否），AP 21 将作为否定响应的“NG”返回到程序库 22（S18）。接收到否定响应的程序库 22 将与在 S5 中接收到的交换提案消息对应的错误通知程序库 12。IC 卡 13 接受来自程序库 12 的错误消息的传送，检测拒绝电子价值交换的情况（S19）。

同样地，在 S14 中，当用户 A 拒绝交换时（S14；否），AP 11 将作为

否定响应的“NG”返回到程序库 12（S20）。接收到否定响应的程序库 12 通过程序库 22，将与在 S11 中接收到的交换确定消息对应的错误通知 IC 卡 23（S21）。由此，IC 卡 23 检测拒绝电子价值交换的情况。

当 S17 中的电子价值的交换处理正常完成时，即 IC 卡 23 取得电子价值 V1 时，IC 卡 23 通过程序库 22、12，将作为交换完成消息的[commit]向 IC 卡 13 发送（S22）。在交换完成消息发送时，在便携式终端 20 中也执行与所述 S6、S7 相同的处理。即，程序库 22 在发送交换完成消息时取得与该消息对应的侦听程序“通知给 AP 21”（S23）。程序库 22 按照在 S23 中读出的所述侦听程序的记述，向 AP 21 传递“committed”（S24）。由此，AP 21 识别出电子价值的交换处理正常完成。

另一方面，IC 卡 13 在接收到 S22 中发送的交换完成消息[commit]后，向程序库 12 输出交换完成消息[committed]（S25）。在交换完成消息输出时，在便携式终端 10 中也执行与所述 S23、S24 同样的处理。

即，程序库 12 在接受交换完成消息的输入时，取得与该消息对应的侦听程序“通知给 AP 11”（S26）。在 S27 中，程序库 12 按照在 S26 中读出的所述侦听程序的记述，向 AP 11 传递“committed”。通过 S27 的处理，AP 11 识别出电子价值的交换正常完成。

以上说明的电子价值交换系统 100 具有以下的作用效果。第 1，接收人侧的程序库 22 在每次发生事件时，对 AP 21 通知其要求内容。对于 IC 卡间直接的电子价值的交换，确保较高的安全性，另一方面，存在 AP 21 难以即时把握 IC 卡间的处理的问题，而通过所述通知则能够解决该问题。即，能够使接收人侧的便携式终端具有使到达 IC 卡的消息被程序库监视的功能。该监视结果为，由于通知给应用程序，因此能够在应用程序中随时把握 IC 卡侧的处理。

另外，通过电子价值交换系统 100，不仅能够使接收人侧的便携式终端 20 具有使到达 IC 卡的消息被程序库监视的功能，也能够使发送人侧的便携式终端 10 具有该功能。该监视结果为，由于也通知给 AP 11，所以能够在 AP 11 中随时把握 IC 卡 13 侧的处理。另外，IC 卡 13、23 间的电子价值的交换处理只要不经利用便携式终端 10、20 的应用程序 11、21

的双方的承诺，就不能正常完成。其结果能够实现更高安全水准的电子价值交换。

第 2，发送人侧的程序库 12 在电子价值的交换完成时，向 AP 11 通知交换完成。与此相同，接收人侧的程序库 22 在电子价值的交换完成时，向 AP 21 通知交换完成。即，由于进行电子价值交换的便携式终端 10、20 的应用程序 11、12 都能够迅速识别交换的正常完成，因此能够在没有所述通知中的至少一个通知的情况下，判断出电子价值交换没有正常完成。

另外，作为电子价值交换不能正常完成的重要因素，可以举出伴随通信源降低产生的线路切断，或者便携式终端的中断指示等。当电子价值的交换处理中断时，便携式终端 10 或便携式终端 20 能够与设置在电子价值交换系统 100 外部的通信控制装置连接。通信控制装置由 TTP（Trusted Third Party）运用/管理，并决定中止或继续进行所述交换处理。

另外，电子价值交换系统 100 维持 IC 卡内的处理的隐匿性，并能够仅将依赖于用户判断的最小限度的必要信息非同步地通知给应用程序。因此，能够抑制 IC 卡处理负荷的增大。

根据本发明，当 IC 卡外部具有应用程序的终端装置，在 IC 卡间交换电子价值时，能够避免伴随着应用程序不能识别在 IC 卡侧执行的处理或 IC 卡间的通信的切断等产生的不良情形。

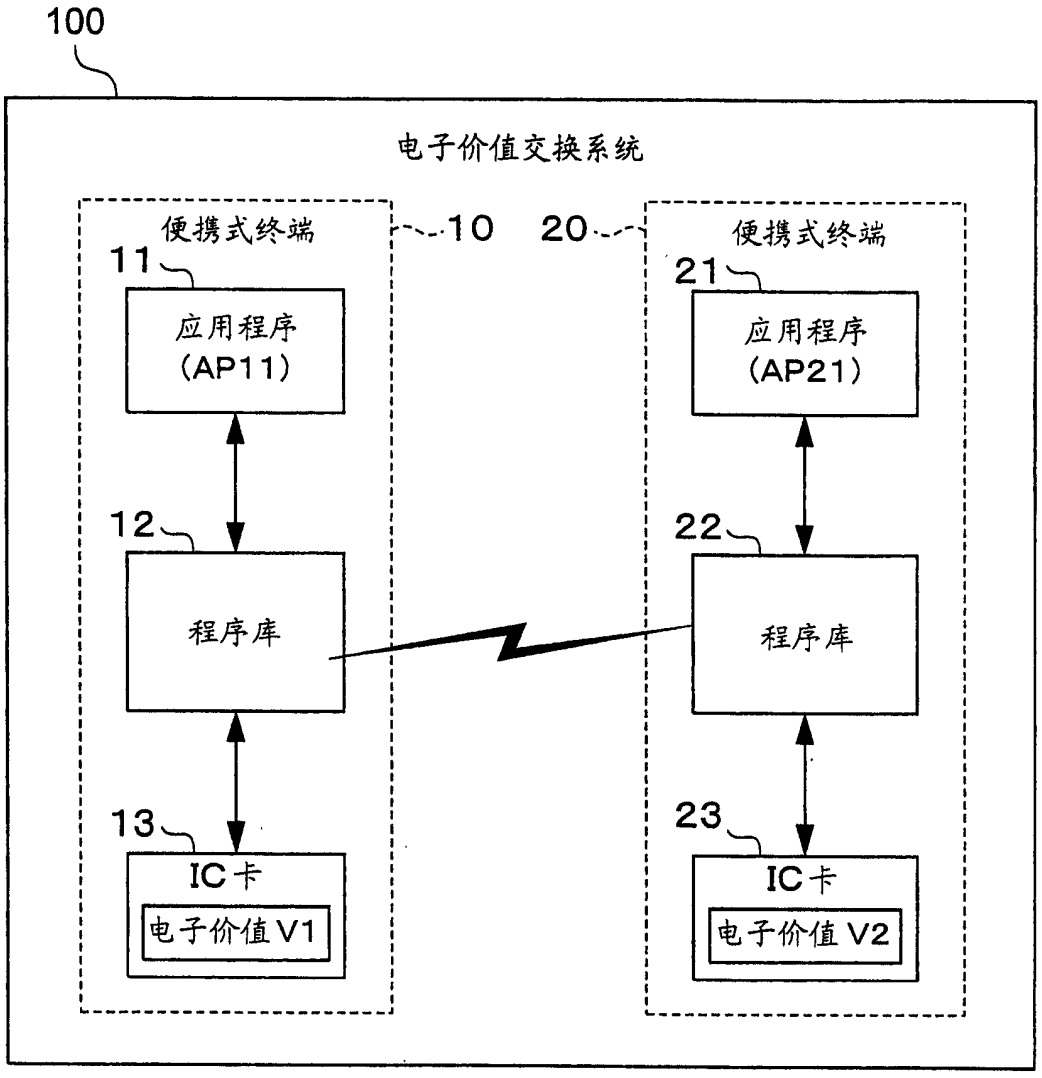

100
电子价值交换系统
便携式终端
10
20
便携式终端
11
应用程序
(AP11)
21
应用程序
(AP21)
12
程序库
22
程序库
13
IC卡
电子价值V1
23
IC卡
电子价值V2

图 1

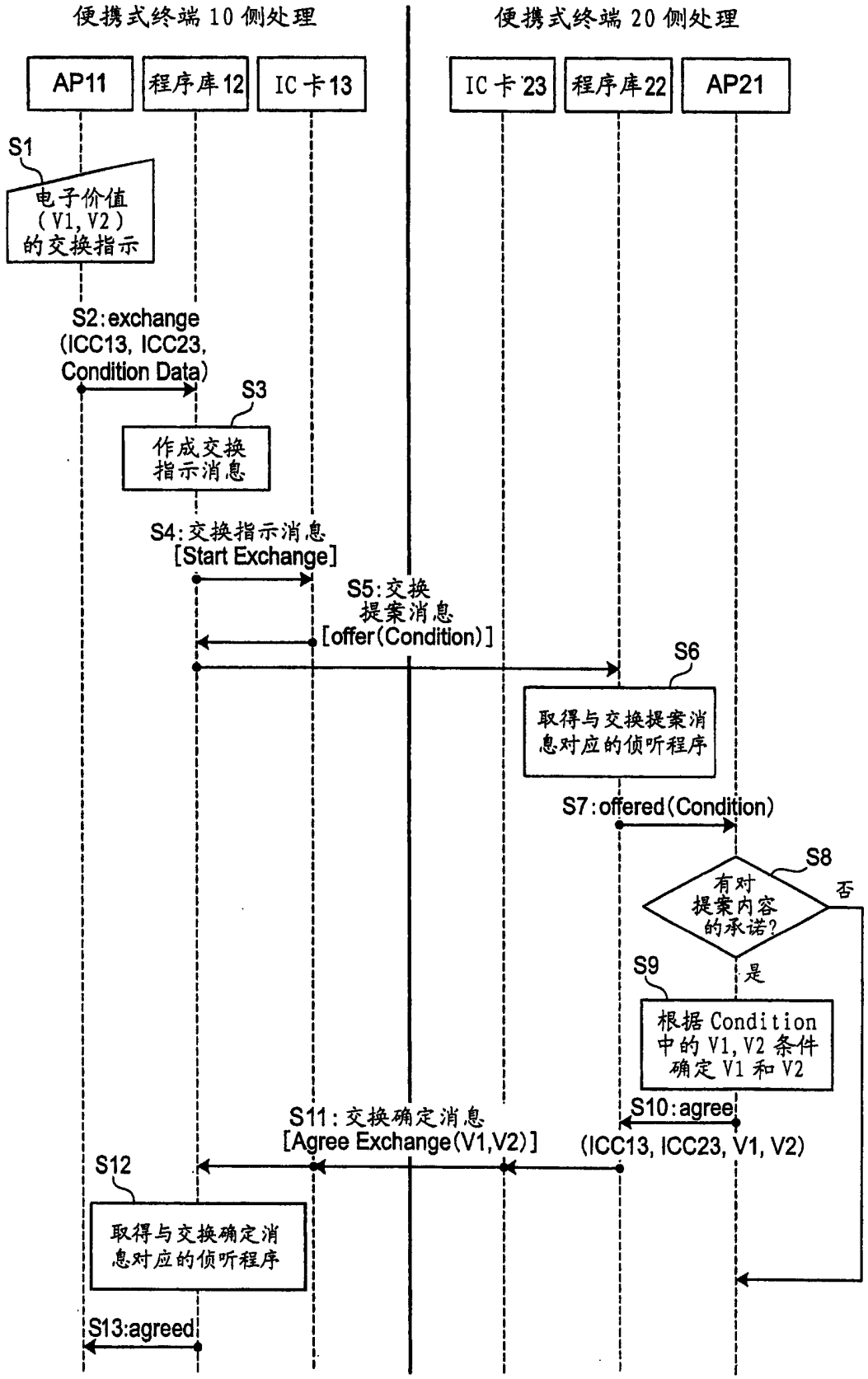

便携式终端 10 侧处理
便携式终端 20 侧处理
AP11
程序库 12
IC 卡 13
IC 卡 23
程序库 22
AP21
S1
电子价值
(V1, V2)
的交换指示
S2:exchange
(ICC13, ICC23,
Condition Data)
S3
作成交换
指示消息
S4:交换指示消息
[Start Exchange]
S5:交换
提案消息
[offer(Condition)]
S6
取得与交换提案消
息对应的侦听程序
S7:offered(Condition)
S8
有对
提案内容
的承诺?
否
是
S9
根据 Condition
中的 V1, V2 条件
确定 V1 和 V2
S10:agree
(ICC13, ICC23, V1, V2)
S11:交换确定消息
[Agree Exchange(V1,V2)]
S12
取得与交换确定消
息对应的侦听程序
S13:agreed

图 2

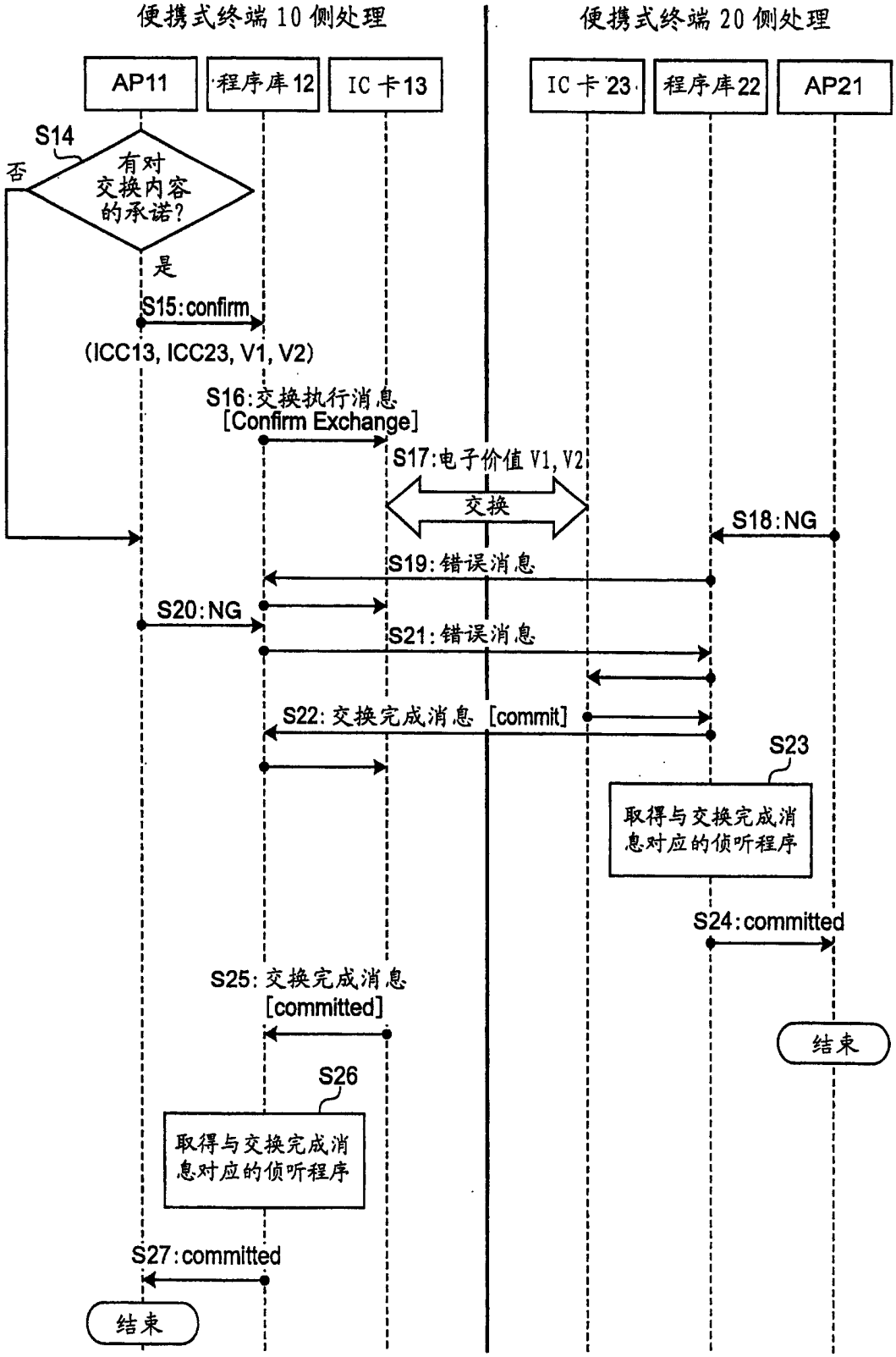

便携式终端 10 侧处理
便携式终端 20 侧处理
AP11
程序库 12
IC 卡 13
IC 卡 23
程序库 22
AP21
S14
有对交换内容的承诺?
否
是
S15:confirm
(ICC13, ICC23, V1, V2)
S16:交换执行消息 [Confirm Exchange]
S17:电子价值 V1, V2 交换
S18:NG
S19:错误消息
S20:NG
S21:错误消息
S22: 交换完成消息 [commit]
S23
取得与交换完成消息对应的侦听程序
S24:committed
S25: 交换完成消息 [committed]
结束
S26
取得与交换完成消息对应的侦听程序
S27:committed
结束

图 3