



(12)发明专利申请

(10)申请公布号 CN 109478282 A

(43)申请公布日 2019.03.15

(21)申请号 201680087704.4

(51)Int.Cl.

(22)申请日 2016.07.15

G06Q 20/30(2006.01)

(85)PCT国际申请进入国家阶段日  
2019.01.14

G06Q 40/02(2006.01)

(86)PCT国际申请的申请数据  
PCT/US2016/042653 2016.07.15

G06Q 20/38(2006.01)

G06Q 20/04(2006.01)

G06Q 20/36(2006.01)

(87)PCT国际申请的公布数据  
W02018/013144 EN 2018.01.18

(71)申请人 维萨国际服务协会  
地址 美国加利福尼亚州

(72)发明人 J·阿伦特 G·普拉卡什  
S·加达姆

(74)专利代理机构 上海专利商标事务所有限公  
司 31100

代理人 陈洁 姬利永

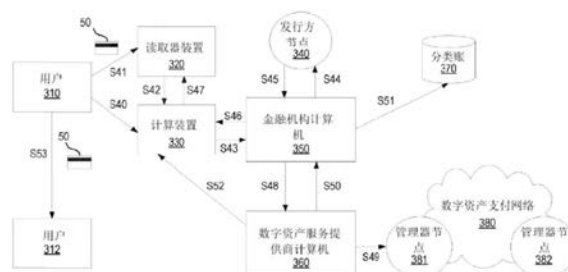
权利要求书2页 说明书16页 附图7页

(54)发明名称

通过交易装置进行数字资产分发

(57)摘要

用户可以将对应于值的数字资产与待由另一用户使用的交易装置关联。例如,第一用户可以将对应于加密货币金额的数字资产加载到交易装置上,然后所述第一用户将所述交易装置提供给第二用户。所述第二用户可以使用所述交易装置上的所述加密货币金额进行交易。可以使用呈区块链形式的存储数据的分类账来管理数字资产的生成和使用。



1. 一种方法,包括:
  - 由服务提供商计算机从第一用户的计算装置接收生成数字资产的请求;
  - 由所述服务提供商计算机生成所述数字资产;
  - 由所述服务提供商计算机相对于待提供给第二用户的交易装置激活所述数字资产;
  - 由所述服务提供商计算机发送更新第一不可改变的电子分类账的请求以指示所述数字资产与所述交易装置的关联;
  - 由所述服务提供商计算机接收所述第二用户使用所述交易装置进行交易的指示;以及
  - 由所述服务提供商计算机发送更新第二不可改变的电子分类账的请求以指示所述第二用户使用所述数字资产。
2. 根据权利要求1所述的方法,还包括:
  - 由所述服务提供商计算机发送更新所述第一不可改变的电子分类账的请求以指示所述第二用户使用所述数字资产。
3. 根据权利要求1所述的方法,还包括:
  - 由所述服务提供商计算机从所述计算装置接收将所述交易装置与交易装置标识符关联的请求;
  - 由所述服务提供商计算机生成所述交易装置标识符;以及
  - 由所述服务提供商计算机将所述交易装置与所述交易装置标识符关联。
4. 根据权利要求3所述的方法,其中与所述计算装置通信的读取器装置为所述交易装置供应所述交易装置标识符。
5. 根据权利要求1所述的方法,其中相对于所述交易装置激活所述数字资产包括:
  - 由所述服务提供商计算机将对应于所述数字资产的数字资产标识符和值与所述交易装置关联。
6. 根据权利要求1所述的方法,其中所述交易装置是卡。
7. 根据权利要求1所述的方法,其中将更新所述第一不可改变的电子分类账的所述请求发送到第一金融机构计算机,其中所述第一金融机构计算机更新所述第一不可改变的电子分类账。
8. 根据权利要求7所述的方法,其中将更新所述第二不可改变的电子分类账的所述请求发送到第二金融机构计算机,其中所述第二金融机构计算机更新所述第二不可改变的电子分类账。
9. 根据权利要求1所述的方法,其中所述第一不可改变的电子分类账和所述第二不可改变的电子分类账各自呈块链的形式。
10. 一种方法,包括:
  - 由计算装置从第一用户接收生成数字资产的请求;
  - 由所述计算装置将所述请求发送到服务提供商计算机,其中所述服务提供商计算机生成所述数字资产;以及
  - 由所述计算装置发起相对于待提供给第二用户的交易装置激活所述数字资产,其中所述服务提供商计算机发送更新第一不可改变的电子分类账的请求以指示所述数字资产与所述交易装置的关联,其中所述第二用户使用所述交易装置进行交易,并且其中所述服务提供商计算机发送更新第二不可改变的电子分类账的请求以指示所述第二用户使用所述

数字资产。

11. 根据权利要求10所述的方法,其中所述服务提供商计算机发送更新所述第一不可改变的电子分类账的请求以指示所述第二用户使用所述数字资产。

12. 根据权利要求10所述的方法,还包括:

由所述计算装置接收将所述交易装置与交易装置标识符关联的请求;以及

由所述计算装置将所述请求发送到所述服务提供商计算机,其中所述服务提供商计算机将所述交易装置与所述交易装置标识符关联。

13. 根据权利要求12所述的方法,其中与所述计算装置通信的读取器装置为所述交易装置供应所述交易装置标识符。

14. 根据权利要求10所述的方法,其中相对于所述交易装置激活所述数字资产包括将对应于所述数字资产的数字资产标识符和值与所述交易装置关联。

15. 根据权利要求10所述的方法,其中所述交易装置是卡。

16. 根据权利要求10所述的方法,其中将更新所述第一不可改变的电子分类账的所述请求发送到第一金融机构计算机,其中所述第一金融机构计算机更新所述第一不可改变的电子分类账。

17. 根据权利要求16所述的方法,其中将更新所述第二不可改变的电子分类账的所述请求发送到第二金融机构计算机,其中所述第二金融机构计算机更新所述第二不可改变的电子分类账。

18. 根据权利要求10所述的方法,其中所述第一不可改变的电子分类账和所述第二不可改变的电子分类账各自呈块链的形式。

19. 一种服务提供商计算机,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括能由所述处理器执行以实现根据权利要求1所述的方法的代码。

20. 一种计算装置,包括:

处理器;以及

耦合到所述处理器的计算机可读介质,所述计算机可读介质包括能由所述处理器执行以实现根据权利要求10所述的方法的代码。

## 通过交易装置进行数字资产分发

[0001] 相关申请交叉引用

[0002] 无。

### 技术领域

### 背景技术

[0003] 用户可能希望与其他用户执行分发过程(例如,用于工资、货物、数据等)。但是,如果这些其他用户与监督分发过程的实体没有任何关系,则很难安全地进行分发过程。例如,其他用户可能没有所述实体托管的注册账户。通常,此类账户可以指示用户可以被信任,因为实体已经为所述用户进行认证过程。因此,将工资、货物或数据分发给没有账户的其他用户的所述用户执行分发过程时没有足够的安全性。

[0004] 本发明的实施例个别地和共同地解决了这些和其他问题。

### 发明内容

[0005] 本发明的一个实施例涉及一种由服务提供商计算机执行的方法。服务提供商计算机可以从第一用户的计算装置接收生成数字资产的请求。然后,服务提供商计算机可以生成数字资产,并且可以相对于将提供给第二用户的交易装置激活数字资产。在一些实施例中,相对于交易装置激活数字资产包括将对应于数字资产的数字资产标识符和值与交易装置关联。在一些情况下,交易装置可以是卡。

[0006] 然后,服务提供商计算机可以发送更新第一不可改变的电子分类账的请求以指示数字资产与交易装置的关联。在一些实施例中,可以将更新第一不可改变的电子分类账的请求发送到第一金融机构计算机,其中所述第一金融机构计算机可以更新第一不可改变的电子分类账。服务提供商计算机可以接收第二用户使用交易装置进行交易的指示,然后可以发送更新第二不可改变的电子分类账的请求以指示第二用户使用数字资产。在一些实施例中,可以将更新第二不可改变的电子分类账的请求发送到第二金融机构计算机,其中所述第二金融机构计算机可以更新第二不可改变的电子分类账。在一些实施例中,服务提供商计算机还可以发送更新第一不可改变的电子分类账的请求以指示第二用户使用数字资产。在一些情况下,第一不可改变的电子分类账和第二不可改变的电子分类账可以呈区块链形式。

[0007] 在一些实施例中,服务提供商计算机可以执行额外步骤,所述额外步骤可以在第二用户使用交易装置之前执行。服务提供商计算机可以从计算装置接收将交易装置与交易装置标识符关联的请求。然后,服务提供商计算机可以生成交易装置标识符,并且可以将交易装置与交易装置标识符关联。在一些实施例中,与计算装置通信的读取器装置可以为交易装置供应交易装置标识符。

[0008] 本发明的另一个实施例涉及一种由计算装置执行的方法。计算装置可以从第一用户接收生成数字资产的请求。然后,计算装置可以将所述请求发送到服务提供商计算机,服

务提供商计算机可以生成数字资产。然后,计算装置可以就待提供给第二用户的交易装置发起数字资产的激活。服务提供商计算机可以发送更新第一不可改变的电子分类账的请求以指示数字资产与交易装置的关联。第二用户可以使用交易装置进行交易,并且服务提供商计算机可以发送更新第二不可改变的电子分类账的请求以指示第二用户使用数字资产。

[0009] 本发明的另一个实施例涉及一种服务提供商计算机。所述服务提供商计算机可以包括处理器和连接到处理器的计算机可读介质。所述计算机可读介质可以包括可由处理器执行以实施本文中描述的方法的代码。

[0010] 本发明的另一个实施例涉及一种计算装置。所述计算装置可以包括处理器和连接到处理器的计算机可读介质。所述计算机可读介质可以包括可由处理器执行以实施本文中描述的方法的代码。

[0011] 本发明的这些和其他实施例更详细地描述如下。

### 附图说明

[0012] 图1示出的框图示出根据本发明实施例的数字资产分发系统。

[0013] 图2示出根据本发明实施例的方法的流程图。

[0014] 图3示出根据本发明实施例的具有由交易装置分配数字资产的流程图的系统。

[0015] 图4示出根据本发明实施例的具有与交易装置相关联的数字资产的使用流程图的系统。

[0016] 图5示出根据本发明实施例的系统的框图。

[0017] 图6示出根据本发明实施例的非财务系统的框图。

[0018] 图7示出根据本发明实施例的呈块链形式的多个条目的框图。

### 具体实施方式

[0019] 在讨论本发明的实施例之前,对一些术语的描述可能有助于提供对本发明的更好理解。

[0020] “数字货币”可以指可用作交易(包括金融交易)的支付形式的值的单位。数字货币可以是由用户计算装置电子生成并存储在用户计算装置中的货币。可以使用常规货币形式(例如,法定货币)来购买数字货币,并以特定值生成数字货币。通常,数字货币可能不具有货币的实物形式,但可以通过用户计算装置(例如,移动装置)使用诸如数字钱包或移动应用程序之类的软件应用程序来访问。数字货币的类型可以是加密货币,其使用加密方法进行验证。

[0021] “数字资产”可以指与值相关联的数字内容。在一些情况下,数字资产还可以指示使用与数字资产相关联的值和其他属性的权利。例如,数字资产可以是指示数字货币值的数据,例如加密货币值。数字资产还可以指示多个数字资产属性,例如银行标识号(BIN)标识符、数字资产标识符、时间戳、收单方公钥、资源提供商标识符和资源提供商位置。在其他实施例中,数字资产可以对应于其他非货币值,例如访问权限数据(例如,授权使用的数量)和时限数据。

[0022] “用户”可以指可以执行交易的实体。在一些实施例中,用户可以是涉及数字资产交易实体。一种类型的用户是分发用户。分发用户可以提供数字资产的生成和分发说明。

分发用户可以通过相对于将由接收方用户使用的交易装置激活数字资产来分配数字资产。接收方用户是可使用与分发用户分发的数字资产相关联的交易装置进行交易的用户。接收方用户可使用与数字资产相关联的交易装置使用数字资产。在一些示例性情况中,分发用户和接收方用户可以分别是雇主和员工、父母和子女,或经理和团队成员。

[0023] “加密货币支付网络”可以指用于操作和维护加密货币系统的一个或多个服务器计算机。加密货币支付网络可以用于促进加密货币支付网络内的装置之间的数字货币的生成/发放和分发。加密货币支付网络还可以用于实现装置之间的交易执行以进行货物/服务的转移和/或资金的转移。加密货币支付网络可以操作管理交易分类账的节点。在一些实施例中,加密货币支付网络也可以被称为数字资产支付网络。

[0024] “交易分类账”可以指来自先前交易的数据汇编。交易分类账可以是数据库或其他相当的文件结构,其可以被配置成存储来自使用数字货币执行的所有先前交易的数据,包括交易的日期和时间、交易金额,以及交易的参与者的识别信息(例如,交易金额的发送方和接收方)。在一些实施例中,交易分类账可以是电子分类账(例如块链)的形式,其中已经存储在电子分类账中的数据是不可改变的。在一些实施例中,加密货币支付网络内的每个节点可以存储他们自己的交易分类账的副本。在其他实施例中,只有一些节点可以存储他们自己的交易分类账的副本。

[0025] “发放方节点”可以是能够管理数字资产的创建和发放的装置或模块。在一些实施例中,发放方节点可以由对应于资源提供商的金融机构计算机操作,所述金融机构计算机可以使用发放方节点来生成数字资产。

[0026] “管理器节点”可以是能够管理分配给消费者并由消费者使用的数字资产的装置或模块。用户使用的数字资产可能是相对于交易装置激活的数字资产。在一些实施例中,管理器节点可以由金融机构计算机操作,所述金融机构计算机可以向管理器节点提交数据以更新加密货币支付网络中的交易分类账。

[0027] “数字签名”可以指对于消息的电子签名。在一些实施例中,数字签名可以用于验证在加密货币支付网络内发送的交易消息的真实性。数字签名可以是使用加密算法从消息和私钥生成的唯一值。在一些实施例中,可以使用采用公钥的确认算法来确认签名。数字签名可以是数字值、字母数字值或包括图形表示的任何其他类型的数据。

[0028] “密钥”可以指用于算法的一条数据或信息。密钥可以是唯一的数据,并且通常是密钥对的一部分,其中第一密钥可以用于加密消息,而第二密钥可以用于解密加密的消息。密钥可以是数字或字母数字值,并且可以使用算法来生成。加密货币支付网络中的管理系统服务器计算机可以为加密货币支付网络中的每个节点生成并分配唯一密钥对。

[0029] 密钥对可以包括公钥和私钥。密钥对可以由节点和/或支付实体用于在加密货币支付网络中进行交易。密钥对可以由与加密货币支付网络相关联的服务器计算机生成,或者可以在创建具有金融机构服务器计算机的账户时由用于支付实体的金融机构服务器计算机生成。公钥可以分布在整个加密货币支付网络中,以便允许对使用相应私钥签名的支付交易消息进行认证。

[0030] “金融机构服务器计算机”可以指与金融机构(例如,银行)相关联的计算机。金融机构服务器计算机的示例可以包括访问装置、终端或托管金融机构服务器互联网网站的Web服务器计算机。

[0031] “资源提供实体”可以是可以使资源对用户可用的实体。资源提供实体也可以称作资源提供商。资源提供实体的示例包括分发方、商家、供应商、供货商、所有者、贸易商等。在一些实施例中，这样的实体可以是单个人、个人的小组或者更大的个人团体（例如公司）。资源提供实体可以与一个或多个物理位置（例如，超市、商场、商店等）和在线平台（例如，电子商务网站、在线公司等）相关联。在物理位置处，资源提供实体可作为访问装置的主机。在一些实施例中，资源提供实体可以向用户提供实物商品（例如，货物、产品、器具等）。在其他实施例中，资源提供实体可以使用户能够使用数字资源（例如，电子文档、电子文件等）或时间（例如，租赁时间、使用时间等）。在其他实施例中，资源提供实体可以管理用户对某些资源的访问。

[0032] “服务器计算机”可以包括功能强大的计算机或计算机集群。例如，服务器计算机可以是大型主机、小型计算机集群或像单元一样工作的一组服务器。在一个示例中，服务器计算机可以是耦合到Web服务器的数据库服务器。服务器计算机可以耦合到数据库并且可以包括用于服务于来自一个或多个客户端计算机的请求的任何硬件、软件、其他逻辑、或前述内容的组合。服务器计算机可以包括一个或多个计算设备并且可以使用各种计算结构、布置和编译中的任何计算结构、布置和编译来服务于来自一个或多个客户端计算机的请求。

[0033] “计算装置”可以指与用户相关联的电子装置。在一些实施例中，计算装置可以用于与另一装置、计算机或系统通信。计算装置可以用于进行交易，并且能够通过网络进行通信。用户装置可以是任何适当形式。例如，适当的用户装置可以是手持式且紧凑的，使得它们能够放到用户的钱包和/或口袋中（例如，口袋大小的）。用户装置可以包括处理器、操作性耦合到处理器的存储器、输入装置和输出装置。便携式装置的具体示例包括蜂窝电话或无线电话、平板计算机、台式计算机、个人数字助理（PDA）、寻呼机、便携式计算机、智能卡等。额外计算装置可以包括可穿戴装置，诸如智能手表、健身手环、脚链、戒指、耳环等。在一些实施例中，移动装置可以包括具有远程通信能力的汽车。

[0034] 本发明的实施例涉及由交易装置分配数字资产。例如，第一用户可以基于将数字资产关联到要提供给多个接收方用户的适当交易装置将对应于值的数字资产分发给多个接收方用户。例如，通过将数字资产相关的信息（例如，数字资产属性）（例如，值和数字资产标识符）加载到交易装置上，可以将数字资产与交易装置相关联。在另一示例中，通过在服务器计算机处存储对应于与关于数字资产的信息相关联的交易装置的交易装置标识符，可以将数字资产与交易装置相关联。接收方用户然后可以使用与其交易装置相关联的数字资产进行交易。在一些实施例中，可以使用交易分类账来管理数字资产的分发和使用。在一些情况下，分类账可以是不可改变的电子分类账，所述不可改变的电子分类账可以是块链形式。

[0035] 在一些情况下，第一用户可以将与加密货币值相关联的数字资产分发给第二用户。在示例性情况中，第一用户可以是雇主，第二用户可以是员工，其中第一用户可以将工资分发给第二用户进行补偿。第一用户可以将指令输入到其计算装置中，以将对应于加密货币金额的数字资产与要提供给第二用户的交易装置相关联。然后，第二用户可以使用交易装置上的加密货币金额进行交易。在一些实施例中，数字资产的生成和使用可以使用以块链形式存储数据的分类账来进行管理。

[0036] 本发明的实施例提供了优点。例如,本发明的实施例摒弃了消费者和资源提供商管理交易现金的需要,而管理交易现金会很繁琐。因此,本发明的实施例使与金融机构(例如,银行)没有关系的消费者能接收数字货币,以及以安全方式执行无现金交易。本发明的实施例还使用户能够方便地将数字资产分发给多个接收方用户,以及容易地管理与分布式数字资产相关的信息(例如,接收方实体、时间分布、值分布等),而不需要实物现金。使用加密技术来管理交易的电子分类账还能实现将数字资产与交易装置相关联的安全系统,因为记录在分类账中的数据可以被配置成不可改变的。例如,电子分类账中存储的数据的任何更改都不会检测不到,因为电子分类账中的每个条目都是基于电子分类账中的先前条目生成的。这可以使恶意方很难不当地重复使用数字资产。由于多个实体可能存储不可改变的电子分类账,这可以实现额外的安全层,因为可以请求多个实体在使用之前验证数字资产的分发或过去使用。

[0037] 图1示出的框图示出根据本发明实施例的数字资产分发系统。图1包括数字资产服务系统110、授权服务系统120、清算和结算服务系统130、分发方数字资产管理系统140、接收方数字资产管理系统150、发行方节点142以及管理器节点152。这些服务系统中的每一个可以在单个计算机或多个系统和计算机上运行,所述系统和计算机可以使用任何合适的通信协议经由任何合适的通信介质(包括互联网)彼此可操作地进行通信。

[0038] 为了简化说明,图1中示出特定数目的部件。然而,应理解,本发明的实施例可以包括多于一个每种部件。另外,本发明的一些实施例可以包括少于或多于图1中所示的所有部件。相对本文描述的其他图描述与图1所示的部件相关的进一步详细信息。

[0039] 数字资产服务系统110使数字资产能够用于交易。数字资产服务系统110可以包括数字资产账户管理服务系统,其能够实现对应于由数字资产服务系统110托管的数字资产账户的数字资产管理。数字资产服务系统110还可以包括使资源提供商和用户由数字资产服务系统110提供的服务的系统。在一些情况下,这些服务可能包括提供可使资源提供商和用户查看、更新和管理与其分发或收到的数字资产相关联的信息的应用程序。

[0040] 在一些情况下,用户(例如,分发用户)可以使用数字资产服务系统110将对应于某些值的数字资产分发给其他用户(例如,接收方用户)。因此,数字资产分发系统可以进一步包括分发方数字资产管理系统140和接收方数字资产管理系统150。

[0041] 分发方数字资产管理系统140允许分发用户将对应于某些值的数字资产分发给接收方用户。对于每个接收方用户,分发方数字资产管理系统140可以允许针对由接收方用户使用的交易装置激活数字资产。分发方数字资产管理系统140还可以基于与生成和分布的数字资产相关的记录信息(例如,生成的时间、接收方用户和分发方用户识别信息、值、数字资产标识符等)来实现对分布式数字资产的管理。在一些实施例中,分发方数字资产管理系统140可以使用发行方节点142记录信息。

[0042] 接收方数字资产管理系统150允许接收方用户使用分发用户分发的数字资产。接收方数字资产管理系统150可以管理与接收方用户使用的交易装置相关联的数字资产。接收方数字资产管理系统150可以基于与接收方用户使用的数字资产相关的记录信息(例如,使用时间、使用的值等)来实现对数字资产的管理。在一些实施例中,接收方数字资产管理系统150可以使用管理器节点152记录信息。

[0043] 发行方节点142管理与数字资产的创建和分发有关的信息。发行方节点142可以在



接收到请求时生成与特定值相对应的数字资产,并记录与创建数字资产并将数字资产发出到由接收方用户使用的交易装置有关的信息。发行方节点142可以通过记录交易分类账中的相关数据来管理信息。在一些实施例中,交易分类账可以呈块链的形式,其中块链中的每个新块引用先前的块(例如,先前块的散列),使得对存储在这些先前块中的数据的任何篡改都不会检测不到。

[0044] 管理器节点152管理与接收方用户关联的数字资产有关的信息。例如,接收方用户可以使用其交易装置进行交易,其中交易装置与对应于特定值的数字资产关联。管理器节点152然后可以记录指示使用与交易装置相关联的数字资产的信息(例如,交易时间、使用的值、参与实体等)。管理器节点152可以记录交易分类账中的信息。在一些实施例中,交易分类账可以呈块链的形式,其中块链中的每个新块引用先前的块(例如,先前块的散列),使得对存储在这些先前块中的数据的任何篡改都不会检测不到。

[0045] 在一个示例性情况中,可使用数字资产分发系统来启用薪资册系统。分发用户可以是雇主,接收方用户可以是员工。雇主可以激活与关于要提供给雇员以进行补偿的交易装置的加密货币金额相对应的数字资产。尽管薪资册系统展示了数字资产分发系统的一种用途,但实施例不限于此。例如,数字资产可以对应于除了可从分发用户向接收方用户提供的加密货币值之外的其他合适值。示例性非货币值包括时间限制数据和访问权限数据(参考图6)。

[0046] 图2示出根据本发明实施例的方法的流程图。所述方法可以由分发用户执行。在相对于图2描绘的示例性情况中,分发用户可以请求生成并分发对应于加密货币值的数字资产。

[0047] 在步骤201,分发用户使用其计算装置设置数字资产账户。分发用户可以通过在其计算装置上安装数字资产应用程序来设置其数字资产账户。被描述为由数字资产应用程序执行的任何动作均可由与数字资产应用程序相关联的服务提供商计算机执行。分发用户可以注册信息,如名称、地址和密码,以便与其数字资产账户关联。在一些实施例中,分发用户还可以注册与其银行账户相关的信息(例如,账户标识符),可以从中借记对应于与分发用户分发的数字资产相关联的加密货币值的金额。数字资产应用程序使分发用户能够轻松管理其生成和分发的数字资产。

[0048] 在步骤202,分发用户获取交易装置。在一些情况下,分发用户可以请求第三方提供交易装置。在一些实施例中,交易装置可以是卡,最初为空白的,且可能没有与其相关联的任何信息。应理解,在其他实施例中,交易装置可以是可用于如本文所述的交易的另一合适的装置。

[0049] 在步骤203,分发用户将生成数字资产的请求输入到其计算装置中。分发用户可以将所述请求连同与数字资产相关的信息一起输入到数字资产应用程序提供的界面中。例如,分发用户可以指定对应于数字资产的加密货币值。然后,数字资产应用程序可以根据分发用户输入的信息生成数字资产。在一些实施例中,数字资产应用程序可以接触与分发用户的银行账户相关联的金融机构计算机,以确保其具有与加密货币值相关的足够资金。生成数字资产之后,数字资产应用程序可以向分发用户指示已成功生成所请求的数字资产。

[0050] 在步骤204,分发用户输入相对于交易装置激活数字资产的请求。分发用户可以将所述请求输入到数字资产应用程序提供的界面中。在一些实施例中,激活过程可以使用与

运行数字资产应用程序的计算装置通信的读取器装置进行。例如,读取器装置可以允许将信息写入交易装置。在一些情况下,如果交易装置是卡且读取器装置启用了刷卡功能,分发用户可以使用读取器装置刷交易装置。刷交易装置后,可以供应与数字资产相关的信息。信息可以指示数字资产标识符(例如,字母数字字符串)和与数字资产相对应的加密货币值。在其他实施例中,读取器装置可以实现使用可用于激活过程的其他接触的非接触信息传送方法。

[0051] 在这种情况下,由于交易装置首次被数字资产激活,因此激活过程还可以包括交易装置标识符与交易装置的关联。在一些实施例中,交易装置标识符可以被格式化为卡号(例如,包括到期日期和卡验证值),并可由管理与交易装置相关联的资金的金融机构计算机生成。如上所述刷交易装置之后,除了与数字资产相关的信息外,还可以供应交易装置标识符。因此,可以通过交易装置标识符使数字资产与交易装置关联。

[0052] 应理解,在其他实施例中,不需要读取器装置就交易装置激活数字资产。例如,在交易装置与交易装置标识符关联之后,分发用户只需将请求与交易装置标识符输入到数字资产应用程序中以将数字资产与交易装置关联。随后,与数字资产应用程序关联的后端服务提供商计算机可以存储指示数字资产与交易装置标识符关联的信息。因此,交易装置不必直接编程以存储与数字资产相关的信息。

[0053] 在步骤205,分发用户可以向接收方用户提供交易装置。例如,分发用户可以直接将交易装置交付或邮寄到接收方用户。接收方用户可以接收交易装置,并使用交易装置进行达到与数字资产相关联的加密货币值的交易。用于交易的值可以从在步骤201注册期间由分发用户指示的银行账户借记。

[0054] 分发用户可以为任何合适数量的接收方用户重复步骤202至205。例如,如果分发用户是将与加密货币值相对应的数字资产分发给员工以进行补偿的雇主,分发用户可以针对要提供给雇员的每个交易装置激活数字资产。关于数字资产的生成、分发和使用的进一步详细信息参考至少图3。

[0055] 虽然参考图2描述了分发用户获得交易装置并向接收方用户提供交易装置的实施例,但实施例不限于此。在其他实施例中,分发用户可以请求关于由接收方用户拥有的交易装置激活数字资产。例如,交易装置可以是由接收方用户操作的移动电话。在这种情况下,交易装置标识符可以是可与移动电话相关联的任何合适的标识符。例如,交易装置标识符可以是移动装置标识符、电子邮件地址、电话号码或其他合适的标识符。分发用户可以(例如,从接收方用户)获取交易装置标识符,然后可以将交易装置标识符输入到其计算装置上的数字资产应用程序中,以注册和识别要激活数字资产的交易装置。为了相对于交易装置标识符激活数字资产,管理数字资产的后端服务提供商计算机然后可以存储或请求其他实体存储指示数字资产与交易装置标识符相关联的信息。

[0056] 图3示出根据本发明实施例的具有由交易装置分配数字资产的流程图的系统。图3包括将交易装置50分发给用户312的用户310、由用户310操作的计算装置330,以及与计算装置330通信的读取器装置320。图3还包括可由金融机构计算机350操作的发行方节点340和分类账370、数字资产服务提供商计算机360,以及驻留在数字资产支付网络380上的管理器节点381和管理器节点382。金融机构计算机350可以与托管用户310的银行账户的金融机构相关联。

[0057] 在相对于图2描述的示例性情况中,用户310是分发用户且用户312是接收方用户。用户310可以操作计算装置330,其运行数字资产应用程序,用户310可以通过所述应用程序输入生成和激活数字资产的请求。可以在数字资产应用程序初始设置期间对应于用户310生成密钥对。用户310可以获得交易装置50,所述交易装置可与相对于图2所述的交易装置标识符相关联。在示例性情况中,交易装置50可以是卡。当最初使用数字资产应用程序向交易装置50供应交易装置标识符时,可以生成与交易装置50相关联的密钥对。

[0058] 在步骤S40,用户310在计算装置330中输入生成数字资产的请求。用户310可以将请求输入到由计算装置330上运行的数字资产应用程序提供的界面中。用户310可以提供与请求有关的附加信息,例如与数字资产关联的加密货币值。

[0059] 在步骤S41,用户310请求关于交易装置50激活数字资产。在一些实施例中,用户310无需明确在计算装置330中输入激活相对于交易装置50的数字资产的指示。例如,用户310可以简单地启用在读取器装置320与交易装置50之间传送信息,以便请求关于交易装置激活数字资产。在一些情况下,用户310可以通过使用读取器装置320刷交易装置50(其可以读取与交易装置50相关联的交易装置标识符)来启用在读取器装置320与交易装置50之间传送信息。在其他实施例中,除了启用在读取器装置320与交易装置50之间传送信息之外,用户310还可以将请求输入到数字资产应用程序提供的界面中。

[0060] 在步骤S42,读取器装置320可以与计算装置330通信。读取器装置320可以通过有线连接或无线连接在通信网络上与计算装置330通信。读取器装置320可以将交易装置标识符发送到计算装置330。计算装置330上的数字资产应用程序可以被配置成使得它在从读取器装置320接收交易装置标识符时发起针对交易装置50的数字资产激活过程。

[0061] 在步骤S43,计算装置330向金融机构计算机350发送生成数字资产的请求。所述请求可以与指示由用户310输入的加密货币值的信息和与交易装置50相关联的交易装置标识符一起发送。在一些情况下,可以与可用于生成数字资产的附加信息一起发送请求,例如与用户310相关联的识别信息(例如,与用户310相关联的公钥)。

[0062] 在步骤S44,金融机构计算机350向发行方节点340发送请求,所述发行方节点340基于请求生成数字资产。在一些实施例中,金融机构计算机350可以在发送生成数字资产的请求之前检查用户310的银行账户是否具有相对于加密货币值的足够资金。如果有足够的资金可用,发行方节点340可以基于与请求一起发送的信息来生成数字资产。发行方节点340可以将数字资产与和交易装置50关联的交易装置标识符关联。

[0063] 数字资产可能是数据,包括与数字资产相对应的数字资产属性。例如,数字资产属性可以包括值和数字资产标识符。所述值可以是用户310输入的加密货币值,并且数字资产标识符可以由发行方节点340生成的唯一地识别数字资产的标识符。例如,数字资产标识符可以是字母数字字符串。在一些实施例中,数字资产可以进一步包括BIN标识符、时间戳,以及与分发用户相关联的识别信息(例如,用户310的公钥)。

[0064] 在步骤S45,发行方节点340向金融机构计算机350发送数字资产。然后,金融机构计算机350可以按任何合适的顺序或并行地在步骤S46将与数字资产相关的信息发送到计算装置330以及在步骤S48发送到数字资产服务提供商计算机360。

[0065] 在步骤S46和S47,与生成的数字资产相关的信息可通过计算装置330发送到读取器装置320,所述计算装置可以将信息供应到交易装置50。在一些情况下,信息可以包括与

数字资产相对应的某些数字资产属性,例如值、数字资产标识符以及与用户310相关联的识别信息。在一些情况下,在步骤S41中进行的同一刷卡期间,可以将信息编程到交易装置50。在其他情况下,计算装置上的数字资产应用程序可以被配置成使得要求用户310使用读取器装置320再次刷交易装置50,以便将信息供应到交易装置50。

[0066] 在步骤S48,金融机构计算机350将与数字资产相关的信息转发到数字资产服务提供商计算机360。在一些实施例中,数字资产服务提供商计算机360可以存储数据库中与对应于交易装置50的交易装置标识符相关联的数字资产有关的信息(未示出)。

[0067] 在步骤S49,数字资产服务提供商计算机360与管理器节点381通信。数字资产服务提供商计算机360可以寻找与交易装置50关联的数字资产账户。如果这是数字资产账户关于交易装置50被激活的第一次,则数字资产账户可能不存在。数字资产服务提供商计算机360随后可以生成与交易装置50相关联的数字资产账户,并将数字资产账户和与交易装置50相关联的公共地址(例如,公钥)绑定。这允许将未来发行给交易装置50的任何数字资产与关联于交易装置50的数字资产账户关联。

[0068] 数字资产服务提供商计算机360可以向管理器节点381发送相关信息,所述信息指示关于交易装置50的数字资产的激活。在这种情况下,信息可以指示至少请求生成数字资产的实体(用户310)和其公共地址(公钥)、激活数字资产的交易装置(交易装置50)和其对应的公共地址(公钥)、数字资产标识符以及与数字资产相对应的值(加密货币值)。在一些实施例中,交易装置50可以由其对应的交易装置标识符指示。

[0069] 数字资产服务提供商计算机360可以包括具有发送到管理器节点381的信息的数字签名。可以使用与用户310相关联的私钥来生成数字签名。基于数字签名,这可以允许可以访问信息的其他实体(例如,节点)验证用户310请求激活关于交易装置50的数字资产。例如,其他实体可以使用与用户310相关联的相应公钥来验证数字签名,并因此验证信息是否有效。此验证可确保将数字资产发行到交易装置50。

[0070] 在步骤S50,数字资产服务提供商计算机360请求金融机构计算机350向与交易装置50关联的数字资产账户发出数字资产。根据请求,金融机构计算机350可以发起更新分类账370以包括管理器节点381接收的信息的过程。

[0071] 在步骤S51,金融机构计算机350发送指令以更新分类账370。分类账370可以呈区块链形式,所述块链可以经过更新以包括新条目,包括由管理器节点381接收的指示数字资产转移的信息。另外,新条目还可以包括数据头,所述数据头包括使得新条目在未经检测的情况下不可改变的信息。例如,数据头可以包括分类账370中前一条目的散列和所有过往交易的根值。由于可以通过包括存储引用其先前条目和先前交易的信息的数据头以类似方式生成分类账370中的每个条目,因此不会在不影响所有后续条目的情况下修改条目。这确保了不能未被察觉地对与交易有关的信息进行任何篡改,例如试图将数字资产重新分配给不适当的实体。图7中示出呈上述块链形式的示例性的条目数。

[0072] 在步骤S52,数字资产服务提供商计算机360将更新的信息推送到在计算装置330上运行的数字资产应用程序。更新的信息可以包括分配给用户310的数字资产账户的更新总值。用户310可以通过数字钱包的界面查看总值。在这种情况下,更新的总值可以显示与相对交易装置50激活的数字资产的加密货币值相对应的减少。

[0073] 在关于交易装置50和分类账370激活数字资产之后,可以执行结算过程(未示出)。

结算过程可以在与用户310相关联的金融机构计算机350与持有对应于与交易装置50相关联的数字资产的资金的金融机构计算机之间执行。下文参考图4更详细地描述这一点。

[0074] 在步骤S53,用户310可以向用户312提供交易装置50。在一些实施例中,用户310可以直接向用户312递送交易装置50。在其他实施例中,用户310可以使用其他方法向用户312提供交易装置50,诸如邮寄交易装置50。在获得交易装置50之后,用户312可以使用交易装置50来使用数字资产进行交易,将关于图4更详细地描述。

[0075] 应理解,在一些情况下,分发用户(例如,用户310)可以相对于多个交易装置激活数字资产,其中每个交易装置可以提供给不同的接收方用户。分发用户可以执行与图3相关的每个交易装置所述的类似过程。

[0076] 在一些实施例中,分发用户可以相对于单个交易装置激活多个数字资产。多个数字资产可在不同时间激活。在一些情况下,分发用户可以在某些时间间隔后相对于交易装置激活新的数字资产。例如,分发用户可以是雇主,所述雇主以与接收方用户的工资周期相对应的常规时间间隔激活新的数字资产。在这种情况下,接收方用户可以使用其交易装置在工资周期之间进行交易。在新工资周期开始时,接收方用户可以向分发用户提供其交易装置,以请求激活新的数字资产。分发用户可以执行与图3相关的相对于交易装置激活新数字资产所述的类似过程。在一些实施例中,接收方用户不必向分发用户提供交易装置,因为分发用户在激活新数字资产时只需向数字资产服务提供商计算机指示与交易装置关联的交易装置标识符。

[0077] 在一些情况下,以前相对于交易装置激活的数字资产可能仍有值,因此接收方用户能够使用与之前激活的数字资产相对应的剩余值,以及与新数字资产相对应的值。因此,交易装置可以存储与多个数字资产相关的信息。

[0078] 图4示出根据本发明实施例的具有与交易装置相关联的数字资产的使用流程图的系统。图4包括图3的一些部件。图4还包括资源提供商计算机410、金融机构计算机420和分类账430。资源提供商计算机410可以关联到与用户312进行交易的资源提供商。资源提供商计算机410可以与数字资产账户一起设置,以便能够支持使用数字资产支付。如上文关于图3所述,金融机构计算机350可以与托管分发用户(图3的用户310)的银行账户的金融机构关联。

[0079] 金融机构计算机420可以与可保存对应于与交易装置50关联的加密货币值的资金的任何合适金融机构关联。在一些情况下,与金融机构计算机420相关联的金融机构可能与与数字资产服务提供商计算机360关联的支付处理器有关系。例如,金融机构可与允许金融机构计算机420保存对应于与交易装置50关联的加密货币值的资金的金融机构有关系。在其他实施例中,金融机构计算机420可以和与金融机构计算机350关联的相同金融机构关联。

[0080] 在步骤S61,用户312可以使用交易装置50与资源提供商计算机410进行交易。用户312可以在资源提供商计算机410的销售点终端处使用交易装置50。例如,用户312可以在访问装置(未示出)上刷交易装置50,所述访问装置可以将交易装置50读取的信息发送到资源提供商计算机410。如关于图3所述,所述信息可以包括与相对于交易装置50激活的数字资产相对应的某些数字资产属性,所述数字资产属性例如与分发用户(图3的用户310)相关联的值、数字资产标识符和识别信息。另外,所述信息可以包括与交易装置50关联的交易装

置标识符。

[0081] 在步骤S62和S63,资源提供商计算机410将从交易装置50读取的信息(见S61)发送到数字资产服务提供商计算机360,所述数字资产服务提供商计算机然后请求对应于交易装置50的数字资产账户的余额验证。数字资产服务提供商计算机360可以确定与用户310关联的接收到的识别信息关联的管理器节点,其在本例中是管理器节点381。数字资产服务提供商计算机360随后可请求管理器节点381验证已相对于交易装置50激活数字资产。

[0082] 管理器节点381可以通过确认数字资产发布到与交易装置50相对应的数字资产账户绑定的公共地址来验证已相对于交易装置50激活数字资产。在确认后,管理器节点381可以通知数字资产服务提供商计算机360此数字资产确实与交易装置50关联。这允许数字资产服务提供商计算机360同时验证与交易装置50相关联的余额,并确保余额至少等于当前交易的交易金额。

[0083] 在步骤S64,数字资产服务提供商计算机360请求金融机构计算机350发起记录与当前交易相关的数据的流程。具体地,数字资产服务提供商计算机360可以请求金融机构计算机350来构建、签名并提交与当前交易有关的交易数据。在一些实施例中,交易数据可以指示至少分发数字资产的实体(图3的用户310)和其公共地址(公钥)、激活数字资产的交易装置(交易装置50)和其公共地址(公钥),以及与数字资产相对应的数字资产标识符。交易装置50可以由其对应的交易装置标识符指示。

[0084] 另外,交易数据还可以指示用于交易的数字资产的值。例如,如果交易金额使用与数字资产相关联的完整加密货币值,交易数据可以指示数字资产的完整值现已分配给资源提供商计算机410而不是交易装置50。在另一个示例中,如果与数字资产关联的完整加密货币值未用于交易,可拆分数字资产的值。在这种情况下,交易数据可以指示分配给资源提供商计算机410的数字资产账户的数值以及由于交易的结果与交易装置50保持关联的数值。

[0085] 金融机构计算机350可以获取私钥,用于数字签署交易数据。私钥可以与用于支付交易的数字资产相关联。当数字资产首次由发行方节点340(参考图3)生成并由金融机构计算机350存储时,可以与对应的公钥一起生成私钥。

[0086] 在步骤S65和S66,金融机构计算机350向管理器节点381提交已签名的交易数据,然后所述管理器节点触发驻留于数字资产支付网络380上的其他管理器节点,以联系保持分类账的实体使用新交易数据更新其分类账。通过将更新传达到驻留于数字资产支付网络380上的其他节点,这确保维护分类账的任何实体均可验证交易的真实性。例如,提交的交易数据包含的数字签名可以通过使用已公开可用的相应公钥进行验证。

[0087] 在步骤S67和S68,管理器节点381将更新其分类账的指令发送到金融机构计算机350,然后所述金融机构计算机使用新交易数据更新分类账370。分类账370可以是区块链的形式,并且新交易数据可以存储在新条目中。新条目还可以包括数据头,所述数据头包括使得新条目在未经检测的情况下不可改变的信息。例如,数据头可以包括分类账370中的前一条目的散列和基于所有过往交易数据计算的根值。由于可以通过包括存储引用其先前条目和先前交易的信息的数据头以类似方式生成分类账370中的每个条目,因此不会在不影响所有后续条目的情况下修改条目。这确保了不能未被察觉地对与交易有关的信息进行任何篡改,例如试图将数字资产重新分配给不适当的实体。图7中示出呈上述区块链形式的示例性的条目数。

[0088] 在步骤S69和S70,管理器节点382将更新其分类账的指令发送到金融机构计算机420,然后所述金融机构计算机使用新交易数据更新分类账430。类似于分类账370,分类账430也可以是区块链的形式,并且新交易数据可以存储在新条目中。新条目还可以包括数据头,所述数据头包括使得新条目在未经检测的情况下不可改变的信息。例如,数据头可以包括分类账430中的前一条目的散列和基于所有过往交易计算的根值。由于可以通过包括存储引用其先前条目和先前交易的信息的数据头以类似方式生成分类账430中的每个条目,因此不会在不影响所有后续条目的情况下修改条目。这确保了不能未被察觉地对与交易有关的信息进行任何篡改,例如试图将数字资产重新分配给不适当的实体。图7中示出呈上述区块链形式的示例性的条目数。

[0089] 当天结束时,可以执行结算过程。具体地,结算过程可使得交易金额从由金融机构计算机420托管的与交易装置50关联的ACH(自动清算所)账户移至与用户312进行交易的资源提供商计算机410关联的ACH账户。

[0090] 尽管在上文详细描述了单个数字资产用于交易的实施例,但实施例不限于此。在一些实施例中,交易装置可以存储与相对于交易装置激活的多个数字资产有关的信息。在这种情况下,访问装置可以读取由交易装置存储的与其所有相应数字资产相关的信息,并将所述信息发送到数字资产服务提供商计算机。然后,数字资产服务提供商计算机可以确定可用于支付交易的适当数字资产集。如果使用多个数字资产进行交易,则数字资产服务提供商计算机可以在交易数据中指示发送给金融机构计算机管理分类账的信息,所述信息识别所使用的每个数字资产的信息(例如,数字资产标识符)和针对每个数字资产的交易的值。

[0091] 本发明的实施例有利地实现了用于分发工资的方便的系统和方法。分发用户无需管理和分发现金,因为其可以在方便时间轻松将数字资产加载到交易装置。此外,分发用户可以使用其数字资产应用程序跟踪其先前分发的数字资产,这在激活(尤其是在不同时间)关于多个接收用户的交易装置的数字资产时是有用的。使用与数字资产相关联的交易装置支付交易对于接收方用户来说也是方便的过程。接收方用户不必创建任何账户以在无现金交易中使用与交易装置相关联的数字资产。另外,交易装置与典型的交易处理系统兼容,因此接收方用户不需要进一步设置流程。如果接收方用户确实想要跟踪与其交易装置相对应的剩余值,则他们可以通过直接(例如,通过数字资产应用程序)或通过中间实体(例如,服务提供商计算机、支付处理服务器计算机等)提供交易装置标识符来简单地查询数字资产服务提供商计算机。

[0092] 图5示出具有用于实现本发明实施例的至少一些部件的示例性系统的框图。图5更详细地描述了可能涉及处理金融交易(例如关于图4所描述的金融交易)的实体。图5包括用户501、交易装置502、访问装置503、资源提供商计算机504、收单方计算机505和支付处理器服务器计算机506。

[0093] 任何计算装置(例如交易装置502、访问装置503、资源提供商计算机504、收单方计算机505、支付处理器服务器计算机506)可以包括处理器以及包括可由处理器执行以实施本文中描述的功能的代码的计算机可读介质。此外,任何计算装置都可以通过任何合适的通信网络通信。

[0094] 通信网络可以包括用于实体之间的数据和信息的安全通信的多个网络。在一些实



施例中,通信网络可以遵循合适的通信协议以便生成一个或多个安全通信信道。可以使用任何合适的通信协议来生成通信信道。在一些情况下,通信信道可以包括可以用任何已知方式建立的“安全通信信道”,包括相互认证和会话密钥的使用以及SSL会话的建立。然而,可以使用创建安全信道的任何方法。通过建立安全信道,可以安全地传送敏感信息以促进交易。

[0095] 用户501(也可以称为消费者)可以操作交易装置502。用户501可以是接收方用户,其中另一个分发用户相对于交易装置502激活数字资产。在一些实施例中,用户501可以从分发用户接收交易装置502。

[0096] 交易装置502可以是进行交易的任何合适的装置。在一些实施例中,交易装置502可以是可编程的交易卡。在其他实施例中,交易装置502可以是包括存储器的计算装置。交易装置502可以通过通信网络与一个或多个实体(例如,访问装置503、资源提供商计算机504、支付处理器服务器计算机等)通信。交易装置502能够与访问装置503通信。在一些实施例中,交易装置502能够通过接触或无线方式与访问装置503通信。在其他情况下,交易装置502可以用于例如通过网站进行无卡交易。交易装置502的一些非限制性示例可以包括移动装置(例如蜂窝电话、钥匙链装置、个人数码助理(PDA)、传呼机、笔记本电脑、膝上型电脑、记事本、智能手表、健身腕带、珠宝等)、具有远程通信功能的汽车、个人计算机、支付卡(例如智能卡、磁条卡,等),等等。

[0097] 访问装置503可以是提供对远程系统的访问的任何合适的装置。访问装置503还可以用于与资源提供商计算机(例如资源提供商计算机504)、交易处理计算机、认证计算机或任何其他合适的系统通信。访问装置503可以位于任何合适的位置,例如位于与资源提供商计算机504关联的资源提供商的所在位置。访问装置503可以是任何适当形式。访问装置的一些示例包括POS或销售点装置(例如,POS终端)、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用读取器、机顶盒、电子现金出纳机(ECR)、自动柜员机(ATM)、虚拟现金出纳机(VCR)、营业亭、安全系统以及访问系统等。

[0098] 访问装置503可以使用任何合适的接触或非接触操作模式以向交易装置502发送或从其接收数据,或与所述交易装置关联。在一些实施例中,在访问装置503包括POS终端的情况下,任何适当的POS终端可以被使用,并且可以包括读取器、处理器和计算机可读介质。读取器可以包含任何合适的接触或非接触操作模式。例如,示例性读取器可以包括射频(RF)天线、光学扫描器、条形码读取器或磁条读取器,以与支付装置和/或移动装置交互。在一些实施例中,用作POS终端的蜂窝电话、平板或其他专用无线装置可以被称为移动销售点或“mPOS”终端。

[0099] 资源提供商计算机504(也成为供应商计算机)可以被配置成接收并处理交易数据。在一些实施例中,可以从交易装置502或与交易装置502通信的访问装置503接收交易数据。资源提供商计算机504可以参与交易、售卖商品或服务、或向消费者提供对商品或服务的访问。资源提供商计算机504可以接受多种形式的支付,并且可以使用多种工具来进行不同类型的交易。例如,资源提供商计算机504还可以经由网站或应用程序来销售商品和/或服务,并且可以通过互联网来接受支付。资源提供商计算机504还可以与使用访问装置503进行面对面交易的实体商店关联。

[0100] 收单方计算机505可以是与资源提供商计算机504具有业务关系的系统或实体(例



如,银行)。收单方计算机505可以管理与资源提供商计算机504相关联的资金。收单方计算机505可以将对交易的授权请求路由到支付处理器服务器计算机506。

[0101] 支付处理器服务器计算机506可以包括数据处理子系统、网络 and 用于支持及递送授权服务以及清算和结算服务的操作。支付处理器服务器计算机506可以与支付处理网络关联。支付处理网络的示例包括由 Visa® 运营的 VisaNet®。支付处理网络可以包括有线或无线网络,包括互联网。在一些实施例中,支付处理器服务器计算机506还可以操作数字资产服务提供商计算机。如参考图4所述,数字资产服务提供商计算机可与一个或多个金融机构计算机通信。

[0102] 虽然以上详细描述了在金融环境中使用的本发明的实施例,但是实施例不限于此。例如,数字资产可以对应于非货币值,例如时间值、访问权限值,以及可以相对于接收方用户要使用的交易装置被激活的其他合适的值。参考图6描述示例性情况。

[0103] 图6示出根据本发明实施例的非财务系统的框图。图6包括用户601、交易装置602、访问装置603、604、和605、数字资产服务提供商计算机606、服务器计算机607、和服务器计算机608。在此示例性情况中,分发用户(未示出)可以向用户601(接收方用户)提供交易装置602。在向用户601提供交易装置602之前,分发用户可以按与至少关于图3所描述的方式类似的方式相对于交易装置602激活数字资产。然而,在这种情况下,数字资产可能对应于非货币值,如访问权限值。访问权限值可以指示分发用户允许用户601使用各种设备的次数。例如,数字资产可能表示用户601可以访问设备A、设备B和设备C中的任何一个共十次。因此,通过向用户601提供交易装置602,分发用户可以使用户601能够将设备用于与激活的数字资产相对应的指定次数的使用。下文描述了相对于交易装置602激活的数字资产的使用。有关图4描述的相应步骤,可以进一步详细描述一些步骤。

[0104] 在接收交易装置602之后,用户601可以使用交易装置602来访问由数字资产启用的设备。设备可以被配置成使得用户可以基于使用交易装置602与访问装置通信来访问设备。例如,当用户601想要使用设备A时,用户601可以使用与设备A相关联的访问装置603来刷交换装置602。类似地,用户601可以使用访问装置604来刷交易装置602以使用设备B并使用访问装置605来刷交易装置602以使用设备C。应当理解,访问装置603、604和605可以支持与交易装置602兼容的其他接触和非接触通信方法。访问装置603、604和605中的每一个可以与数字资产服务提供商计算机606通信。

[0105] 在示例性情况下,用户601可以使用访问装置来刷交易装置602以使用设备A。访问装置603可以读取与相对于交易装置602激活的数字资产有关的信息。在这种情况下,访问装置603可以读取:先前由分发用户激活的数字资产与交易装置602相关并且对应于十次使用的值。访问装置603可以将与从交易装置602读取的数字资产相关的信息发送到数字资产服务提供商计算机606。在一些实施例中,所述信息可以包括与数字资产相对应的数字资产标识符,与交易装置602相关联的交易装置标识符,以及与数字资产的分发用户相关联的标识信息。

[0106] 然后,数字资产服务提供商计算机606可以与服务器计算机607和服务器计算机608通信。服务器计算机607可以与分发用户关联,并且可以管理由分发用户分发的数字资产。服务器计算机607可以管理分类账(未示出),所述分类账记录与分发用户分发的数字资产有关的信息。服务器计算机608可以与想要跟踪设备A的使用的实体(例如,所有者)相关

联。在一些实施例中,服务器计算机608还可以与设备B和设备C相关联。服务器计算机608可以管理分类账(未示出),所述分类账记录与设备A、B和C相关的数字资产使用情况的信息。

[0107] 数字资产服务提供商计算机606可以与服务器计算机607通信,以验证与数字资产有关的详细信息。数字资产服务提供商计算机606可以请求服务器计算机607验证用户601使用的数字资产先前是否已经相对于交易装置602被激活。然后,服务器计算机607可以基于检查其分类账来验证数字资产,以获得数字资产确实由分发用户分发并且相对于交易装置602被激活的指示。服务器计算机607还可以验证存在与数字资产相关联的值(例如,并非所有十次使用都已被使用)。服务器计算机607可以向数字资产服务提供商计算机606指示已经验证数字资产。

[0108] 随后,数字资产服务提供商计算机606可以请求服务器计算机607和服务器计算机608更新其分类账以指示对应于交易装置602的数字资产的使用。在一些实施例中,数字资产服务提供商计算机606可以构建交易数据,所述交易数据包括与数字资产相关的信息(例如,数字资产标识符、分发用户识别信息)和与交易装置602相关联的交易装置标识符。交易数据还可以指示设备A被使用一次,将与数字资产相关联的值带到设备的总共九次剩余使用中。数字资产服务提供商计算机606可以将交易数据发送到服务器计算机607和服务器计算机608,所述服务器计算机可以用交易数据更新其分类账。这确保了所涉及的实体各自具有对应于与交易装置602关联的数字资产的剩余使用记录。实体可以在后续交易期间使用此信息来确定交易装置602是否对于设备的进一步使用是有效的。

[0109] 如本文所述,由服务器计算机607和服务器计算机608管理的分类账可以是块链的形式。分类账中的新条目可以包括数据头,所述数据头包括使得新条目在未经检测的情况下不可改变的信息。例如,数据头可以包括分类账中前一条目的散列和所有过往交易的根值。由于可以通过包括存储引用其先前条目和先前交易的信息的数据头以类似方式生成分类账中的每个条目,因此不会在不影响所有后续条目的情况下修改条目。这确保了不能未被察觉地对与交易有关的信息进行任何篡改,例如试图将数字资产重新分配给不适当的实体。图7中示出呈上述块链形式的示例性的条目数。

[0110] 本发明的实施例具有优点。例如,即使用户601可能与数字资产服务提供商计算机606或服务器计算机608没有关系,分发方也可以向用户601提供访问权限。这很方便,因为用户601不必花时间注册账户。另外,用户601可能只需要暂时访问装置(例如,有限次数),在这种情况下,生成账户可能浪费用于存储账户数据的计算资源。另外,由于服务器计算机607和608维护记录与过去交易有关的信息的分类账,这使得多个实体能够验证提供给用户601并由用户601使用的数字资产。这提供了额外的安全层,因为这使得用户601难以滥用(例如,过度使用)设备的访问权限。

[0111] 计算机系统可以用于实施上述任何实体或部件。计算机系统的子系统可以经由系统总线互连。附加的子系统可以包括打印机、键盘、固定磁盘(或包括计算机可读介质的其他存储器)、耦合到显示适配器的监视器以及其他装置。耦合到I/O控制器(可以是处理器或任何合适的控制器)的外设和输入/输出(I/O)装置可以通过任何数量的本领域已知手段(诸如串行端口)连接到计算机系统。例如,串行端口或外部接口能够用来将计算机装置连接至广域网(诸如互联网)、鼠标输入装置或扫描器。经由系统总线的互连允许中央处理器能够与每个子系统通信,并控制来自系统存储器或固定磁盘的指令的执行以及信息在子系

统之间的交换。系统存储器 and/或固定磁盘可以体现计算机可读介质。在一些实施例中，监视器可以是触敏显示屏。

[0112] 上文提供了关于上述一些方面的具体细节。在不偏离本技术的实施例的精神和范围的情况下，具体方面的特定细节可以以任何适当方式组合。例如，在本技术的一些实施例中，后端处理、数据分析、数据收集以及其他交易可以全部组合。不过，本技术的其他实施例可以涉及与每个单独的方面有关的特定实施例，或者这些单独的方面的特定组合。

[0113] 应当理解，如以上描述的本技术可以用控制逻辑的形式以模块化或集成方式使用计算机软件（存储在有形物理介质中）来实现。尽管已经使用形式为控制逻辑和编程代码和指令的硬件和软件的特定组合描述了本发明，但应当认识到，硬件和软件的其他组合也在本发明的范围内。基于本文提供的公开内容和教导，本领域普通技术人员将知道并理解使用硬件以及硬件和软件的组合来实施本技术的其他方式和/或方法。

[0114] 本申请中描述的任何软件组件或功能可以实施为由处理器使用任何合适的计算机语言（例如Java、C++或Perl）、使用例如常规或面向对象的技术执行的软件代码。软件代码可以被存储为计算机可读介质（例如，随机存取存储器（RAM）、只读存储器（ROM）、磁介质（例如硬盘驱动器或软盘）或光介质（例如CD-ROM））上的一系列指令或命令。任何这样的计算机可读介质可以驻留在单个计算装置上或内部，并且可以存在于系统或网络内的不同计算装置上或内部。

[0115] 以上描述是说明性的而不是限制性的。本领域技术人员在阅读本公开后，会明白技术的许多变形。因此，技术范围应当不参照上文描述确定，而是应当参照所附权利要求连同其全部范围或等同物确定。

[0116] 在一些实施例中，本文中描述的任何实体可以由执行所公开的任何或全部功能和步骤的计算机实现。

[0117] 在不偏离技术的范围下，任何实施例的一个或多个特征可以与任何其他实施例的一个或多个特征组合。

[0118] 除非明确指示有相反的意思，否则“一个”、“一”或“所述”的叙述旨在表示“一个或多个”。

[0119] 本文提及的所有专利、专利申请、公开案和描述都出于所有目的以全文引用的方式并入。不承认它们是现有技术。

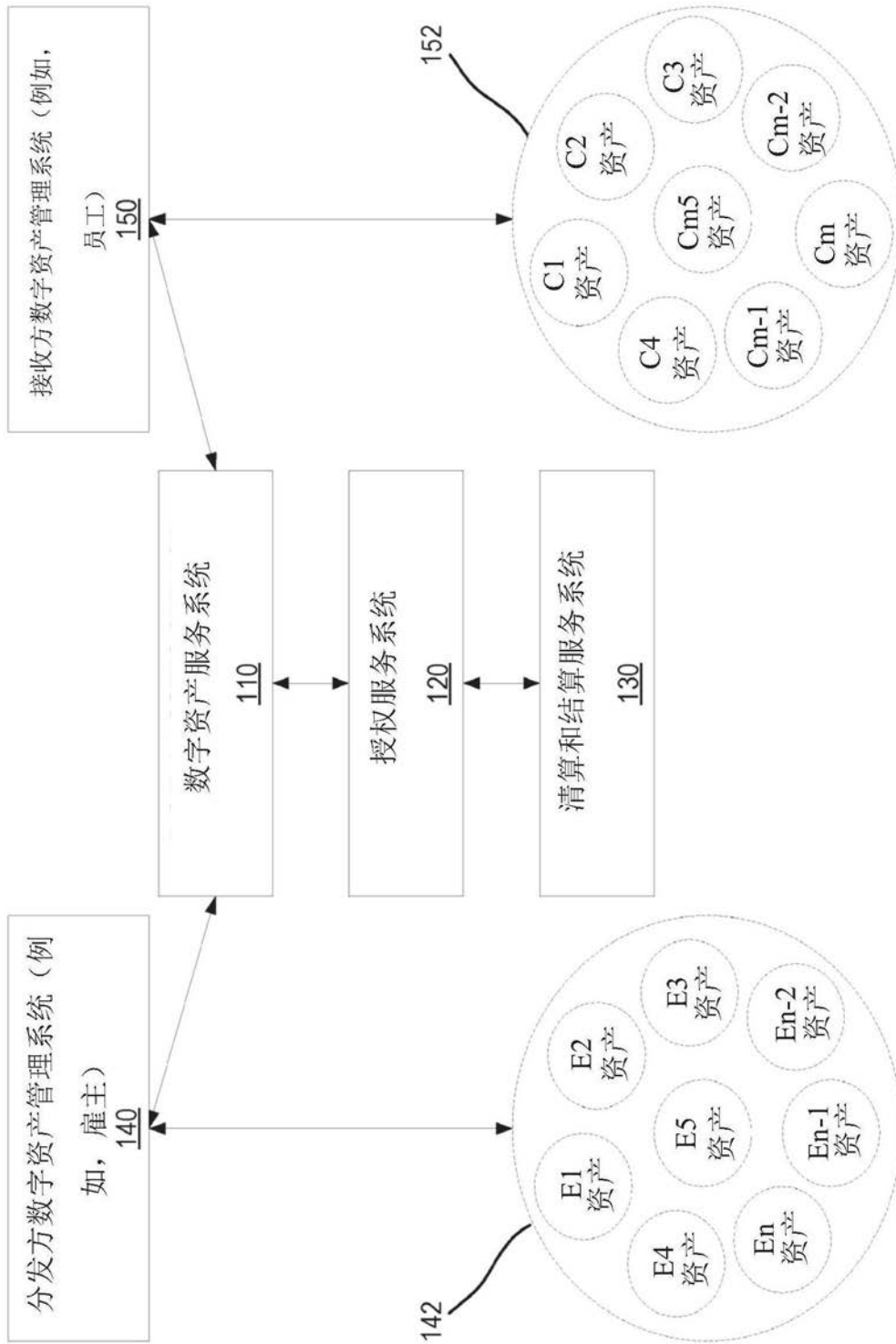


图1

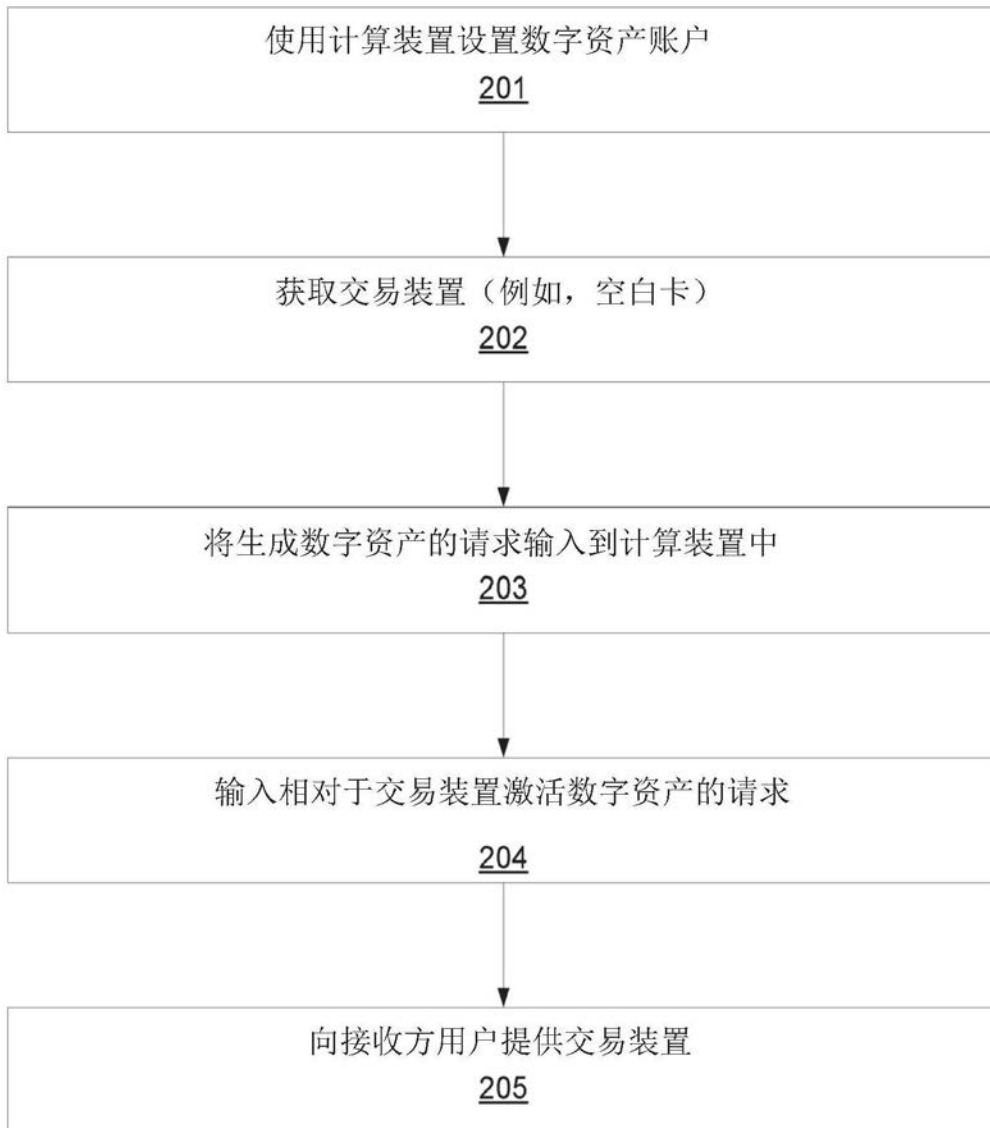


图2

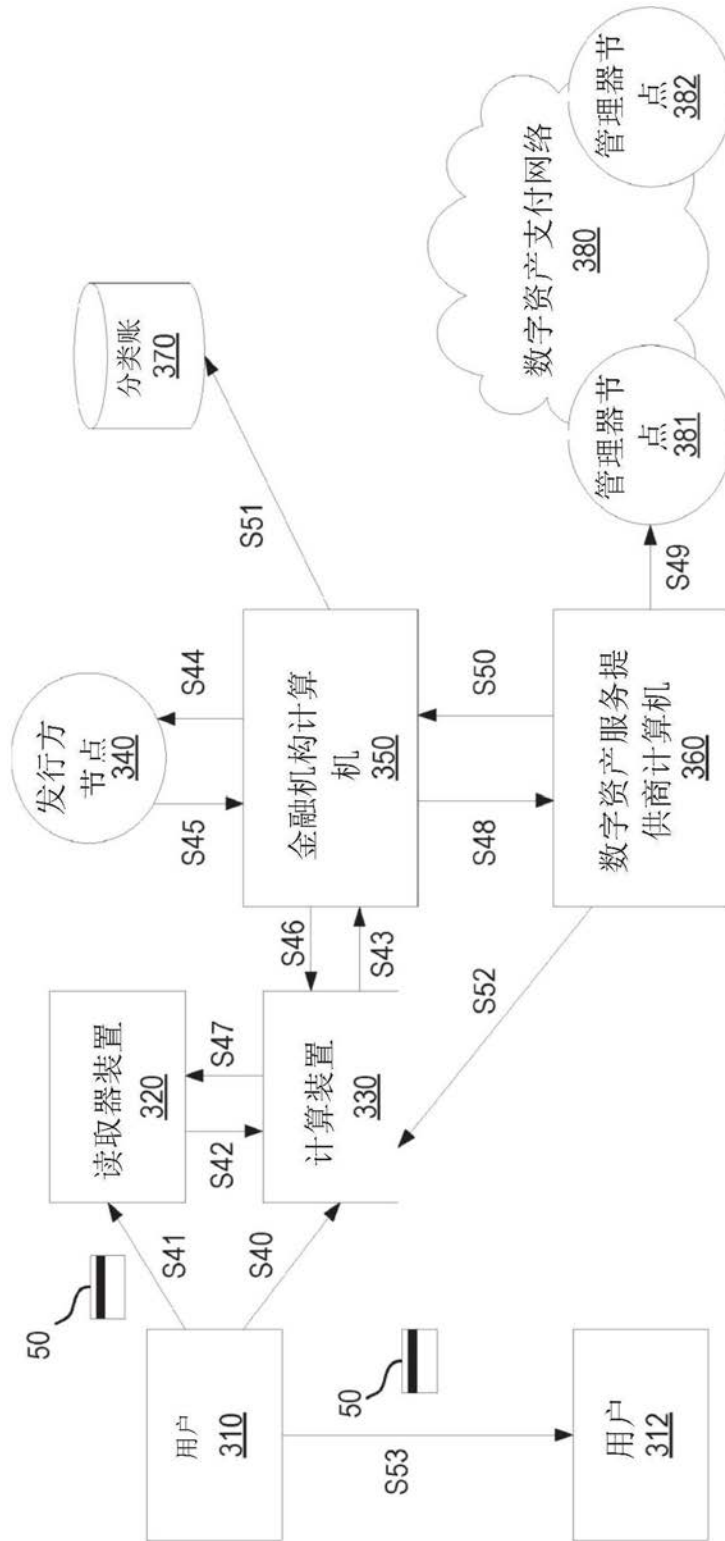


图3

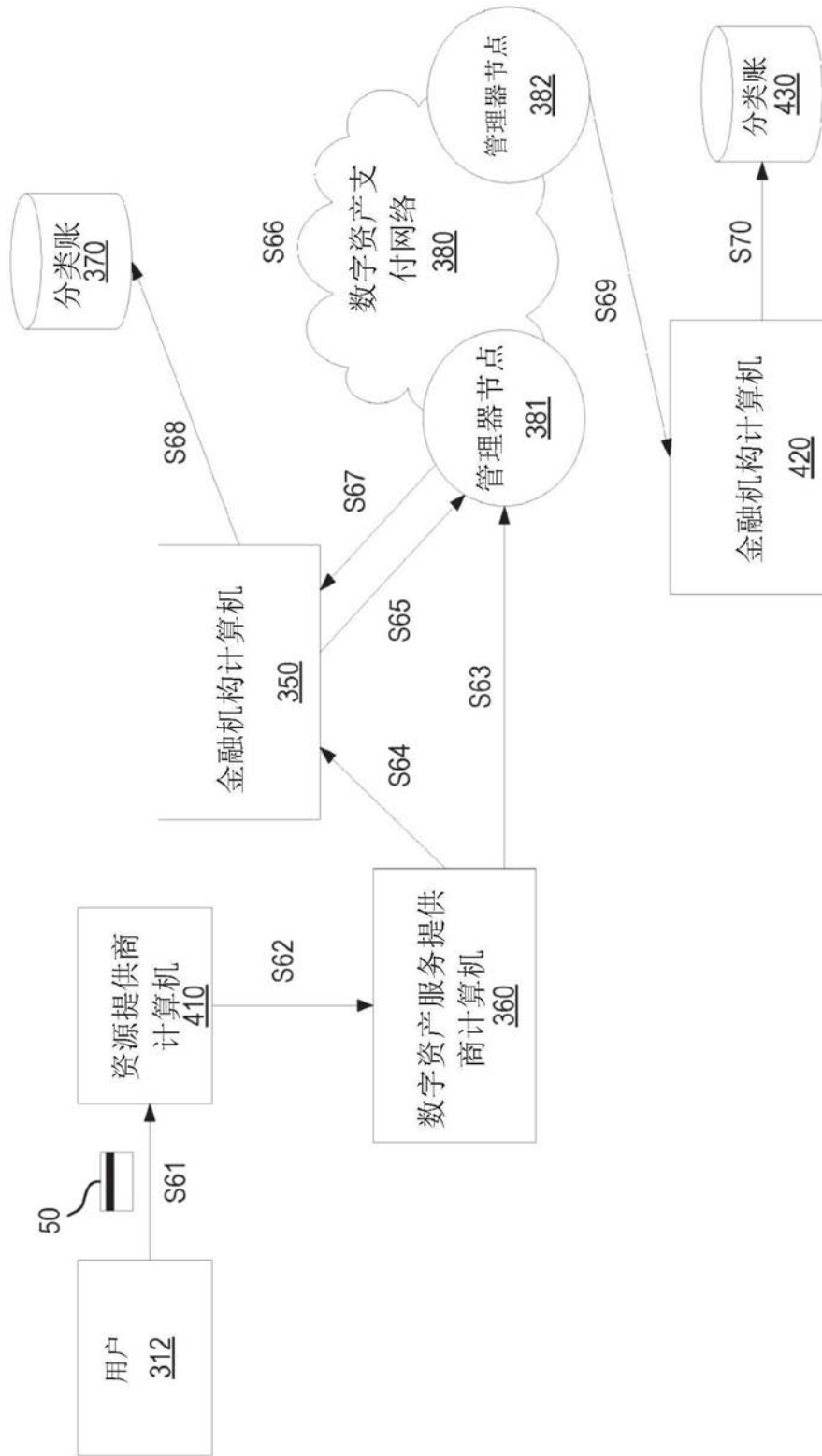


图4

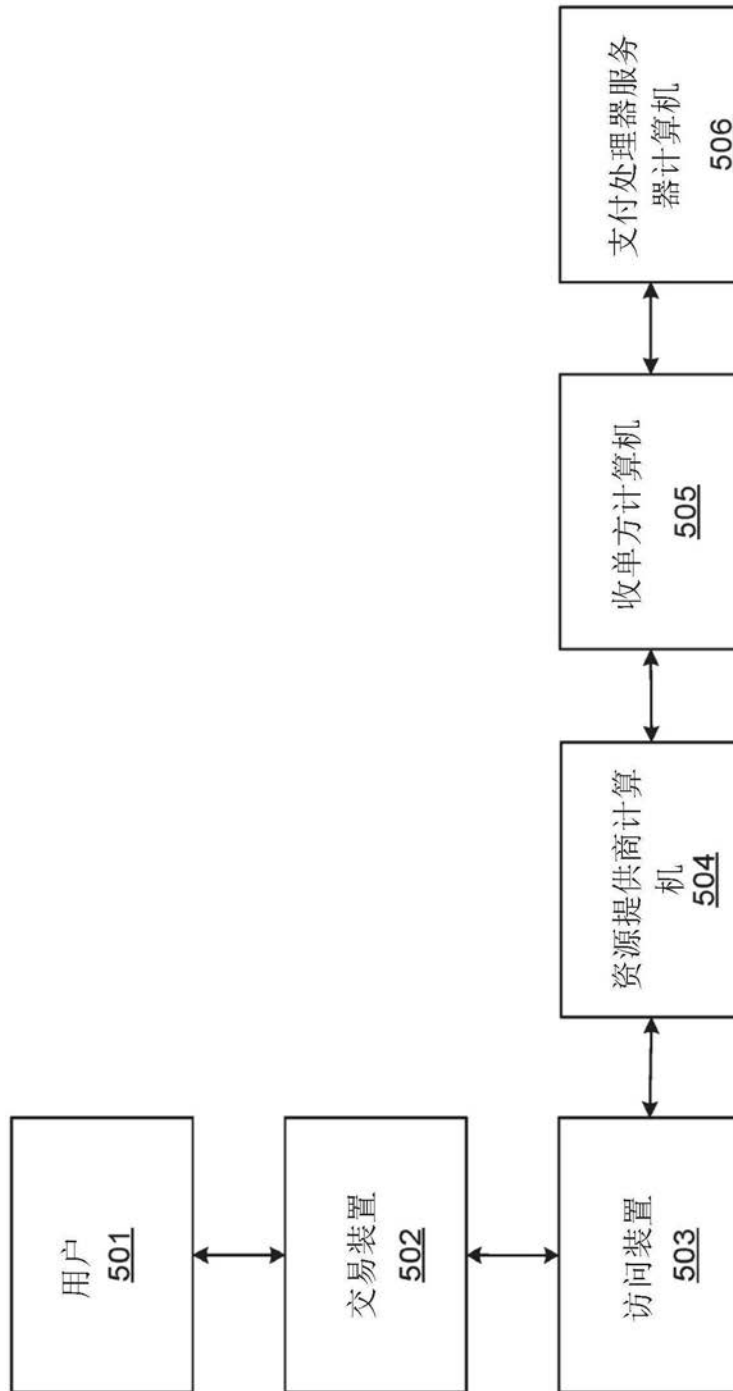


图5



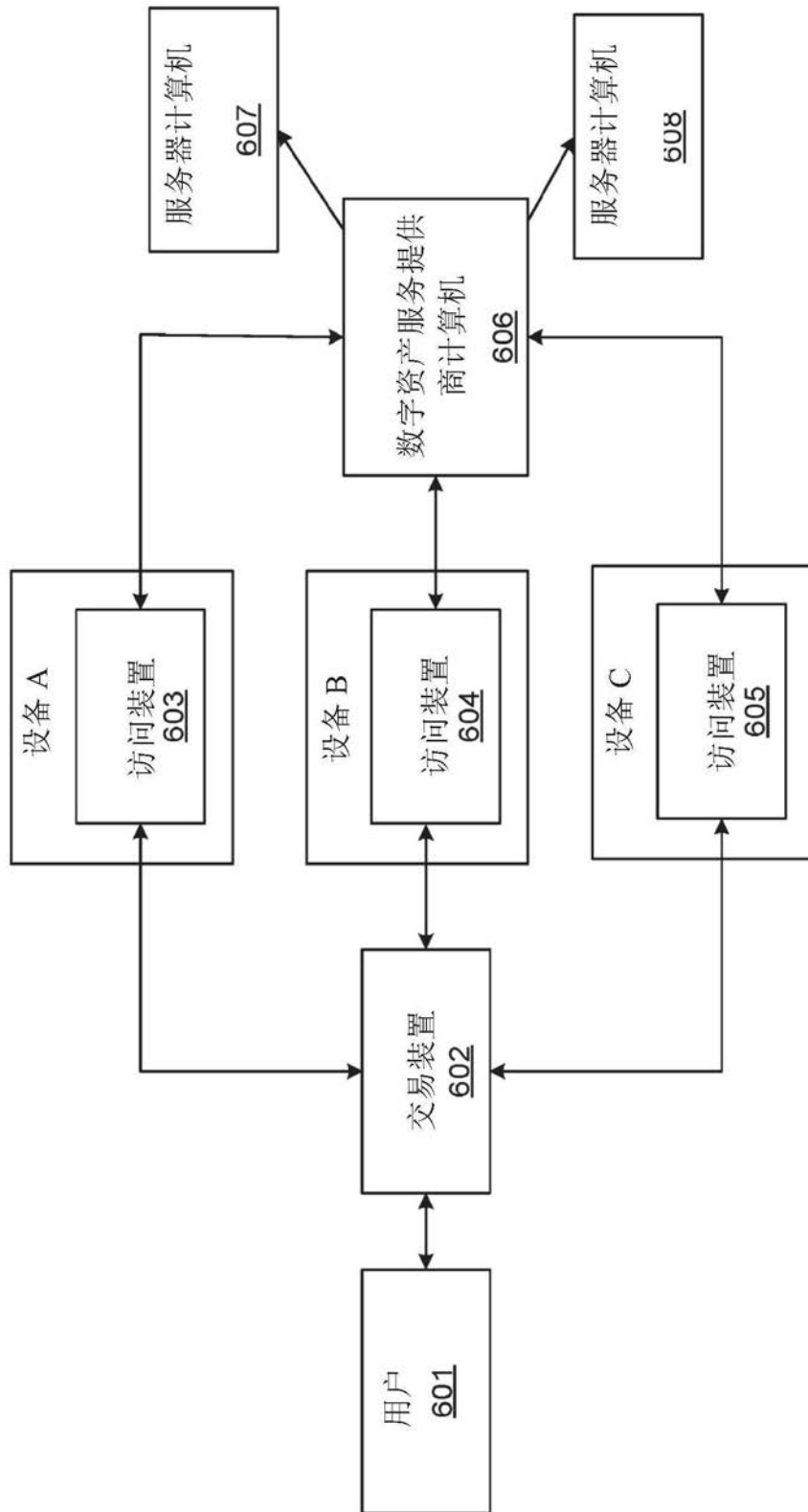


图6

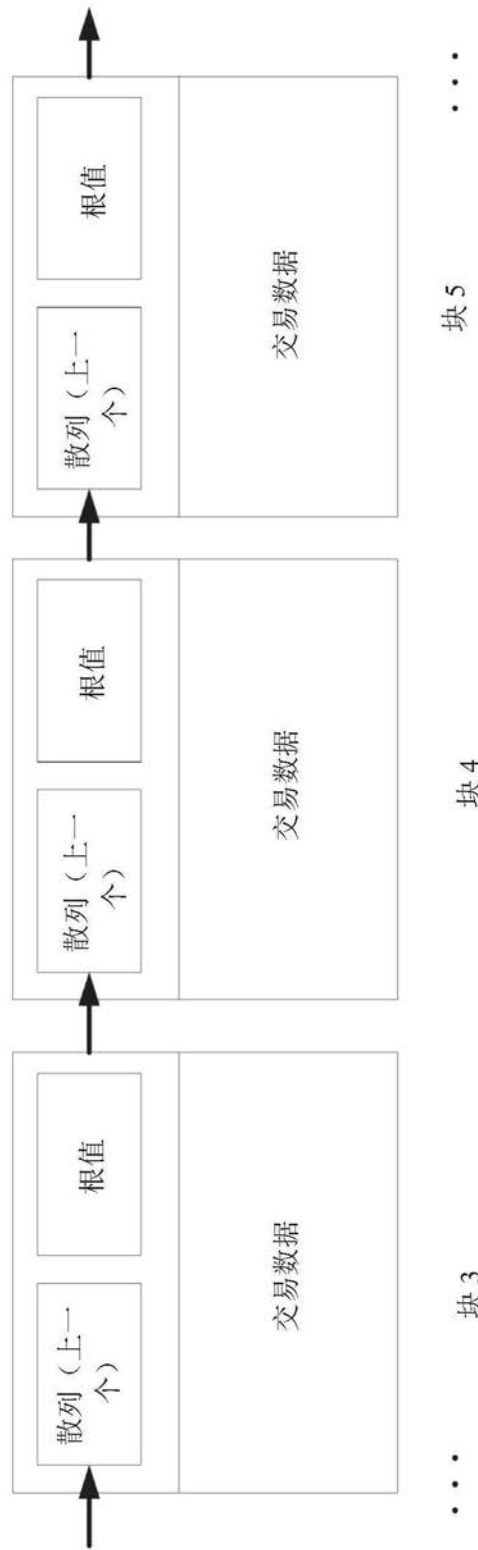


图7