(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110268432 A
(43)申请公布日 2019.09.20

(21)申请号 201780062333.9

(22)申请日 2017.08.07

(30)优先权数据
15/233,719 2016.08.10 US

(85)PCT国际申请进入国家阶段日
2019.04.09

(86)PCT国际申请的申请数据
PCT/US2017/045665 2017.08.07

(87)PCT国际申请的公布数据
WO2018/031433 EN 2018.02.15

(71)申请人 摩根大通国家银行
地址 美国纽约

(72)发明人 K·T·汉拉恩 D·K·周
D·J·沃尔什 T·W·朱 P·邱
L·卡拉米塔

(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 徐东升 孙尚白

(51)Int.Cl.
G06Q 20/10(2006.01)
G06Q 30/04(2006.01)
G06Q 40/02(2006.01)

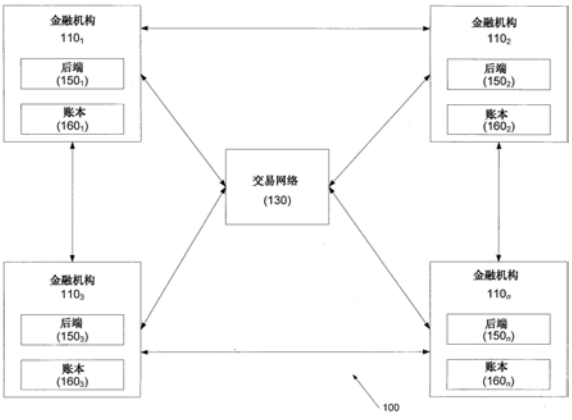
权利要求书1页 说明书6页 附图2页

(54)发明名称

用于使用分布式账本进行账户对账的系统和方法

(57)摘要

公开了用于使用分布式账本进行账户对账的系统和方法。在一个实施例中，一种用于使用分布式账本进行账户对账的方法可以包括：(1)支付发送金融机构接收涉及由支付发送金融机构为支付接收金融机构维护的账户的交易；(2)支付发送金融机构使用交易网络向支付接收金融机构传送交易；(3)支付发送金融机构将交易作为第一账本条目写入支付发送金融机构的分布式交易账本的副本；(4)支付发送金融机构从支付接收金融机构接收第二账本条目；以及(5)支付发送金融机构使用第一账本条目和第二账本条目核对账户。



CN 110268432 A

1.一种用于使用分布式账本进行账户对账的方法,包括:

支付发送金融机构接收涉及由所述支付发送金融机构为支付接收金融机构维护的账户的交易;

所述支付发送金融机构使用交易网络向所述支付接收金融机构传送所述交易;

所述支付发送金融机构将所述交易作为第一账本条目写入所述支付发送金融机构的分布式交易账本的副本;

所述支付发送金融机构从所述支付接收金融机构接收第二账本条目;以及

所述支付发送金融机构使用所述第一账本条目和所述第二账本条目核对所述账户。

2.根据权利要求1所述的方法,其中第一账本条目包括智能合约。

3.根据权利要求2所述的方法,其中所述智能合约包括用于所述支付发送金融机构以将所述第一账本条目与所述第二账本条目进行匹配的指令。

4.根据权利要求2所述的方法,其中所述智能合约包括所述账户的期初余额。

5.根据权利要求2所述的方法,其中所述智能合约包括用于响应于对账失败来警告所述发送金融机构的指令。

6.根据权利要求1所述的方法,其中所述第一账本条目包括所述账户的贷方条目。

7.根据权利要求1所述的方法,其中所述第二账本条目包括所述账户的借方条目。

8.根据权利要求1所述的方法,其中所述账户是存放同业账户。

9.根据权利要求1所述的方法,其中所述分布式账本是区块链分布式账本。

10.一种用于使用分布式账本进行账户对账的方法,包括:

支付接收金融机构通过交易网络接收涉及由支付发送金融机构为所述支付接收金融机构维护的账户的交易;

所述支付接收金融机构将所述交易作为第一账本条目写入所述支付接收金融机构的分布式交易账本的副本;

所述支付接收金融机构从所述支付第二金融机构接收第二账本条目;以及

所述支付接收金融机构使用所述第一账本条目和所述第二账本条目核对所述账户。

11.根据权利要求10所述的方法,其中第一账本条目包括智能合约。

12.根据权利要求11所述的方法,其中智能合约包括用于所述支付发送金融机构以将所述第一账本条目与所述第二账本条目进行匹配的指令。

13.根据权利要求11所述的方法,其中所述智能合约包括所述账户的期初余额。

14.根据权利要求11所述的方法,其中所述智能合约包括用于响应于对账失败来警告所述发送金融机构的指令。

15.根据权利要求10所述的方法,其中所述第一账本条目包括所述账户的贷方条目。

16.根据权利要求10所述的方法,其中所述第二账本条目包括所述账户的借方条目。

17.根据权利要求10所述的方法,其中所述账户是存放同业账户。

18.根据权利要求10所述的方法,其中所述分布式账本是区块链分布式账本。

用于使用分布式账本进行账户对账的系统和方法

技术领域

[0001] 本公开总体涉及用于使用分布式账本(ledger)进行账户对账的系统和方法。

背景技术

[0002] 为了支持外汇市场并以外币进行交易,银行在其他国家与其合作银行维护存放同业(nostro)账户。这些账户的数量很大,因此核对和控制这项活动以避免账户被透支并管理特定货币的多头或空头风险非常重要。

发明内容

[0003] 公开了用于使用分布式账本进行账户对账的系统和方法。在一个实施例中,一种用于使用分布式账本进行账户对账的方法可以包括:(1)支付发送金融机构接收涉及由支付发送金融机构为支付接收金融机构维护的账户的交易;(2)支付发送金融机构使用交易网络向支付接收金融机构传送交易;(3)支付发送金融机构将交易作为第一账本条目写入支付发送金融机构的分布式交易账本的副本;(4)支付发送金融机构从支付接收金融机构接收第二账本条目;以及(5)支付发送金融机构使用第一账本条目和第二账本条目核对账户。

[0004] 在一个实施例中,第一账本条目可以包括智能合约。智能合约可以包括用于支付发送金融机构以将第一账本条目与第二账本条目进行匹配的指令。

[0005] 在一个实施例中,智能合约可以包括账户的期初余额和/或用于响应于对账失败来警告发送金融机构的指令。

[0006] 在一个实施例中,第一账本条目可以包括账户的贷方条目。

[0007] 在一个实施例中,第二账本条目可以包括账户的借方条目。

[0008] 在一个实施例中,账户可以是存放同业账户。

[0009] 在一个实施例中,分布式账本可以是区块链分布式账本。

[0010] 根据另一个实施例,一种用于使用分布式账本进行账户对账的方法可以包括:(1)支付接收金融机构通过交易网络接收涉及由支付发送金融机构为支付接收金融机构维护的账户的交易;(2)支付接收金融机构将交易作为第一账本条目写入支付接收金融机构的分布式交易账本的副本;(3)支付接收金融机构从支付第二金融机构接收第二账本条目;以及(4)支付接收金融机构使用第一账本条目和第二账本条目核对账户。

[0011] 在一个实施例中,第一账本条目可以包括智能合约。智能合约可以包括用于支付发送金融机构以将第一账本条目与第二账本条目进行匹配的指令。

[0012] 在一个实施例中,智能合约可以包括账户的期初余额和/或用于响应于对账失败来警告发送金融机构的指令。

[0013] 在一个实施例中,第一账本条目可以包括账户的贷方条目。

[0014] 在一个实施例中,第二账本条目可以包括账户的借方条目。

[0015] 在一个实施例中,账户是存放同业账户。

[0016] 在一个实施例中,分布式账本可以是区块链分布式账本。

附图说明

[0017] 为了更完整地理解本发明、其目的和优点,现在参考以下结合附图的描述,其中:

[0018] 图1描绘了根据一个实施例的用于使用分布式账本进行账户对账的系统;以及

[0019] 图2描绘了根据一个实施例的用于使用分布式账本进行账户对账的方法。

具体实施方式

[0020] 通过参考图1-图2可以理解本发明的若干实施例及其优点。

[0021] 实施例涉及使用分布式账本进行账户对账。

[0022] 大多数金融机构通过全球银行间金融电信协会(或SWIFT)网络从其存放同业代理处接收存放同业账户报表。然后将存放同业报表条目与银行中维护的镜像账户条目进行核对。如果在交易条目中发现不匹配,金融机构通常会立即采取补救措施。

[0023] 由于在一天结束时接收到并核对报表,因此在白天没有对存放同业账户余额(balance)的可见性。因此,在一天结束时接收到报表之前,金融机构不能跟踪、检测和/或解决交易错误。

[0024] 非SWIFT金融机构通过传真或电子邮件接收报表,这将导致进一步延迟并导致对账错误。

[0025] 实施例公开了一种系统和方法,由此存放同业代理金融机构和客户(client)金融机构可以使用分布式账本,以便基本上实时地核对交易。这种分布式账本的一个示例是基于区块链的账本,其包含保存有时间戳的批量有效交易的块。每个块可以包括先前块的散列(hash),从而将块链接在一起。链接的块形成链,其中每个附加的块加强它之前的块。

[0026] 在一个实施例中,分布式账本可以是以太坊平台。

[0027] 在一个实施例中,该系统和方法可以提供实时对账。

[0028] 在一个实施例中,(一个或更多个)存放同业代理和(一个或更多个)客户银行可以连接在“许可”或专用网络中,其中只有分布式账本对账中的参与者可以访问。在另一个实施例中,(一个或更多个)存放同业代理和客户银行可以在公共网络中,其中包括那些不参与分布式账本对账的实体也可以访问。

[0029] 在一个实施例中,在已经发送了支付和已经处理了收据时,客户银行可以向网络广播内部账本交易。一旦将账户条目发布到存放同业账户,存放同业代理就可以将存放同业交易广播到网络。

[0030] 当交易被进行匹配和验证时,它们可以被“确认”并被添加到分布式账本,并且可以与网络中的所有参与者共享。在一个实施例中,分布式账本的主机可以执行该功能。

[0031] 在一个实施例中,客户银行可以更新其分布式账本的副本。

[0032] 如果在合理的时间段内未确认条目,则可以向所涉及的存放同业代理和客户银行发送警报。

[0033] 实施例可以提供以下益处中的一些或全部:(1)减少的对账时间(例如,最多一天);(2)降低的成本(例如,没有SWIFT费用);(3)更快的错误检测和解决;(4)最小化风险并且改善对存放同业账户的控制;以及(5)任何银行都易于加入。

[0034] 参考图1,根据一个实施例公开了一种用于使用分布式账本进行账户对账的系统。

[0035] 系统100可以包括多个金融机构110_1-110_n,每个金融机构可以是例如银行。在一个实施例中,金融机构110中的一个可以充当其他金融机构110之一的存放同业代理,并且可以为其他金融机构110维护单独的存放同业账户。例如,对于金融机构110_1可以维护与其开展业务的金融机构110之一的存放同业账户。

[0036] 在一个实施例中,每个金融机构110可以以不同的货币进行交易。例如,金融机构110_1可以位于美国,并且可以用美元进行交易;金融机构110_2可以基于日本,并且可以用日元进行交易;金融机构110_3可以位于英国,并且可以用英镑进行交易;等等。因此,金融机构110_2和110_3可以被认为是金融机构110_1的存放同业代理。

[0037] 在一个实施例中,金融机构110_1-110_n可以直接、间接等地彼此传送交易。在一个实施例中,金融机构110_1-110_n中的一个或更多个可以使用交易网络130来传送交易。在一个实施例中,交易网络130可以是SWIFT网络。

[0038] 在一个实施例中,金融机构110_1可以维护镜像存放同业账户,其镜像与其他金融机构110的每个存放同业账户。

[0039] 在一个实施例中,每个金融机构110可以具有后端(backend)150和分布式账本160。例如,每个金融机构110可以维护其分布式账本160的副本。在一个实施例中,账本160可以是分布式账本,诸如基于区块链的账本。

[0040] 在一个实施例中,每个后端150可以维护其相关联的账本160。例如,每个后端150可以写入其分布式账本160的副本,并且可以基于该活动向其他金融机构110发送通知。例如,当金融机构110_1使用交易网络130向金融机构110_2发送交易时,后端150_1可以将交易写入其分布式账本160_1的副本,并且还可以将交易传送到后端150_2-150_n以写入其分布式账本160_2-160_n的副本。

[0041] 参考图2,根据一个实施例公开了一种用于使用分布式账本进行账户对账的方法。在步骤205中,多个金融机构可以注册以参与分布式账本存放同业账户网络。在一个实施例中,一个金融机构可以为一个或更多个其他金融机构保持存放同业账户。

[0042] 在步骤210中,支付发送金融机构可以使用诸如SWIFT网络的交易网络将交易发送到另一金融机构。

[0043] 在一个实施例中,交易可以是支付、支付的收据等。

[0044] 在步骤215中,支付发送金融机构可以将交易写入其分布式账本的副本。在一个实施例中,支付发送金融机构的后端可以将交易写入金融机构的分布式账本的副本。

[0045] 在一个实施例中,交易可以被写为智能合约。例如,智能合约可以包括匹配发布到分布式账本网络的账本条目的指令。作为对账过程的一部分,智能合约可以维护存放同业账户的期初余额和当前运行余额。如果在可配置的时间内不能核对账本条目,则智能合约可以向相应的金融机构发送警报。

[0046] 在步骤220中,支付发送金融机构可以将交易传送到网络中的其他参与金融机构。在一个实施例中,支付发送金融机构的后端可以执行该传送。

[0047] 在步骤225中,网络中的每个金融机构可以将交易写入其分布式账本的副本。例如,每个金融机构的后端可以将交易写入其分布式账本的副本。

[0048] 在步骤230中,支付接收金融机构通过交易网络接收交易,并且在步骤235中,可以

将交易的收据写入其分布式账本的副本。

[0049] 在步骤235中，接收金融机构可以将交易写入其分布式账本的副本。在一个实施例中，支付接收金融机构的后端可以将交易写入金融机构的分布式账本的副本。

[0050] 在一个实施例中，交易可以被写为智能合约。由支付发送金融机构和支付接收金融机构写入的账本条目可以是相同的格式，并且可以包含相同的数据元素。由支付发送金融机构和支付接收金融机构写入的账本条目的内容是相对的条目。例如，支付发送金融机构可以将存放同业账户的贷方(CR)条目写入账本网络，并且支付接收金融机构可以将借方条目(DR)写入账本网络。其他数据属性(货币、金额、计息日和交易参考)在两个条目中相同。智能合约可以匹配并核对两个条目。

[0051] 在步骤240中，支付接收金融机构可以将交易传送到网络中的其他参与金融机构。在一个实施例中，支付接收金融机构的后端可以执行该传送。

[0052] 在步骤245中，网络中的每个金融机构可以将交易写入其分布式账本的副本。例如，每个金融机构的后端可以将交易写入其分布式账本的副本。

[0053] 在步骤250中，支付发送金融机构和/或支付接收金融机构可以基于通过交易网络发送/接收的交易和分布式账本来核对他们的账户。例如，金融机构的存放同业代理可以更新存放同业账户，并且金融机构可以更新其用于存放同业账户的镜像账户。

[0054] 在一个实施例中，如果账本与账户之间存在任何差异，则具有差异的(一个或更多个)金融机构可以采取适当的行动来解决差异。

[0055] 尽管已经公开了若干实施例，但应该认识到，这些实施例并非彼此排斥。

[0056] 在下文中，将描述本发明的系统和方法的实施方式的一般方面。

[0057] 例如，本发明的系统或本发明的系统的部分可以是“处理机器”的形式，诸如通用计算机。如本文所使用的，术语“处理机器”应理解为包括使用至少一个存储器的至少一个处理器。至少一个存储器存储指令集。指令可以永久地或临时地存储在处理机器的一个或更多个存储器中。处理器执行存储在一个或更多个存储器中的指令以处理数据。该指令集可以包括执行一个或更多个特定任务(诸如上述那些任务)的各种指令。用于执行特定任务的这种指令集可以被表征为程序、软件程序或简单地表征为软件。

[0058] 在一个实施例中，处理机器可以是专用处理器。

[0059] 如上所述，处理机器执行存储在一个或更多个存储器中的指令以处理数据。例如，该数据处理可以响应于处理机器的一个或更多个用户的命令，响应于先前的处理，响应于另一个处理机器的请求和/或任何其他输入。

[0060] 如上所述，用于实现本发明的处理机器可以是通用计算机。然而，上述处理机器还可以利用各种其他技术中的任何一种，所述各种其他技术包括专用计算机、计算机系统(包括例如微型计算机、小型计算机或大型机)、编程微处理器、微控制器、外围集成电路元件、CSIC(客户专用集成电路)或ASIC(专用集成电路)或其他集成电路、逻辑电路、数字信号处理器、可编程逻辑器件(诸如FPGA、PLD、PLA或PAL)，或者能够实现本发明的过程的步骤的任何其他设备或设备的布置。

[0061] 用于实现本发明的处理机器可以使用合适的操作系统。因此，本发明的实施例可以包括运行以下操作系统的处理机器：iOS操作系统、OS X操作系统、Android操作系统、Microsoft Windows™操作系统、Unix操作系统、Linux操作系统、Xenix操作系统、IBM AIX™

操作系统、Hewlett-Packard UX™操作系统、Novell Netware™操作系统、Sun Microsystems Solaris™操作系统、OS/2™操作系统、BeOS™操作系统、Macintosh操作系统、Apache操作系统、OpenStep™操作系统或其他操作系统或平台。

[0062] 应当理解，为了实践如上所述的本发明的方法，处理机器的处理器和/或存储器不一定物理地位于相同的地理位置。也就是说，处理机器使用的处理器和存储器中的每一个可以位于地理上不同的位置并且被连接以便以任何合适的方式通信。另外，应当理解，处理器和/或存储器中的每一个可以由不同的物理设备组成。因此，处理器不必需是一个位置中的单件设备，并且存储器不必需是另一个位置中的另一个单件设备。也就是说，预期处理器可以是两个不同物理位置中的两件设备。两个不同的设备可以以任何合适的方式连接。另外，存储器可以包括两个或更多个物理位置中的两个或更多个存储器部分。

[0063] 为了进一步解释，如上所述的处理由各种组件和各种存储器执行。然而，应当理解，根据本发明的另一实施例，由如上所述的两个不同组件执行的处理可以由单个组件执行。此外，由如上所述的一个不同组件执行的处理可以由两个不同的组件执行。以类似的方式，根据本发明的另一实施例，由如上所述的两个不同存储器部分执行的存储器存储可以由单个存储器部分执行。此外，如上所述由一个不同的存储器部分执行的存储器存储可以由两个存储器部分执行。

[0064] 此外，可以使用各种技术来提供各种处理器和/或存储器之间的通信，以及允许本发明的处理器和/或存储器与任何其他实体通信；即，例如，以便获得进一步的指令或访问和使用远程存储器存储。例如，用于提供这种通信的这些技术可以包括网络、因特网、内联网、外联网、LAN、以太网、经由蜂窝塔或卫星的无线通信，或者提供通信的任何客户端服务器系统。例如，这些通信技术可以使用任何合适的协议，诸如TCP/IP、UDP或OSI。

[0065] 如上所述，可以在本发明的处理中使用指令集。该指令集可以是程序或软件的形式。例如，软件可以是系统软件或应用软件的形式。例如，软件也可以是单独程序的集合、较大程序内的程序模块、或程序模块的一部分的形式。所使用的软件还可以包括以面向对象编程形式的模块化编程。软件告诉处理机器如何处理正在处理的数据。

[0066] 此外，应当理解，在本发明的实施方式和操作中使用的指令或指令集可以是合适的形式，使得处理机器可以读取指令。例如，形成程序的指令可以是合适的编程语言的形式，其被转换为机器语言或目标代码以允许一个或更多个处理器读取指令。也就是说，使用编译器、汇编器或解释器将特定编程语言形式的编程代码或源代码的编写行转换为机器语言。机器语言是二进制编码的机器指令，其特定于特定类型的处理机器，即，例如，特定于特定类型的计算机。计算机理解机器语言。

[0067] 可以根据本发明的各种实施例使用任何合适的编程语言。说明性地，例如，所使用的编程语言可以包括汇编语言、Ada、APL、Basic、C、C++、COBOL、dBase、Forth、Fortran、Java、Modula-2、Pascal、Prolog、REXX、Visual Basic和/或JavaScript。此外，不一定将单一类型的指令或单一编程语言与本发明的系统和方法的操作结合使用。相反，可以根据需要和/或期望使用任何数量的不同编程语言。

[0068] 此外，在本发明的实践中使用的指令和/或数据可以根据需要使用任何压缩或加密技术或算法。加密模块可以用于加密数据。此外，例如，可以使用合适的解密模块来解密文件或其他数据。

[0069] 如上所述，本发明可以说明性地以处理机器的形式体现，处理机器包括例如包括至少一个存储器的计算机或计算机系统。应当理解，根据需要，使计算机操作系统能够执行上述操作的指令集(即例如，软件)可以被包含在任何各种一个或更多个介质上。此外，由指令集处理的数据也可以被包含在任何各种一个或更多个介质上。也就是说，用于保持本发明中使用的指令集和/或数据的特定介质(即处理机器中的存储器)可以采用例如各种物理形式或传输中的任何一种。说明性地，介质可以是以下形式：纸、纸透明胶片、高密度磁盘、DVD、集成电路、硬盘、软盘、光盘、磁带、RAM、ROM、PROM、EPROM、电线、电缆、光纤、通信信道、卫星传输、存储卡、SIM卡或其他远程传输，以及可以由本发明的处理器读取的任何其他介质或数据源。

[0070] 此外，在实现本发明的处理机器中使用的一个或更多个存储器可以是各种形式中的任何一种，以允许存储器根据需要保存指令、数据或其他信息。因此，存储器可以是用于保存数据的数据库的形式。例如，数据库可以使用任何期望的文件布置，诸如平面文件布置或关系数据库布置。

[0071] 在本发明的系统和方法中，可以利用各种“用户界面”来允许用户与用于实现本发明的一个或更多个处理机器接合。如本文所使用的，用户界面包括由处理机器使用的任何硬件、软件或硬件和软件的组合，其允许用户与处理机器交互。例如，用户界面可以是对话屏幕的形式。用户界面还可以包括鼠标、触摸屏、键盘、小键盘、语音读取器、语音识别器、对话屏幕、菜单框、列表、复选框、切换开关、按钮或允许用户接收与在处理机器处理指令集时的处理机器的操作有关的信息和/或向处理机器提供信息的任何其他设备中的任何一个。因此，用户界面是提供用户和处理机器之间的通信的任何设备。用户通过用户界面提供给处理机器的信息可以是例如命令、数据选择或一些其他输入的形式。

[0072] 如上所述，执行指令集的处理机器利用用户界面，使得处理机器处理用户的数据。用户界面通常由处理机器用于与用户交互以传达信息或从用户接收信息。然而，应当理解，根据本发明的系统和方法的一些实施例，人类用户实际上不必需与本发明的处理机器使用的用户界面交互。相反，还预期本发明的用户界面可以与另一个处理机器而不是人类用户交互，即传达和接收信息。因此，其他处理机器可以被表征为用户。此外，预期在本发明的系统和方法中利用的用户界面可以部分地与另一个处理机器或另一些处理机器交互，同时还部分地与人类用户交互。

[0073] 本领域技术人员将容易理解，本发明易于广泛利用和应用。在不脱离本发明的实质和范围的情况下，除本文描述的那些之外的本发明的许多实施例和改变以及许多变体、修改和等同布置将根据本发明及其前面的描述变得明显，并且将由本发明及其前面的描述合理地建议。

[0074] 因此，尽管这里已经关于其示例性实施例详细描述了本发明，但是应该理解，本公开仅是本发明的说明性和示例性描述，并且用于提供本发明的可行公开。因此，前述公开内容不旨在被解释为限制或不旨在限制本发明或以其他方式排除任何其他这样的实施例、改变、变体、修改或等同布置。

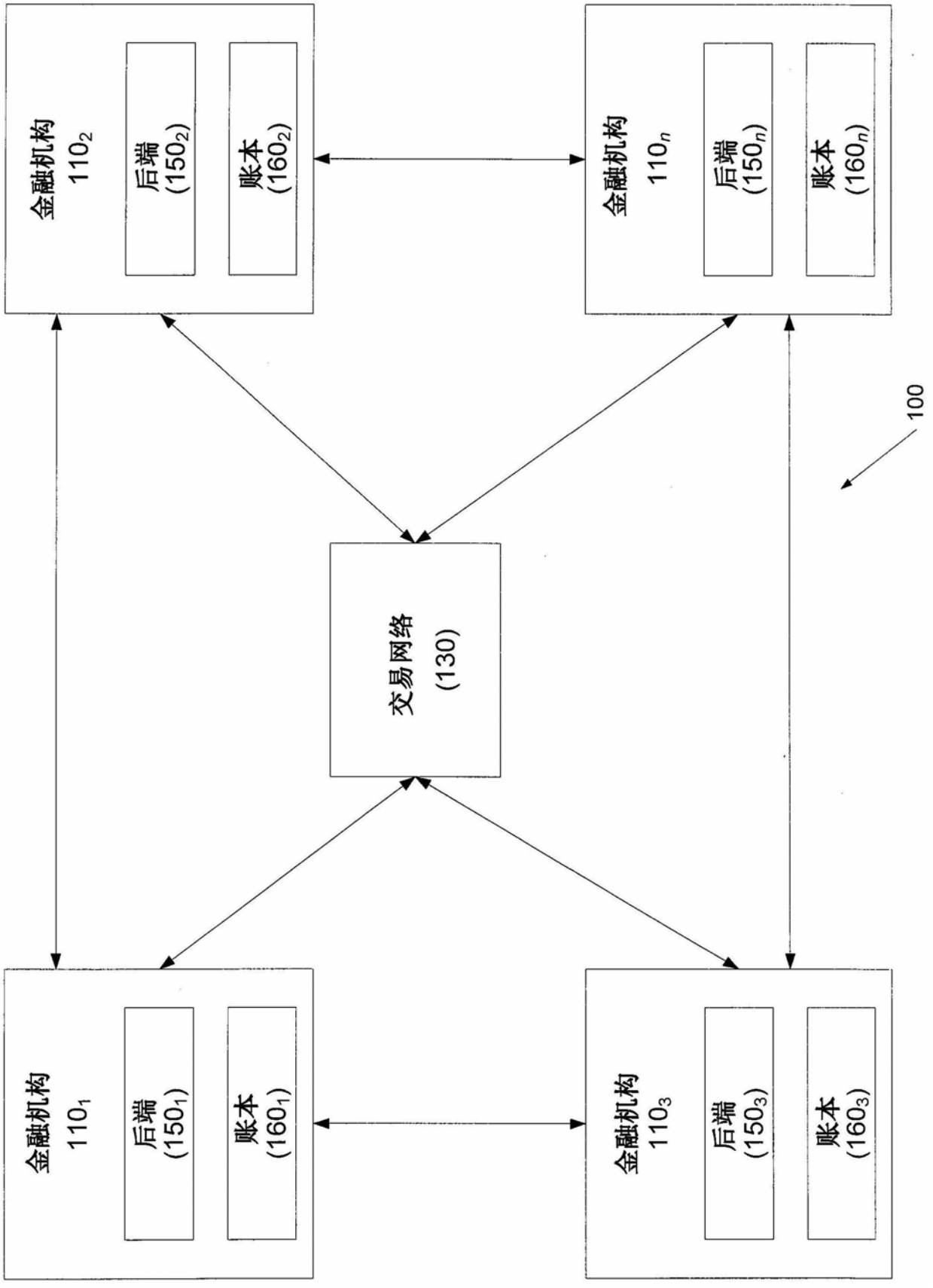

金融机构
110_2
后端
(150_2)
账本
(160_2)
金融机构
110_n
后端
(150_n)
账本
(160_n)
100
交易网络
(130)
金融机构
110_1
后端
(150_1)
账本
(160_1)
金融机构
110_3
后端
(150_3)
账本
(160_3)

图1

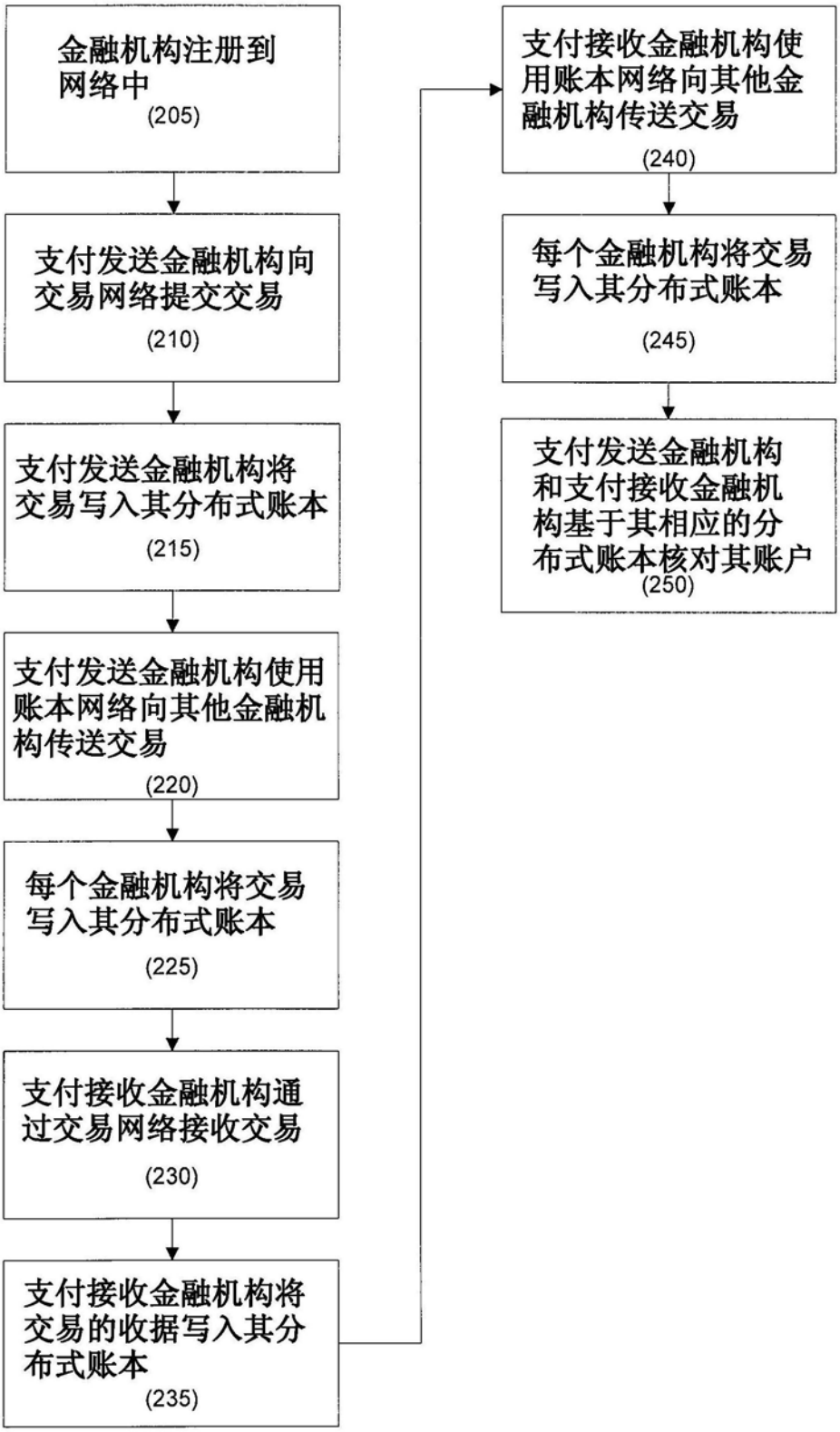

金融机构注册到网络中
(205)
支付发送金融机构向交易网络提交交易
(210)
支付发送金融机构将交易写入其分布式账本
(215)
支付发送金融机构使用账本网络向其他金融机构传送交易
(220)
每个金融机构将交易写入其分布式账本
(225)
支付接收金融机构通过交易网络接收交易
(230)
支付接收金融机构将交易的收据写入其分布式账本
(235)
支付接收金融机构使用账本网络向其他金融机构传送交易
(240)
每个金融机构将交易写入其分布式账本
(245)
支付发送金融机构和支付接收金融机构基于其相应的分布式账本核对其账户
(250)

图2