(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110383756 B
(45)授权公告日 2023.06.09

(21)申请号 201780059173.2
(22)申请日 2017.07.27
(65)同一申请的已公布的文献号
申请公布号 CN 110383756 A
(43)申请公布日 2019.10.25
(30)优先权数据
62/368,408 2016.07.29 US
(85)PCT国际申请进入国家阶段日
2019.03.26
(86)PCT国际申请的申请数据
PCT/US2017/044186 2017.07.27
(87)PCT国际申请的公布数据
WO2018/022891 EN 2018.02.01
(73)专利权人 奇跃公司
地址 美国佛罗里达州
(72)发明人 A·克勒
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 魏子翔 杨晓光
(51)Int.Cl.
G06F 1/00(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
(56)对比文件
US 2003172297 A1,2003.09.11
US 2014032913 A1,2014.01.30
US 5005200 A,1991.04.02
US 2002083126 A1,2002.06.27
审查员 柳倩

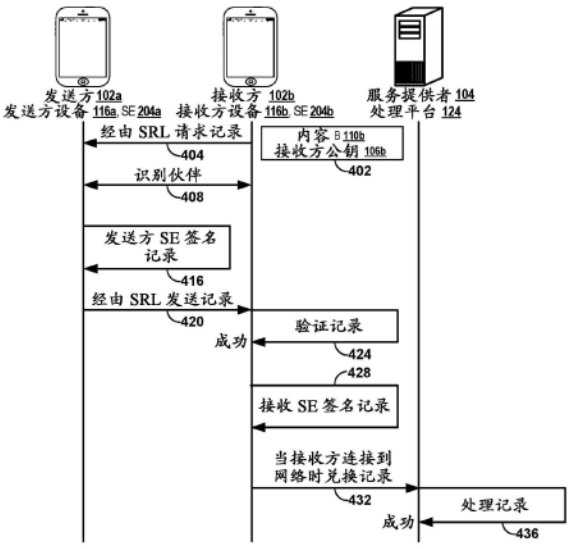
权利要求书3页 说明书74页 附图38页

(54)发明名称

加密签名记录的安全交换

(57)摘要

公开了用于安全地交换加密签名记录的系统和方法。在一个方面,在接收到内容请求之后,发送方设备可以向发出请求的接收方设备(例如,代理设备)发送记录。记录可以以分散(例如,对等)方式经由短程链路发送,而设备可以不与集中处理平台通信。该记录可以包括使用发送方设备的私钥创建的发送方签名。接收方设备可以使用发送方设备的公钥来验证发送方签名的真实性。在添加基于加密的接收方签名之后,接收方设备可以与平台来兑换记录。在成功验证记录时,平台可以如记录的内容(例如,修改或更新用户帐户)指示地执行。



CN 110383756 B

1.一种用于安全地交换加密签名记录的方法,包括:

在硬件处理器的控制下:

从记录接收方设备接收接收方个体记录,

其中,所述接收方个体记录包括发送方个体记录和所述接收方个体记录的接收方签名,

其中,在从所述记录接收方设备接收到记录内容请求以及识别所述记录接收方设备之后,由记录发送方设备创建所述发送方个体记录,

其中,所述发送方个体记录包括记录内容、所述记录发送方设备的发送方公钥、所述记录接收方设备的接收方公钥,以及所述发送方个体记录的发送方签名,

其中,使用所述记录发送方设备的发送方私钥创建所述发送方签名,其中,所述发送方公钥和所述发送方私钥形成发送方公钥加密对,

其中,在从所述记录发送方设备接收到所述发送方个体记录以及经由所述记录接收方设备至少部分地基于所述发送方公钥验证所述发送方个体记录之后,由所述记录接收方设备创建所述接收方个体记录,

其中,至少部分地基于所述记录接收方设备的接收方私钥创建所述接收方签名,以及其中,所述接收方公钥和所述接收方私钥形成接收方公钥加密对;

至少部分地基于所述接收方公钥验证所述接收方个体记录;

如由所述接收方个体记录指示地执行所述记录接收方设备以提供经由所述记录内容请求所请求的内容;

从中央记录生成公共记录,其中,所述中央记录包括所述发送方公钥、所述接收方公钥、所述记录发送方设备的用户记录状态,以及所述记录接收方设备的用户记录状态;

确定所述记录发送方的所述用户记录状态禁止处理平台如由所述接收方个体记录指示地执行所述记录接收方设备;以及

向缺点列表添加所述记录发送方设备。

2.根据权利要求1所述的方法,其中,识别所述记录接收方设备包括执行伙伴标识,其中,伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

3.根据权利要求1所述的方法,其中,所述发送方个体记录进一步包括记录标识符。

4.根据权利要求1所述的方法,其中,从所述记录接收方设备接收所述发送方个体记录包括直接或通过中间设备经由短程链路从所述记录发送方设备接收所述发送方个体记录。

5.根据权利要求1所述的方法,其中,所述接收方个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

6.根据权利要求1-5中任一项所述的方法,其中,在接收到记录发送方的认证信息之后由所述记录发送方设备创建所述发送方个体记录,以及其中,在接收到记录接收方的认证信息之后由所述记录接收方设备创建所述接收方个体记录。

7.根据权利要求1-5中任一项所述的方法,进一步包括向所述记录发送方设备或所述记录接收方设备提供公共记录,其中,所述公共记录包括所述发送方公钥和所述接收方公钥。

8.根据权利要求1所述的方法,其中,验证所述发送方个体记录被离线执行。

9.一种用于安全地交换加密签名记录的方法,包括:

在硬件处理器的控制下：

从记录接收方设备接收内容请求；

识别所述记录接收方设备；

创建发送方个体记录，

其中，所述发送方个体记录包括记录内容、记录发送方设备的发送方公钥、所述记录接收方设备的接收方公钥，以及所述发送方个体记录的发送方签名，

其中，使用所述记录发送方设备的发送方私钥创建所述发送方签名，以及其中，所述发送方公钥和所述发送方私钥形成发送方公钥加密对；

向所述记录接收方设备发送所述发送方个体记录；以及

接收所述记录接收方设备的指示：

接收所述发送方个体记录；

经由所述记录接收方设备至少部分地基于所述发送方公钥验证所述发送方个体记录；

创建接收方个体记录，其中，所述接收方个体记录包括所述发送方个体记录和所述接收方个体记录的接收方签名，其中，至少部分地基于所述记录接收方设备的接收方私钥创建所述接收方签名，以及其中，所述接收方公钥和所述接收方私钥形成接收方公钥加密对；

与处理平台兑换所述接收方个体记录；

如由所述接收方个体记录指示地接收所述处理平台的执行以提供经由所述记录内容请求所请求的内容；

从中央记录生成公共记录，其中，所述中央记录包括所述发送方公钥、所述接收方公钥、所述记录发送方设备的用户记录状态，以及所述记录接收方设备的用户记录状态；

确定所述记录发送方的所述用户记录状态禁止所述处理平台如由所述接收方个体记录指示地执行所述记录接收方设备；以及

向缺点列表添加所述记录发送方设备。

10.根据权利要求9所述的方法，其中，所述内容请求包括所述接收方公钥和所请求的内容，以及其中，所述记录内容与所请求的内容相关。

11.根据权利要求9-10中任一项所述的方法，其中，由所述记录发送方设备的安全元件使用所述发送方私钥创建所述发送方签名，以及其中，所述发送方私钥被存储在所述记录发送方设备的所述安全元件中。

12.根据权利要求9所述的方法，其中，验证所述发送方个体记录被离线执行。

13.一种用于安全地交换加密签名记录的方法，包括：

在硬件处理器的控制下：

向记录发送方设备发送内容请求；

从所述记录发送方设备接收发送方个体记录，

其中，在从记录接收方设备接收到所述内容请求并识别所述记录接收方设备之后，由所述记录发送方设备创建所述发送方个体记录，

其中，所述发送方个体记录包括记录内容、所述记录发送方设备的发送方公钥、所述记录接收方设备的接收方公钥，以及所述发送方个体记录的发送方签名，

其中，使用所述记录发送方设备的发送方私钥创建所述发送方签名，以及其中，所述发送方公钥和所述发送方私钥形成发送方公钥加密对；

经由所述记录接收方设备至少部分地基于所述发送方公钥验证所述发送方个体记录；

创建接收方个体记录，其中，所述接收方个体记录包括所述发送方个体记录和所述接收方个体记录的接收方签名，

其中，至少部分地基于所述记录接收方设备的接收方私钥创建所述接收方签名

其中，所述接收方公钥和所述接收方私钥形成接收方公钥加密对；

与处理平台兑换所述接收方个体记录；

如由所述接收方个体记录指示地接收所述处理平台的执行以提供经由所述记录内容请求所请求的内容；

从中央记录生成公共记录，其中，所述中央记录包括所述发送方公钥、所述接收方公钥、所述记录发送方设备的用户记录状态，以及所述记录接收方设备的用户记录状态；

确定所述记录发送方的所述用户记录状态禁止所述处理平台如由所述接收方个体记录指示地执行所述记录接收方设备；以及

向缺点列表添加所述记录发送方设备。

14.根据权利要求13所述的方法，其中，所述内容请求包括所述接收方公钥和所请求的内容，以及其中，所述记录内容与所请求的内容相关。

15.根据权利要求13所述的方法，其中，验证所述发送方个体记录包括使用所述发送方公钥来确定使用所述发送方私钥创建所述发送方签名。

16.根据权利要求13-15中任一项所述的方法，其中，使用所述记录接收方设备的安全元件使用所述接收方私钥创建所述接收方签名，以及其中，所述接收方私钥被存储在所述记录接收方设备的所述安全元件中。

17.根据权利要求13所述的方法，进一步包括向所述记录发送方设备发送公共记录。

18.根据权利要求13所述的方法，进一步包括从所述记录发送方设备接收公共记录，其中，所述公共记录包括所述发送方公钥和所述接收方公钥。

19.根据权利要求17-18中任一项所述的方法，

其中，所述公共记录进一步包括所述公共记录的第三签名，以及其中，使用所述处理平台的第三私钥创建所述第三签名，

其中，所述方法进一步包括使用所述处理平台的第三公钥验证所述公共记录而不一定与所述处理平台通信，

其中，所述第三公钥和所述第三私钥形成第三公钥加密对，以及

其中，验证所述公共记录包括使用所述第三公钥来确定使用所述第三私钥创建所述第三签名。

20.根据权利要求13所述的方法，其中，验证所述发送方个体记录被离线执行。

加密签名记录的安全交换

[0001] 相关申请的交叉引用

[0002] 本申请要求2016年7月29日提交的题为“SECURE EXCHANGE OF CRYPTOGRAPHICALLY SIGNED RECORDS”的美国临时申请号62/368408的优先权,其内容通过引用整体并入在此。

技术领域

[0003] 本公开一般涉及用于加密的系统和方法,并且更特别地涉及通过计算机网络安全地交换加密签名的记录。

背景技术

[0004] 诸如数字传输的传统系统对于通过计算机网络交换内容和记录是有用的。这种数字传输可以取代记录的传统物理交换的需要。利用这种传统系统的各方需要在交换时连接到诸如因特网的网络。这些传统系统要求交换的各方连续访问中央数据中心以便验证交换。

发明内容

[0005] 公开了用于安全地交换加密签名记录的系统和方法。该系统和方法可以使用公钥和私钥加密技术。在一个方面,在接收到内容请求之后,发送方设备可以向发出请求的第一接收方设备发送记录。记录可以以分散(例如,对等)方式经由短程链路发送,而设备可以不与集中处理平台通信。该记录可以包括使用发送方设备的私钥创建的发送方签名。第一接收方设备可以使用发送方设备的公钥来验证发送方签名的真实性。在添加“仅用于处理认可”和接收方签名之后,第一接收方设备可以与处理平台兑换记录。基于成功验证发送方签名和接收方签名,处理平台可以如记录内容所指示地执行。

[0006] 在另一方面,第一接收方设备能够在向记录添加第一接收方签名之后向第二接收方设备发送记录。第二接收方设备可以使用发送方设备和第一接收方设备的公钥来验证签名的真实性。在添加“仅用于处理认可”和第二接收方签名之后,第二接收方设备可以与处理平台兑换记录。

[0007] 在另一方面,在接收到内容请求之后,发送方设备能够向代表委托人发出请求的代理设备发送记录。代理设备可以使用发送方设备的公钥来验证记录中的发送方签名的真实性。代理设备可以在委托人与处理平台兑换记录之前向记录添加“由认可处理”。

[0008] 在一个方面,发送方设备可以向接收方设备发送记录。接收方设备可以通过检测恶意行为(诸如具有单个接收方的发送方克隆,窥探(mousing),重影(ghosting),具有多个接收方的发送方克隆,或分叉)来验证所接收的记录。在检测到恶意行为之后,接收方设备可以在向处理平台发送所认可的记录之前向记录添加恶意认可。处理平台可以在执行模糊判定或布尔分析后将发送方设备添加到黑名单。在另一方面,处理平台可以通过检测诸如接收方克隆或重影的恶意行为来验证从设备接收的记录。

[0009] 公开了用于安全地交换加密签名记录的系统和方法的实施例。在一个方面，在接收到内容请求之后，发送方设备可以向发出请求的接收方设备发送记录。记录能够以分散(例如，对等)方式经由短程链路发送，而设备可以不与集中处理平台通信。该记录能够包括使用发送方设备的私钥创建的发送方签名。接收方设备可以使用发送方设备的公钥来验证发送方签名的真实性。在添加“仅用于处理认可”和接收方签名之后，接收方设备可以与处理平台兑换记录。基于成功验证发送方签名和接收方签名，处理平台能够如记录内容指示地执行。

[0010] 公开了用于安全地交换加密签名记录的系统和方法的实施例。在一个方面，在接收到内容请求之后，发送方设备可以向代表委托人发出请求的代理设备发送记录。记录能够以分散(例如，对等)方式经由短程链路发送，而设备可以不与集中处理平台通信。该记录能够包括使用发送方设备的私钥创建的发送方签名。代理设备可以使用发送方设备的公钥来验证发送方签名的真实性。代理设备可以在委托人与处理平台兑换记录之前向记录添加“由认可处理”。基于成功验证发送方签名和接收方签名，处理平台能够如记录内容指示地执行。

[0011] 公开了用于安全地交换涉及多个接收方的加密签名记录链的系统和方法的实施例。在一个方面，发送方设备能够向第一接收方设备发送记录。该记录可以包括使用发送方设备的私钥创建的发送方签名。第一接收方设备可以使用发送方设备的公钥来验证签名的真实性。在向记录添加第一接收方签名之后，第一接收方设备能够向第二接收方设备发送记录。第二接收方设备可以使用发送方设备和第一接收方设备的公钥来验证签名的真实性。在添加“仅用于处理认可”和第二接收方签名之后，第二接收方设备可以与处理平台兑换记录。基于成功验证签名，处理平台可以如记录的内容指示地执行。

[0012] 公开了用于验证加密签名记录的系统和方法的实施例。在一个方面，发送方设备能够向接收方设备发送记录。接收方设备可以通过检测恶意行为(诸如具有单个接收方的发送方克隆，窥探，重影，具有多个接收方的发送方克隆，或分叉)来验证所接收的记录。在检测到恶意行为之后，接收方设备能够在向处理平台发送所认可的记录之前向记录添加恶意认可。处理平台能够在执行模糊判定或布尔分析后将发送方设备添加到黑名单。在另一方面，处理平台能够通过检测诸如接收方克隆或重影的恶意行为来验证从设备接收的记录。

[0013] 在附图和以下描述中阐述了本说明书中描述的主题的一个或多个实施方式的细节。从说明书、附图和权利要求中，其它特征、方面和优点将变得显而易见。该概要和以下具体实施方式都不旨在限定或限制发明主题的范围。

附图说明

[0014] 图1A和图1B示意性地示出通过无线网络安全地交换加密签名的内容和记录的一个实施例。

[0015] 图2是被配置为存储公共和私人加密密钥的示例用户设备的框图。

[0016] 图3是被配置为存储用户设备的公共加密密钥的示例处理平台的框图。

[0017] 图4是示出安全地交换和兑换针对一个记录接收方创建的个体记录的一个实施例的交互图。

[0018] 图5示意性地示出针对一个记录接收方创建的个体记录的一个示例。

[0019] 图6是示出安全地交换和兑换针对两个记录接收方创建的个体记录的一个实施例的交互图。

[0020] 图7示意性地示出针对两个记录接收方创建的示例个体记录。

[0021] 图8示意性地示出针对多个记录接收方创建的示例个体记录。

[0022] 图9是示出安全地交换和兑换涉及代理和接收方的个体记录的一个实施例的交互图。

[0023] 图10示意性地示出涉及代理和记录接收方的示例个体记录。

[0024] 图11是示出安全地交换和兑换涉及查询认可的个体记录的一个实施例的交互图。

[0025] 图12示意性地示出涉及查询认可的示例个体记录。

[0026] 图13是示出从处理平台分发公共记录的一个实施例的交互图。

[0027] 图14示意性地示出用于分发的示例公共记录。

[0028] 图15是示出由记录接收方设备传播公共记录的示例的交互图。

[0029] 图16是示出由记录发送方设备传播公共记录的示例的交互图。

[0030] 图17是示出通过具有多个接收方的发送方克隆的恶意行为的示例的交互图。

[0031] 图18是示出通过具有单个接收方的发送方克隆的恶意行为的示例的交互图。

[0032] 图19是示出通过分叉的恶意行为的示例的交互图。

[0033] 图20是示出通过接收方克隆的恶意行为的示例的交互图。

[0034] 图21是示出通过窥探的恶意行为的示例的交互图。

[0035] 图22是示出通过重影的恶意行为的示例的交互图。

[0036] 图23是示例用户设备的框图。

[0037] 图24是示例处理平台的框图。

[0038] 图25示意性地示出标准交易的示例。

[0039] 图26示意性地示出具有多个卖方的买方克隆的示例。

[0040] 图27示意性地示出具有单个卖方的买方克隆的示例。

[0041] 图28示意性地示出支票分叉的示例。

[0042] 图29示意性地示出卖方克隆的示例。

[0043] 图30示意性地示出用窥探的示例。

[0044] 图31示意性地示出重影的示例。

[0045] 图32示意性地示出销售点(PoS)交易的示例。

[0046] 图33A-33B示意性地示出安全地交换加密签名的数字支票的一个实施例。图33C示意性地示出安全地交换加密签名的数字支票的另一实施例。

[0047] 图34A是示出安全地交换和兑换加密签名的数字支票的一个实施例的交互图。图34B是示出安全地交换和兑换加密签名的数字支票的另一实施例的交互图。

[0048] 图35示意性地示出可穿戴显示系统的示例。

[0049] 在整个附图中,可以重复使用附图标记来指示所引用的元件之间的对应关系。提供附图是为了说明在此描述的示例实施例,并且不旨在限制本公开的范围。

具体实施方式

[0050] 概述

[0051] 在此公开的系统和方法解决了与数字传输和物理交换相关的各种挑战。例如，可以使用混合系统通过网络安全地传输和交换内容和记录。混合系统提供内容或记录的有意义或令人满意的集中式和对等交换。其它优点包括易用性、交换速度、验证能力、安全性、匿名性、不可逆性和不可否认性。

[0052] 在此公开的系统和方法可能面临物理交换可能发生的类似问题。由于虚拟和物理环境的差异，解决了与数字传输相关的各种挑战，诸如可以复制交易工具的非平凡性。公开了基于数字平台上可用的数字工具和技术的特征，例如使用数字加密、传统手写签名的更强大的加密模拟，用于文档的认可。

[0053] 安全地交换加密签名记录的示例

[0054] 图1A示意性地示出安全地交换加密签名的内容和记录(例如加密签名的个体记录100)的一个实施例。记录发送方102a使用记录发送者设备可以创建个体记录100并将其发送到记录接收方102b。记录发送方102a可以是希望向记录接收方102b传送内容或记录的人。记录接收方102b可以是希望从记录发送方102a接收内容或记录的人。

[0055] 记录接收方102b然后使用记录接收者设备可以修改个体记录100以创建修改的个体记录100m1，其中m指示个体记录100已被修改，并且m1指示个体记录100的第一次修改。记录接收方102b可以与服务提供者104兑换修改的个体记录100m1。在服务提供者104操作安全电子处理平台成功地处理个体记录100m1之后，服务提供者104可以向记录接收方102b提供例如由修改的个体记录100m1指示的文档。记录发送方102a和记录接收方102b能够以分布式或分散式(例如，对等)方式交换个体记录100。

[0056] 出于说明的目的，以下示例将描述发送方102a和接收方102b之间的电子记录的交换。应该理解，发送方102a和接收方102b使用物理电子设备来执行电子记录的交换。例如，发送方和接收方电子设备可以包括蜂窝电话、便携式计算设备(例如，膝上型计算机、平板计算机、电子阅读器)、台式计算设备、增强现实设备(例如，头戴式增强、虚拟或混合现实显示器)等等。应该理解，服务提供商104可以使用物理电子设备来处理交换的电子记录。例如，服务提供商电子设备可以包括一个或多个集中式或分布式服务器计算机。

[0057] 记录发送方102a使用其用户设备可以例如使用短距离链路(例如蓝牙链路)以对等方式直接向记录接收方102b发送个体记录100或直接通过系统的另一用户发送。当发送个体记录100时，记录发送方102a和记录接收方102b的用户设备可以在线或离线。例如，记录发送方102a和记录接收方102b的用户设备二者都可以在线并连接到诸如因特网的网络。作为另一个示例，记录发送方102a和记录接收方102b的用户设备中的一者或两者可以离线并且不连接到网络。当记录接收方102b的用户设备与服务提供者104通信时，记录接收方102b可以与服务提供者104兑换修改的个体记录100m1。

[0058] 个体记录100可以是包括多个块的数字对象，该块可以从记录发送方102a发送到记录接收方102b。在一些实施例中，个体记录100可包括块105a。块105a可包括许多组成部分。

[0059] 为了提供交换的安全性，可以在电子记录中使用加密技术。例如，可以使用公钥加密技术，其中交易的每一方(发送方102a和接收方102b)或交易的每个设备(发送方设备和

接收方设备)都与公钥(可以广泛传播)和私钥(仅针对当事方保密和已知)二者相关联。任何发送方都可以使用接收方的公钥针对接收方加密消息,但加密的消息只能由接收方使用接收方的私钥解密。消息的接收方可以通过采用发送方公钥加密回复消息来安全地回复发送方,使得只有发送方可以使用发送方的私钥来解密回复消息。如下面将进一步描述的,发送方和接收方的电子设备可以包括可以安全地存储相应方的私钥并使用传播的公钥执行加密和解密的硬件或软件。公钥加密是非对称加密的示例,其中用于加密的密钥(例如,接收方的公钥)与用于解密的密钥(例如,接收方的私钥)不同。在其它实施例中,可以使用其它不对称加密技术。

[0060] 例如,块105a可以包括“来自字段”中的记录发送方设备的公钥106a、“到字段”中的记录接收方设备的公钥106b、记录标识符(ID)108、内容110以及块105a的记录发送方签名112a。记录发送方设备的公钥106a可以识别个体记录100的发起者,即记录发送方102a。记录接收方设备的公钥106b可以识别个体记录100的接受者,即记录接收方102b。

[0061] 记录ID 108可以增加,例如单调增加,使得由记录发送方设备创建的两个个体记录100不具有相同的记录ID 108。例如,内容110可以识别记录接收方102b在与服务提供者104兑换修改的个人记录100m1时可以接收的文档。服务提供者104可以如内容100自身或通过第三方间接所指示地执行。

[0062] 用户可以通过创建个体记录的安全加密签名来对个体记录100签名。记录发送方102a可以通过创建记录发送方签名112a来使用他的用户设备对个体记录100签名。为了对个体记录100签名,记录发送方设备可以要求记录发送方102a的认证。认证的非限制性示例包括密码短语认证、诸如指纹认证或虹膜认证的生物认证,或生物数据认证。记录发送方签名112a可以是使用加密创建的数字签名。例如,记录发送方设备可以使用诸如Rivest-Shamir-Adleman(RSA)加密的公钥加密来加密诸如个体记录100的安全散列算法(SHA)-2的散列。例如,可以使用具有224、245、384或512位的记录摘要的任何SHA-2散列函数(例如,SHA-256)。可以使用记录发送方设备公钥加密对的私钥来创建记录发送方签名112a。记录发送方设备可以安全地存储私钥。记录发送方签名112a可以被其他人验证为由发送方102a(例如由具有记录发送方设备的公钥106a的记录接收方102b)真实地签名。记录接收方102b可以从个体记录100获得记录发送方设备的公钥106a。一旦创建,记录发送方签名112a就对块105a进行签名。记录发送方设备的公钥106a、记录接收方设备的公钥106b、记录ID 108、内容110和记录发送方签名112a可以完成个体记录100的块105a。

[0063] 一旦具有了记录接收方102b,记录接收方102b就可以向个体记录100添加认可块105b中的认可以创建修改的个体记录100m1。例如,认可可以是“仅用于处理的认可”114,其指定修改的个体记录100m1只能由块105a中的个体记录的接受者(记录接收方102b)兑换。一旦认可,例如添加“仅用于处理的认可”114,记录接收方102b就可以重复针对认可块105b生成记录接收方签名112b以创建修改的个体记录100的过程。记录接收方签名112b可以基于修改的个体记录100m1的一个或多个部分。例如,记录接收方签名112b可以基于认可块105b。作为另一示例,记录接收方签名112b可以基于块105a、认可块105b或其任何组合。修改的个体记录100m1可以电子方式向服务提供者104或向另一方的电子设备传送。

[0064] 因此,个体记录可以包括块链,每个块标识其发起者。在每个块处,链的整个先前部分可以由当时处理块的用户签名。用户可以使用与他的用户设备相关联的私钥来对链的

整个先前部分签名。例如，修改的个体记录100m1可以是包括两个块105a和105b的链。个体记录100的块105a可以包含记录发送方设备的公钥106a，其与记录发送方设备的公钥106a一起可以识别记录发送方102a。记录发送方签名112a可以由使用记录发送方设备公钥加密对的私钥的记录发送方设备来签名。认可块105b可以包含记录接收方签名112b，其与记录接收方设备的公钥106b一起可以识别记录接收方设备。记录接收方签名112b可以由使用记录接收方设备公钥加密对的私钥的记录接收方设备来签名。记录接收方签名112b可以基于认可块105b，或者可以基于认可块105b、在认可块105b之前的一个或多个块(例如块105a)，或其任何组合。

[0065] 个体记录(例如修改的个体记录100m1，其最后一个块包含“仅用于处理认可”(FPOE)114)可以与服务提供者104电子地通信和兑换。在兑换时，服务提供者104可以通过验证块105a和105b链中的一个或多个签名的真实性，处理修改的个体记录100m1。例如，服务提供者104可以验证修改的个体记录100m1中的所有签名(包括记录发送方签名112a和记录接收方签名112b)的真实性。签名的真实性可以指使用特定私钥创建的签名。例如，为了使记录发送方签名112a可信，可以使用记录发送方设备的公钥来验证记录发送方签名112a，并且确定已经使用记录发送方设备的私钥创建记录发送方签名112a。因此，只要记录发送方102a声称他的私钥保持私密，记录发送方102a就不能拒绝由记录发送方设备数字签名的个体记录100。

[0066] 如果内容110包括应该给予记录接收方102b访问例如具有特定ID的文档的指令，并且链中的所有签名被验证为真实的，则可以向在修改的个体记录100m1中链的终点处的记录接收方102b或记录接收方102b的用户设备给出文档。例如，如果验证修改的原始记录100m1中的记录发送方签名112a和记录接收方签名112b是可信的，则服务提供者104可以向记录接收方102b提供例如由内容110指示的文档。记录接收方102b连接到服务提供者104并兑换修改的个体记录100m1的时间构成了兑换事件。

[0067] 记录100的内容110可以包括例如消息、数据、向实体提供文档或其它信息的指令、执行计算机程序的指令、合同义务或权利(例如，智能合约)，转移对价(consideration)(例如货币、加密货币、证券、实物或无形资产等)的指示，等等。某些实施例的优点在于，通过利用不是承载文档的个体记录，可以在双方在中央存管处没有出现的情况下交换大量的对价。

[0068] 在一个非限制性示例中，发送方102a是来自卖方的资产的买方，该卖方是接收方102b。内容110包括服务提供者104将加密货币金额从发送方102a的账户转移到接收方102b的账户的指令。发送方的设备使用发送方设备的私钥对记录100进行数字签名，并将记录100电子地传送给接收方的设备。接收方设备认可具有认可114的记录(例如，在该上下文中，认可可以是“仅用于存款的认可”)并使用接收方设备的私钥对记录进行数字签名以创建修改的记录100m1。接收方设备将修改的记录100m1传送给服务提供者104，该服务提供者104兑换修改的记录100m1。服务提供者104可以验证修改的记录100m1由发送方102a和接收方102b二者(使用它们相应的公钥)真实地签名，并且可以将加密货币金额(在内容110中)从发送方的账户转移到接收方的账户。

[0069] 因此，在该非限制性示例中，记录用作数字支票系统中的支票，并且可以由买方(发送方102a)用于向卖方(接收方102b)支付资产。在一些这种情况下，资产是电子资产(例

如,为买方提供所需功能的计算机代码)。卖方(接收方102b)可以创建具有作为内容的电子资产的记录(类似于记录100)并对其进行数字签名,并将记录电子地传送给买方(发送方102a)。因此,买方和卖方可以相互交换加密安全记录以将资产从卖方转移到买方以作为对价(例如,加密货币金额)的回报。服务提供者104可以充当至少一些该交换的清算所(例如,借记买方的加密货币账户并贷记卖方的加密货币账户)。

[0070] 用于交换加密签名的个体记录的示例系统

[0071] 示例用户设备

[0072] 用于安全地交换本公开的内容和记录的方法和系统可以由一个或多个用户设备和一个或多个处理平台来实施。在图1B中所示的非限制性示例系统中,用户可以操作用户设备来创建、发送、接收、修改或兑换个体记录100。例如,记录发送方102a可以操作记录发送方设备116a,并且记录接收方102b可以操作记录接收方设备116b。

[0073] 用户设备(例如记录发送方设备116a和记录接收方设备116b)可以是相同的或可以是不同的。用户设备可以包括蜂窝电话、平板计算机、电子阅读器、智能手表、头戴式增强、虚拟或混合现实显示系统、可穿戴显示系统或计算机。用户设备116a、116b可以包括下面参考图35描述的可穿戴显示系统3500的实施例。用户设备116a或116b可以使用通信链路120a、120b(例如蜂窝通信链路)与网络118上的其它设备通信。网络118可以是可通过有线或无线通信链路(例如实施电气和电子工程师协会(IEEE)802.11标准)访问的局域网(LAN)、广域网(WAN)或因特网。

[0074] 当发送个体记录100时,记录发送方设备116a和记录接收方设备116b中的一个或二者可以离线并且不连接到网络118。记录发送方102a使用记录发送方设备116a可以使用短程链路(SRL)122向记录接收方102b发送个体记录100。短程链路(SRL)122可以是用户设备116a或116b可以通过其彼此通信的对等无线或其它链路。短程链路(SRL)122可以基于红外数据协会(IrDA)/红外物理层规范(IrPHY)、蓝牙、近场通信(NFC)、ad hoc 802.11或任何其它有线或无线通信方法或系统。

[0075] 由服务提供者104操作的处理平台124可以使用通信链路126与网络118上的其它设备(例如用户设备116a和116b)通信。通信链路120a、120b或126可以是有线或无线通信、蜂窝通信、蓝牙®、局域网(LAN)、广域网(WLAN)、射频(RF)、红外(IR)或任何其它通信方法或系统。用户102a或102b可以用处理平台124兑换个体记录。例如,记录接收方102b使用记录接收方设备116b可以与处理平台124兑换修改的个体记录100m1。

[0076] 图2是被配置为存储公共和私有加密密钥的示例用户设备116的框图。用户设备116可以包括个体记录容器202、安全元件(SE)204和公共记录206。个体记录容器202可以是被配置为包含未兑换的个体记录208的数字数据结构。例如,记录接收方设备116b的个体记录容器202b可以在修改的个体记录100m1被电子地传送到处理平台124并与处理平台124兑换之前包含修改的个体记录100m1。

[0077] 安全元件(SE)204可以安全地存储用户设备的私钥210和服务提供者公钥212。安全元件(SE)204可以使用用户设备的私钥212来对个体记录100和修改的个体记录100m1签名。例如,记录发送方设备116a的安全元件(SE)204a可以创建个体记录100的记录发送方签名112a。作为另一示例,记录接收方设备116b的安全元件(SE)204b可以创建修改的个体记录100m1的记录接收方签名112b。在一些实施例中,记录发送方设备116a的安全元件(SE)

204a可以添加记录发送方设备的公钥106a、记录接收方设备的公钥106b、记录ID 108以及到个体记录100的内容110中的一个或多个。

[0078] 安全元件(SE)204可以使用服务提供者公钥212来验证从服务提供者104接收的信息的真实性。例如,服务提供者104使用处理平台124可以向用户设备116a或116b发送设备214的更新的公钥。处理平台124可以采用服务提供者公钥加密对的私钥对设备214的公钥进行签名。在一些实施例中,服务提供者私钥是服务提供者具有独占的。安全元件(SE)204可以验证设备214的更新的公钥的真实性。验证设备214的更新的公钥的真实性可以包括使用服务提供者公钥212确定设备214的公钥的签名是否已经采用服务提供者公钥创建。在一些实施例中,可以存在两个或更多个独立操作的处理平台124。并且用户设备116可以包括用于两个或更多个处理平台124的一个或多个服务提供者公钥212。

[0079] 公共记录206可以包括关于服务提供者处理平台124的用户的有效用户身份和附加信息。公共记录206在处理平台124的用户之间公开传播和共享。例如,公共记录206可以包括由系统传播的用户设备214的公钥,使得其他用户可以加密地验证数字签名。记录发送方设备116a的公共记录206a中的用户设备214a的公钥和记录接收方设备116b的公共记录206b中的用户设备214b的公钥可以相同或可以不同。参考图1B,为了使记录发送方116a使用新的用户设备116a2,处理平台104可能必须向系统的其他用户设备116通知用户设备116'的公钥。当其他用户设备116连接到网络118时,处理平台124可以向其他用户设备116发送包括设备214的更新的公钥(包括用户设备116'的公钥)的更新公共记录206。如果用户设备116a连接到网络118并且用户设备116b没有连接,则用户设备116a可以接收设备214a的更新的公钥。因此,用户设备116b的公共记录206b中的设备214b的公钥可以是用户设备116a的公共记录206a中的设备214a的更新的公钥的子集。

[0080] 在一些实施例中,一些公钥可能不再使用,并且可以由处理平台124从设备214的公钥中移除。例如,如果记录发送方102a不再使用记录发送方设备116a,处理平台124可以从处理平台的记录中删除记录发送方设备的公钥106a。处理平台124可以向其他用户设备116发送设备214的更新公钥(其排除记录发送方设备的公钥106a)。为了保持加密安全性,如果不再使用记录发送方设备116a,则应永久删除设备私钥210或销毁设备。

[0081] 用户设备可以使用用户设备214的公钥来验证所接收的个体记录的真实性。例如,记录接收方设备116b的公共记录206b中的用户设备214b的公钥可以包括记录发送方设备的公钥106a。并且记录接收方设备116b可以通过使用记录发送方设备的公钥106a确定是否已经使用记录发送方设备116a的私钥创建了个体记录112a的记录签名112a来验证个体记录100的真实性。

[0082] 示例处理平台

[0083] 图3是被配置为存储用户设备的公共加密密钥的示例处理平台124的框图。处理平台124可以包括可以是系统基础结构的服务器或服务器集合。处理平台124可以直接连接到网络118,并且可以通过网络118间接地并且可能仅间歇地连接到用户设备116。处理平台124可以包含和维护中央记录302以跟踪用户、用户设备116并访问记录中识别的内容。处理平台124可以处理在记录100的内容110中包含的指令。例如,如上所述,如果记录100的内容110包含在用户帐户之间转移加密货币的指令,则平台124可以在兑换记录时执行转移。

[0084] 处理平台124可以维护公共记录206或者可以从中央记录302中生成公共记录206。

中央记录302可以包含设备214的公钥。用户设备116的公共记录206中的设备214的公钥可以是中央记录302中的用户设备214的公钥的子集。例如，用户设备214的公钥可能已被更新，并且用户设备116可能尚未接收到用户设备214的更新的公钥。

[0085] 中央记录302可以包括用户102a或102b或用户设备116a或116b的识别信息和辅助信息。中央记录302可以包括可以识别用户与用户设备的关联的用户信息304。例如，中央记录302可以包括记录发送方102a与两个记录发送方设备116a和116a'的关联。在一些实施例中，具有多个设备的一个用户可以被认为是多个用户。在一些实施例中，具有多个设备的一个用户可以被认为是一个用户。公共记录206可以不包含用户信息304。

[0086] 中央记录302可以包括用于跟踪用户信息的用户记录状态306。例如，个体记录100的内容110可以指示处理平台124向记录接收方102b提供对具有存储在内容110中的其文档ID的文档的访问。然而，用户记录状态306可以指示只有记录发送方102a自身可以访问该文档；并且记录发送方102a不能授权其他用户访问该文档。作为另一示例，用户记录状态306可以指示记录发送方102a可以向其他用户提供对文档的访问。作为另一示例，用户记录状态306可以指示记录发送方102a可以仅多次(诸如一次)向用户提供对文档的访问；并且用户记录状态306可以保持跟踪个体记录100是否已被任何用户(例如记录接收方102b)兑换和访问。

[0087] 作为非限制性示例，用户记录状态306可以跟踪记录发送方的(例如加密货币中)帐户余额。记录发送方的帐户可以是付款方帐户。如果个体记录100的内容110指示处理平台124向记录接收方102b支付小于或等于记录发送方的帐户余额的金额，则处理平台124可以将记录发送方的帐户借记指定的金额并将记录接收方的帐户贷记相同的金额。记录接收方的帐户可以是收款方帐户。如果个体记录100的内容110指示处理平台124向记录接收方102b支付大于记录发送方的帐户余额的金额，则处理平台124可以拒绝将记录接收方的帐户贷记指定的金额。然而，记录发送方的帐户可能会以透支费用借记。公共记录206可以不包含用户记录状态306。

[0088] 在此公开的加密签名的个体记录的交换可包括许多益处。益处包括例如易用性或交换速度。如图1中所示，记录发送方设备116a可以经由短程链路(SRL)122向记录接收方设备116b发送个体记录100，而没有任何一方通过网络118与服务提供者104通信。附加或替代的益处可以包括例如，数字签名的验证或认证的能力。如图2中所示，用户设备的公钥214在公共记录206中传播。因此，记录接收方设备116b可以验证个体记录100中的记录发送方签名112a的真实性，并且记录发送方设备116a已经发送了个体记录100。另一个益处可以是例如加密安全性。如图1A中所示，记录发送方设备116a可以用记录发送方签名112a对个体记录100进行签名，并且记录接收方设备116b可以用记录接收方签名112b对修改的个体记录100m1进行签名。不是记录接收方设备116b的恶意用户设备不能伪造记录接收方签名112b，因为它们不知道记录接收方私钥。恶意用户设备不能与处理平台124兑换修改的个体记录100m1，因为个体记录100示出其接受者是记录接收方设备116b而不是恶意用户设备。附加或替代的益处可以包括例如匿名(不需要使用实际的法定名称，仅需要用户识别与公钥相关联的信息)，或不可否认性(数字签名可以使用公钥进行认证，并且签名者在声称他的私钥仍然私密时不能否认签名)。另一个益处可以是例如不可逆性。一旦记录发送方设备116a向记录接收方设备116b发送个体记录100，处理平台124就可以拒绝如记录发送方设备116a

请求处理平台124不按照个体记录的内容110的所指示的执行。另一个益处可以是，例如，个体记录100可以包括不同的内容110。此外，记录发送方102a可以使记录接收方102b访问大量信息，例如具有存储在个体记录100的内容110中的ID的文档，而不直接向记录接收方102b发送信息。

[0089] 示例的一个接收方

[0090] 在一些实施例中，记录接收方可以从记录发送方接收个体记录。图4是示出安全地交换和兑换针对一个记录接收方创建的个体记录的一个实施例的交互图。记录接收方102b使用记录接收方设备116b可以通过向记录发送方设备116a发送内容请求402来从记录发送方102a请求个体记录100。记录接收方102b可以在交互404处使用短程链路(SRL)122向记录发送方102a发送内容请求402。内容请求402可以包括内容(例如内容B 110b)和记录接收方设备的公钥106b。内容B 110b可以包括对例如具有存储在内容B 110b中的其文档ID的文档的请求。在一些实施例中，记录接收方设备的公钥106b可以唯一地识别记录接收方设备116b。在一些实施例中，记录接收方设备的公钥106b可以唯一地识别记录接收方102b。在一些实施例中，公钥106b可以位于可以存储在安全元件(SE)204b中的公共记录中。

[0091] 示例伙伴标识

[0092] 参考图4，在交互408处，记录发送方设备116a使用其交易伙伴标识符可以通过伙伴标识来确认记录接收方设备116b的标识。因为内容请求402可能已经电子地发送到记录发送方设备116a，所以记录发送方设备116a可能不确定发送内容请求402的用户设备的标识。伙伴标识可能是有利的。例如，利用伙伴标识，记录发送方设备116a可以将内容请求402与记录接收方设备116b和恶意用户区分开。作为另一示例，通过伙伴标识，恶意用户不能接收不是针对它的个体记录。作为又一示例，通过伙伴标识，恶意用户即使在接收到不是针对它的个体记录之后也不能兑换个体记录。

[0093] 示例个体记录创建

[0094] 图5示意性地示出针对一个记录接收方创建的一个示例个体记录。如图4-5中所示，在记录发送方设备116a的安全元件(SE)204a验证记录发送方的认证信息512a之后，安全元件(SE)204a可以在交互416处对个体记录100进行签名。在交互416处对个体记录100签名之前，安全元件(SE)204a可以要求提供要被数字签名的块(例如个体记录100的块105a)以及记录发送方102a的认证二者。认证的非限制性示例可以包括密码认证、诸如指纹认证或虹膜认证的生物认证、生物数据认证或其任何组合。生物度量认证可以利用基于例如指纹或眼睛图像的生物特征模板。安全元件(SE)204a可以实施用于识别生物度量模板的生物度量模糊库。

[0095] 个体记录100可以是包括一个或多个块的数字对象。个体记录100可以包括块105a，并且块105a可以包括“来自字段”中的记录发送方设备的公钥106a、“到字段”中的记录接收方设备的公钥106b、记录ID 108、内容A 110a以及块105a的记录发送方签名112a。记录发送方设备的公钥106a可以识别个体记录100的发起者，即记录发送方设备116a。记录接收方设备的公钥106b可以识别个体记录100的原始接受者，即记录接收方设备116b。内容A 110a的内容可以变化。内容A 110a和内容B A 110b可以相同、类似、相关或不同。内容A 110a可以与内容B 110b相同，例如特定文档。内容A 110a可以与内容B 110b类似或相关。例如，内容B110b可以请求访问文档，并且内容A 110a可以授权访问文档。作为另一示例，内容

B 110b可以请求访问两个文档，并且内容A 110a可以授权仅访问两个文档。如上所述，在加密货币的情境中，内容A 110a和内容B 110b可以是相同金额的加密货币。内容A 110a和内容B 110b可以类似或相关。例如，内容B 110b可以是税前金额，并且内容A 110a可以是税后金额。作为另一示例，内容B 110b可以是预付小费(pre-tip)金额，并且内容A110a可以是已付小费(after-tip)金额。

[0096] 参考图4，在交互420处，记录发送方102a可以例如使用短程链路(SRL)以对等方式向记录接收方102b发送个体记录100。一旦具有了记录接收方102b，记录接收方102b就可以在交互424处验证个体记录100。验证个体记录100可以包括认证记录发送方签名112a。认证记录发送方签名112a可以包括使用记录发送方设备的公钥106a确定是否已经使用记录发送方设备的私钥210创建了记录发送方签名112a。记录发送方设备的公钥106a可以通过多种方式获得。例如，记录发送方设备的公钥106a可以从个体记录100中获得。作为另一示例，记录发送方设备的公钥106a可以从记录接收方设备116b的公共记录206中获得。

[0097] 示例个体记录兑换

[0098] 参考图4，在成功验证个体记录100之后，记录接收方设备116b可以使用其安全元件204b在交互428处创建修改的个体记录100m1并对其签名。在交互428处对修改的个体记录100m1签名之前，安全元件(SE)204b可以要求提供要被数字签名的块(例如修改的个体记录100m1的块105b)以及记录接收方的认证信息512b。修改的个体记录100m1可以包括个体记录100的块105a和认可块105b。例如，认可可以是“仅用于处理的认可”(FPOE)114，其与记录接收方的公钥106b一起指定修改的个体记录100m1只能由记录接收方102b兑换。如上所述，在加密货币的情境中，FPOE认可的示例包括“仅用于存款的认可”(FDOE)，其中处理平台124将加密货币金额存入记录接收方102b的账户但是将不承认对另一方的进一步认可。

[0099] 在对修改的个体记录100m1签名之后，当记录接收方102b通过例如网络与处理平台124通信时，记录接收方102b可以在交互432处与处理平台124兑换修改的个体记录100m1。在兑换时，操作处理平台124的服务提供者104可以通过验证修改的个体记录100m1中的块105a和105b链中的一个或多个签名(例如记录发送方签名112a和记录接收方签名112b)的真实性，在交互436处处理修改的个体记录100m1。在成功验证之后，处理平台124可以如修改的个体记录100m1的内容A 110a所指示地执行。

[0100] 发送方设备116a可以接收处理平台124已经或尚未如修改的个体记录100m1的内容A 110a所指示地执行的指示。例如，处理平台124可以向发送方设备116a发送电子邮件，该电子邮件指出处理平台124已经如修改的个体记录100m1的内容A 110a所指示地执行。作为另一示例，处理平台124可以向发送方设备116a发送电子消息，该电子消息指出处理平台124没有如修改的个体记录100m1的内容A 110a所指示地执行，因为内容A 110a指示处理平台124向记录接收方设备116b提供存储在存储库中的文档，并且存储库暂时或永久不可用。作为另一示例，处理平台124可以周期性地(诸如每小时、每天、每周、每月或每年)向发送方设备116a提供其用户记录状态306。当满足一个或多个条件(诸如记录发送方设备116不再能够使另一个用户设备访问文档)时，处理平台124可以向发送方设备116a提供其用户记录状态306。

[0101] 示例伙伴标识

[0102] 伙伴标识可以基于各种方法。用于伙伴标识的方法的非限制性示例包括内容授

权、敲击(knocking)、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0103] 示例内容授权

[0104] 在一些实施例中，伙伴标识可以包括内容授权。利用内容授权，记录发送方102a可以基于内容请求402中的公钥106b向记录接收方设备116b发出交换个体记录的意图。交换个体记录的意图的内容可以变化。例如，交换个体记录的意图的内容可以是空的，或者可以包含一个或多个零值。在记录接收方设备116b接收到交换个体记录的意图之后，记录接收方102b可以通过非电子手段确认他是交换个体记录的意图的接受者。例如，记录接收方102b可以口头通知记录发送方102a他已经接收到交换个体记录的意图。作为另一示例，记录接收方102b可以通知记录发送方102a他已经接收到以电子方式交换个体记录的意图。在确认之后，可以验证来自记录接收方102b的内容请求402，并且记录发送方102a可以向记录接收方设备116b发送具有适当内容的个体记录100。

[0105] 示例敲击

[0106] 在一些实施例中，伙伴标识可包括敲击。记录发送方设备116a和记录接收方设备116b每个可包括运动传感器。利用敲击，记录发送方设备116a和记录接收方设备116b可以进行物理接触。这种接触可以由记录发送方设备116a和记录接收方设备116b的运动传感器测量。接触以及发送和接收内容请求402的相对定时可以变化。例如，记录接收方设备116b可以在接触时(例如，在“敲击”时)发送内容请求402。作为另一示例，记录接收方设备116b可以在接触之后不久(例如，在10秒、20秒、30秒、1分钟、10分钟等的阈值时间内)发送内容请求402。如果内容请求未在阈值时间内发送，则伙伴标识可能要求再次敲击设备。

[0107] 记录发送方设备116a可以基于接触的时间并发和内容请求402的接收来接受内容请求402。在一些实施例中，记录接收方设备116b可以向记录发送方设备116a发送接触签名。可以使用记录接收方设备公钥加密对的私钥来创建接触的签名。接触的签名可以基于由记录接收方设备116b的运动传感器测量的接触和测量的接触的定时。接触的签名可以是内容请求402的一部分，或者可以是从记录接收方设备116b到记录发送方设备116a的单独通信。因为接触可以在记录发送方设备116a中产生相等且相反的反应，所以记录发送方设备116a可以验证接触的签名。

[0108] 示例物理指示

[0109] 在一些实施例中，伙伴标识可包括物理指示。记录发送方设备116a和记录接收方设备116b可包括成像传感器(例如，数码相机)。记录发送方设备116a和记录接收方设备116b可以被定向成使用它们的成像传感器彼此“看到”。记录接收方设备116b可以向记录发送方设备116a发送其捕获的记录发送方设备116a的图像。图像可以是内容请求402的一部分，或者可以是从记录接收方设备116b到记录发送方设备116a的单独通信。因为记录发送方设备116a的图像和记录接收方设备116b的图像可以彼此相反，所以记录发送方设备116a可以通过图像的定性或定量比较来确认记录接收方设备116b的标识。例如，如果记录发送方设备116a“看到”记录接收方设备116b向上和向左，则记录接收方设备116b应该看起来在由记录接收方设备116b捕获的记录发送方设备116a的图像中向下和向右。

[0110] 在一些实施例中，物理指示可以基于记录发送方设备116a和记录接收方设备116b的环境的同时观察。记录发送方设备116a和记录接收方设备116b可以包括麦克风。物理指示可以基于记录发送方设备116a和记录接收方设备116b的麦克风对环境的同时音频记录。

记录发送方设备116a和记录接收方设备116b二者都可以使用麦克风同时“听到”它们的环境。记录接收方设备116b可以向记录发送方设备116a发送其捕获的其环境的音频记录和记录的时间。音频记录可以是内容请求402的一部分，或者可以是从记录接收方设备116b到记录发送方设备116a的单独通信。因为由记录接收方设备116b发送的声音记录可以与记录发送方设备116a同时“听到”的声音记录相同或类似，所以记录发送方设备116a可以通过声音记录的定性或定量比较以及它“听到”的内容来确认记录接收方设备116b的标识。作为另一个示例，物理指示可以基于记录发送方设备116a和记录接收方设备116b彼此的同时音频观察。作为另一示例，物理指示可以基于记录发送方设备116a和记录接收方设备116b对环境的同时视觉观察。

[0111] 示例波束成形

[0112] 在一些实施例中，伙伴标识可包括波束成形。用户设备116可以包括定向(例如，使用波束成形或定向天线)的短程链路(SRL)接口。记录发送方设备116a和记录接收方设备116b可以使它们的短程链路(SRL)接口彼此指向。利用波束成形，记录发送方设备116a可以接收来自记录接收方设备116b的内容请求402，而不是从例如恶意用户的其它方向发送的其它内容请求。利用波束成形，只有记录发送方设备116a而不是其他用户可以从记录接收方设备116b接收内容请求402。

[0113] 示例在先布置

[0114] 在一些实施例中，伙伴标识可包括在先布置。例如，记录发送方设备116a可以在从记录接收方设备116b接收内容请求402之前具有记录接收方设备的公钥106b的先验知识。作为另一示例，记录发送方设备116a可以具有公钥106b的记录接收方设备将向其发送内容请求(例如内容请求402)的先验知识。例如，发送方102a可能先前已经告知接收方102b记录将被发送。接收方102b可以利用接收方设备116b上的用户接口(UI)来提供预期记录来自发送方设备116a(例如，在阈值时间段内)的指示。

[0115] 示例粗略验证

[0116] 在一些实施例中，伙伴标识可以包括粗略验证。例如，公共记录206可以包含识别字符串，例如BigBoxStore，其可以用于内容请求402的粗略验证。作为其中接收方102b是商家的示例，记录接收方102b可以被识别为公共记录206中的商家。该标识可以与公共记录206中标识已经由处理平台124验证的指示(例如位)相关联。这种验证的标识可以与所分配的或由用户自己提供的标识区分开。

[0117] 示例内容和交换

[0118] 个体记录100的内容110可以变化。例如，内容110可以包括用于向记录接收方102b提供其文档ID存储在内容110中的文档的指令。作为另一个示例，内容110可以包括用于向记录接收方102b支付特定数量的货币单位(例如美元)的指令。支付可以是例如国家货币、法定货币、商品或商品货币、加密货币、金融产品或证券(例如股票或债券)或其任何组合的形式。

[0119] 个体记录100的内容110可以包含软件代码。当满足某些条件时，处理平台124可以执行软件代码。条件可以是基于时间的，诸如记录接收方102b兑换包含软件代码的个体记录100的时间。内容110可以包括自执行软件代码。当满足某些条件时，自执行代码可以自动执行。在一些实施例中，例如，当检测到诸如欺诈的特定条件时，用户可以防止或延迟软件

代码的执行。在一些实施例中，用户可能无法阻止或延迟软件代码的执行。

[0120] 个体记录100的内容110可以包括发送方和接收方之间的合同义务或权利(例如，智能合约)。例如，记录接收方102b可以承担执行诸如备份记录发送方的计算机基础架构的服务的合同义务，并且可以具有接收服务支付的合同权利；并且记录发送方102a可以承担向服务的记录接收方102b支付的合同义务，并且可以具有接收记录接收方执行的合同权利。智能合约可以在个人用户、合作伙伴、公司或集团之间进行。智能合约可能涉及软件代码的重复执行。软件代码可以包括可以在满足某些条件时执行的软件代码。作为示例，软件代码可以包括用于接收方的计算机基础架构的备份或安全扫描的软件代码。软件代码可能在条件发生时执行(例如，将每月支付的加密货币转移给发送方)。在一些实施例中，智能合约可以在满足某些条件时涉及经常性支付。例如，智能合约可能要求记录接收方102b定期(诸如每周)备份记录发送方的计算机基础架构。当满足周期执行的条件时，记录发送方102a在智能合约下具有合同义务以定期支付记录接收方102b。

[0121] 内容110可以涉及第三方托管。例如，记录发送方102a和记录接收方102b想要交换诸如软件代码的代码。在向存储库(例如处理平台124)提供第一软件代码之后，记录发送方102a可以向记录接收方102b提供第一个体记录100，如果满足第一条件，则指示存储库向记录接收方102b提供第一软件代码。类似地，原始记录接收方102b可以向原始记录发送方102a提供第二个体记录100m1，如果满足第二条件，则指示存储库向原始记录发送方102a提供第二软件代码。第一条件和第二条件可以基于时间。第一条件和第二条件可以相同或不同。

[0122] 在一些实施例中，记录发送方102a可以向记录接收方102b提供作为交换的一部分的个体记录100。例如，个体记录的内容110可以指示处理平台124以第一金额借记记录发送方的帐户，并以第二金额贷记记录接收方的帐户。帐户借记和贷记可以伴随记录接收方102b，向记录发送方102a提供例如产品或一些代码。

[0123] 示例两个接收方

[0124] 示例第一内容请求

[0125] 在一些实施例中，在从记录发送方接收到个体记录之后，记录接收方可以向后续记录接收方发送所接收的个体记录。图6是示出安全地交换和兑换针对两个记录接收方创建的个体记录的一个实施例的交互图。如图4-5中所示，第一记录接收方102b使用第一记录接收方设备116b可以通过在交互404处向第一记录发送方设备116a发送第一内容请求402来从第一记录发送方102a请求个体记录。第一内容请求402可以包括内容B 110b和第一记录接收方设备的第一公钥106b。

[0126] 在交互408处，第一记录发送方设备116a可以通过伙伴标识来确认第一记录接收方设备116b的标识。在第一记录发送方设备116a的安全元件(SE)204a验证第一记录发送方的认证信息512a之后，安全元件(SE)204a可以在交互416处对个体记录100进行签名。

[0127] 图7示意性地示出针对两个记录接收方创建的示例个体记录。如图6-7中所示，个体记录100可以是包括块105a的数字对象。块105a可以包括“来自字段”中的第一记录发送方设备的第一公钥106a、“到字段”中的第一记录接收方设备的第一公钥106b、记录ID 108、内容A 110a以及块105a的第一记录发送方签名112a。

[0128] 在交互420处，第一记录发送方102a可以使用短程链路(SRL)122以例如对等方式

向第一记录接收方102b发送个体记录100。一旦具有第一记录接收方102b，第一记录接收方102b可以在交互424处验证个体记录100。

[0129] 示例第二内容请求

[0130] 参考图6，第二记录接收方使用记录接收方设备可以通过在交互604处使用短程链路(SRL)122向记录发送方设备发送内容请求来从记录发送方请求个体记录。例如，第二记录接收方102c使用第二记录接收方设备116c可以通过向第一记录接收方设备116b发送第二内容请求602来从第一记录接收方102b请求个体记录。第一记录接收方102b可以是第二记录发送方，并且第一记录接收方设备116b可以称为第二记录发送方设备。第二内容请求602可以包括内容(例如内容C 110c)和第二记录接收方设备的公钥106c。

[0131] 在交互608处，第二记录发送方设备116b可以通过伙伴标识来确认第二记录接收方设备116c的标识。在第二记录发送方设备/第一记录接收方设备116b的安全元件(SE)204b验证第二记录发送方的认证信息512b之后，由于各种原因和目的，第二记录发送方设备116b可以在签名之后决定向第二记录接收方设备116c发送第一修改记录100m1。例如，第二记录接收方102c可以是第二记录发送方102b的受让人。代替如内容A110a所指示地执行第一记录接收方/第二记录发送方102b的处理平台124，处理平台124可以执行第二记录接收方102c。内容A 110a、内容B 110b和内容C 110c可以相同、类似、相关或不同。

[0132] 安全元件(SE)204b可以在交互612处对第一修改的个体记录100m1进行签名。对第一修改的个体记录100m1进行签名可以包括将块(例如块105b)添加到个体记录100以创建第一修改的个体记录100m1。第一修改的个体记录100m1的块105b可以包括第二记录接收方设备的第二公钥106c和块105b的第二记录发送方签名/第一记录接收方签名112b。

[0133] 在交互616处，第二记录发送方102b可以例如使用短程链路(SRL)122以对等方式向第二记录接收方102c发送第一修改的个体记录100m1。一旦具有第二记录接收方102c，则第二记录接收方102c可以在交互620处验证第一修改的个体记录100m1。验证第一修改的个体记录100m1可以包括例如使用第一修改的个体记录100m1中的第一记录发送方设备的公钥106a和第二记录发送方设备的公钥106b来认证第一记录发送方签名112a和第二记录发送方签名112b。

[0134] 示例个体记录兑换

[0135] 参考图6，在成功验证第一修改的个体记录100m1之后，第二记录接收方设备116c可以使用其安全元件(SE)204c在交互624处创建第二修改的个体记录100m2并对其签名，其中m指示个体记录100已被修改，并且m2指示个体记录100已被修改至少两次。在对第二修改的个体记录100m2签名之前，安全元件(SE)204c可以要求提供要被数字签名的块(例如第二修改的个体记录100m2的块105c)以及第二记录接收方的认证信息512c两者。第二修改的个体记录100m2可以包括个体记录100的块105a、第一修改的个体记录的块105b以及认可块105c。例如，认可可以是“仅用于处理的认可”(FPOE)114，其与记录接收方设备的公钥106c一起指定第二修改的个体记录100m2只能由第二记录接收方102c兑换。

[0136] 在对第二修改的个体记录100m2签名之后，第二记录接收方102c可以在交互628处与处理平台124兑换第二修改的个体记录100m2。在兑换时，操作处理平台124的服务提供者104可以通过验证第二修改的个体记录100m2中的块105a、105b和105c链中的一个或多个签名的真实性来在交互632处处理第二修改的个体记录100m2。验证的签名可包括第一记录发

送方签名112a、第二记录发送方签名/第一记录接收方签名112b以及第二记录接收方签名112c。在成功验证之后，处理平台124可以如第二修改的个体记录100m1的内容A 110a所指示地执行。

[0137] 示例N个接收方

[0138] 在一些实施例中，在从记录发送方接收到个体记录之后，记录接收方可以向后续记录接收方发送所接收的个体记录。后续记录接收方进而可以向另一个记录接收方发送它已接收的个体记录。最后一个记录接收方可以与处理平台兑换它已接收的个体记录。记录链中的发送方/接收方的数量N可以是2、3、4、5、6、10、20、100或更多。

[0139] 示例第一内容请求

[0140] 图8示意性地示出针对多个记录接收方创建的示例个体记录。如图4-7中所示，第一记录接收方102b使用第一记录接收方设备116b可以通过使用短程链路(SRL)122向第一记录发送方设备116a发送第一内容请求来从第一记录发送方102a请求个体记录。第一内容请求可以包括内容B和第一记录接收方设备的第一公钥106b。

[0141] 第一记录发送方设备116a可以通过伙伴标识来确认第一记录接收方设备116b的标识。在第一记录发送方设备116a的安全元件(SE)204a验证第一记录发送方的认证信息512a之后，安全元件(SE)204a可以在交互416处对个体记录100进行签名。

[0142] 个体记录100可以是包括块105a的数字对象。块105a可以包括“来自字段”中的第一记录发送方设备的第一公钥106a、“到字段”中的第一记录接收方设备的第一公钥106b、记录ID 108、内容A 110a以及块105a的第一记录发送方签名112a。

[0143] 第一记录发送方102a可以使用短程链路(SRL)122以例如对等方式向第一记录接收方102b发送个体记录100。一旦具有第一记录接收方102b，第一记录接收方102b就可以验证个体记录100。

[0144] 示例第二内容请求

[0145] 参考图8，第二记录接收方使用记录接收方设备可以通过使用短程链路(SRL)122向记录发送方设备发送内容请求来从记录发送方请求个体记录。例如，第二记录接收方102c使用第二记录接收方设备116c可以通过使用短程链路(SRL)122向第二记录发送方设备116b发送第二内容请求来从第二记录发送方102b请求个体记录。第一记录接收方102b可以是第二记录发送方，并且第一记录接收方设备116b可以被称为第二记录发送方设备。第二内容请求可以包括内容C和第二记录接收方设备的公钥106c。

[0146] 第二记录发送方设备/第一记录接收方设备116b可以通过伙伴标识来确认第二记录接收方设备116c的标识。在第二记录发送方设备/第一记录接收方设备116b的安全元件(SE)204b验证第二记录发送方的认证信息512b之后，第二记录发送方设备116b可以在签名之后决定向第二记录接收方设备116c发送第一修改记录100m1。

[0147] 第二记录发送方设备116b的安全元件(SE)204b可以在交互612处对第一修改的个体记录100m1进行签名。对第一修改的个体记录100m1进行签名可以包括将块(例如块105b)添加到个体记录100以创建第一修改的个体记录100m1。第一修改的个体记录100m1的块105b可以包括块105b的第二记录接收方设备的第二公钥106c和第二记录发送方签名/第一记录接收方签名112b。

[0148] 第二记录发送方102b可以使用短程链路(SRL)122以例如对等方式向第二记录接

收方102c发送第一修改的个体记录100m1。一旦具有第二记录接收方102c，第二记录接收方102c可以验证第一修改的个体记录100m1。验证第一修改的个体记录100m1可以包括使用例如第一修改的个体记录100m1中的第一记录发送方设备的公钥106a和第二记录发送方设备的公钥106b来认证第一记录发送方签名112a和第二记录发送方签名112b。

[0149] 示例第三内容请求

[0150] 参考图8，第三记录接收方使用第三记录接收方设备可以通过使用短程链路(SRL)122向记录发送方设备发送内容请求来从记录发送方请求个体记录。例如，第三记录接收方使用第三记录接收方设备可以通过使用短程链路(SRL)122向第三记录发送方设备116c发送第三内容请求来从第三记录发送方请求个体记录。第二记录接收方102b可以是第三记录发送方，并且第二记录接收方设备116b可以被称为第三记录发送方设备。第三内容请求可以包括内容和第三记录接收方设备的公钥。

[0151] 第三记录发送方设备116c可以通过伙伴标识来确认第三记录接收方设备的标识。在第三记录发送方设备/第二记录接收方设备116c的安全元件(SE)204c验证第三记录发送方的认证信息512c之后，第三记录发送方设备可以在签名之后向第三记录接收方设备发送第二修改记录100m2。

[0152] 安全元件(SE)204c可以在交互624处对第二修改的个体记录100m2进行签名。对第二修改的个体记录100m2进行签名可以包括将块(例如块105c)添加到第一修改的个体记录100m1以创建第二修改的个体记录100m2。第二修改的个体记录100m2的块105c可以包括块105c的第二记录接收方设备的第三公钥106c和第三记录发送方签名/第二记录接收方签名112c。

[0153] 第三记录发送方102c可以使用短程链路(SRL)122以例如对等方式向第三记录接收方发送第二修改的个体记录100m2。一旦具有第三记录接收方，第三记录接收方可以验证第二修改的个体记录100m2。验证第二修改的个体记录100m2可以包括使用例如第二修改的个体记录100m2中的第一记录发送方设备、第二记录发送方设备和第三记录发送方设备的公钥106a、106b和106c认证第一记录发送方签名112a、第二记录发送方签名/第一记录接收方签名112b和第三记录发送方签名/第二记录接收方签名112c。

[0154] 示例第n个内容请求

[0155] 参考图8，第n个记录接收方使用第n个记录接收方设备可以通过使用短程链路(SRL)122向第n个记录发送方设备发送第n个内容请求来从第n个记录发送方请求个体记录。第n个记录发送方可以是第(n-1)个记录接收方，并且第(n-1)个记录接收方设备可以被称为第n个记录发送方设备。第n个内容请求可以包括内容和第n个记录接收方设备的公钥。

[0156] 第n个记录发送方设备可以通过伙伴标识来确认第n个记录接收方设备的标识。在第n个记录发送方设备/第(n-1)个记录接收方设备的安全元件(SE)验证第n个记录发送方的认证信息之后，第n个记录发送方设备可以在签名之后向第n个记录接收方设备发送第(n-1)个修改记录100m(n-1)，其中m指示个体记录100已被修改，并且m(n-1)指示个体记录100已被修改至少(n-1)次。

[0157] 第n个记录发送方设备的安全元件(SE)可以对第(n-1)个修改的个体记录100m(n-1)进行签名。对第(n-1)个修改的个体记录100m(n-1)进行签名可以包括将块105(n-1)添加到第(n-2)个修改的个体记录以创建第(n-1)个修改的个体记录100m(n-1)。第(n-1)个修改

的个体记录100m(n-1)的块105(n-1)可以包括块105(n-1)的第n个记录接收方设备的第n个公钥106n和第n个记录发送方签名/第(n-1)个记录接收方签名112(n-1)。

[0158] 第n个记录发送方可以使用短程链路(SRL)122以例如对等方式向第n个记录接收方发送第(n-1)个修改的个体记录100m(n-1)。一旦具有第n个记录接收方,第n个记录接收方就可以验证第(n-1)个修改的个体记录100m(n-1)。验证第(n-1)个修改的个体记录100m(n-1)可以包括使用例如第(n-1)个修改的个体记录100m(n-1)中的第一记录发送方设备112a,第二记录发送方设备112b,第三记录发送方设备112c,...,以及第n个记录发送方设备的公钥来认证第一记录发送方签名112a,第二记录发送方签名112b,....,以及第(n-1)个记录发送方签名112(n-1)。

[0159] 示例个体记录兑换

[0160] 参考图8,在成功验证第(n-1)个修改的个体记录100m(n-1)之后,第n个记录接收方设备可以使用其安全元件创建第n个修改的个体记录100mn并对其签名,其中m指示个体记录100已被修改,并且mn指示个体记录100已被修改至少N次。在对第n个修改的个体记录100MM进行签名之前,安全元件(SE)可以要求提供要被数字签名的块(例如第n个修改的个体记录100mn的块105n)以及第n个记录接收方的认证信息。第n个修改的个体记录100mn可以包括认可块105n。例如,认可可以是“仅用于处理的认可”(FPOE)114,其与第n个修改的个体记录100mn中的公钥一起指定第n个修改的个体记录100mn只能由第n个记录接收方兑换。

[0161] 在对第n个修改的个体记录100mn进行签名之后,第n个记录接收方可以与处理平台兑换第n个修改的个体记录100mn。在兑换时,操作处理平台的服务提供者可以通过验证第n个修改的个体记录100mn中的块105a,105b,105c,...,105(n-1)和105n的链中的签名的真实性来处理第n个修改的个体记录100mn。在成功验证之后,处理平台124可以如第n个修改的个体记录100mn的内容A 110a所指示地执行。

[0162] 代理和记录接收方之间的示例交互

[0163] 从记录发送方到代理的示例

[0164] 在一些实施例中,代理可以代表记录接收方行动。在商家或委托人的示例情境中,商家或委托人可以是记录接收方,并且代理可以是结账通道或支付亭的服务员。在另一示例情境中,代理可以是自助结账机或自助服务终端,其允许客户从商家处理他们自己的购买。服务员通常使用诸如收银机的销售点(POS)设备来接收从客户的电子设备116a发送的支付以在客户结账时代表商家接受支付。

[0165] 图9是示出安全地交换和兑换涉及代理和接收方的个体记录的一个实施例的交互图。记录接收方102b的代理102d使用代理设备116d可以通过在交互404处使用短程链路(SRL)122向记录发送方设备116a发送内容请求402来从记录发送方102a请求个体记录。内容请求402可以包括内容B 110b和记录接收方的公钥106b。

[0166] 记录接收方102b(例如商家)可以具有或可以与一个或多个代理102d(例如十个代理(例如,检查者))相关联。代理102d和代理设备116d之间的关系可以变化。例如,一些代理102d可以共享一个代理设备116d,并且代理设备116d可以支持授权代理102d的多个登录。作为另一示例,一些代理102d不共享代理设备116d。作为另一示例,一些代理102d每个可以具有多于一个的代理设备116d。一些代理102d可以具有它们自己的代理设备116d。

[0167] 记录接收方102b可以具有或可以与一个或多个公钥106b相关联。例如,记录接收

方102b可以具有一个公钥106b。作为另一示例，记录接收方102b可以对于每个位置(例如物理位置或虚拟位置)具有一个公钥106b。物理位置可以是商店位置或交换位置。作为另一示例，记录接收方102b可以对于每个外部设备具有一个公钥106b。

[0168] 代理102d可以有利地与不是本公开的系统和方法的一部分的外部设备交互。外部设备的非限制性示例包括蜂窝电话、平板计算机、电子阅读器、智能手表、头戴式增强、虚拟或混合现实显示系统、可穿戴显示系统、计算机、服务器计算机、销售点系统或收银机。外部设备可以固定在一定位置，例如物理位置(诸如商店位置)。外部设备可以是基础架构(例如现有基础架构)的一部分。

[0169] 公钥106b的管理可以变化。例如，记录接收方102b可以使用记录接收方设备116b或其操作的一个或多个其它计算机来管理公钥106b本身。作为另一个示例，服务提供者104可以将记录接收方的公钥106b管理为类似于“软件即服务”(Saas)的服务。

[0170] 有利地，代理102d不能与处理平台124兑换个体记录100或第一修改的个体记录100m1，因为块105a包含记录接收方设备116b的公钥106b，而不是代理设备116d的公钥106d。

[0171] 在交互408处，记录发送方设备116a可以通过伙伴标识来确认代理设备116d的标识或记录接收方设备116b的标识。在记录发送方设备116a的安全元件(SE)204a验证记录发送方的认证信息512a之后，安全元件(SE)204a可以在交互416处对个体记录100进行签名。

[0172] 图10示意性地示出涉及代理和记录接收方的示例个体记录。如图9-10中所示，个体记录100可以是包括块105a的数字对象。块105a可以包括“来自字段”中的记录发送方设备的公钥106a、“到字段”中的记录接收方设备的公钥106b、记录ID 108、内容A 110a以及块105a的记录发送方签名112a。

[0173] 在交互420处，记录发送方102a可以使用短程链路(SRL)122以例如对等方式向代理102d发送个体记录100。一旦具有代理102d，代理102d可以在交互424处验证个体记录100。在一些实施例中，代理设备116d可以通过记录接收方102b的专用网络连接到网络，例如网络118。使用到网络118的该连接，代理设备116d可以采用处理平台124验证个体记录100。在一些实施例中，代理设备116d而不是记录发送方设备116a可以访问网络。

[0174] 从代理到记录接收方的示例

[0175] 参考图9，在一些实施例中，在交互908处向记录接收方102b发送第一修改的个体记录100m1之前，代理设备116d的安全元件(SE)204d可以在交互904处创建第一修改的个体记录100m1并对其进行签名。对第一修改的个体记录100m1进行签名可以包括将块105b添加到第一个体记录100以创建第一修改的个体记录100m1。第一修改的个体记录100m1的块105b可以包括块105b的代理设备的公钥106d、认可和代理签名112d。例如，认可可以是“由认可处理”(HBE)114a。“由认可处理”(HBE)、代理设备的公钥106d和代理签名112d与记录发送方设备的公钥106a和记录接收方设备的公钥106b一起可以指示代理设备116d可以代表记录接收方102b从记录发送方设备116a接收到个体记录100。

[0176] 在交互908处，代理102d可以直接通过通信链路或间接地向记录接收方102b发送第一修改的个体记录100m1。例如，代理102d可以使用短程链路(SRL)122以例如对等方式向记录接收方102b发送第一修改的个体记录100m1。作为另一示例，代理102d可以通过网络(例如网络118)向记录接收方102b发送第一修改的个体记录100m1。记录接收方设备116b的

配置可以变化。例如，记录接收方设备116b可以与图2中所示的用户设备116、图3中所示的处理平台124或其任何组合类似或相同。

[0177] 在一些实施例中，一旦具有记录接收方102b，记录接收方102b就可以验证第一修改的个体记录100m1。验证第一修改的个体记录100m1可以包括确定与代理设备相关联的公钥106d是否与授权代理102d相关联。记录接收方102b可以拒绝由未授权人员接收或者在未被授权代理认可的情况下接收的个体记录。验证第一修改的个体记录100m1可以包括使用例如第一修改的个体记录100m1中的记录发送方设备的公钥106a和代理设备的公钥106d来认证记录发送方签名112a和代理签名112d。

[0178] 示例个体记录兑换

[0179] 参考图9，记录接收方设备116b可以使用例如其安全元件(SE)204b来创建第二修改的个体记录100m2并对其签名。在一些实施例中，在交互912处对第二修改的个体记录100m2进行签名之前，记录接收方设备116b的安全元件(SE)204b可以要求提供要被数字签名的块(例如第二修改的个体记录100m2的块105c)以及记录接收方或为记录接收方102b工作的授权人员的认证信息二者。

[0180] 第二修改的个体记录100m2的内容可以变化。例如，第二修改的个体记录100m2可以包括第一修改的个体记录100m1的块105b。作为另一示例，第二修改的个体记录100m2可以不包括第一修改的个体记录100m1的块105b。第二修改的个体记录100m2可以包括认可块105c。例如，认可可以是“仅用于处理的认可”(FPOE)114b，其与记录接收方的公钥106b一起指定第二修改的个体记录100m2只能由记录接收方102b兑换。

[0181] 在对第二修改的个体记录100m2进行签名之后，记录接收方102b可以在交互916处与处理平台124兑换第二修改的个体记录100m2。在兑换时，操作处理平台124的服务提供者104可以通过验证第二修改的个体记录100m2中的块105a、105b和105c的链中的一个或多个签名的真实性，在交互920处处理第二修改的个体记录100m2。例如，处理平台124可以验证记录发送方签名112a、代理签名112d和记录接收方签名112b。在成功验证之后，处理平台124可以如第二修改的个体记录100m2的内容A110a所指示地执行。

[0182] 在一些实施例中，处理平台124可以在交互924处通知记录接收方设备116b已经成功处理了第二修改的个体记录100m2。记录接收方设备116b进而可以在交互928处通知代理设备116d已经使用例如“由认可处理”(HBE)成功处理了修改的个体记录100m1。

[0183] 代理设备116d可以将存储在代理设备116d的个体记录容器202中的修改的个体记录100m1移除为未兑换的个体记录208之一。代理设备116d可以将个人记录100的内容A 110a输入到外部设备中，伴随有例如诸如“记录清除”的消息。

[0184] 买方/付款方和卖方/收款方的示例情境

[0185] 在一些实施例中，内容请求402可以是包括金额B 110b的支付请求402。个体记录100可以包括数字支票100。个体记录100的内容A 110a可以包括金额A 110a。金额B和金额A可以相同、类似或不同。金额可以是法定货币、加密货币(例如，比特币)、金融证券(例如股票或债券)，或任何类型的真实、无形或虚拟资产。记录ID 108可以包括支票ID 108。创建个体记录100可以包括创建数字支票100，并且创建修改的个体记录100m1可以包括创建修改的数字支票100m1。“仅用于处理的认可”(FPOE)可以是“仅用于存款的认可”(FDOE)。

[0186] 记录发送方102a可以是买方或付款方102a，并且记录接收方102b可以是卖方或收

款方102b。记录发送方设备116a和记录接收方设备116b可以是买方设备或付款方设备116a和卖方设备或收款方设备116b。涉及个体记录100的交换可以是记录发送方102a从记录接收方102b购买例如计算机，并且记录发送方102a用数字支票100支付购买，其中金额A 110a是计算机的购买价格。图9中示出的代理102d可以是检查者或收银员102d。图9中所示的记录接收方102b可以是商家102b。外部设备可以是销售点系统或收银机。

[0187] 公共记录容器240中的公共记录206可以是公共分类帐容器240中的公共分类帐206。存储在个体记录容器202中的未兑换的个体记录208可以是存储在钱包202中的未兑换的支票208。

[0188] 处理平台124可以处理支付。处理平台124如由修改的个体记录100m1的内容110所指示地针对记录接收方102b执行可以包括如由修改的数字支票100m1所指示地向收款方设备提供金额A 110a。中央记录容器332可以是中央分类帐，并且中央记录302可以包括公共分类帐。用户记录状态306可以包括用户当前余额306。

[0189] 成本/费用的示例

[0190] 除了用户102a或102b以及服务提供者104之外的第三方可以针对某些活动收取第三方费用。例如，维护例如具有存储在个体记录100的内容110中的其文档ID的文档的第三方可以向处理平台124收取访问这些文档的访问费用。处理平台124进而可以向用户102a或102b收取访问费用。

[0191] 处理平台124可以对某些交易收取交易费用。例如，处理平台124可以收取用于处理个体记录100或者用于维护用户帐户的交易费用。作为另一示例，处理平台124可以如个体记录100的内容110所指示地收取用于访问文档的交易费用。作为另一示例，处理平台124可以收取交易费用以向记录接收方提供对具有存储在个体记录100的内容110中的其文档ID的文档的访问。处理平台124可以针对相同或类似交易(诸如访问相同或类似的文档)向不同的用户收取不同的费用。作为另一示例，处理平台124可以针对不期望的行为向用户收取费用，例如，当它们不应该时授权其他用户访问文档。交易费用可以基于交易规模或交易数量，可以是固定的，或其任何组合。

[0192] 处理平台124可以用代理102d向记录接收方102b收费，例如，用于密钥对的维护费用。例如，当处理平台124向记录接收方102b提供密钥对时，可以收取维护费用一次，或者可以定期收费。费用可以是固定的，协商的，打折的，优惠的，排他的或其任何组合。

[0193] 示例查询认可

[0194] 在一些实施例中，即使记录发送方可能不连接，记录接收方也可以连接到网络。例如，记录发送方102a和记录接收方102b可以在记录发送方的营业地点交换个体记录100。由记录接收方102b操作的记录接收方设备116b可以通过由例如记录接收方106b操作的专用网络连接到网络118。并且由记录发送方102a操作的记录发送方设备116a可能由于例如差的蜂窝连接性而不能连接到网络118。在接受涉及个体记录100的交换之前，当个体记录100以电子方式传送到处理平台124并与处理平台124兑换时，记录接收方102b可以电子地查询处理平台124关于处理平台124是否将如个人记录100的内容A 110a中所指示地执行的内容。例如，内容A 110a可以使记录接收方设备102b访问具有在内容A 110a中存储的其文档ID的文档。接收方102b可以使用例如处理平台124的“查询认可”(QE)来验证记录发送方102a可以向记录接收方102b提供对文档的访问。

[0195] 图11是示出安全地交换和兑换涉及查询认可的个体记录的一个实施例的交互图。如图4-5中所示，记录接收方102b使用记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向记录发送方设备116A发送内容请求402来从记录发送方102A请求个体记录100。内容请求402可以包括内容B 110b和记录接收方设备的公钥106b。

[0196] 在交互408处，记录发送方设备116A可以通过伙伴标识来确认记录接收方设备116b的标识。在记录发送方设备116A的安全元件(SE)204A验证记录发送方的认证信息512A之后，安全元件204A可以在交互416处对个体记录100进行签名。在交互416处对个体记录100进行签名之前，安全元件204A可以要求提供要被数字签名的块(例如个体记录100的块105A)以及认证记录发送方102A。

[0197] 图12示意性地示出涉及查询认可的示例个体记录。如图11-12中所示，个体记录100可以是包括一个或多个块的数字对象。个体记录100可包括块105a。块105a可以包括“来自字段”中的记录发送方设备的公钥106a、记录接收方设备的公钥106b、“到字段”中的记录ID 108、内容A 110a以及块105a的记录发送方签名112a。

[0198] 如图11中所示，在交互420处，记录发送方102a可以使用短程链路(SRL)122以例如对等方式向记录接收方102b发送个体记录100。一旦具有记录接收方102b，记录接收方102b可以在交互424处验证个体记录100。验证个体记录100可以包括使用例如个体记录100中的记录发送方设备的公钥106a来认证记录发送方签名112a。

[0199] 示例查询

[0200] 参考图11，在成功验证个体记录100之后，记录接收方设备116b可以使用其安全元件204b创建第一修改的个体记录100m1并对其签名。在交互1104处对第一修改的个体记录100m1进行签名之前，安全元件(SE)204b可以要求提供要被数字签名的块(例如修改的个体记录100m1的块105b)以及记录接收方的认证信息512b。第一修改的个体记录100m1可以包括个体记录100的块105a和块105b。块105b可以包括块105b的认可和记录接收方签名112b。例如，认可可以是“查询认可”(QE)114a。“查询认可”114a可以指示第一修改的个体记录用于查询，而不用于兑换。如果满足一个或多个条件，则“查询认可”114a可以指示或可以包括接收方设备102b想要知道处理平台124是否将如第一修改的个体记录100m1的内容A 110a所指示地执行的查询。条件的非限制性示例包括基于具有由记录接收方102b与处理平台124电子地通信和兑换的“仅用于处理的认可”(FPOE)的个体记录100的第二修改的个体记录100m2，记录发送方102a或记录接收方102b已经执行了任务，或者诸如从另一个用户或非用户接收授权的事件发生，或特定时间。在一些实施例中，处理平台124可以向记录接收方102b提供寻求来源(sourcing)信息和费用分割信息。

[0201] 在对第一修改的个体记录100m1进行签名之后，记录接收方102b可以在交互1108处向处理平台124发送修改的个体记录100m1。在交互1112处处理第一修改的个体记录100m1中的查询认可114a之后，处理平台124可以在交互1116处向记录接收方102b提供查询结果。例如，查询结果可以指示处理平台124将如第一修改的个体记录100m1的内容A 110a和执行的定时所指示地执行或不执行。作为另一示例，查询结果可以是如果已经满足一个或多个条件，则处理平台124将如内容A 110a所指示地执行。作为另一示例，查询结果可包括源信息或成本。

[0202] 示例个体记录兑换

[0203] 参考图11,给定查询结果,记录接收方102b可以决定是否接受涉及个体记录100与记录发送方102a的交换。如果记录接收方102b决定接受交换个体记录100并与处理平台124兑换个体记录100,则记录接收方设备116b可以使用其安全元件204b创建第二修改的个体记录100m2并对其签名。在交互428处对修改的个体记录100m1进行签名之前,安全元件(SE)204b可以要求提供要被数字签名的块(例如第二修改的个体记录100m2的块105c)以及记录接收方的认证信息512b。修改的个体记录100m1可以包括个体记录100的块105a和认可块105c。块105c可以包括块105c的认可和记录接收方签名112b'。例如,认可可以是"仅用于处理的认可"(FPOE)114b,其指定修改的个体记录100m1只能由记录接收方102b兑换。在一些实施例中,第二修改的个体记录100m2可以包括第一修改的个体记录100m1的块105b。

[0204] 在对第二修改的个体记录100m2进行签名之后,记录接收方102b可以在交互432处与处理平台124兑换第二修改的个体记录100m2。在兑换时,操作处理平台124的服务提供者104可以通过验证修改的个体记录100m1中的块105a和105c链中的一个或多个签名的真实性在交互436处处理第二修改的个体记录100m2。认证的签名可包括记录发送方签名112a和第二记录接收方签名112b。在成功验证之后,处理平台124可以如第二修改的个体记录100m2的内容A 110a所指示地执行。

[0205] 涉及个体记录100的交换被认为完成的定时在不同的实施方式中可以是不同的。例如,当记录接收方102b在交互1116处接收到查询结果之后接受涉及个体记录100与记录发送方102a的交换时,可以认为涉及个体记录100的交换完成。查询结果可以指示处理平台124将如第一修改的个体记录100m1的内容A 110a和执行的定时所指示地执行。作为另一示例,当操作处理平台124的服务提供者104在交互436处成功地处理第二修改的个体记录100m2时,可以认为涉及个体记录100的交换完成。处理平台124可以验证修改的个体记录100m1中的块105a和105c的链中的一个或多个签名的真实性。作为另一示例,当中央平台124如第二修改的个体记录100m2的内容A 110a所指示地执行时,可以认为涉及个体记录100的交换完成。

[0206] 示例公共记录的分布

[0207] 示例更新频率

[0208] 处理平台124可以通过向一个或多个用户设备发送更新的公共记录206来不时地或以规则间隔更新公共记录206。在一些实施例中,规则间隔可以是基于时间的,例如每小时、每天、每周或每月。

[0209] 在一些实施例中,规则间隔可以基于具有改变状态的用户或用户设备的数量或百分比。改变状态的非限制性示例包括设备变为用户设备116,设备116不再是用户设备,用户102a或102b或用户设备116被添加到过失列表或从过失列表中移除(下面将描述过失),在过失列表上用户102a或102b或用户设备116a或116b的过失状态改变,诸如过失点的增加或减少,或者用户102a或102b或用户设备116被添加到黑名单或从黑名单中移除。例如,具有改变状态的用户或用户设备116的数量可以是100。作为另一示例,具有改变状态的用户或用户设备116的百分比可以是所有用户或用户设备116的1%。

[0210] 在一些实施例中,规则间隔可以基于由处理平台124的错误管理器检测到的或由用户设备116的错误管理器确定的错误事件的数量,例如100个错误事件。例如,错误事件可以是处理平台接收具有"恶意代码"(MC)认可的个体记录(下面进一步描述)。

[0211] 从处理平台接收的示例公共记录

[0212] 图13是示出从处理平台124分发公共记录206的一个实施例的交互图。在交互1304处，使用例如公共记录生成器的处理平台124可以创建公共记录消息1308。图14示意性地示出用于分发的示例公共记录。如图13-14中所示，公共记录消息1308可以包括更新的公共记录206，其可以包括设备214的更新的公钥。公共记录消息1308可以包括过失列表1402和黑名单1404。通过将服务提供者签名1312添加到公共记录消息1308，处理平台124可以对公共记录消息1308进行签名。可以使用服务提供者拥有的服务提供者私钥348，由公共记录生成器340创建服务提供者签名1312。

[0213] 处理平台124的公共记录分发器可以将公共记录消息1308分发给用户设备。处理平台124可以顺序地将公共记录消息1308分发给用户设备。例如，处理平台124可以首先在交互1316a处将公共记录消息1308分发给记录接收方设备102b，并且随后在交互1316b处将公共记录消息1308分发给记录发送方设备102a。这种顺序分布可以有利地避免业务拥堵和带宽瓶颈。记录发送方设备102a和记录接收方设备102b的公共记录接收方可以从处理平台124接收公共记录消息1308。

[0214] 处理平台124可以同时或在时间上接近将公共记录消息1308分发给一个或多个用户设备116。例如，公共记录分发器可以同时将公共记录消息1308分发给100个用户设备116。作为另一示例，公共记录分发器344可以同时将公共记录消息1308分发给10％的用户设备116。作为另一示例，公共记录分发器344可以以100个批次将公共记录消息1308分发给用户设备116。

[0215] 在交互1320处，记录接收方设备102b的安全元件(SE)130b可以验证公共记录消息1308的真实性。验证公共记录消息1308的真实性可以包括验证服务提供者签名1308。服务提供者签名1308可以包括使用存储在安全元件204b中的服务提供者公钥212确定是否已经使用服务提供者私钥348创建了服务提供者签名1308。类似地，在交互1328处，记录发送方设备102a的安全元件204a可以验证公共记录消息1308的真实性。

[0216] 从记录接收方接收的示例公共记录

[0217] 在从处理平台124接收到公共记录消息1308之后，用户设备(例如记录接收方设备)可以将公共记录消息1308传播到包括记录发送方设备的其他用户设备。例如，已经接收到公共记录消息1308的用户设备可以在接收到公共记录消息1308之后的一段时间内或者连续地将接收到的公共记录消息1308广播到其他用户设备，直到从处理平台124接收到新的公共记录消息为止。

[0218] 图15是示出由记录接收方设备传播公共记录的示例的交互图。在交互1304处创建公共记录消息1308并对其签名之后，处理平台124可以在交互1316处将公共记录消息1308分发给用户设备(例如记录接收方设备102b)。在交互1320处，记录接收方设备102b的安全元件(SE)204b可以验证公共记录消息1308的真实性。

[0219] 在交换个体记录(例如图4-12中所示的个体记录100)之前，记录发送方设备102a可能尚未从处理平台124或任何其他用户设备116接收到公共记录消息1308。在交互1504处，记录接收方设备102b可以通过提供发送公共记录消息1308并将其发送到记录发送方设备102a来传播公共记录消息1308。从记录接收方设备102b接收的记录发送方设备102a的公共记录消息1308可以包括记录接收方设备的签名。在交互1508处，记录发送方设备102a的

安全元件(SE)204a可以验证公共记录消息1308的真实性。

[0220] 从记录发送方接收的示例公共记录

[0221] 在从处理平台124接收公共记录206之后,用户设备(例如记录发送方设备)可以将公共记录206传播到包括记录接收方设备的其他用户设备。图16是示出由记录发送方设备传播公共记录的示例的交互图。在交互1304处创建公共记录消息1308并对其签名之后,处理平台124可以在交互1316处将公共记录消息1308分发给用户设备(例如记录发送方设备102b)。在交互1328处,记录发送方设备102a的安全元件(SE)204a可以验证公共记录消息1308的真实性。

[0222] 在交换个体记录(例如图4-12中所示的个体记录100)之前,记录接收方设备102b可能尚未从处理平台124或任何其他用户设备116接收到公共记录消息1308。例如,记录发送方设备116a可以是新用户设备,并且记录接收方设备116b可以不具有记录发送方设备的公钥106a。在没有接收到包含记录发送方设备的公钥106的公共记录消息1308的情况下,记录接收方102b可能无法验证记录发送方设备116a是有效的用户设备。

[0223] 在交互1504处,记录发送方设备102a可以通过提供发送公共记录消息1308并将其发送到记录接收方设备102b来传播公共记录消息1308。在交互1508处,记录接收方设备102b的安全元件(SE)204b可以验证公共记录消息1308的真实性。这种传播有利地允许交换单独的记录,即使记录接收方设备102b在从记录发送方设备102a接收公共记录消息1308之前可能不具有记录发送方设备的公钥102a。

[0224] 示例错误管理

[0225] 处理平台124从用户设备接收的个体记录可以包含预期或非预期的错误。用户可以通过创建无效的个体记录(例如具有无效签名的个体记录)来进行恶意行为。不道德的用户可能通过例如导致其他用户创建无效的个体记录来导致其他用户显示为恶意用户。

[0226] 具有多个接收方的发送方克隆的示例

[0227] 在一些实施例中,恶意记录发送方可以向两个不同的记录接收方发送个体记录。图17是示出该恶意行为的交互图,该恶意行为可被称为具有多个接收方的发送方克隆。第一记录接收方102b使用第一记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向第一记录发送方设备116a发送第一内容请求402来从记录发送方102a请求个体记录。第一内容请求402可以包括内容B 110b和第一记录接收方设备的第一公钥106b。第二记录接收方102c使用第二记录接收方设备116c可以通过在交互1704处使用短程链路122向记录发送方设备116a发送第二内容请求1702来从记录发送方102a请求个体记录。第二内容请求402可以包括内容C 110c和第二记录接收方设备的第二公钥106c。记录发送方102a可以在接收第二内容请求1702之前、之后或同时接收第一内容请求402。

[0228] 在交互420处向第一记录接收方设备116b发送个体记录100的第一副本之前,记录发送方设备116a的安全元件(SE)204a可以在交互416处创建个体记录100并对其签名。在交互424处成功验证个体记录100之后,第一记录接收方设备116b可以在交互432处与处理平台124兑换个体记录100。在兑换时,操作处理平台124的服务提供者104可以通过验证兑换的个体记录100中的一个或多个签名的真实性在交互436处处理个体记录100。在成功验证之后,处理平台124可以如个体记录100的内容A 110a所指示地执行。

[0229] 在交互416处创建个体记录100并对其签名之后,记录发送方设备116a还可以在交

互1720处向第二记录接收方设备116b发送个体记录100的第二副本。记录发送方102a可以在向第二记录接收方102c发送个体记录100的另一个副本之前、之后或同时向第一记录接收方102b发送个体记录100的副本。

[0230] 内容B 100b和内容C 100c可以相同或类似，使得内容A 100a可以对第一记录接收方102b和第二记录接收方102c显示为分别满足第一内容请求402和第二内容请求1702。然而，在交互1724处由第二记录接收方116c对个体记录100的验证可能失败，因为个体记录100可以包括第一记录接收方设备的公钥106b，而不包括第二记录接收方设备的公钥106c。这可以指示个体记录100旨在用于第一记录接收方102b，而不是第二记录接收方102c。由于不成功验证，第二记录接收方106c可以拒绝涉及第二内容请求1702与记录发送方102a的交换。在一些实施例中，在不成功验证之后，第二记录发送方设备116c可以在交互1728处将个体记录100发送到处理平台124之前将“恶意记录认可”(MRE)添加到个体记录100。

[0231] 具有单个接收方的发送方克隆的示例

[0232] 在一些实施例中，恶意记录发送方可以向一个记录接收方发送同一个体记录的两个副本。图18是示出该恶意行为的交互图，该恶意行为可被称为具有单个接收方的发送方克隆。记录接收方102b使用记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向记录发送方设备116a发送第一内容请求402来从记录发送方102a请求个体记录。第一内容请求402可以包括内容B 110b和记录接收方设备的公钥106b。类似地，记录接收方102b可以通过在交互1804处使用短程链路122向记录发送方设备116a发送第二内容请求1802来从记录发送方102a请求另一个体记录。第二内容请求1802可以包括内容B’110b’和记录接收方设备的公钥106b。记录接收方102b可以同时或在不同时间发送第一内容请求402和第二内容请求1802。

[0233] 在交互420处向记录接收方设备116b发送个体记录100的第一副本之前，记录发送方设备116a的安全元件(SE)204a可以在交互416处创建个体记录100并对其签名。个体记录100的记录ID例如可以是N。在交互424处成功验证个体记录100之后，记录接收方设备116b可以在交互432处与处理平台124兑换个体记录100。在兑换时，操作处理平台124的服务提供者104可以通过验证兑换的个体记录100中的一个或多个签名的真实性在交互436处理个体记录100。在成功验证之后，处理平台124可以如个体记录100的内容A 110a所指示地执行。

[0234] 在交互1820处，记录发送方设备116a可以向记录接收方设备116b发送个体记录100的第二副本。内容B 100b和内容B’100b’可以相同或类似，使得内容A 100a可以向记录接收方102b显示为满足第一内容请求402和第二内容请求1802。

[0235] 然而，在交互1820处由记录接收方116b对个体记录100的第二副本的验证可能失败。对于记录接收方设备116b已经从其接收到一个或多个个体记录的每个用户设备，记录接收方设备116b的记录历史跟踪器可以跟踪从用户设备接收的最后一个个体记录的记录ID。例如，记录历史跟踪器可以跟踪它从记录发送方设备116a接收的最后一个个体记录100的记录ID 108N。因此，记录发送方设备116a不应该已经向记录接收方设备116b发送包含相同记录ID 108N的个体记录100的第二副本。

[0236] 在一些实施例中，对于记录接收方设备116b已经从其接收到一个或多个个体记录的每个用户设备，记录历史跟踪器可以采用所接收的最大记录ID 108跟踪个体记录100。有

利地，对于记录接收方设备116b已经从其接收到一个或多个个体记录的每个用户设备，记录接收方设备116b可以仅跟踪从用户设备接收的最后一个个体记录100的记录ID 108，因为由一个记录发送方创建的个体记录的记录ID 108可以单调增加。在一些实施例中，记录历史跟踪器可以跟踪所接收的所有个体记录的记录ID 108。

[0237] 由于不成功的验证，记录接收方106b可以拒绝涉及第二内容请求1802与记录发送方102a的交换。在一些实施例中，在不成功验证之后，记录发送方设备116b可以在交互1828处将个体记录100发送到处理平台124之前将“恶意记录认可”添加到个体记录100的第二副本。

[0238] 示例分叉

[0239] 在一些实施例中，恶意记录接收方可以在对其进行认可之前复制个体记录，并尝试向第二记录接收方发送所保存的个体记录的副本。图19是示出该恶意行为的交互图，该恶意行为可被称为分叉。第一记录接收方102b使用第一记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向第一记录发送方设备116a发送第一内容请求402来从第一记录发送方102a请求个体记录。第一内容请求402可以包括内容B 110b和第一记录接收方设备的公钥106b。

[0240] 在交互420处向第一记录接收方设备116b发送个体记录100之前，第一记录发送方设备116a的安全元件(SE)204a可以在交互416处创建个体记录100并对其签名。在交互424处的个体记录100的成功验证之后，第一记录接收方设备116b可以在交互428处创建具有第一记录接收方签名112b的修改的个体记录100m1。在交互432处与处理平台124兑换修改的个体记录100m1时，操作处理平台124的服务提供者104可以通过验证修改的个体记录100m1中的一个或多个签名的真实性来在交互436处处理修改的个体记录100m1。在成功验证之后，处理平台124可以如修改的个体记录100m1的内容A 110a所指示地执行。

[0241] 第二记录接收方102c使用第二记录接收方设备116c可以通过向第一记录接收方设备116b发送第二内容请求1902来从第一记录接收方102b请求个体记录。第一记录接收方102b可以是第二记录发送方102b，并且第一记录发送方设备116b可以被称为第二记录发送方设备116b。第二内容请求1902可以包括内容C 110c和第二记录接收方设备的公钥106c。

[0242] 第二记录发送方设备116b可以在交互1916处向第二记录接收方设备116c发送个体记录100的副本。然而，在交互1920处由第二记录接收方116c对个体记录100的验证可能失败，因为个体记录100可以包括第二记录发送方设备的公钥106b，而不包括第二记录接收方设备的公钥106c。这可以意味着个体记录100旨在用于第一记录接收方102b，而不是第二记录接收方102c。由于不成功的验证，第二记录接收方106c可以拒绝涉及第二内容请求1902与第二记录发送方102b的交换。在一些实施例中，在不成功验证之后，第二记录发送方设备116c可以在交互1924处将个体记录100发送到处理平台124之前将“恶意记录认可”添加到个体记录100。

[0243] 示例接收方克隆

[0244] 在一些实施例中，恶意记录接收方可以尝试两次兑换个体记录。在一些实施例中，恶意记录接收方可以两次兑换个体记录，以试图归咎于具有单个接收方的记录发送方克隆的记录发送方。图20是示出该恶意行为的交互图，该恶意行为可被称为接收方克隆。记录接收方102b使用记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向记录发

送方设备116a发送内容请求402来从记录发送方102a请求个体记录。内容请求402可以包括内容B 110b和记录接收方设备的公钥106b。

[0245] 在交互420处向记录接收方设备116b发送个体记录100之前，记录发送方设备116a的安全元件(SE)204a可以在交互416处创建具有记录ID 108N的个体记录100并对其签名。在424处的个体记录100的成功验证之后，记录接收方设备116b可以在交互432处与处理平台124兑换修改的个体记录100m1的第一副本之前，在交互428处创建具有记录接收方签名112b的修改的个体记录100m1。在兑换时，操作处理平台124的服务提供者104可以通过验证修改的个体记录100m1中的一个或多个签名的真实性来在交互436处处理修改的个体记录100m1。在成功验证之后，处理平台124可以如个体记录100的内容A 110a所指示地执行。

[0246] 记录发送方设备116b可以尝试在交互2032处与处理平台124兑换修改的个体记录100m1的第二副本。然而，在交互2036处，修改的个体记录100m1的第二副本的处理可能失败。处理平台124先前已经在交互436处成功处理了修改的个体记录100m1的第一副本。对于每个记录发送方设备，中央记录302的用户记录状态306可以包含处理平台302已经处理的个体记录的记录ID。例如，对于记录发送方设备116a，中央记录302的用户记录状态306可以包含修改的个体记录100m1的记录ID 108N。当记录发送方设备116b尝试用相同的记录ID 108N兑换修改的个体记录100m1的第二副本时，处理平台124可以通过比较修改的个体记录100m1的记录ID 108N和用户记录状态306来检测该恶意兑换。

[0247] 示例窥探

[0248] 在一些实施例中，恶意记录发送方可以通过绕过其记录发送方设备的安全元件(SE)来创建具有不适当签名的个体记录。图21是示出该恶意行为的交互图，该恶意行为可被称为窥探。记录接收方102b使用记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向记录发送方设备116a发送内容请求402来从记录发送方102a请求个体记录。内容请求402可以包括内容B 110b和记录接收方设备的公钥106b。

[0249] 通过非法侵入或绕过其安全元件(SE)204a，记录发送方设备116a可以在交互420处向记录接收方设备116b发送个体记录100之前在交互416处创建具有不适当签名112a'的个体记录100。不适当的签名112'可以是随机签名，或者可以使用与记录发送方设备106b不相关联的私钥来创建。

[0250] 由记录接收方116b在交互424处对个体记录100的验证可能失败。记录接收方设备116b不能确定使用记录发送方设备的私钥210a创建了不适当的签名112'。记录接收方设备116b不能使用记录发送方设备的公钥106a来解密不适当的签名112'。由于不成功的验证，记录接收方106b可拒绝涉及内容请求402与记录发送方102a的交换。在一些实施例中，在不成功验证之后，记录发送方设备116b可以在交互2124处将个体记录100发送到处理平台124之前将“恶意记录认可”添加到个体记录100。

[0251] 示例重影

[0252] 在一些实施例中，恶意记录发送方可以创建具有不适当签名的个体记录。图22是示出该恶意行为的交互图，该恶意行为可被称为重影。记录接收方102b使用记录接收方设备116b可以通过在交互404处使用短程链路(SRL)122向记录发送方设备116a发送内容请求402来从记录发送方102a请求个体记录。内容请求402可以包括内容B 110b和记录接收方设备的公钥106b。

[0253] 通过非法侵入或绕过其安全元件(SE)204a，记录发送方设备116a可以在交互420处向记录接收方设备116b发送个体记录100之前在交互416'处创建具有不适当的公钥106a'和不适当的签名112'的个体记录100。记录发送方设备的不适当的公钥106'和公钥106a可以是不同的。可以使用不适当的私钥210'来创建不适当的签名112'。

[0254] 如果记录接收方设备具有设备214b的最新公钥，则由记录接收方116b在424a处对个体记录100的验证可能失败。即使记录接收方设备116b可以解密不适当的签名112'，记录接收方设备116b也可以知道不适当的公钥106'可能不属于用户设备。不适当的公钥106'可以不在公共记录206的设备214b的公钥中。由于验证不成功，记录接收方106b可以拒绝涉及内容请求402与记录发送方102a的交换。在一些实施例中，在不成功验证之后，记录发送方设备116b可以在交互2224处将个体记录100发送到处理平台124之前向个体记录100添加“恶意记录认可”(MRE)。

[0255] 在一些实施例中，记录接收方116b在交互424b处对个体记录100的验证可以是成功的，因为记录接收方设备可能不具有设备的最新公钥214b。因为使用不适当的私钥210'创建了不适当的签名112'，所以记录接收方设备116b可以使用个体记录100a中的不适当的公钥106'成功地解密不适当的签名112'。在交互424b处成功验证个体记录100之后，第一记录接收方设备116b可以在交互432处与处理平台124兑换修改的个体记录100m1之前在交互428处创建具有记录接收方签名112b的修改的个体记录100m1。然而，修改的个体记录100m1的处理可能在交互436处失败，因为不适当的公钥106a'不在中央记录302的设备214的公钥中。在一些实施例中，即使在交互424b处由记录接收方116b对个体记录100的验证可以成功，记录接收方102b可以拒绝涉及内容请求402与记录发送方102a的交换，因为不适当的公钥106a不在公共记录206的设备214的公钥中。在一些实施例中，可以采用加密算法的专有变体，从而使得重影不可能。

[0256] 示例过失和黑名单

[0257] 在此公开的方法和系统中，用户的某些动作是不期望的。在一些实施例中，不期望的动作可能不需要改变或黑客攻击用户设备。例如，不期望的动作可以是记录发送方116a创建具有不适当的内容110的个体记录100的结果。例如，用户记录状态306可以指示只有记录发送方102a本身可以访问具有存储在内容110中的其文档ID的文档；并且记录发送方102a不能授权其他用户访问该文档。如果个体记录100的内容110试图授权记录接收方102b访问该文档，则内容110可能是不适当的。通过用不适当的内容110创建个体记录100，记录发送方102a可能不合需要地起作用。

[0258] 处理平台124可以包括过失列表，该过失列表被配置为跟踪用户的不期望动作的数量。过失列表可以跟踪并且可以基于处理的不期望的动作的数量或者具有所处理的不适当内容110的个体记录100的数量、不期望的动作或不适当的内容110的类型、不期望的动作已经何时以及如何发生、已经何时以及如何处理具有不适当内容110的个体记录100，或其任何组合。在一些实施例中，过失列表可以确定用户和用户设备116的过失。过失点可以基于过失列表可以跟踪的信息。可以关于所有用户或一些用户(例如新用户)对过失进行标准化。

[0259] 在一些实施例中，不期望的动作可能需要改变或黑客攻击用户设备。需要改变用户设备的不期望动作的非限制性示例可以包括具有多个接收方的发送方克隆，具有单个接

收方的发送方克隆，分叉，接收方克隆，用窥探，重影或其任何组合。可以用多种检测方案和方法来检测不期望的动作。如图17-22中所示，可以检测这些不期望的动作。作为另一示例，处理平台124可以基于用户设备116上的软件和硬件的校验和签名认证来检测设备改变。

[0260] 处理平台124可以包括黑名单，该黑名单可以通过检测他们参与需要设备改变的不期望动作来跟踪已经被改变的用户设备。在一些实施例中，如果用户的用户设备在黑名单上，则用户的所有用户设备都可以在黑名单1404上。如果用户设备在黑名单上，则可以暂时或永久地禁止在此公开的方法和系统。在一些实施例中，具有一定数量的过失点的用户和用户设备116可以被放置在黑名单上。

[0261] 示例恶意记录认可

[0262] 对于一些不期望的动作，记录接收方设备116b可以检测记录发送方设备116a自身的改变或黑客攻击。例如，使用图17中所示的具有多个接收方的发送方克隆，第二记录接收方设备116c可以自己检测个体记录100是否旨在用于第一记录接收方设备116b。在一些实施例中，在不成功验证时，第二记录发送方设备116c可以在交互1724处将个体记录100发送到处理平台124之前向个体记录100添加“恶意记录认可”(MRE)。第二记录发送方设备116c可以将具有“恶意记录认可”的个体记录100与可以被称为签名的“恶意记录认可”的记录接收方签名112c一起发送到处理平台124。当记录发送方设备116c连接到网络118时，记录发送方设备116c可以发送具有“恶意记录认可”的个体记录100。

[0263] 示例模糊判定

[0264] 当处理平台124接收具有签名的“恶意记录认可”的个体记录100时，处理平台124可以确定存在恶意用户。然而，处理平台124可能无法区分某些不期望的动作，诸如具有单个接收方的发送方克隆和接收方克隆。并且处理平台124可能无法将过失或故障分配给特定用户或用户设备116。

[0265] 对于某些不期望的动作，处理平台124可以能够向特定用户分配过失或故障。例如，如果在处理平台124处兑换涉及记录发送方102a和第一记录接收方102b的个体记录100的两个相同副本，则不是记录发送方102a就是第一记录接收方102b是恶意用户。基于不是记录发送方102a就是第一记录接收方102b是恶意用户，处理平台124可以生成许多规则。非限制性示例规则是：

[0266] M(发送方)+M(第一接收方)＝真，(规则1)

[0267] 其中M()表示布尔运算符，其用于确定参数是否为恶意，并且“+”表示逻辑OR运算。

[0268] 可以存储该信息以供将来使用。例如，如果在处理平台124处兑换涉及记录发送方102a和第二记录接收方102b’的另一个体记录的两个相同副本，则处理平台124可以生成许多规则。非限制性示例规则是：

[0269] (M(发送方)+M(第一接收方))*(M(发送方)+M(第二接收方))＝真，(规则2)

[0270] 其中“*”表示逻辑AND运算。

[0271] 规则2可以重写为：

[0272] M(发送方)+(M(第一接收方))*M(第二接收方))＝真。(规则3)

[0273] 在解释规则时，处理平台124可以例如假设没有两个用户是恶意的。如果没有两个用户是恶意的，则处理平台124可以从规则3推断记录发送方102a是恶意的。作为另一个示例，处理平台124可以断言恶意用户可能罕见的先验信念，其概率“p”大于0且小于1。然后第

一记录接收方102b和第二记录接收方102b'二者都是恶意的概率在规则3中可以是p*p。规则3的左侧可以表达为p+p*p。

[0274] 类似地，可以扩展这种解释和假设以包括处理平台124对所有用户的所有观察，并且可以以乘积形式的总和来表达。因此，乘积中具有最少元素的术语最可能是真实的。例如，在规则3中，术语M(发送方)可以具有最少元素并且可以最可能是真实的。这些用户和用户设备可以被标记为恶意和黑名单，立即、临时或可以被进一步调查。

[0275] 示例用户设备

[0276] 示例处理器、存储器、存储装置、网络接口和短程链路接口

[0277] 图23示意性地示出示例用户设备116。用户设备116可以是记录发送方设备、记录接收方设备和代理设备。用户设备116可以包括处理器2304，该处理器2304被配置为执行存储在存储器2308(例如随机存取存储器(RAM))中的指令。存储器2308可以被配置为在用户设备116通电时存储指令和数据。存储器2308可以包括只读和可写存储器二者。用户设备116可以包括存储装置2312，该存储装置2312被配置为在用户设备116通电或断电时存储指令和数据。存储器2308和存储装置2312中的一个或二者可以存储用于安全地交换内容和记录的指令。

[0278] 用户设备116可以包括网络接口2316和短程链路(SRL)接口2320。网络接口2316可以被配置为同步或异步地与网络118上的其它设备(例如处理平台124)通信。网络接口2316的非限制性示例包括有线通信、无线通信、蜂窝通信和使用蓝牙®、射频(RF)或红外(IR)的通信。短程链路(SRL)接口2320可以被配置为通过短程链路(SRL)122与其他用户设备116通信。短程链路接口2320可以是对等无线或用户设备116a或116b通过其可以彼此通信的其它接口。短程链路接口2320可以基于红外数据协会(IrDA)/红外物理层规范(IrPHY)、蓝牙®、近场通信(NFC)、adhoc电气和电子工程师协会(IEEE)802.11，或者任何其它无线通信方法和系统。

[0279] 示例传感器

[0280] 用户设备116可以包括用于感测用户设备周围的一个或多个传感器2324。在一些实施例中，传感器2324可包括运动传感器、定向传感器、位置传感器或其任何组合。运动传感器可以被配置为感测、检测和确定操作用户设备116的用户的运动，例如用户摇动用户设备116。在一些实施例中，运动传感器可以将用户的运动转换为电信号以供用户设备116处理。例如，运动传感器可以包括单轴加速度计，该单轴加速度计被配置用于感测、检测和确定用户在用户设备116上施加的运动。作为另一示例，运动传感器可包括多个加速度计，例如单轴加速度计和3D加速度计，以使得能够检测多个方向中的定向运动和振动并且增加检测灵敏度。

[0281] 定向传感器可以被配置为确定用户设备116的取向。例如，发送方设备116a的定向传感器可以确定相对于固定平面(例如记录发送方102a和记录接收方102b正在安全地交换个体记录100的营业场所的地板)的记录发送方的头部。在一些实施例中，定向传感器可以将取向信息转换成电信号以供用户设备116处理。位置传感器可以被配置为基于用户设备116的位置来确定用户的位置。位置传感器的非限制性示例包括全球定位系统(GPS)或辅助GPS(aGPS)收发机。

[0282] 传感器2324可包括成像传感器(例如,数码相机)、麦克风或生物度量传感器。成像传感器可以配置为捕获用户看到的内容。例如,记录发送方设备116a的成像传感器可以捕获记录发送方102a看到的内容的一个或多个图像。作为另一示例,当记录发送方102a和记录接收方102b安全地交换个体记录100时,记录发送方设备116a的成像传感器可以捕获记录接收方设备116b的图像,以便认证记录发送方设备116a。在一些实施例中,成像传感器可以将光子转换成电信号和图像以供用户设备116处理。

[0283] 麦克风可以被配置为检测来自用户周围的环境和来自用户的声波。用户设备116可以检测并"听到"用户听到和说出的内容。在一些实施例中,麦克风可以将声波转换为电信号以供用户设备116处理。生物度量传感器可以被配置为捕获用户的生物度量信息。生物度量信息的非限制性示例包括虹膜扫描、肤色、皮肤纹理或指纹。

[0284] 示例个体记录处理器、容器、通信器和跟踪器

[0285] 用户设备116可以包括个体记录处理器2326、个体记录容器202、个体记录通信器2328和记录历史跟踪器2332。个体记录处理器2326可以被配置为创建和修改个体记录。个体记录容器202可以被配置为存储未兑换的个体记录208。个体记录通信器2328可以被配置为发送、接收或兑换个体记录和修改的个体记录。记录历史跟踪器2332可以被配置为跟踪用户设备116已经创建、接收、修改或兑换的个体记录。

[0286] 例如,记录发送方设备116a的个体记录处理器2326可以创建个体记录100。记录发送方设备116a的个体记录通信器2328可以向记录接收方设备116b发送个体记录100。记录接收方设备116b可以使用其个体记录通信器2328接收个体记录100。记录接收方设备116b的个体记录处理器2326可以修改个体记录100以创建修改的个体记录100m1。记录接收方设备116b可以将修改的个体记录100m1存储在个体记录容器202中作为未兑换的个体记录208之一。记录接收方116b可以使用其个体记录通信器2328与处理平台124兑换修改的个体记录100m1。

[0287] 记录历史跟踪器2332可以包含最高记录ID 2336,用于跟踪用户设备116最近创建的个体记录100的记录ID。在用户设备116创建具有大于最高记录ID 2336的记录ID的新个体记录之后,用户设备116可以更新最高记录ID 2336。作为另一示例,记录历史跟踪器2332可以跟踪用户设备116已创建、接收、修改或兑换的所有个体记录100。记录发送方设备116a可以包含个体记录100的副本,并且记录接收方设备116b可以包含修改的个体记录100m1的副本。

[0288] 示例安全元件(SE)

[0289] 用户设备116可以包括安全元件(SE)204。安全元件204可以被配置为安全地存储用户设备的私钥210和一个或多个服务提供者公钥212。在一些实施例中,安全元件204可以包括服务提供者124的公钥。在一些实施例中,安全元件204可以包括一个服务提供者124的两个或更多个服务提供者公钥212。在一些实施例中,安全元件204可以包括两个或更多个服务提供者的两个或更多个服务提供者公钥212。安全元件204可以使用用户设备的私钥210来对个体记录100进行签名。记录发送方设备116a的安全元件204a可以将接收方公钥106b和记录ID 108添加到个体记录100。ID 108可以基于例如由记录历史跟踪器2332跟踪的最高记录ID 2336。在一些实施例中,安全元件204可以包括记录历史跟踪器2332和最高记录ID 2336中的一个或多个。

[0290] 安全元件(SE)204可以使用服务提供者公钥212来验证从服务提供者104接收的信息的真实性。例如,从服务提供者104接收的信息可以包括使用服务提供者公钥加密对的私钥创建的服务提供者签名。验证从服务提供者104接收的信息的真实性可以包括使用服务提供者公钥212确定是否已经使用服务提供者私钥创建了服务提供者签名。在一些实施例中,服务提供者公钥212可以在安全元件204中被硬编码。在一些实施例中,服务提供者公钥212可以由处理平台124更新。

[0291] 安全元件(SE)204可以具有不同的实施方式,包括硬件实施方式、安全虚拟化、安全执行环境或其任何组合。例如,安全元件204可以包括集成电路或可以安全地存储与用户设备116相关联的私钥210的另一硬件组件。作为另一个示例,安全元件204可以由虚拟化基础架构实施。虚拟化基础架构可以由用户设备116中的处理器(例如处理器2304)中的一个或多个硬件特征支持。作为另一个示例,安全元件204可以实施为安全执行环境。安全执行环境可以是基础架构(诸如可以运行Java Card小程序的全局平台(GP))的虚拟实施方式。全局平台系统可以由例如提供可信执行环境(TEE)的用户设备116的高级精简指令集计算(RISC)机器(ARM)处理器的信任区特征来托管。

[0292] 示例公共记录接收方和容器

[0293] 用户设备116可以包括公共记录接收方2338,该公共记录接收方2338可以被配置为接收公共记录206以存储在公共记录容器2340中。公共记录206可以包含设备214的公钥。在一些实施例中,公共记录206可以包含用户记录状态306。在一些实施例中,公共记录206可以包含过失列表1402和黑名单1404。如果用户或用户设备已经创建了指示处理平台124在用户或用户设备不应该执行时执行任务的个体记录,则用户或用户设备可以在过失列表1402上。如果用户或用户设备例如通过使用未分配给用户设备的私钥对其进行签名来尝试兑换个体记录,则用户或用户设备可以在黑名单1404上。

[0294] 示例交易伙伴标识符

[0295] 用户设备116可以包括被配置为识别记录发送方设备和记录接收方设备的交易伙伴标识符2348。例如,如图1B中所示,为了使记录发送方设备116a创建个体记录100并将其发送到记录接收方设备116b,记录发送方设备116a可能需要识别记录接收方设备116b的公钥106b。记录接收方设备116b可以使用例如短程链路接口2320向记录发送方设备116a发送公钥。记录发送方设备116a的交易伙伴标识符2348可以确认例如从记录接收方设备116b接收的公钥实际上是记录接收方设备的公钥106b。

[0296] 示例错误管理器

[0297] 用户设备116可以包括用于处理接收的不正确的个体记录的错误管理器2356。例如,记录接收方设备116b可能无法验证从记录发送方设备116a接收的个体记录100的记录发送方签名112a的真实性。在一些实施例中,响应于接收到不正确的个体记录,错误管理器2356可以在将“恶意记录认可”添加到不正确的个体记录之后向处理平台124发送个体记录。

[0298] 示例寻求来源

[0299] 用户设备116可以包括被配置为维护源信息2364的源容器2360。源信息2364可以与标识字符串(例如存储处的名称)相关联。源信息2364可以识别多个源,用于获得例如具有存储在个体记录100的内容110中的其ID的文档。源可以是也可以不是处理平台264的一

部分。

[0300] 用户设备116可以创建具有用于存储源信息的源字段的个体记录100。在一些实施例中，如果个体记录100具有空的源字段或者不具有源字段，则可以假设个体记录100具有默认源。例如，如果个体记录100指示处理平台124向记录接收方102b提供文档，则个体记录100可以包括源字段，诸如用于获得文档的特定存储处。如果个体记录100不包含源字段或包含空的源字段，则处理平台124可以从默认存储处获得文档。

[0301] 在一些实施例中，个体记录100可以包含关于记录发送方102a或记录接收方102b是否将支付或分摊与寻求来源相关联的寻求来源费用的费用分摊字段。例如，存储处可以如由个体记录100所指示地向处理平台100收取用于访问文档的费用，并且费用分摊字段可以指示记录发送方102a或记录发送方102b是否将由存放处负责收费或他们是否以及如何分摊费用。在一些实施例中，用户设备116可以拒绝具有某些源字段、费用分摊字段或其任何组合的个体记录100。

[0302] 用户设备116可以包括用于从用户接收源信息2364的源用户界面2368。例如，用户可以使用web界面或用户设备116上的应用程序输入源信息2364。作为另一个示例，源用户界面2368可以提供用于从包含源信息264的文档中提取源信息2364的可视界面。可视界面可以利用传感器2324(例如成像传感器)和计算机视觉算法。

[0303] 示例处理平台

[0304] 示例处理器、存储器、存储装置和网络接口

[0305] 处理平台124可包括一个或多个服务器计算机。服务器计算机可以是集中式或分布式的。图24示意性地示出示例处理平台124。处理平台124可以包括处理器2404，该处理器2404被配置为执行存储在存储器2408(例如随机存取存储器(RAM))中的指令。存储器2408可以被配置为在处理平台124通电时存储指令和数据。存储器2408可以包括只读和可写存储器二者。处理平台124可以包括存储器2412，该存储器2412被配置为在处理平台124通电或断电时存储指令和数据。存储器2408和存储装置2412中的一个或二者可以存储用于处理个体记录(例如记录接收方设备116b已经与处理平台104兑换的修改的个体记录100m1)的指令。处理平台124可以包括网络接口2416，该网络接口2416被配置为与网络118上的其它设备(例如用户设备116)同步或异步地，连续地或间歇地通信。处理平台124的网络接口2416和用户设备116的网络接口306可以相同或不同。

[0306] 示例个体记录接收方和处理器

[0307] 处理平台124可以包括个体记录接收方2420，该个体记录接收方2420被配置为从用户设备116接收个体记录100。处理平台124的个体记录处理器2424可以被配置为处理由个体记录接收方2420从用户设备116接收的个体记录100。例如，处理平台124的个体记录处理器2424可以处理由个体记录接收方2420从记录接收方102b接收的修改的个体记录100m1。

[0308] 处理个体记录100可以包括将个体记录100中的一些或所有签名从个体记录100的发起者认证为“仅用于处理的认可”(FPOE)的签名者。例如，处理修改的个体记录100m1可以包括认证记录发送方签名112a和记录接收方签名112b中的一个或二者。

[0309] 认证个体记录100中的签名可以基于存储在包含中央记录302的中央记录容器2432中的用户设备214的公钥。例如，个体记录处理器2424可以认证修改的个体记录100m1

中的记录发送方签名112a和记录接收方签名112b。认证记录发送方签名112a和记录接收方签名112b可以包括确定是否已经分别使用记录发送方设备的私钥212a和记录接收方设备116b的私钥212b创建了记录发送方签名112a和记录接收方签名112b。确定记录发送方签名112a和记录接收方签名112b是否已经使用记录发送方设备的私钥212a和记录接收方设备的私钥212b创建可以包括使用记录发送方设备的公钥106a和记录接收方设备的公钥106b来确定签名的真实性。

[0310] 处理个体记录可以包括如由处理的个体记录100的内容110所指示地进行操作。例如，如果修改的个体记录100m1的内容110包括应该给予记录接收方设备116b访问具有特定文档ID的文档的指令，则处理修改的个体记录100m1可以包括给予记录接收方设备116b这种访问。

[0311] 示例中央记录处理器和容器

[0312] 在个体记录处理器2424完成处理所接收的个体记录之后，处理平台124的中央记录处理器2428可以被配置为更新包含在中央记录容器2432中的中央记录302。中央记录处理器2428可以将包含在中央记录容器2432中的中央记录302备份到例如备份存储装置。在一些实施例中，包含在中央记录容器2432中的中央记录302是权威的。例如，中央记录302的用户记录状态306可以包含用户或用户设备的最新和最准确的信息。在一些实施例中，在任何给定时间，可能存在未被兑换的个体记录，并且可能不被中央记录302反映。

[0313] 中央记录302可以包括用户设备214的公钥、用户信息304、用户记录状态306、过失列表1402、黑名单1404和源信息2436。例如，在个体记录处理器2424如修改的个体记录100m1的内容110所指示地给予记录接收方设备116b访问文档之后，中央记录处理器2428可以更新用户记录状态306以反映这种访问授权。

[0314] 源信息2436可以包括关于可以如何处理个体记录100的内容110的信息。例如，修改的个体记录100m1可以指示处理平台124给予记录接收方设备116b访问具有特定文档ID的文档，并且该文档可以存储在两个数据库中。源信息2436可以指示可以从任一数据库获得文档，或者如果可能的话，应该从两个数据库之一获得文档。

[0315] 示例公共记录生成器和分发器

[0316] 处理平台124的公共记录生成器2440可以从中央记录302创建公共记录206，以便由公共记录分发器2444分发给用户设备116。公共记录206的内容可以变化。例如，公共记录206可以与中央记录302相同。作为另一个示例，公共记录206可以是中央记录302的子集。公共记录206可以包含设备214的公钥、用户信息304、用户记录状态306、过失列表1402、黑名单1404和源信息2436中的一个或多个。公共记录分发器2444可以使用服务提供者私钥2448创建的公共记录206的签名来分发公共记录206。服务提供者公钥212和服务提供者私钥2448中的一个或二者可以存储在处理平台124的安全元件(SE)中。服务提供者私钥2448可以专有或非专有具有处理平台124。

[0317] 示例错误管理器

[0318] 处理器平台124可以包括错误管理器2452，该错误管理器2452被配置为处理不正确的个体记录。例如，记录接收方设备116b可以在认可块105b中发送具有“恶意记录认可”的修改的个体记录100m1。错误管理器2452可以被配置为基于由处理平台124接收的不正确的个体记录来确定记录发送方设备116a是应该被放置在过失列表1402还是黑名单1404上。

[0319] 示例寻求来源

[0320] 处理平台124可以包括用于管理存储在中央记录302中的源信息2436的源管理器2456。源管理器2456可以被配置用于促进与源的交互以及用于确定要与之交互的源。源信息2436可以识别多个源(包括默认源和不同源的偏好),用于如兑换的个体记录100的内容110所指示地执行。源信息2436可以包括与访问源相关联的成本,例如源为访问它们所花费的成本。源信息2436可以包括从用户接收的信息。

[0321] 用于加密安全转移资金的示例系统

[0322] 在此公开了用于资金的离线数字转移的系统和方法。例如,可以使用混合系统安全地转移和交换诸如数字支票的交易工具。当并非交易的所有各方都连接到可以认证交易的中央数据服务器时,混合系统可以提供有意义或令人满意的数字支票或价值传输的集中和对等的交换。数字支票可以具有可变价值,而不是不记名文件(诸如现金),它们允许将大量价值从一个人或实体转移到另一个人或实体,而不需要双方出现在诸如银行的中央存储处。解决了与数字传输相关的挑战,诸如可以复制数字支票所带来的琐碎之事。公开了基于数字平台上可用的数字工具和技术的特征,例如使用数字加密,其是传统手写签名的更强大的加密模拟,用于数字支票的认可。

[0323] 混合系统可以包括一个或多个组件,用于将资金从系统的一个用户转移到另一个用户。混合系统既可以具有集中式组件以及对等组件二者。采用混合系统,用户可以在交易时彼此进行金融交易而无需访问系统的中央组件。该系统可以利用网络,诸如可以通过实施诸如电气和电子工程师协会(IEEE)802.11标准802.11的协议的有线或无线通信访问的全球网络的因特网,或诸如蜂窝电话网络的远程网络。

[0324] 系统的一个或多个组件可以包括数字支票、诸如买方或卖方的用户、移动计算机(MC)、钱包、短程链路(SRL)、处理平台、中央分类帐、公共分类帐或公司。数字支票可以是数字对象、数据块,其可以从系统的一个组件发送到另一个组件。买方可以是希望将资金转移给另一个人(例如卖方)的付款方。卖方可以是希望从另一个人(例如买方)接收资金的收款方。移动计算机可以是买方和卖方具有的计算设备。买方和卖方具有的移动计算机可以相同或不同。例如,移动计算机可以是蜂窝电话。钱包可以是驻留在移动计算机上数字数据结构,该移动计算机包含尚未被发送到处理平台上的该移动计算机接收的所有数字支票。短程链路可以是对等无线或允许移动计算机彼此通信的其它链路。该链路可以基于红外数据协会(IrDA)/红外物理层规范(IrPHY)、蓝牙®、近场通信(NFC)、adhoc电气和电子工程师协会(IEEE)802.11或任何其它无线通信方法和系统。

[0325] 处理平台可以是包括机器或机器集合的服务器,其可以是系统的基础结构。处理平台可以连接到网络并且间接地(但可能仅间歇地)连接到移动计算机。处理平台可以维护中央分类帐以及公共分类帐。中央分类帐可以是维护以货币单位计量的余额的数据库。货币单位可以是现有的国家货币(例如美元)。货币单位可能是针对系统创建的新型法定货币。可以针对系统的每个用户存储该余额信息。中央分类帐可以维护关于每个用户的其它辅助或识别信息。与中央分类帐相关联的公共分类帐可以分布在整个系统中。公共分类帐可以包含有效用户标识符(ID)的列表。公共分类帐还可以包含有关用户的其它信息。公共分类帐与中央分类帐的区别在于,在一些实施例中,公共分类帐不包含帐户余额。公共分类帐可以省略中央分类帐中的其它信息。公司可以是服务提供者或运营处理平台的实体。

[0326] 示例基本交易

[0327] 图25示意性地示出标准交易的示例。买方可以向中央分类帐发出可以提供给卖方的指令。这种指令可以是数字支票。然后卖方可以将该数字支票兑换到维护中央分类帐的处理平台，以便转账。买方和卖方之间的交易可以离线完成，使得任何一方都不连接到网络，而数据传输也可以经由短程链路(SRL)完成。然后，卖方可以在卖方的移动计算机通过网络连接到处理平台时的任何稍后时间与维护中央分类帐的处理平台兑换数字支票。

[0328] 买方和卖方二者都可以具有移动计算机(MC)。移动计算机可以配备有安全元件(SE)。安全元件可以具有不同的实施方式，包括硬件实施方式、安全虚拟化、安全执行环境或其任何组合。例如，安全元件可以是芯片或其它硬件组件，其能够安全地存储诸如Rivest-Shamir-Adleman(RSA)加密的公钥加密算法的私钥。作为另一示例，SE可以是可由MC中的另一处理器中的硬件特征支持的虚拟化基础架构。作为另一示例，SE可以是诸如在其上运行Java Card小程序的全球平台(GP)的基础架构的虚拟实施方式。整个GP系统可以借助于移动设备的高级精简指令集计算(RISC)机器(ARM)处理器的TrustZone特征(例如ARM全球平台可信执行环境(TEE))来托管。

[0329] 安全元件可以对数字支票的数据块进行签名。安全元件可以具有SE也可以具有的其它可能不相关的功能。在对数据块进行签名时，安全元件还可以在块中完成两个附加字段。第一附加字段可以是与用户相关联的公钥，其可以存储在SE中。第二附加字段可以是支票标识符(ID)，其是在SE内部均匀递增的数字，使得相同的数字永远不会出现两次。

[0330] SE的动作可以通过提供要被数字签名的数字支票块以及密码短语或生物度量模板两者来触发。可能需要密码短语或生物度量模板以便SE发布签名。生物度量模板可以源自指纹、虹膜或任何其它来源。SE可以实施配置用于识别生物度量模板的生物度量模糊库。签名可以完成并对块进行签名。该签名可以是数字签名，并且可以使用诸如RSA的算法创建以加密诸如块的安全散列算法(SHA)-2的散列。可以采用存储在SE中的私钥来创建签名，但是可以由用户的相关联公钥的任何持有者来验证。

[0331] 买方可以借助于SRL或任何其它手段将签名的数字支票直接发送给卖方，或通过任何其他方间接地发送。一旦卖方具有，卖方可以选择将认可块添加到数字支票。该认可可以是“仅用于存款的认可”(FDOE)，其指定可以仅存入数字支票。该认可可以进一步将数字支票重定向到第三方。一旦添加了认可，卖方就可以重复针对整个数字支票(包括原始块、买方签名和认可块)生成签名的过程。因此，任何数字支票都可以是块链，每个块都识别其发起者。在每个块处，链的整个先前部分可以由当时使用其移动计算机的私钥来处理块的一方进行签名。

[0332] 可以与处理平台兑换其最后一个块是FDOE的任何数字支票。在兑换时，处理平台可以验证返回到数字支票的发起者(例如原始买方)的链中每个签名的真实性。如果所有签名都是真实的，则该资金将从发起者的账户转移并放置在数字支票中链的终点处的用户账户中。卖方连接到处理平台并在他的钱包中兑换数字支票的时间可以是兑换事件。

[0333] 示例中央分类帐

[0334] 公司可以负责维护处理平台，并且处理平台可以被配置为维护中央分类帐。中央分类帐可以是或可以包括用户数据库。中央分类帐可以包含有关用户的已知信息，包括其公钥和当前余额。在一些实施例中，中央分类帐可以包含关于系统中已知的用户的所有信

息。公钥可以与移动计算机的SE中的私钥相关联。中央分类帐中的记录可以是设备的记录，而不是个人的记录。如果这些信息可用，则用户拥有的移动计算机可以由用户一起分组。在一些实施例中，可以合并与特定用户相关联的设备之间的余额。

[0335] 即使可以存在中央分类帐的备份副本，中央分类帐也可以是唯一的，使得其包含的余额是系统中的权威余额。在任何给定时间，系统中可能存在未完成的数字支票，其中央分类帐可能不知道。维护中央分类帐的处理平台可以使用中央分类帐中的信息来验证从其起始点到FDOE的签名者的任何数字支票。

[0336] 示例公共分类帐

[0337] 系统中的各个移动计算机可以维护称为公共分类帐的数据结构。公共分类帐可以是中央分类帐的衍生产品，其不包含财务余额信息。公共分类帐可以包含系统中所有有效公钥(即用户标识)的列表。公共分类帐还可以包含有关各个用户的信息，诸如其过失或黑名单状态(下面进一步描述)。

[0338] 可以由处理平台不时地更新公共分类帐。当分发时，可以使用仅对于处理平台知道的私钥对公共分类帐进行加密签名。可以事先为每个接受者提供验证公共分类帐上签名所需的相应公钥。

[0339] 示例交易伙伴标识

[0340] 因为系统的数字支票可以从买方电子地发送给卖方，所以买方可能不确定卖方的标识。例如，当充当卖方的商家希望从充当收款方的买方支付时，商家可以经由SRL发出“支付请求”(PR)。支付请求可以包含商家的标识符(ID)，例如商家的公钥和请求的值。恶意行为者可能在与商家大致同时生成支付请求，希望买方可能错误地向他而不是发出支付请求的商家发送数字支票。因此，买方可能需要能够识别卖方。买方可以通过伙伴标识识别卖方。用于伙伴标识的方法的非限制性示例包括支付授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0341] 示例支付授权

[0342] 在一些实施例中，伙伴标识可以包括支付授权(PA)。例如，买方可以发出支付意图(IP)。支付意图可以是发送给买方的零价值交易，例如在支付请求中提供的卖方移动计算机的公钥。如果支付意图到达卖方的MC，则卖方可以通过非电子方法指示他是支付意图的接受者。例如，卖方可以口头通知买方他已接收到支付意图。当卖方向买方指示他是支付意图的接受者时，可以验证卖方的请求支付并且买方可以向卖方发送支付。

[0343] 示例敲击

[0344] 在一些实施例中，伙伴标识可包括敲击。例如，买方的移动计算机(MC)和卖方的移动计算机可以进行物理接触，例如敲击。移动计算机可包括运动传感器。并且买方移动计算机的运动传感器和卖方的移动计算机可以测量物理接触。由买方的移动计算机和卖方的移动计算机测量的物理接触的同时性可以是真实性的证明。卖方的移动计算机可以在发生敲击时发送支付授权。买方的移动计算机可以基于其自身测量的物理接触的时间并发和接收支付授权来接受支付授权。在一些实施例中，为了提供额外的安全性，卖方可以向买方发送其测量的接触签名。由于接触可以在买方的移动计算机中产生相同且相反的反应，买方的移动计算机可以验证由卖方移动计算机测量的接触。

[0345] 示例物理指示

[0346] 在一些实施例中，伙伴标识可包括物理指示。例如，如果移动计算机(MC)能够感知环境(例如，经由诸如相机的成像传感器)，则可以对两个移动计算机定向以便彼此感知。当敲击用于伙伴标识时，观察到的另一个MC的姿势起到类似于敲击的签名的作用。例如，如果A的移动计算机的相机看到B的MC向上和向左，则B的移动计算机的相机应该看到A的MC向下和向右。可以定性或定量地比较感知的取向。

[0347] 示例波束成形

[0348] 在一些实施例中，伙伴标识可包括波束成形。例如，移动计算机的短程链路(SRL)可以是定向的(例如，使用波束成形或定向天线)。采用波束成形，买方的移动计算机和卖方的移动计算机在发送或接收支付请求时可以彼此指向。因此，来自卖方移动计算机的支付请求(PR)可以被发送到买方的移动计算机(MC)。如果从另一个方向发送另一个PR，则买方的移动计算机可能不会接收到响应，因为买方的MC被定向为朝向卖方的MC。

[0349] 示例在先布置

[0350] 在一些实施例中，伙伴标识可包括在先布置。例如，买方可以知道特定卖方的标识符(ID)；因此验证可能是不必要的。

[0351] 示例粗略验证

[0352] 在一些实施例中，伙伴标识可以包括粗略验证。公共分类帐可以包含识别字符串，例如BigBoxStore，其可用于粗略验证支付请求。例如，可以通过操作公共分类帐中的处理平台的公司将商家识别为BigBoxStore。这种标识可以与公共分类帐中的指示(例如，位)相关联，该指示指示BigBoxStore的标识已经由公司验证。可以将验证的标识与用户自己分配或提供的标识区分开。

[0353] 错误管理

[0354] 在此公开的系统能够在数字支票是真实的时候认证数字支票中的任何的认可链。然而，数字支票可能包含错误。在系统内操作的不道德用户可以通过创建无效的数字支票来攻击系统，或者不道德的实体可以通过使其他用户看起来像恶意攻击者来攻击系统的这些其他用户。在一些实施例中，一些攻击最初可能与其它攻击无法区分。

[0355] 示例的具有多个卖方的买方克隆

[0356] 恶意买方可以在签名之后复制数字支票并将数字支票的相同副本发送给两个不同的卖方，其目的是它可以从两个卖方接收商品而仅支付一次。

[0357] 图26示意性地示出该恶意行为的示例，该恶意行为可以被称为具有多个卖方的买方克隆。例如，当数字支票旨在用于第一卖方时，恶意买方可以向第一卖方和第二卖方发送数字支票的相同副本。在接收到数字支票的副本后，第二卖方可以立即确定其接收到的数字支票未被认可。因此，第二卖方可以拒绝数字支票。

[0358] 示例的具有单个卖方的买方克隆

[0359] 恶意买方可以在对数字支票签名之后复制数字支票，并且稍后尝试将该数字支票重新用于同一卖方，其目的在于它可以从该卖方接收商品两次而仅支付一次。图27示意性地示出了该恶意行为，该恶意行为可以被称为具有单个卖方的买方克隆。卖方的移动计算机(MC)可以检测到这种恶意行为。例如，卖方的移动计算机可以保持来自其已经从其接收到数字支票的任何特定用户的最后一次数字支票的支票ID的记录。在一些实施例中，因为支票ID可以严格递增的顺序发出，所以卖方的移动计算机可以跟踪它从任何特定用户接收

的最后一次数字支票的ID。在一些实施例中，卖方的移动计算机可以跟踪它已经接收的所有数字支票的ID。从特定用户接收到的任何新数字支票应具有大于记录上的最高支票ID的支票ID。

[0360] 因为中央分类帐总是可以检测到复制的数字支票，所以处理平台将永远不会支付复制的数字支票。因此，卖方有责任保留该交易记录。卖方的MC可以执行软件程序，或者硬件程序可以自动记录它已接收到的交易和数字支票，并将所有新交易与该日志进行比较。

[0361] 示例分叉

[0362] 恶意卖方可以从买方接收数字支票。在接收到数字支票之后，卖方可以在认可数字支票之前复制数字支票，并尝试使用接收到的数字支票向第二卖方支付，其目的是在不支付费用的情况下从第二卖方购买商品。图28示意性地示出该恶意行为，该恶意行为可以被称为支票分叉。第二卖方可以拒绝从恶意卖方接收到的数字支票，因为它可以验证接收到的数字支票并不指示它是预定的接受者。

[0363] 示例卖方克隆

[0364] 恶意卖方可以复制所接收的数字支票并将其存入两次，其目的是针对交易卖方可以被支付两次。图29示意性地示出可被称为卖方克隆的该恶意行为。恶意卖方可以尝试卖方克隆，意图是买方被归咎于买方克隆。

[0365] 因为中央分类帐可以包含来自买方的相同支票ID号，所以当恶意卖方第二次存入所接收的数字支票时，处理平台可以识别出该恶意行为。为了检测该攻击，中央分类帐可以保留已从移动计算机的特定始发ID兑换的所有支票ID号的记录。在一些实施例中，公共分类帐可以包含该记录并且可以分发给系统的用户或移动设备。因此，用户或用户设备可以接收无序接收的数字支票。

[0366] 示例窥探

[0367] 恶意买方可绕过其移动计算机的安全元件并生成用于数字支票的虚假签名。虚假签名可以是不使用恶意买方的移动计算机的私钥创建的签名。图30示意性地示出可被称为用窥探的该恶意行为。恶意买方的目的可能是当数字支票无法兑现时，因为卖方无法验证它是否来自恶意买方。卖方可以立即检测到该恶意行为，因为数字支票的签名不能用买方的ID(例如作为数字支票一部分的恶意买方的公钥)解密。因此，卖方可以立即拒绝数字支票。

[0368] 示例重影

[0369] 恶意买方可以使用与其自身ID不同的ID生成数字支票，然后使用与不同ID相关联的私钥对其进行签名。图31示意性地示出可被称为重影的该恶意行为。如果卖方具有系统中所有用户的最新列表而处理平台在数字支票到达分类帐时可以检测到，则卖方可以检测重影。卖方可以具有公共分类帐的副本，并且可以拒绝数字支票或在其公共分类帐在数字支票上不包含买方ID的情况下自行承担风险地接受数字支票。在一些实施例中，系统可以采用加密算法的专有变体，从而使重影不可能。

[0370] 示例优点、过失和黑名单

[0371] 用户的某些活动可能是不期望的。系统可以以各种方式响应参与不期望活动的用户。第一类不期望的活动不需要对移动计算机或在移动计算机(MC)上运行的计算机程序进行任何明确的修改。第一类不期望的活动，透支，可以包括“拒付”数字支票，例如在数字支

票中发行高于发行人的余额可以支持的价值的价值。当用户参与透支时，系统可能会给他们带来过失。例如，过失系统可以跟踪以下中的一个或多个：基于拒付数字支票的数量的过失，基于拒付数字支票的价值的过失，基于拒付数字支票的新近度的过失，或其任何组合。过失系统可以通过兑换的数字支票总数或兑换的所有数字支票的价值来标准化其跟踪的一些或所有过失。

[0372] 第二种不期望的活动，黑客攻击，可能需要篡改移动计算机、移动计算机的安全元件(SE)或在移动计算机上运行的计算机程序。第二种不期望的活动可能包括上一节中提到的攻击，例如分叉、克隆或用窥探，这些攻击需要对移动计算机、移动计算机的安全元件、运行在移动计算机上的计算机程序进行明确的黑客攻击或修改(即移动计算机的行为、安全元件或计算机程序的未授权修改)。系统可以使用用于在移动计算机上运行的计算机程序的校验和与签名证书来检测一些黑客攻击。当用户参与黑客攻击时，系统可以将其置于黑名单中。黑名单可以是临时禁止或未来所有交易的用户ID列表。由于用户ID可以唯一地绑定到移动计算机，因此将用户ID列入黑名单可能等同于将移动计算机列入黑名单。任何被表明参与了来自黑客设备的黑客攻击的用户都可以列入黑名单。

[0373] 示例签名对账单

[0374] 卖方可以立即检测到某些类型的黑客攻击。例如，在具有多个卖方的买方克隆的情况下，第二卖方可以立即检测到它已经接收到恶意的“黑客”支票。如果将这种黑客攻击事件报告给处理平台可能是有利的。例如，卖方的移动计算机可以认可通过“恶意支票”(MC)认可接收的数字支票。可以像来自第二卖方的任何其它数字支票一样对MC认可进行签名，并且当与处理平台兑换该卖方拥有的其它数字支票时，可以将认可的支票发送到处理平台。

[0375] 处理平台接收签名的MC认可可以意味着系统中存在恶意行为者。然而，恶意行为者的标识可能不清楚。例如，由卖方提供的MC可以指示来自其实际与之交易的恶意买方的买方克隆；然而，它也可能是恶意卖方接收到的合法数字支票，该恶意卖方本身克隆买方的支票，目的是归咎于买方克隆的买方。在任何一种情况下，系统中都存在恶意行为者。

[0376] 示例模糊判定

[0377] 对于一些类别的黑客攻击，可能很难或不可能明确地将过失分配给交易中的特定方。然而，由于数字支票使用仅可用于交易各方的签名进行签名，因此可能会将责任归咎于某些方中的一方。例如，如果在处理平台处兑换了两个相同的数字支票，则发起人(买方)或存款人(卖方)可以是恶意行为者。在这种观察中，可以生成非限制性规则：

[0378] M(买方)+M(发送方)＝真，(规则4)

[0379] 其中M()表示布尔运算符，其确定参数是否为恶意，并且“+”表示逻辑OR运算。

[0380] 可以存储该信息以供将来使用。例如，如果中央分类帐稍后从不同卖方和同一买方接收到另一对相同的数字支票，则可以生成另一个非限制性规则：

[0381] (M(买方)+M(第一卖方))*(M(买方)+M(第二卖方))＝真，(规则5)

[0382] 其中“*”表示逻辑AND运算。规则5可以重写为：

[0383] M(买方)+(M(第一卖方))*M(第二卖方))＝真。(规则6)

[0384] 例如，在解释规则时，处理平台可以假设没有两个行为者是恶意的。因此，处理平台可以从规则6推断买方是恶意的。作为另一示例，处理平台可以断言恶意行为者是罕见的

先验信念，发生概率“p”大于0且小于1。然后，在规则6中两个卖方都是恶意的概率可以是p*p。规则6的左边大小可以表达为p+p*p。

[0385] 类似地，这种解释和假设可以扩展到包括系统对所有用户的所有观察，并且可以以乘积形式的总和来表达。因此，乘积中具有最少元素的项最可能是真实的。这些行为者可以被标记为恶意并列入黑名单，无论是立即、临时还是进一步调查。

[0386] 示例销售点

[0387] 系统可以与销售点系统交互。图32示意性地示出销售点(PoS)交易的示例。销售点(PoS)系统可以是收银机或等同物。销售点系统可以位于固定位置。销售点系统可以是基础架构(例如在诸如BigBoxStore的商家处具有收银机的现有基础架构)的一部分。

[0388] 商家可以与一个或多个用户标识符(ID)相关联。商家可以具有单个帐户，每个收银机一个帐户或每个商店位置一个帐户。商家的帐户可以与其他用户一样与移动计算机相关联，或者可以与由系统发布给商家的密钥对相关联。商家密钥对可以由商家拥有的计算机管理，或者可以由公司托管为类似于“软件即服务”(SaaS)的服务。

[0389] 为商家工作的检查者、收银员或PoS操作员可以访问专门发给他的移动计算机(MC)，或者移动计算机可以支持由为商家工作的授权的检查者、收银员或PoS操作员的多个登录。

[0390] 当买方希望从商家购买商品或服务时，买方可以创建发布给商家的用户ID但是经由短程链路(SRL)发送给检查者的数字支票。一旦具有检查者，检查者就可以通过访问例如商家的网络来验证数字支票是否有效。商家的网络可以是检查者而不是买方可以访问的安全的电气和电子工程师协会(IEEE)802.11网络或类似的网络。检查者可以经由例如商家的安全网络将数字支票发送到商家的钱包。

[0391] 在涉及销售点系统的交易中，可以为商家发出但是给予检查者的来自买方的原始数字支票。然后，在将数字支票发送给商家之前，检查者可以添加“由认可处理”(HBE)。然后，商家可以添加“仅用于存款的认可”(FDOE)并与处理平台兑换数字支票。

[0392] 在将数字支票发送给商家之前，检查者可以添加包含其自己的用户ID并由其移动计算机的安全元件签名的“被处理的”认可(HBE)。商家可以选择仅处理来自其检查者之一的标有HBE的数字支票。

[0393] 当由商家兑换数字支票时，可以例如使用HBE向检查者发送消息，指示处理平台已经清除了数字支票。此时，检查者可以通过将数字支票的价值输入收银机作为“兑现的支票”或适当的指定来结束销售。

[0394] 商家的PoS系统可能需要很少或不需要改变。商家可以向其检查者发布移动计算机。一些检查者可能具有自己的MC，并且商家可能会选择接受从检查者私人拥有的MC发布的HBE的数字支票。

[0395] 相对于中央分类帐的示例资金进出

[0396] 资金可以从其它普通货币工具进入和退出中央分类帐。当用户或用户设备希望将钱添加到中央分类帐时，处理平台可以通过转入方法将该钱转移到用户或用户设备的账户中。转入方法可以是从信用卡、自动清算所(ACH)转移、实物支票的邮寄或物理现金工具的处理中提取。处理平台可以在接收到钱之后贷记用户或用户设备的账户。对于存在交易费用的这种工具，处理平台可能会或可能不会补偿这些费用。

[0397] 当用户或用户设备希望从中央分类帐中移除钱时，处理平台可以通过转出方法将该钱从用户或用户设备的账户中转出。转出方法可以是ACH转移、实物支票的邮寄或任何类似手段。处理平台可以在使用转出方法发送钱之前借记用户或用户设备的账户。处理平台可以针对移除的钱收取费用。对于不同的客户或不同类型的客户，该费用可能不同。

[0398] 可以向商家或用户针对密钥对收取费用。例如，商家或用户可以定期(例如，每月)或仅一次(例如，在设置期间)被收费。密钥对可以以固定价格或协商价格出售，其可以包括具有多个活动密钥对的商家的批量折扣。处理平台可以为某些用户或商家提供优惠或独家定价。

[0399] 示例费用

[0400] 如上所述，可以对进入、离开或在系统内的任何转移收取费用。这些转移费用可能与交易规模成比例，固定或两者的组合。对于账户余额不足的用户设备发出的数字支票，也可能会对费用进行评估。处理平台可以选择承担所产生的债务，并且在这种情况下可以收取与所产生的债务相关联的利息或费用。

[0401] 示例来源的交易

[0402] 在此公开的系统中的交易可以“来源”自中央分类帐上的买方账户中的可用余额。如果买方发出数字支票可能是有利的，该数字支票是从对于公共分类帐已知的来源自动提取资金，而不是其中的一部分。例如，买方可能希望以100美元从商家购买商品，并且可能希望中央分类帐从特定来源(诸如买方在其银行的支票帐户)或从特定信用卡提取100美元。该系统可以包括用于将源信息(SI)(诸如银行账户信息或信用卡信息)输入到中央分类帐的接口。买方的移动计算机可以存储带有标识字符串(SAIS)的源帐户。数字支票可以包括用于存储SAIS的数据字段。

[0403] 用于将源信息输入到系统中的界面在不同的实施方式中可以是不同的。例如，界面可以包括MC上的网页或“应用(app)”。这种界面可以包括可视界面(例如，使用数字相机和实施计算机视觉算法的软件)，用于从物理支票、银行对账单、实体信用卡、信用卡对账单或其任何组合中提取源信息。

[0404] 系统可能不接受具有空白SAIS字段的数字支票。如果系统接受具有空白SAIS字段的数字支票，则空白SAIS字段可以被解释为暗示处理平台应该在用户帐户或其它默认来源中提取资金。

[0405] 数字支票可以包含指示费用分摊政策的费用分摊字段。费用分摊字段可以是位、位字段或指示费用分摊政策(诸如买方将支付与来源相关联的费用或卖方或买方将如何分摊与来源相关联的费用)的其它数值。例如，数字支票可以包括指示买方将(或将不)支付与源账户相关联的来源费用(例如，信用卡费用)的位，以及指示买方将(或将不)支付转移费用(例如，处理平台收取的用于将资金从买方账户转移到卖方账户的费用)的第二位。

[0406] 系统可以使这些费用对买方或卖方可见或不可见。在一些实施例中，卖方可以能够基于其相关费用和买方的费用分摊政策选择性地拒绝数字支票。

[0407] 示例资金验证

[0408] 卖方可以经由诸如因特网的网络连接到处理平台，即使买方可能不是。例如，商家可以通过其专用网络连接来连接具有到因特网的有线或无线连接，即使买方可能由于例如差的蜂窝电话连接性而未连接到处理平台。当卖方访问因特网时，它可以在接受交易之前

验证买方帐户中的资金可用性。

[0409] 例如,可以允许卖方提交由买方发出的具有诸如“查询认可”(QE)的认可的数字支票的认可版本,指示数字支票仅用作查询。这种查询认可(QE)可以由卖方签名。在接收到QE的数字支票时,处理平台可以向卖方返回关于买方和买方完成交易的能力的信息。例如,处理平台可以返回诸如即时资金可用性(当前中央分类帐余额,或者如果当前中央分类帐余额达到或超过数字支票的值)的信息、如果数字支票借助于SAIS字段获取的源信息(例如,如果预期对当前资金透支,则包括默认源信息),或其任何组合。源信息可能包括有关费用的信息。费用分摊字段可用于确定是否响应于QE数字支票来分摊费用信息(例如,可能不与持有指示买方正在承担费用的数字支票的卖方分摊费用信息)。

[0410] 涉及金融机构的示例安全交换加密签名数字支票

[0411] 用于安全地交换本公开的内容和记录(例如,加密签名的数字支票)的系统和方法可以由一个或多个用户设备、一个或多个处理平台以及一个或多个金融机构服务器来实施。图33示意性地示出安全地交换涉及一个金融机构的加密签名数字支票的另一实施例。在图33中所示的非限制性示例实施例中,用户可以操作用户设备来创建、发送、接收、修改或兑换个体记录100,诸如加密签名的数字支票。例如,数字支票的发送方102a可以操作支票发送方设备116a或116a'。数字支票的接收方102b可以操作支票接收方设备116b。

[0412] 用户设备,例如支票发送方设备116a和支票接收方设备116b,可以相同或可以不同。用户设备可以包括蜂窝电话、平板计算机、电子阅读器、智能手表、头戴式增强、虚拟或混合现实显示系统、可穿戴显示系统或计算机。用户设备116a或116b可以使用通信链路120a、120b(例如蜂窝通信链路)与网络118上的其它设备通信。网络118可以是可通过有线或无线通信链路(例如实施电气和电子工程师协会(IEEE)802.11标准)访问的局域网(LAN)、广域网(WAN)或因特网。

[0413] 当发送数字支票100时,支票发送方设备116a和支票接收方设备116b中的一个或二者可以离线并且不连接到网络118。支票发送方102a使用支票发送方设备116a可以使用短程链路(SRL)122向支票接收方102b发送加密签名的数字支票100。短程链路(SRL)122可以是对等无线或用户设备116a或116b可以通过其彼此通信的其它链路。短程链路(SRL)122可以基于红外数据协会(IrDA)/红外物理层规范(IrPHY)、蓝牙®、近场通信(NFC)、ad hoc 802.11或任何其它有线或无线通信方法或系统。

[0414] 由服务提供者104操作的处理平台124可以使用通信链路126与网络118上的其它设备(例如用户设备116a、116b)通信。由服务提供者104操作的金融机构服务器3304或附属于处理平台104的金融机构可以与网络118上的其它设备(例如,处理平台124)通信。通信链路120a、120b、126或3304可以是有线或无线通信、蜂窝通信、蓝牙®、局域网(LAN)、广域网(WLAN)、射频(RF)、红外(IR)或任何其它通信方法或系统。

[0415] 用户102a或102b可以与处理平台124兑换加密签名的数字支票。例如,操作支票发送方设备116a的发送方102a可以是来自卖方的产品或服务的买方,其是操作支票接收方设备116b的接收方102b。参考图33B,数字支票100的内容110可以包括用于从发送方102a的账户到接收方102b的账户转移加密货币(或真实货币)的金额或者处理平台124从发送方102a的帐户到接收方102b的帐户(或从支票发送方设备116a的帐户到支票接收方设备116b的帐

户)转移加密货币金额的指令。支票发送方设备116a可以使用发送方设备私钥对数字支票100进行数字签名,并将数字支票100电子地传送给接收方设备116b。接收方设备116b认可具有认可114的支票(例如,在该情境中,认可可以是“仅用于存款的认可”)并使用接收方设备私钥对数字支票进行数字签名以创建修改的数字支票100m1。接收方设备116b将修改的数字支票100m1传送到服务提供者104,该服务提供者104兑换修改的数字支票100m1。

[0416] 处理平台124可以验证修改的数字支票100m1由发送方设备116a和接收方设备116b(使用它们相应的公钥)进行了真实签名。处理平台124进而可以指示金融机构服务器3304从发送方102a的账户到接收方102b的账户(或从支票发送方设备116a的账户转移到支票接收方设备116b的账户)转移加密货币的金额。金融机构服务器3304可以维护发送方102a的账户和接收方102b的账户。在一些实施方式中,处理平台124还可以跟踪发送方102a的账户余额和接收方102b的账户余额。因此,在该非限制性示例中,记录用作数字支票系统中的支票,并且可以由买方(发送方102a)用于向卖方(接收方102b)支付资产。服务提供者104可以充当该交换(例如,借记买方的加密货币或真实货币账户并贷记卖方的加密货币账户)中的至少一些交换的清算所。

[0417] 图33C示意性地示出安全地交换加密签名的数字支票的另一实施例。在接收到修改的数字支票100m1之后,处理平台124可以验证修改的数字支票100m1由发送方设备116a和接收方设备116b(使用它们相应的公钥)二者进行了真实签名。处理平台124可以进而指示金融机构的服务器3304a从金融机构处的发送方102a的账户到另一金融机构处的接收方102b的账户(或者从金融机构处的支票发送方设备116a的账户到另一金融机构处的支票接收方设备116b的账户)转移加密货币的金额。金融机构服务器3304a可以维护发送方102a的账户。金融机构服务器3304b可以维护接收方102b的账户。在接收到加密货币金额的转移之后,另一金融机构的服务器3304b可以更新另一金融机构处的接收方102b的账户(或支票接收方设备116b的账户)余额。在一些实施方式中,处理平台124还可以跟踪发送方102a的账户余额和接收方102b的账户余额。

[0418] 在一些实施例中,在此描述的一些术语可具有如15U.S.C§1693(消费者保护定义)中所定义的含义。例如,金融机构可以是州或国家银行、州或联邦储蓄和贷款协会、共同储蓄银行、州或联邦信用合作社,或直接或间接持有属于消费者的帐户的任何其他人。作为另一示例,账户可以是活期存款、储蓄存款或其它资产账户(除了信用余额之外)。

[0419] 示例数字支票

[0420] 在一些实施例中,支票接收方可以从支票发送方接收加密签名的数字支票。图4是示出安全地交换和兑换针对一个记录接收方创建的个体记录的一个实施例的交互图。支票接收方102b(例如,收款方)使用支票接收方设备116b可以通过向支票发送方设备116a发送支付请求402来从支票发送方102a(例如,付款方)请求数字支票100。支票接收方102b可以在交互404处使用短程链路(SRL)122向支票发送方102a发送支付请求402。支付请求402可以包括内容,例如支票接收方设备的支付金额110b和公钥106b。支付金额110b可以是支票接收方102b期望从支票发送方102a接收的金额。在一些实施例中,支票接收方设备的公钥106b可以唯一地识别支票接收方设备116b。在一些实施例中,支票接收方设备的公钥106b可以唯一地识别支票接收方102b。公钥106b可以在公共记录中,在一些实施例中,该公共记录可以存储在安全元件(SE)204b中。

[0421] 示例伙伴标识

[0422] 参考图34A，在交互408处，支票发送方设备116a使用其交易伙伴标识符可以通过伙伴标识来确认支票接收方设备116b的标识。因为支付请求402可能已经电子地发送到支票接收方设备116a，所以支票接收方设备116a可能不确定发送支付请求402的用户设备的标识。伙伴标识可能是有利的。例如，通过伙伴标识，支票发送方设备116a可以区分支付请求402与支票接收方设备116b和恶意用户。作为另一示例，通过伙伴标识，恶意用户不能接收不旨在用于它的数字支票。作为另一示例，通过伙伴标识，即使在接收到不旨在用于它的数字支票之后，恶意用户也不能兑换数字支票。

[0423] 示例数字支票创建

[0424] 在支票发送方设备116a的安全元件(SE)204a验证记录发送方的认证信息之后，安全元件(SE)204a可以在交互416处对数字支票100进行签名。在交互416处对个体记录100进行签名之前，安全元件(SE)204a可以要求提供要被数字签名的块(例如数字支票100的块105a)以及记录发送方102a的认证二者。认证的非限制性示例可以包括密码认证、诸如指纹认证或虹膜认证的生物度量认证、生物数据认证或其任何组合。生物度量认证可以利用基于例如指纹或眼睛图像的生物度量模板。安全元件(SE)204a可以实施用于识别生物度量模板的生物度量模糊库。

[0425] 参考图33B，数字支票100可以是包括一个或多个块的数字对象。数字支票100可以包括块105a，并且块105a可以包括“来自字段”中的支票发送方设备116a的公钥106a、“到字段”中的支票接收方设备的公钥106b、支票ID 108、支付金额110a以及块105a的支票发送方签名112a。支票发送方设备116a的公钥106a可以识别数字支票100的发起者，即支票发送方设备116a。支票接收方设备的公钥106b可以识别数字支票100的原始接受者，即支票接收方设备116b。支付金额110a可以变化。数字支票100a中的支付金额110a和图34A中请求的支付金额110b可以相同、类似、相关或不同。在加密货币的情境中，发送的支付金额110a和请求的支付金额110b可以是加密货币的相同金额。发送的支付金额110a和请求的支付金额110b可以类似或相关。例如，请求的支付金额110b可以是税前金额，并且发送的支付金额110a可以是税后金额。作为另一示例，请求的支付金额110b可以是预付小费金额，并且发送的支付金额110a可以是付小费后金额。

[0426] 参考图34A，在交互420处，支票发送方102a可以例如使用短程链路(SRL)以对等方式向支票接收方102b发送数字支票100。一旦具有支票接收方102b，支票接收方102b就可以在交互424处验证数字支票100。验证数字支票100可以包括认证支票发送方签名112a。认证支票发送方签名112a可以包括使用支票发送方设备的公钥106a确定是否已经使用支票发送方设备的私钥210创建了支票发送方签名112a。可以通过多种方式获得支票发送方设备的公钥106a。例如，可以从数字支票100获得支票发送方设备的公钥106a。作为另一示例，支票发送方设备的公钥106a可以从支票接收方设备116b的公共记录206中获得。

[0427] 示例个体记录兑换-一个金融机构

[0428] 参考图33B和图34A，在成功验证数字支票100之后，支票接收方设备116b可以使用其安全元件204b在交互428处创建修改的数字支票100m1并对其签名。在交互428处对修改的数字支票100m1进行签名之前，安全元件(SE)204b可以要求提供要被数字签名的块(例如修改的数字支票100m1的块105b)以及支票接收方的认证信息512b二者。修改的数字支票

100m1可以包括数字支票100的块105a和认可块105b。例如，认可可以是“仅用于存款的认可”(FPOE)114，其与支票接收方的公钥106b一起指定修改的数字支票100m1只能由支票接收方102b兑换。在加密货币的情境中，在接收到“仅用于存款的认可”(FDOE)的数字支票之后，处理平台124可以存入或指示存入加密货币金额到支票接收方102b的账户但是不会识别对另一方的进一步认可。

[0429] 在对修改的数字支票100m1进行签名之后，当支票接收方102b通过例如网络118与处理平台124通信时，支票接收方102b可以在交互432处与处理平台124兑换修改的数字支票100m1。在兑换时，操作处理平台124的服务提供者104可以通过验证修改的数字支票100m1中的块105a和105b链中的一个或多个签名(例如支票发送方签名112a和支票接收方签名112b)的真实性，在交互436处处理修改的个体记录100m1。在成功验证之后，处理平台124可以基于修改的数字支票100m1的支付金额110a来执行。

[0430] 处理平台124可以指示金融机构服务器3304从发送方102a的账户到接收方102b的账户(或者从支票发送方设备116a的帐户到支票接收方设备116b的帐户)转移例如加密货币或真实货币的支付金额110a。操作服务器3304a的金融机构可以维护发送方102a的帐户和接收方102b的帐户。在交互3404处，处理平台124可以指示金融机构或由金融机构操作的服务器3304a借记发送方帐户并贷记接收方帐户支付金额110a。在对发送方账户中的处理平台124进行认证和资金充足之后，金融机构可以在交互3408处借记发送方账户并贷记接收方账户支付金额110a。在从金融机构服务器3304a接收到账户已经在交互3424处借记并贷记的指示之后，处理平台124可以基于交互3428处的修改的数字支票100m1的发送支付金额110a向接收方设备116b发送处理平台124已经执行的指示。在一些实施方式中，处理平台124可以跟踪发送方102a的账户余额和接收方102b的账户余额，并在交互3424之后更新账户余额。

[0431] 示例个体记录兑换-多个金融机构

[0432] 图34B是示出安全地交换和兑换涉及两个金融机构的加密签名数字支票的另一实施例的交互图。参考图34A描述图34B中的支付请求402和交互404、408、416、420、424、428、432和436。在交互436处成功验证之后，处理平台124可以基于修改的数字支票100m1的支付金额110a来执行。

[0433] 处理平台124可以指示金融机构服务器3304从发送方102a的账户到接收方102b的账户(或者从支票发送方设备116a的账户到支票接收方设备116b的账户)转移发送的支付金额110a。操作服务器3304a的金融机构可以维护发送方102a的帐户。操作服务器3304a的金融机构可以维护接收方102b的账户。在交互3404处，处理平台124可以指示金融机构或由金融机构操作的服务器3304a借记发送方帐户并且贷记接收方帐户请求的支付金额110a。在认证处理平台124和发送方账户中的资金充足之后，金融机构可以在交互3408处借记发送方账户。金融机构服务器3304a可以进而请求另一金融机构或由另一金融机构操作的服务器3304b在交互3412处贷记接收方帐户发送的支付金额110a。在交互3412处成功贷记接收方帐户发送的支付金额110a之后，服务器3304b可以向金融机构的服务器3304a发送接收方帐户已成功贷记的指示。

[0434] 在从金融机构服务器3304a接收到账户已经在交互3424处借记并贷记的指示之后，处理平台124可以向接收方设备116b发送处理平台124基于交互3428处的修改的数字支

票100m1的发送的支付金额110a已经执行的指示。在一些实施方式中，处理平台124可以跟踪发送方102a的账户余额和接收方102b的账户余额，并在交互3424之后更新账户余额。

[0435] 示例支付类型

[0436] 从发送方102a到接收方102b的支付可以类似于支票交易、借记交易、信用卡交易、自动清算所(ACH)交易、电汇或其组合。支票类型的交易可能需要“条款”，例如，在统一商业代码(UCC)下。支票交易可以被认为是金融机构(例如，操作服务器3304a的金融机构)和在金融机构拥有账户的客户(例如，发送方102a)之间的合同。(1)如果在金融机构的柜台(例如，虚拟柜台)处理则可以立即完成支付，或者(2)在金融机构接收到修改的支票100m1的那天的午夜可完成支付。金融机构可能对欺诈活动或未授权的支付负责，除非账户持有人疏忽。

[0437] 借记类型交易可以被认为是UCC条款定义的例外，因为借记交易可以涉及完成交易的“信号”。可以在销售时(例如，当卖方、收款方或支票接收方接收数字支票时)完成支付，其中立即授权金融机构将账户借记给卖方。在一些实施例中，未授权的支付受制于支票发送方“免赔”责任。例如，如果声称的支票发送方在短时间段(例如，两天)内报告未授权的支付，则免赔额可以是50美元。如果声称的支票发送方在中等时间段(例如，60天)内报告未授权的支付，则免赔额可以是500美元。如果未在中等时间段内报告未授权的支付，则声称的支票发送方应对未授权的支付负责。除非账户持有人疏忽，否则声称的支票发送方的金融机构可能对剩余的未授权的余额负责。

[0438] 利用信用卡类型的交易，当支票发送方支付金融机构(例如，信用卡公司)时，支付完成。如果已经支付了对账单(两个计费周期来提出争议)，则可能不允许针对收费提出争议。只要对账单尚未支付，金融机构始终负有责任。

[0439] ACH类型的交易可以包括信用ACH支付和借记ACH支付。对于信用ACH支付，金融机构可以出于任何原因取消支付。对于借记ACH支付，帐户持有人(例如，支票发送方)具有1个工作日来停止支付，否则支付通过并且客户有15天通知未授权的支付。可以在销售时考虑支付，或者对于借记ACH在最多一天之后支付，或对于信用ACH在最多两天之后支付。

[0440] 电汇可以是金融机构之间的转账。电子资金转移法案允许涉及自然人的电汇。电汇涉及两个阶段的支付订单：首先，付款方或支票发送方向诸如操作服务器3304a(或处理平台124)的金融机构的第一金融机构提供转移信息，以向第二金融机构(例如，操作服务器3304b的其它金融机构)转移钱。其次，第一金融机构可以向第二金融机构提供关于转移的指令。无论资金是否实际从第一金融机构转移到第二金融机构，当步骤2完成时，可以认为支付已完成。因此，支票发送方或付款方对支票接收方的收款方负有非常快的责任，但如果他们在转账中犯了错误，则第二金融机构可能要负责。

[0441] 在一些实施方式中，在此公开的系统和方法可以用于复杂的讨价还价。例如，卖方或供应商可以以一种价格出售借记型交易，因为卖方可以更快地获得资金。然而，买方可能是恶意的，由于可扣除的起征点，卖方可能会自动阻止借记请求支付少于50美元的商品。作为另一个示例，卖方可以请求电汇支付，因为他们知道将发生金融机构之间的验证。然而，买方可以拒绝这种请求，因为除非涉及费用分摊，否则买方可能不想支付两个步骤的转移费用。

[0442] 示例可穿戴显示系统

[0443] 用户设备116可以是或可以包括在可穿戴显示设备中，该可穿戴显示设备可以有利地提供更加沉浸式虚拟现实(VR)、增强现实(AR)或混合现实(MR)体验，其中数字再现图像或者其部分以其似乎是或可能被认为是真实的方式呈现给佩戴者。

[0444] 不受理论的限制，据信人眼通常可以解释有限数量的深度平面以提供深度感知。因此，通过向眼睛提供与这些有限数量的深度平面中的每一个深度平面相对应的图像的不同呈现，可以实现高度可信的感知深度模拟。例如，包含波导堆叠的显示器可以被配置为佩戴定位在用户或观察者的眼睛前方。通过使用多个波导将来自图像注入装置(例如，离散显示器或多路复用显示器的输出端，其经由一根或多根光纤传输图像信息)的光以对应于与特定波导相关联的深度平面的特定角度(和发散量)引导到观察者的眼睛，可以利用波导堆叠来向眼睛/大脑提供三维感知。

[0445] 在一些实施例中，可以利用两个波导堆叠，一个用于观察者的每只眼睛，以向每只眼睛提供不同的图像。作为一个示例，增强现实场景可以使得AR技术的佩戴者看到以人、树、背景中的建筑物和具体平台为特征的真实世界公园式设置。除了这些项目之外，AR技术的佩戴者还可以感知到他“看到”站在真实世界平台上的机器人雕像，以及似乎是大黄蜂的拟人化的飞行的卡通一样的头像角色，即使机器人雕像和大黄蜂在真实世界中不存在。(多个)波导堆叠可用于生成对应于输入图像的光场，并且在一些实施方案中，可穿戴显示器包括可穿戴光场显示器。用于提供光场图像的可穿戴显示设备和波导堆叠的示例在美国专利公开No.2015/0016777中描述，其全部内容通过引用整体结合在此。

[0446] 图35示出可穿戴显示系统3500的示例，其可用于向佩戴者3504呈现AR、MR或VR体验。可穿戴显示系统3500可被编程以执行在此描述的任何应用或实施例。显示系统3500包括显示器3508，以及支持该显示器3508的功能的各种机械和电子模块和系统。显示器3508可以耦合到框架3512，该框架3512可由显示系统佩戴者或观察者3504佩戴，并且被配置为将显示器3508定位在佩戴者3504的眼睛前方。显示器3508可以是光场显示器。在一些实施例中，扬声器35616耦合到框架3512并且在一些实施例中邻近用户的耳道放置，另一个扬声器(未示出)邻近用户的另一耳道放置以提供立体声/可成形声音控制。显示器3508诸如通过有线引线或无线连接可操作地耦合3520到本地数据处理模块3524，该本地数据处理模块3524可以以各种配置安装，诸如固定地附接到框架3512，固定地附接到头盔或用户佩戴的帽子，嵌入耳机或以其它方式可拆卸地附接到用户3504(例如，背包式配置、带式连接式配置)。

[0447] 本地处理和数据模块3524可以包括硬件处理器，以及非暂态数字存储器，诸如非易失性存储器(例如闪存)，两者都可以用于辅助处理、缓存和存储数据。数据包括如下数据：(a)从传感器(诸如图像捕获设备(诸如相机)、麦克风、惯性测量单元、加速度计、指南针、GPS单元、无线设备和/或陀螺仪)捕获(其可以例如可操作地耦合到框架3512或以其它方式附接到佩戴者3504)；和/或(b)使用远程处理模块3528和/或远程数据存储库3532获取和/或处理，可能用于在这种处理或取得之后传递到显示器3508。本地处理和数据模块3524可以通过通信链路3536、3540(诸如经由有线或无线通信链路)可操作地耦合到远程处理模块3528和远程数据存储库3532，使得这些远程模块3528、3532可操作地彼此耦合，并且可用作本地处理和数据模块3524的资源。

[0448] 在一些实施例中，远程处理模块3528可以包括一个或多个处理器，其被配置为分

析和处理数据和/或图像信息，诸如由图像捕获设备捕获的视频信息。视频数据可以本地存储在本地处理和数据模块3524中和/或在远程数据存储库3532中。在一些实施例中，远程数据存储库3532可以包括数字数据存储设施，其可以通过因特网或“云”资源配置中的其它网络配置而可用。在一些实施例中，存储所有数据并且在本地处理和数据模块3524中执行所有计算，允许从远程模块完全自主使用。

[0449] 在一些实施方式中，本地处理和数据模块3524和/或远程处理模块3528被编程为执行在此公开的系统和方法的实施例。图像捕获设备可以捕获用于特定应用的视频(例如，用于眼睛跟踪应用的佩戴者眼睛的视频或者用于手势识别应用的佩戴者的手或手指的视频)。视频可以由处理模块3524、3528中的一个或二者进行分析。在一些情况下，将至少一些分析卸载到远程处理模块(例如，在“云”中)可以提高计算的效率或速度。在此公开的系统和方法的参数可以存储在数据模块3524和/或3532中。

[0450] 分析结果可以由处理模块3524、3528中的一个或二者使用以用于附加操作或处理。例如，可穿戴显示系统3500可以使用生物度量、眼睛跟踪、手势、对象、姿势等的识别或分类。例如，可穿戴显示系统3500可以分析佩戴者3504的手的捕获的视频，并且通过佩戴者的手识别手势(例如，拾取真实或虚拟对象，发信号通知同意或异议(例如，“拇指向上”或“拇指向下”)等)，并且可穿戴显示系统3500可以响应于佩戴者的手势执行适当的动作(例如，移动虚拟对象，基于佩戴者的同意/异议执行附加操作)。作为另一示例，佩戴者的眼睛的视频可以由可穿戴显示系统3500分析，以通过显示器3508确定佩戴者3504的注视方向。作为另一示例，处理模块3524、3528可以分析佩戴者周围环境的视频来识别(或计数)特定类别对象的对象(例如，识别佩戴者3504附近的“猫”或“汽车”)。可穿戴显示系统3500的处理模块3524、3528可以被编程为执行在此描述的任何方法或视频或图像处理应用或用于在此描述的加密签名记录的安全交换的任何方法或应用。例如，可穿戴显示系统3500的实施例可以被配置为用户设备116a(例如，发送方102a)或用户设备116b(例如，接收方102b)并且用于以如在此所述的加密安全的方式创建、发送、接收、修改或兑换记录100。

[0451] 附加方面

[0452] 加密签名记录的安全交换

[0453] 在第一方面，公开了一种用于安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从记录接收方设备接收接收方个体记录，其中，接收方个体记录包括发送方个体记录和接收方个体记录的接收方签名，其中，在从记录接收方设备接收记录内容请求以及识别记录接收方设备之后，由记录发送方设备创建发送方个体记录，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，其中，使用记录发送方设备的发送方私钥创建发送方签名，其中，发送方公钥和发送方私钥形成发送方公钥加密对，其中，在从记录发送方设备接收发送方个体记录以及使用发送方公钥验证发送方个体记录而不一定与处理平台通信之后，由记录接收方设备创建接收方个体记录，其中，使用记录接收方设备的接收方私钥创建接收方签名，以及其中，接收方公钥和接收方私钥形成接收方公钥加密对；验证接收方个体记录；以及如由接收方个体记录指示地执行记录接收方设备。

[0454] 在第2方面，根据方面1所述的方法，其中，内容请求包括接收方公钥和所请求的内容，并且其中，记录内容与所请求的内容相关。

[0455] 在第3方面，根据方面1-2中任一方面所述的方法，其中，识别记录接收方设备包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0456] 在第4方面，根据方面1-3中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0457] 在第5方面，根据方面4所述的方法，其中，记录标识符是单调递增的数字。

[0458] 在第6方面，根据方面1-5中任一方面所述的方法，其中，从记录接收方设备接收发送方个体记录包括直接或通过中间设备经由短程链路从记录发送方设备接收发送方个体记录。

[0459] 在第7方面，根据方面6所述的方法，其中短程链路是对等通信链路。

[0460] 在第8方面，根据方面1-7中任一方面所述的方法，其中，接收方个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0461] 在第9方面，根据方面1-8中任一方面的方法，其中，在接收到记录发送方的认证信息之后由记录发送方设备创建发送方个体记录，以及其中，在接收到记录接收方的认证信息之后由记录接收方设备创建接收方个体记录。

[0462] 在第10方面，根据方面1-9中任一方面的方法，其中，验证发送方个体记录包括：使用发送方公钥来确定使用发送方私钥创建发送方签名；并使用发送方公钥来确定使用发送方私钥创建发送方签名。

[0463] 在第11方面，根据方面1-10中任一方面所述的方法，进一步包括向记录发送方设备或记录接收方设备提供公共记录，其中，公共记录包括发送方公钥和接收方公钥。

[0464] 在第12方面，根据方面1-10中任一方面所述的方法，进一步包括：向记录发送方设备提供公共记录，其中，公共记录包括发送方公钥和接收方公钥；并使记录发送方设备向记录接收方设备发送公共记录。

[0465] 在第13方面，根据方面1-10中任一方面所述的方法，进一步包括：向记录接收方设备提供公共记录，其中，公共记录包括发送方公钥和接收方公钥；以及使记录接收方设备向记录发送方设备发送公共记录。

[0466] 在第14方面，根据方面11-13中任一方面所述的方法，其中，公共记录进一步包括公共记录的第三签名，其中，公共记录进一步包括公共记录的第三签名，并且其中，第三签名使用处理平台的第三私钥来创建。

[0467] 在第15方面，根据方面11-14中任一方面所述的方法，进一步包括：从中央记录生成公共记录，其中，中央记录包括发送方公钥、接收方公钥、记录发送方设备的用户记录状态，以及记录接收方设备的用户记录状态。

[0468] 在第16方面，根据方面15所述的方法，进一步包括：确定记录发送方的用户记录状态禁止处理平台如由接收方个体记录指示地执行记录接收方设备；以及将付款方设备添加到过失列表。

[0469] 在第17方面，公开了一种用于安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从记录接收方设备接收内容请求；识别记录接收方设备；创建发送方个体记录，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，其中，使用记录发送方

设备的发送方私钥创建发送方签名，以及其中，发送方公钥和发送方私钥形成发送方公钥加密对；向记录接收方设备发送发送方个体记录；以及接收记录接收方设备的指示：接收发送方个体记录；使用发送方公钥验证发送方个体记录而不一定与处理平台通信；创建接收方个体记录，其中，接收方个体记录包括发送方个体记录和接收方个体记录的接收方签名，其中，接收方签名使用记录接收方设备的接收方私钥创建，以及其中，接收方公钥和接收方私钥形成接收方公钥加密对；与处理平台兑换接收方个体记录；以及如由接收方个体记录指示地接收处理平台的执行。

[0470] 在第18方面，根据方面17所述的方法，其中，内容请求包括接收方公钥和所请求的内容，并且其中，记录内容与所请求的内容相关。

[0471] 在第19方面，根据方面17-18中任一方面所述的方法，其中，识别记录接收方设备包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0472] 在第20方面，根据方面17-19中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0473] 在第21方面，根据方面20所述的方法，其中，记录标识符是单调递增的数字。

[0474] 在第22方面，根据方面17-21中任一方面所述的方法，其中，向记录接收方设备发送发送方个体记录包括直接或通过中间设备经由短程链路向记录接收方设备发送发送方个体记录。

[0475] 在第23方面，根据方面22所述的方法，其中，短程链路是对等通信链路。

[0476] 在第24方面，根据方面17-23中任一方面所述的方法，其中，接收方个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0477] 在第25方面，根据方面24所述的方法，其中，接收方个体记录进一步包括查询认可，其中如由接收方个体记录所指示地对记录接收方设备执行包括向记录接收方设备发送查询结果，并且其中，查询结果指示处理平台将如接收方个体记录所指示地执行。

[0478] 在第26方面，根据方面17-25任一方面所述的方法，其中，创建发送方个体记录包括由记录发送方设备接收记录发送方的认证信息，并且其中，创建接收方个体记录包括由记录接收方设备接收记录接收方的认证信息。

[0479] 在第27方面，根据方面17-26中任一方面所述的方法，其中，验证发送方个体记录包括使用发送方公钥来确定使用发送方私钥创建发送方签名。

[0480] 在第28方面，根据方面17-27中任一方面所述的方法，其中，发送方签名由记录发送方设备的安全元件使用发送方私钥创建，并且其中，发送方私钥存储在记录发送方设备的安全元件中。

[0481] 在第29方面，根据方面17-28中任一方面所述的方法，其中，接收方签名由记录接收方设备的安全元件使用接收方私钥创建，并且其中，接收方私钥存储在记录接收方设备的安全元件中。

[0482] 在第30方面，根据方面17-29中任一方面所述的方法，进一步包括从处理平台接收公共记录，其中，公共记录包括发送方公钥和接收方公钥。

[0483] 在第31方面，根据方面17-29中任一方面所述的方法，进一步包括从记录接收方设备接收公共记录，其中，公共记录包括发送方公钥和接收方公钥。

[0484] 在第32方面，根据方面30-31中任一方面所述的方法，其中，公共记录进一步包括公共记录的第三签名，其中，第三签名使用处理平台的第三私钥创建，该方法进一步包括使用处理平台的第三公钥来验证公共记录而不一定与处理平台通信，其中，第三公钥和第三私钥形成第三公钥加密对，并且其中，验证公共记录包括使用第三公钥来确定使用第三私钥创建第三签名。

[0485] 在第33方面，提供了一种用于安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并包括：向记录发送方设备发送内容请求；从记录发送方设备接收发送方个体记录，其中，在从记录接收方设备接收内容请求并识别记录接收方设备之后，由记录发送方设备创建发送方个体记录，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，其中，使用记录发送方设备的发送方私钥创建发送方签名，以及其中，发送方公钥和发送方私钥形成发送方公钥加密对；使用发送方公钥验证发送方个体记录而不一定与处理平台通信；创建接收方个体记录，其中，接收方个体记录包括发送方个体记录和接收方个体记录的接收方签名，以及其中，使用记录接收方设备的接收方私钥创建接收方签名，以及其中，接收方公钥和接收方私钥形成接收方公钥加密对；用处理平台兑换接收方个体记录；以及如由接收方个体记录指示地接收处理平台的执行。

[0486] 在第34方面，根据方面33所述的方法，其中，内容请求包括接收方公钥和所请求的内容，并且其中，记录内容与所请求的内容相关。

[0487] 在第35方面，根据方面33-34中任一方面所述的方法，其中，识别收款方设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略确认，或其任何组合。

[0488] 在第36方面，根据方面33-35中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0489] 在第37方面，根据方面36所述的方法，其中，记录标识符是单调递增的数字。

[0490] 在第38方面，根据方面33-37中任一方面所述的方法，其中，从记录发送方设备接收发送方个体记录包括直接或通过中间设备经由短程链路从记录发送方设备接收发送方个体记录。

[0491] 在第39方面，根据方面38所述的方法，其中，短程链路是对等通信链路。

[0492] 在第40方面，根据方面33-39中任一方面所述的方法，其中，接收方个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0493] 在第41方面，根据方面33-40中任一方面所述的方法，其中，在由记录发送方设备接收记录发送方的认证信息之后创建发送方个体记录，并且其中，创建接收方个体记录包括由记录接收方设备接收记录接收方的认证信息。

[0494] 在第42方面，根据方面33-41中任一方面所述的方法，其中，验证发送方个体记录包括使用发送方公钥来确定使用发送方私钥创建发送方签名。

[0495] 在第43方面，根据方面33-42中任一方面所述的方法，其中，使用发送方私钥使用记录发送方设备的安全元件创建发送方签名，并且其中，发送方私钥存储在记录发送方设备的安全元件中。

[0496] 在第44方面，根据方面33-43中任一方面所述的方法，其中，使用接收方私钥使用

记录接收方设备的安全元件创建接收方签名，并且其中，接收方私钥存储在记录接收方设备的安全元件中。

[0497] 在第45方面，根据方面33-44中任一方面所述的方法，进一步包括从处理平台接收公共记录，其中，公共记录包括发送方公钥和接收方公钥。

[0498] 在第46方面，根据方面45所述的方法，进一步包括向记录发送方设备发送公共记录。

[0499] 在第47方面，根据方面33-44中任一方面所述的方法，进一步包括从记录发送方设备接收公共记录，其中，公共记录包括发送方公钥和接收方公钥。

[0500] 在第48方面，根据方面45-47中任一方面所述的方法，其中，公共记录进一步包括公共记录的第三签名，并且其中，使用处理平台的第三私钥来创建第三签名，该方法进一步包括使用处理平台的第三公钥验证公共记录而不一定与处理平台通信，其中，第三公钥和第三私钥形成第三公钥加密对，并且其中，验证公共记录包括使用第三公钥来确定使用第三私钥创建第三签名。

[0501] 在第49方面，公开了一种计算机系统。该计算机系统包括：硬件处理器；以及具有存储在其上的指令的非暂态存储器，该指令在由处理器执行时使处理器执行方面1-48中任一方面的方法。

[0502] 在第50方面，根据方面49所述的计算机系统，其中，计算机系统是移动设备。

[0503] 在第51方面，根据方面50所述的计算机系统，其中，移动设备是可穿戴显示系统。

[0504] 代理的加密签名记录的安全交换

[0505] 在第52方面，公开了一种用于由代理安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从主设备接收主修改的个体记录，其中，主修改的个体记录包括代理修改的个体记录和主修改的个体记录的签名，其中，代理修改的个体记录包括原始个体记录、代理设备的代理公钥，以及代理修改的个体记录的签名，其中，原始个体记录包括记录内容、记录发送方设备的发送方公钥、主设备的主公钥和原始个体记录的签名，其中，主修改的个体记录的签名使用主设备的主私钥创建，并且其中，主公钥和主私钥形成主公钥加密对，其中，在从主设备接收到原始个体记录之后，由代理设备创建代理修改的个体记录，其中，使用代理设备的代理私钥创建代理修改的个体记录的签名，其中，代理公钥和代理私钥形成代理公钥加密对，并且其中，在从代理设备接收到内容请求并识别代理设备之后，由记录发送方设备创建原始个体记录，其中，使用记录发送方设备的发送方私钥创建原始个体记录的签名，以及其中，发送方公钥和发送方私钥形成发送方公钥加密对；验证主修改的个体记录；并如主修改的个体记录所指示地执行主设备。

[0506] 在第53方面，根据方面52所述的方法，其中，内容请求包括主公钥和所请求的内容，其中，记录内容与所请求的内容相关。

[0507] 在第54方面，根据方面52-53中任一方面所述的方法，其中，识别代理设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0508] 在第55方面，根据方面54所述的方法，其中，原始个体记录进一步包括记录标识符。

[0509] 在第56方面，根据方面55所述的方法，其中，记录标识符是单调递增的数字。

[0510] 在第57方面，根据方面52-56中任一方面所述的方法，其中，从记录发送方设备接收原始个体记录包括直接或通过中间设备经由短程链路从记录发送方设备接收原始个体记录。

[0511] 在第58方面，根据方面57所述的方法，其中，短程链路是对等通信链路。

[0512] 在第59方面，根据方面52-58中任一方面所述的方法，其中，代理修改的个体记录进一步包括由认可处理、查询认可、恶意记录认可或其任何组合，并且其中，主修改的个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0513] 在第60方面，根据方面52-59中任一方面所述的方法，其中，在由记录发送方设备接收到记录发送方的认证信息之后由记录发送方设备创建原始个体记录，并且其中，在由代理设备接收到代理的认证信息之后，由代理设备创建代理修改的个体记录。

[0514] 在第61方面，根据方面52-60中任一方面所述的方法，其中，验证原始个体记录包括：使用发送方公钥来确定使用发送方私钥创建原始个体记录的签名；使用代理公钥确定使用代理私钥创建代理修改的个体记录的签名；并使用主公钥来确定使用主私钥创建主设备的签名。

[0515] 在第62方面，根据方面52-61中任一方面所述的方法，进一步包括向记录发送方设备、代理设备和主设备提供公共记录，其中，公共记录包括发送方公钥和主公钥。

[0516] 在第63方面，根据方面52-61中任一方面所述的方法，进一步包括向记录发送方设备提供公共记录，其中，公共记录包括发送方公钥和主公钥；并使记录发送方设备向代理提供公共记录。

[0517] 在第64方面，根据方面52-61中任一方面所述的方法，进一步包括向代理提供公共记录，其中，公共记录包括发送方公钥和主公钥；并使代理向记录发送方设备提供公共记录。

[0518] 在第65方面，根据方面52-61中任一方面所述的方法，进一步包括向主设备提供公共记录，其中，公共记录包括发送方公钥和主公钥；并使主设备向代理提供公共记录。

[0519] 在第66方面，根据方面65所述的方法，进一步包括使代理向记录发送方设备提供公共记录。

[0520] 在第67方面，根据方面62-66中任一方面所述的方法，其中，公共记录进一步包括公共记录签名，其中，使用处理平台的处理平台私钥来创建公共记录签名，该方法进一步包括使用处理平台的处理平台公钥验证公共记录而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台公钥加密对，并且其中，验证公共记录包括使用处理平台公钥来确定使用处理平台私钥创建公共记录签名。

[0521] 在第68方面，根据方面62-67中任一方面所述的方法，进一步包括：从中央记录生成公共记录，其中，中央记录包括发送方公钥、主公钥、代理公钥、记录发送方设备的用户记录状态，以及主设备的用户记录状态。

[0522] 在第69方面，根据方面52-68中任一方面所述的方法，进一步包括：周期性地或一次性地针对代理公钥加密对或主加密对向商家收取费用。

[0523] 在第70方面，公开了一种用于通过代理安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从代理设备接收内容请求；识别代理设备；创建原始个体记录，其中，原始个体记录包括记录内容、记录发送方设备的发送方公钥、主设备的

主公钥，以及原始个体记录的签名，其中，使用记录发送方设备的发送方私钥创建原始个体记录的签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对；向代理设备发送原始个体记录；接收代理设备的指示：接收原始个体记录；使用发送方公钥验证原始个体记录而不一定与处理平台通信；创建代理修改的个体记录，其中，代理修改的个体记录包括原始个体记录、代理设备的代理公钥和代理修改的个体记录的签名，其中，代理修改的个体记录的签名使用代理设备的代理私钥创建，并且其中，代理公钥和代理私钥形成代理公钥加密对；并向主设备发送代理修改的个体记录；并接收主设备的指示：接收代理修改的个体记录；创建主修改的个体记录，其中，主修改的个体记录包括代理修改的个体记录和主修改的个体记录的签名，其中，使用主设备的主私钥创建主修改的个体记录的签名，以及其中，主公钥和主私钥形成主公钥加密对；与处理平台兑换主修改的个体记录；如主修改的个体记录所指示地接收处理平台的执行；并通知代理设备接收执行。

[0524] 在第71方面，根据方面70所述的方法，其中，内容请求包括主公钥和所请求的内容，其中，记录内容与所请求的内容相关。

[0525] 在第72方面，根据方面70-71中任一方面所述的方法，其中，识别代理设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0526] 在第73方面，根据方面70-72中任一方面所述的方法，其中，原始个体记录进一步包括记录标识符。

[0527] 在第74方面，根据方面73所述的方法，其中，记录标识符是单调递增的数字。

[0528] 在第75方面，根据方面70-74中任一方面所述的方法，其中，向代理设备发送原始个体记录包括直接或通过中间设备经由短程链路向代理设备发送原始个体记录。

[0529] 在第76方面，根据方面75所述的方法，其中，短程链路是对等通信链路。

[0530] 在第77方面，根据方面70-76中任一方面所述的方法，其中，代理修改的个体记录进一步包括由认可处理、查询认可、恶意记录认可或其任何组合，并且其中，主修改的个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0531] 在第78方面，根据方面70-77中任一方面所述的方法，其中，创建原始个体记录包括由记录发送方设备接收记录发送方的认证信息，并且其中，创建代理修改的个体记录包括由代理设备接收代理的认证信息。

[0532] 在第79方面，根据方面70-78中任一方面所述的方法，其中，验证原始个体记录包括使用发送方公钥来确定使用发送方私钥创建原始个体记录的签名。

[0533] 在第80方面，根据方面70-79中任一方面所述的方法，其中，原始个体记录的签名由记录发送方设备的安全元件使用发送方私钥创建，并且其中，发送方私钥存储在记录发送方设备的安全元件中。

[0534] 在第81方面，根据方面70-80中任一方面所述的方法，其中，代理修改的个体记录的签名由代理设备的安全元件使用代理私钥创建，并且其中，代理私钥存储在代理设备的安全元件中。

[0535] 在第82方面，根据方面70-81中任一方面所述的方法进一步包括从处理平台接收公共记录，其中，公共记录包括发送方公钥和主公钥。

[0536] 在第83方面，根据方面70-81中任一方面所述的方法进一步包括从代理设备接收

公共记录，其中，公共记录包括发送方公钥和主公钥。

[0537] 在第84方面，根据方面82-83中任一方面所述的方法，其中，公共记录进一步包括公共记录签名，其中，使用处理平台的处理平台私钥创建公共记录签名，该方法进一步包括使用处理平台的处理平台公钥验证公共记录而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台公钥加密对，并且其中，验证公共记录包括使用处理平台公钥来确定使用处理平台私钥创建公共记录签名。

[0538] 在第85方面，公开了一种用于通过代理安全地交换加密签名记录的方法。该方法在硬件处理器的控制下执行，并包括：向记录发送方设备发送内容请求；从记录发送方设备接收原始个体记录，其中，在从记录发送方设备接收到内容请求并识别代理设备之后由记录发送方设备创建原始个体记录，其中，原始个体记录包括记录内容、记录发送方设备的发送方公钥、主设备的主公钥，以及原始个体记录的签名，其中，原始个体记录的签名使用记录发送方设备的发送方私钥创建，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对；使用发送方公钥验证原始个体记录而不一定与处理平台通信；创建代理修改的个体记录，其中，代理修改的个体记录包括原始个体记录、代理设备的代理公钥和代理修改的个体记录的签名，其中，代理修改的个体记录的签名使用代理设备的代理私钥创建，并且其中，代理公钥和代理私钥形成代理公钥加密对；向主设备发送代理修改的个体记录；并接收主设备的指示：接收代理修改的个体记录；创建主修改的个体记录，其中，主修改的个体记录包括代理修改的个体记录和主修改的个体记录的签名，其中，使用主设备的主私钥创建主修改的个体记录的签名，以及其中，主公钥和主私钥形成主公钥加密对；与处理平台兑换主修改的个体记录；并如主修改的个体记录所指示地接收处理平台的执行。

[0539] 在第86方面，根据方面85所述的方法，其中，内容请求包括主公钥和所请求的内容，其中，记录内容与所请求的内容相关。

[0540] 在第87方面，根据方面85-86中任一方面所述的方法，其中，识别代理设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0541] 在第88方面，根据方面85-87中任一方面所述的方法，其中，原始个体记录进一步包括记录标识符。

[0542] 在第89方面，根据方面88所述的方法，其中，记录标识符是单调递增的数字。

[0543] 在第90方面，根据方面85-89中任一方面所述的方法，其中，从记录发送方设备接收原始个体记录包括直接或通过中间设备经由短程链路从记录发送方设备接收原始个体记录。

[0544] 在第91方面，根据方面90所述的方法，其中，短程链路是对等通信链路。

[0545] 在第92方面，根据方面85-91中任一方面所述的方法，其中，代理修改的个体记录进一步包括由认可处理、查询认可、恶意记录认可或其任何组合，并且其中，主修改的个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0546] 在第93方面，根据方面85-92中任一方面所述的方法，其中，创建原始个体记录包括由记录发送方设备接收记录发送方的认证信息，并且其中，创建代理修改的个体记录包括由代理设备接收代理的认证信息。

[0547] 在第94方面，根据方面85-93中任一方面所述的方法，其中，验证原始个体记录包

括使用发送方公钥来确定使用发送方私钥创建原始个体记录的签名。

[0548] 在第95方面，根据方面85-94中任一方面所述的方法，其中，由记录发送方设备的安全元件使用发送方私钥创建原始个体记录的签名，并且其中，发送方私钥存储在记录发送方设备的安全元件中。

[0549] 在第96方面，根据方面85-95中任一方面所述的方法，其中，由代理设备的安全元件使用代理私钥创建代理修改的个体记录的签名，并且其中，代理私钥存储在代理设备的安全元件中。

[0550] 在第97方面，根据方面85-96中任一方面所述的方法，进一步包括从处理平台接收公共记录，其中，公共记录包括发送方公钥和主公钥。

[0551] 在第98方面，根据方面97所述的方法，进一步包括向记录发送方设备发送公共记录。

[0552] 在第99方面，根据方面85-96中任一方面所述的方法，进一步包括从主设备接收公共记录，其中，公共记录包括发送方公钥和主公钥。

[0553] 在第100方面，根据方面97-99中任一方面所述的方法，其中，公共记录进一步包括公共记录签名，其中，使用处理平台的处理平台私钥来创建公共记录签名，该方法进一步包括使用处理平台的处理平台公钥验证公共记录而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台公钥加密对，并且其中，验证公共记录包括使用处理平台公钥来确定使用处理平台私钥创建公共记录签名。

[0554] 在第101方面，公开了一种计算机系统。该计算机系统包括：处理器；具有存储在其上的指令的非暂态存储器，该指令在由处理器执行时使处理器执行方面52-100中任一方面的方法。

[0555] 在第102方面，根据方面101所述的计算机系统，其中，计算机系统是移动设备。

[0556] 在第103方面，根据方面102所述的计算机系统，其中，移动设备是可穿戴显示系统。

[0557] 加密签名记录链的安全交换

[0558] 在第104方面，公开了一种用于安全地交换加密签名记录链的方法。该方法在硬件处理器的控制下执行，并且包括：从后续记录接收方设备接收后续接收方个体记录，其中，后续接收方个体记录包括原始接收方个体记录和后续接收方个体记录的后续接收方签名，其中，原始接收方个体记录包括发送方个体记录、后续记录接收方设备的后续接收方公钥，以及原始接收方个体记录的原始接收方签名，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、原始记录接收方设备的原始接收方公钥，以及发送方个体记录的发送方签名，其中，在从原始记录接收方设备接收到原始内容请求并识别原始记录接收方设备之后由记录发送方设备创建发送方个体记录，其中，使用记录发送方设备的发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对，其中，在从后续记录接收方设备接收后续内容请求并识别后续记录接收方设备之后，由原始记录接收方设备创建原始接收方个体记录，其中，使用原始记录接收方设备的原始接收方私钥创建原始接收方签名，并且其中，原始接收方公钥和原始接收方私钥形成原始接收方公钥加密对，其中，使用后续记录接收方设备的后续接收方私钥创建后续接收方签名，并且其中，后续接收方公钥和后续接收方私钥形成后续接收公钥加密对；验证后续接收方个体记录；

并如由后续接收方个体记录所指示地执行后续记录接收方。

[0559] 在第105方面，根据方面104所述的方法，其中，原始内容请求包括原始接收方公钥和原始内容，其中，记录内容与原始内容相关，其中，后续内容请求包括后续接收方公钥和后续内容，其中，原始内容与后续内容相关。

[0560] 在第106方面，根据方面104-105中任一方面所述的方法，其中，识别原始内容请求者或识别后续内容请求者包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0561] 在第107方面，根据方面104-106中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0562] 在第108方面，根据方面107所述的方法，其中，记录标识符是单调递增的数字。

[0563] 在第109方面，根据方面104-108中任一方面所述的方法，其中，发送方个体记录由记录发送方设备直接或通过中间设备经由第一短程链路发送到原始记录接收方设备，并且其中，向后续记录接收方设备发送原始接收方个体记录包括直接或通过中间设备经由第二短程链路向后续记录接收方设备发送原始接收方个体记录。

[0564] 在第110方面，根据方面109所述的方法，其中，第一短程链路是对等通信链路，或者其中，第二短程链路是对等通信链路。

[0565] 在第111方面，根据方面104-110中任一方面所述的方法，其中，后续接收方个体记录进一步包括用于仅兑换的认可、查询认可、恶意记录认可或其任何组合。

[0566] 在第112方面，根据方面104-111中任一方面所述的方法，其中，在接收到记录发送方的认证信息之后由记录发送方设备创建发送方个体记录，其中，在接收到原始记录接收方设备的认证信息之后由原始记录接收方设备创建原始接收方个体记录，以及其中，在接收到后续记录接收方设备的认证信息之后由后续记录接收方设备创建后续接收方个体记录。

[0567] 在第113方面，根据方面104-112中任一方面所述的方法，其中，验证后续接收方个体记录包括：使用发送方公钥来确定使用发送方私钥创建发送方签名；使用原始接收方公钥确定使用原始接收方私钥创建原始接收方签名；并使用后续接收方公钥来确定使用后续接收方私钥创建后续接收方签名。

[0568] 在第114方面，根据方面104-113中任一方面所述的方法，其中，由记录发送方设备的安全元件使用发送方私钥创建发送方签名，其中，发送方私钥存储在记录发送方设备的安全元件中，其中，由原始记录接收方设备的安全元件使用原始接收方私钥创建原始接收方签名，其中，原始接收方私钥存储在原始记录接收方设备的安全元件中，其中，由后续记录接收方设备的安全元件使用后续接收方私钥创建后续接收方签名，并且其中，后续接收方私钥存储在后续记录接收方设备的安全元件中。

[0569] 在第115方面，公开了一种用于安全地交换加密签名记录链的方法。该方法在硬件处理器的控制下执行，并且包括：从原始记录接收方设备接收原始内容请求；识别原始记录接收方设备；创建发送方个体记录，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、原始记录接收方设备的原始接收方公钥，以及发送方个体记录的发送方签名，其中，使用记录发送方设备的发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对；向原始内容请求者发送发送方个体记录；并接收原始内

容请求者的指示:接收发送方个体记录;使用发送方公钥验证发送方个体记录而不一定与处理平台通信;从后续记录接收方设备接收后续内容请求;识别后续记录接收方设备;创建原始接收方个体记录,其中,原始接收方个体记录包括发送方个体记录、后续记录接收方设备的后续接收方公钥,以及原始接收方个体记录的原始接收方签名,其中,使用原始记录接收方设备的原始接收方私钥创建原始接收方签名,并且其中,原始接收方公钥和原始接收方私钥形成原始接收方公钥加密对;向后续记录接收方设备发送原始接收方个体记录;并接收后续记录接收方的指示:接收原始接收方个体记录;使用发送方公钥和原始接收方公钥验证原始接收方个体记录而不一定与处理平台通信;创建后续接收方个体记录,其中,后续接收方个体记录包括原始接收方个体记录和后续接收方个体记录的后续接收方签名,其中,使用后续记录接收方设备的后续接收方私钥创建后续接收方签名,以及其中,后续接收方公钥和后续接收方私钥形成后续接收方公钥加密对;与处理平台兑换原始接收方个体记录;并如后续接收方个体记录所指示地接收处理平台的执行。

[0570] 在第116方面,根据方面115所述的方法,其中,原始内容请求包括原始接收方公钥和原始内容,其中,记录内容与原始内容相关,其中,后续内容请求包括后续接收方公钥和后续内容,其中,原始内容与后续内容相关。

[0571] 在第117方面,根据方面115-116中任一方面所述的方法,其中,识别原始内容请求者或识别后续内容请求者包括执行伙伴标识,其中,伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0572] 在第118方面,根据方面115-117中任一方面所述的方法,其中,发送方个体记录进一步包括记录标识符。

[0573] 在第119方面,根据方面118所述的方法,其中,记录标识符是单调递增的数字。

[0574] 在第120方面,根据方面115-119中任一方面所述的方法,其中,向原始记录接收方设备发送发送方个体记录包括直接或通过中间设备经由第一短程链路向原始记录接收方设备发送发送方个体记录,并且其中,向后续记录接收方设备发送原始接收方个体记录包括直接或通过中间设备经由第二短程链路向后续记录接收方设备发送原始接收方个体记录。

[0575] 在第121方面,根据方面120所述的方法,其中,第一短程链路是对等通信链路,或者其中,第二短程链路是对等通信链路。

[0576] 在第122方面,根据方面115-121中任一方面所述的方法,其中,后续接收方个体记录进一步包括用于仅兑换的认可、查询认可、恶意记录认可或其任何组合。

[0577] 在第123方面,根据方面115-122中任一方面所述的方法,其中,创建发送方个体记录包括由记录发送方设备接收记录发送方的认证信息,其中,创建原始接收方个体记录包括由原始记录接收方设备接收原始记录接收方的认证信息,其中,创建后续接收方个体记录包括由后续记录接收方设备接收后续记录接收方的认证信息。

[0578] 在第124方面,根据方面115-123中任一方面所述的方法,其中,验证发送方个体记录包括使用发送方公钥来确定使用发送方私钥创建发送方签名,并且其中,验证原始接收方个体记录包括使用原始接收方公钥来确定使用原始接收方私钥创建原始接收方签名。

[0579] 在第125方面,根据方面115-124中任一方面所述的方法,其中,由记录发送方设备的安全元件使用发送方私钥创建发送方签名,其中,发送方私钥存储在记录发送方设备的

安全元件中，其中，由原始记录接收方设备的安全元件使用原始接收方私钥创建原始接收方签名，其中，原始接收方私钥存储在原始记录接收方设备的安全元件中，其中，由后续记录接收方设备的安全元件使用后续接收方私钥创建后续接收方签名，并且其中，后续接收方私钥存储在后续记录接收方设备的安全元件中。

[0580] 在第126方面，公开了一种用于安全地交换加密签名记录链的方法。该方法在硬件处理器的控制下执行，并包括：向记录发送方设备发送原始内容请求；从记录发送方设备接收发送方个体记录，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、原始记录接收方设备的原始接收方公钥，以及发送方个体记录的发送方签名，其中，使用记录发送方设备的发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对；使用发送方公钥验证发送方个体记录而不一定与处理平台通信；从后续记录接收方设备接收后续内容请求；识别后续记录接收方设备；创建原始接收方个体记录，其中，原始接收方个体记录包括发送方个体记录、后续记录接收方设备的后续接收方公钥，以及原始接收方个体记录的原始接收方签名，其中，使用原始记录接收方设备的原始接收方私钥创建原始接收方签名，并且其中，原始接收方公钥和原始接收方私钥形成原始接收方公钥加密对；向后续记录接收方设备发送原始接收方个体记录；并接收后续记录接收方的指示：接收原始接收方个体记录；使用发送方公钥和原始接收方公钥验证原始接收方个体记录而不一定与处理平台通信；创建后续接收方个体记录，其中，后续接收方个体记录包括原始接收方个体记录和后续接收方个体记录的后续接收方签名，其中，使用后续记录接收方设备的后续接收方私钥创建后续接收方签名，以及其中，后续接收方公钥和后续接收方私钥形成后续接收方公钥加密对；与处理平台兑换原始接收方个体记录；并如后续接收方个体记录所指示地接收处理平台的执行。

[0581] 在第127方面，根据方面126所述的方法，其中，原始内容请求包括原始接收方公钥和原始内容，其中，记录内容与原始内容相关，其中，后续内容请求包括后续接收方公钥和后续内容，其中，原始内容与后续内容相关。

[0582] 在第128方面，根据方面126-127中任一方面所述的方法，其中，识别原始内容请求者或识别后续内容请求者包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0583] 在第129方面，根据方面126-128中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0584] 在第130方面，根据方面129所述的方法，其中，记录标识符是单调递增的数字。

[0585] 在第131方面，根据方面126-130中任一方面所述的方法，其中向原始记录接收方设备发送发送方个体记录包括直接或通过中间设备经由第一短程链路向原始记录接收方设备发送发送方个体记录，并且其中，向后续记录接收方设备发送原始接收方个体记录包括直接或通过中间设备经由第二短程链路向后续记录接收方设备发送原始接收方个体记录。

[0586] 在第132方面，根据方面131所述的方法，其中，第一短程链路是对等通信链路，或者其中，第二短程链路是对等通信链路。

[0587] 在第133方面，根据方面126-132中任一方面所述的方法，其中，后续接收方个体记录进一步包括用于仅兑换的认可、查询认可、恶意记录认可或其任何组合。

[0588] 在第134方面，根据方面126-133中任一方面所述的方法，其中，创建发送方个体记录包括由记录发送方设备接收记录发送方的认证信息，其中，创建原始接收方个体记录包括由原始记录接收方设备接收原始记录接收方的认证信息，以及其中，创建后续接收方个体记录包括由后续记录接收方设备接收后续记录接收方的认证信息。

[0589] 在第135方面，根据方面126-134中任一方面所述的方法，其中，验证发送方个体记录包括使用发送方公钥来确定使用发送方私钥创建发送方签名，并且其中，验证原始接收方个体记录包括使用原始接收方公钥来确定使用原始接收方私钥创建原始接收方签名。

[0590] 在第136方面，根据方面126-135中任一方面所述的方法，其中，由记录发送方设备的安全元件使用发送方私钥创建发送方签名，其中，发送方私钥存储在记录发送方设备的安全元件中，其中，由原始记录接收方设备的安全元件使用原始接收方私钥创建原始接收方签名，其中，原始接收方私钥存储在原始记录接收方设备的安全元件中，其中，由后续记录接收方设备的安全元件使用后续接收方私钥创建后续接收方签名，并且其中，后续接收方私钥存储在后续记录接收方设备的安全元件中。

[0591] 在第137方面，公开了一种用于安全地交换加密签名记录链的方法。该方法在硬件处理器的控制下执行，并且包括：向原始记录接收方设备发送后续内容请求，从原始记录接收方设备接收原始接收方个体记录，其中，原始接收方个体记录包括发送方个体记录、后续记录接收方设备的后续接收方公钥，以及原始接收方个体记录的原始接收方签名，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、原始记录接收方设备的原始接收方公钥以及发送方个体记录的发送方签名，其中，在从原始记录接收方设备接收到原始内容请求并识别原始记录接收方设备之后由记录发送方设备创建发送方个体记录，其中，发送方签名使用记录发送方设备的发送方私钥创建，以及其中，发送方公钥和发送方私钥形成发送方公钥加密对，其中，在从后续记录接收方设备接收到后续内容请求并识别后续记录接收方设备之后由原始记录接收方设备创建原始接收方个体记录，其中，使用原始记录接收方设备的原始接收方私钥创建原始接收方签名，并且其中，原始接收方公钥和原始接收方私钥形成原始接收方公钥加密对；验证原始接收方个体记录而不一定与处理平台通信；创建后续接收方个体记录，其中，后续接收方个体记录包括原始接收方个体记录和后续接收方个体记录的后续接收方签名，其中，使用后续记录接收方设备的后续接收方私钥创建后续接收方签名，以及其中，后续接收方公钥和后续接收方私钥形成后续接收方公钥加密对；与处理平台兑换后续接收方个体记录；并如后续接收方个体记录所指示地接收处理平台的执行。

[0592] 在第138方面，根据方面137所述的方法，其中，原始内容请求包括原始接收方公钥和原始内容，其中，记录内容与原始内容相关，其中，后续内容请求包括后续接收方公钥和后续内容，其中，原始内容与后续内容相关。

[0593] 在第139方面，根据方面137-138中任一方面所述的方法，其中，识别原始内容请求者或识别后续内容请求者包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证或其任何组合。

[0594] 在第140方面，根据方面137-139中任一方面所述的方法，其中，发送方个体记录进一步包括记录标识符。

[0595] 在第141方面，根据方面140所述的方法，其中，记录标识符是单调递增的数字。

[0596] 在第142方面，根据方面137-141中任一方面所述的方法，其中，从原始记录接收方设备接收原始接收方个体记录包括直接或通过中间设备经由短程链路从原始记录接收方设备接收原始接收方个体记录。

[0597] 在第143方面，根据方面142所述的方法，其中，短程链路是对等通信链路。

[0598] 在第144方面，根据方面137-143中任一方面所述的方法，其中，后续接收方个体记录进一步包括仅用于兑换的认可、查询认可、恶意记录认可或其任何组合。

[0599] 在第145方面，根据方面137-144中任一方面所述的方法，其中，在接收到记录发送方的认证信息之后由记录发送方设备创建发送方个体记录，其中，在接收到原始记录接收方设备的认证信息之后由原始记录接收方设备创建原始接收方个体记录，并且其中，创建后续接收方个体记录包括由后续记录接收方设备接收后续记录接收方的认证信息。

[0600] 在第146方面，根据方面137-145中任一方面所述的方法，其中，验证原始接收方个体记录包括：使用发送方公钥来确定使用发送方私钥创建发送方签名；并使用原始接收方公钥来确定使用原始接收方私钥创建原始接收方签名。

[0601] 在第147方面，根据方面137-146中任一方面所述的方法，其中，由记录发送方设备的安全元件使用发送方私钥创建发送方签名，其中，发送方私钥存储在记录发送方设备的安全元件中，其中，由原始记录接收方设备的安全元件使用原始接收方私钥创建原始接收方签名，其中，原始接收方私钥存储在原始记录接收方设备的安全元件中，其中，由后续记录接收方设备的安全元件使用后续接收方私钥创建后续接收方签名，并且其中，后续接收方私钥存储在后续记录接收方设备的安全元件中。

[0602] 加密签名数字支票的安全交换

[0603] 在第148方面，公开了一种用于安全地交换加密签名的数字支票的方法。该方法在硬件处理器的控制下执行，并且包括：从收款方设备接收认可的数字支票，其中，认可的数字支票包括原始数字支票和认可的数字支票的收款方签名，其中，在接收到来自收款方的支付请求并识别收款方设备之后由付款方创建原始数字支票，其中，原始数字支票包括支付金额、付款方公钥、收款方公钥和原始数字支票的付款方签名，其中，使用付款方设备的付款方私钥创建付款方签名，其中，付款方公钥和收款方公钥形成收款方公钥加密对，其中，在从付款方设备接收到原始数字支票并使用付款方公钥验证原始数字支票而不一定与处理平台通信之后，由收款方设备创建认可的数字支票，其中，由收款方设备使用收款方私钥创建收款方签名，以及其中，收款方公钥和收款方公钥形成收款方公钥加密对；验证认可的数字支票；并向收款方提供支付金额的支付。

[0604] 在第149方面，根据方面148所述的方法，其中，支付请求包括收款方公钥和请求的金额，并且其中，支付金额与请求的金额相关。

[0605] 在第150方面，根据方面148-149中任一方面所述的方法，其中，识别收款方设备包括执行伙伴标识，其中，伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0606] 在第151方面，根据方面148-150中任一方面所述的方法，其中，原始数字支票进一步包括支票标识符。

[0607] 在第152方面，根据方面151所述的方法，其中，支票标识符是单调递增的数字。

[0608] 在第153方面，根据方面148-152中任一方面所述的方法，其中，从付款方设备接收

原始数字支票包括直接或通过中间设备经由短程链路从付款方设备接收原始数字支票。

[0609] 在第154方面，根据方面153所述的方法，其中，短程链路是对等通信链路。

[0610] 在第155方面，根据方面148-154中任一方面所述的方法，其中，认可的数字支票进一步包括仅用于兑换的认可、查询认可、恶意支票认可或其任何组合。

[0611] 在第156方面，根据方面148-155中任一方面所述的方法，其中，在由付款方设备接收付款方的验证信息之后创建原始数字支票，并且其中，在由收款方设备接收到收款方的认证信息之后创建认可的数字支票。

[0612] 在第157方面，根据方面148-156中任一方面所述的方法，其中，验证原始数字支票包括：使用付款方公钥来确定使用付款方私钥创建付款方签名；并使用收款方公钥来确定使用收款方私钥创建收款方签名。

[0613] 在第158方面，根据方面148-157中任一方面所述的方法，进一步包括向付款方设备和收款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0614] 在第159方面，根据方面148-157中任一方面所述的方法，进一步包括：向付款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥；并使付款方设备向收款方设备提供公共分类帐。

[0615] 在第160方面，根据方面148-157中任一方面所述的方法，进一步包括：向收款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥；并使收款方设备向付款方设备提供公共分类帐。

[0616] 在第161方面，根据方面158-160中任一方面所述的方法，其中，公共分类帐进一步包括公共分类帐签名，其中，使用处理平台的处理平台私钥来创建公共分类帐签名，该方法进一步包括使用处理平台的处理平台公钥验证公共分类帐而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台的公钥加密对，并且其中，验证公共分类帐包括使用处理平台公钥来确定使用处理平台私钥创建公共分类帐签名。

[0617] 在第162方面，根据方面158-161中任一方面所述的方法，进一步包括：从公共分类帐生成中央分类帐，其中，中央分类帐包括付款方设备的付款方帐户和收款方设备的收款方帐户，其中，付款方帐户包括付款方公钥和付款方帐户的帐户余额，并且其中，收款方帐户包括收款方公钥和收款方帐户的帐户余额。

[0618] 在第163方面，根据方面162所述的方法，其中，向收款方设备提供支付金额的支付包括：确定付款方账户具有足够的余额来对支付金额进行支付；将付款方帐户借记支付金额；并将收款方帐户贷记支付金额。

[0619] 在第164方面，根据方面163所述的方法，进一步包括：从收款方设备接收从收款方账户转出资金的请求，其中，从收款方账户转出资金的请求包括转出金额和转出方法，其中，转出方法是自动清算所(ACH)转移、电汇或发送物理支票；借记收款方帐户转出金额；并使用转出方法发送转出金额。

[0620] 在第165方面，根据方面164所述的方法，进一步包括：借记收款方账户转移费用，其中，费用与转出金额成比例或固定。

[0621] 在第166方面，根据方面162-165中任一方面所述的方法，其中，向收款方设备提供支付金额的支付包括：确定付款方帐户的余额不足以对支付金额进行支付；借记付款方账户余额不足的费用；并将付款方设备添加到过失列表。

[0622] 在第167方面，根据方面162-166中任一方面所述的方法，其中，原始数字支票进一步包括源账户，其中，向收款方设备提供支付金额的支付包括：从源帐户接收支付金额；并贷记收款方帐户支付金额。

[0623] 在第168方面，根据方面148-167中任一方面所述的方法，其中，原始数字支票包括费用分摊策略。

[0624] 在第169方面，一种用于安全地交换加密签名的数字支票的方法，包括：在硬件处理器的控制下：从收款方设备接收支付请求；识别收款方设备；创建原始数字支票，其中，原始数字支票包括支付金额、付款方设备的付款方公钥、收款方设备的收款方公钥，以及原始数字支票的付款方签名，其中，使用付款方设备的付款方私钥创建付款方签名，并且其中，付款方公钥和付款方私钥形成付款方公钥加密对；向收款方设备发送原始数字支票；并接收收款方设备的指示：接收原始数字支票；使用付款方公钥验证原始数字支票而不一定与处理平台通信；创建认可的数字支票，其中，认可的数字支票包括原始数字支票和认可的数字支票的收款方签名，其中，使用收款方私钥创建收款方签名，并且其中，收款方公钥和收款方私钥形成收款方公钥加密对；与处理平台兑换认可的数字支票；并从处理平台接收支付金额的支付。

[0625] 在第170方面，根据方面169所述的方法，其中，支付请求包括收款方公钥和请求的金额，并且其中，支付金额与请求的金额相关。

[0626] 在第171方面，根据方面169-170中任一方面所述的方法，其中，识别收款方设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略验证，或其任何组合。

[0627] 在第172方面，根据方面169-171中任一方面所述的方法，其中，原始数字支票进一步包括支票标识符。

[0628] 在第173方面，根据方面172所述的方法，其中，支票标识符是单调递增的数字。

[0629] 在第174方面，根据方面169-173中任一方面所述的方法，其中向收款方设备发送原始数字支票包括直接或通过中间设备经由短程链路向收款方设备发送原始数字支票。

[0630] 在第175方面，根据方面174所述的方法，其中，短程链路是对等通信链路。

[0631] 在第176方面，根据方面169-175中任一方面所述的方法，其中，认可的数字支票进一步包括仅用于兑换的认可、查询认可、恶意支票认可或其任何组合。

[0632] 在第177方面，根据方面169-176中任一方面所述的方法，其中，创建原始数字支票包括由付款方设备接收付款方的认证信息，并且其中，创建认可的数字支票包括由收款方设备接收收款方的认证信息。

[0633] 在第178方面，根据方面169-177中任一方面所述的方法，其中，验证原始数字支票包括使用付款方公钥来确定使用付款方私钥创建付款方签名。

[0634] 在第179方面，根据方面169-178中任一方面所述的方法，其中，由付款方设备的安全元件使用付款方私钥创建付款方签名，并且其中，付款方私钥存储在付款方设备的安全元件中。

[0635] 在第180方面，根据方面169-179中任一方面所述的方法，其中，收款方签名由收款方设备的安全元件使用收款方私钥创建，并且其中，收款方私钥存储在收款方设备的安全元件中。

[0636] 在第181方面，根据方面169-180中任一方面所述的方法，进一步包括从处理平台接收公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0637] 在第182方面，根据方面169-180中任一方面所述的方法进一步包括从收款方设备接收公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0638] 在第183方面，根据方面181-182中任一方面所述的方法，其中，公共分类帐进一步包括公共分类帐签名，其中，使用处理平台的处理平台私钥创建公共分类帐签名，该方法进一步包括使用处理平台的处理平台公钥验证公共分类帐而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台的公钥加密对，并且其中，验证公共分类帐包括使用处理平台公钥来确定使用处理平台私钥创建公共分类帐签名。

[0639] 在第184方面，公开了一种用于安全地交换加密签名的数字支票的方法。该方法在硬件处理器的控制下执行，并包括：向付款方设备发送支付请求；从付款方设备接收原始数字支票，其中，在从收款方设备接收到支付请求并识别收款方设备之后由付款方设备创建原始数字支票，其中，原始数字支票包括支付金额、付款方设备的付款方公钥、收款方设备的收款方公钥以及原始数字支票的付款方签名，其中，付款方签名使用付款方设备的付款方私钥创建，并且其中，付款方公钥和收款方公钥形成付款方公钥加密对；使用付款方公钥验证原始数字支票而不一定与处理平台通信；创建认可的数字支票，其中，认可的数字支票包括原始数字支票和认可的数字支票的收款方签名，其中，使用收款方设备的收款方私钥创建收款方签名，并且其中，收款方公钥和收款方公钥形成收款方公钥加密对；与处理平台兑换认可的数字支票；并从处理平台接收支付金额的支付。

[0640] 在第185方面，根据方面184所述的方法，其中，支付请求包括收款方公钥和请求的金额，并且其中，支付金额与请求的金额相关。

[0641] 在第186方面，根据方面184-185中任一方面所述的方法，其中，识别收款方设备包括执行伙伴标识，其中，伙伴标识包括支付授权、敲击、物理指示、波束成形、在先布置、粗略确认，或其任何组合。

[0642] 在第187方面，根据方面184-186中任一方面所述的方法，其中，原始数字支票进一步包括支票标识符。

[0643] 在第188方面，根据方面187所述的方法，其中，支票标识符是单调递增的数字。

[0644] 在第189方面，根据方面184-188中任一方面所述的方法，其中从付款方设备接收原始数字支票包括直接或通过中间设备经由短程链路从付款方设备接收原始数字支票。

[0645] 在第190方面，根据方面189所述的方法，其中，短程链路是对等通信链路。

[0646] 在第191方面，根据方面184-190中任一方面所述的方法，其中，认可的数字支票进一步包括用于仅兑换的认可、查询认可、恶意支票认可或其任何组合。

[0647] 在第192方面，根据方面184-191中任一方面所述的方法，其中，创建原始数字支票包括由付款方设备接收付款方认证信息，并且其中，创建认可的数字支票包括通过收款方设备接收收款方认证信息。

[0648] 在第193方面，根据方面184-192中任一方面所述的方法，其中，验证原始数字支票包括使用付款方公钥来确定使用付款方私钥创建付款方签名。

[0649] 在第194方面，根据方面184-193中任一方面所述的方法，其中，由付款方设备的安全元件使用付款方私钥创建付款方签名，并且其中，付款方私钥存储在付款方设备的安全

元件中。

[0650] 在第195方面，根据方面184-194中任一方面所述的方法，其中，由收款方设备的安全元件使用收款方私钥创建收款方签名，并且其中，收款方私钥存储在收款方设备的安全元件中。

[0651] 在第196方面，根据方面184-195中任一方面所述的方法，进一步包括从处理平台接收公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0652] 在第197方面，根据方面196所述的方法，进一步包括向付款方设备发送公共记录。

[0653] 在第198方面，根据方面184-195中任一方面所述的方法进一步包括从付款方设备接收公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0654] 在第199方面，根据方面196-198中任一方面所述的方法，其中，公共分类帐进一步包括公共分类帐签名，其中，使用处理平台的处理平台私钥来创建公共分类帐签名，该方法进一步包括使用处理平台的处理平台公钥验证公共分类帐而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台的公钥加密对，并且其中，验证公共分类帐包括使用处理平台公钥来确定使用处理平台私钥创建公共分类帐签名。

[0655] 在第200方面，公开了一种计算机系统。该计算机系统包括：硬件处理器；以及具有存储在其上的指令的非暂态存储器，该指令当由处理器执行时，使处理器执行方面148-199中任一方面的方法。

[0656] 在第201方面，根据方面200所述的计算机系统，其中，计算机系统是移动设备。

[0657] 在第202方面，根据方面201所述的计算机系统，其中，移动设备是可穿戴显示系统。

[0658] 加密签名记录的验证

[0659] 在第203方面，公开了一种用于验证加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从记录发送方设备接收发送方个体记录，其中，发送方个体记录包括记录标识符、记录内容、发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，并且其中，在从记录接收方设备接收到内容请求并识别记录接收方设备之后由记录发送方设备创建发送方个体记录；确定发送方个体记录无效而不一定与处理平台通信；创建接收方个体记录，其中，接收方个体记录包括发送方个体记录、恶意记录认可和接收方个体记录的接收方签名，其中使用记录接收方设备的接收方私钥创建接收方签名，并且其中，接收方公钥和接收方私钥形成接收方公钥加密对；并向处理平台发送接收方个体记录。

[0660] 在第204方面，根据方面203所述的方法，其中，确定发送方个体记录是无效的包括检测具有单个接收方的发送方克隆，检测窥探或检测重影。

[0661] 在第205方面，根据方面204所述的方法，其中，发送方个体记录的记录标识符是单调递增的数字，其中，记录接收方设备保持先前接收的个体记录的最高记录标识符，其中记录发送方设备的发送方公钥作为先前接收的个体记录的发送方公钥，并且其中，检测发送方克隆包括确定发送方个体记录的记录标识符不大于最高记录标识符。

[0662] 在第206方面，根据方面205所述的方法，其中，发送方个体记录的记录标识符对于由记录发送方设备创建的个体记录不同，其中，记录接收方设备保持先前从记录发送方设备接收的个体记录的记录标识符，并且其中，检测发送方克隆包括确定发送方个体记录的

记录标识符不在先前从记录发送方设备接收的所有个体记录的记录标识符中。

[0663] 在第207方面，根据方面205-206中任一方面所述的方法，其中，发送方公钥是记录发送方设备的发送方公钥，其中，使用记录发送方设备的发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对。

[0664] 在第208方面，根据方面204-207中任一方面所述的方法，其中，发送方公钥是记录发送方设备的发送方公钥，其中，检测窥探包括确定不使用记录发送方设备的发送方私钥创建发送方签名，其中，发送方公钥和发送方私钥形成发送方公钥加密对，并且其中，确定发送方签名不使用记录发送方设备的发送方私钥创建包括使用发送方公钥来确定不使用发送方私钥创建发送方签名。

[0665] 在第209方面，根据方面204-208中任一方面所述的方法，其中，检测重影包括确定发送方公钥不是用户设备的有效公钥，其中，确定发送方公钥不是有效公钥包括：从处理平台接收公共记录，其中，公共记录包括用户设备的有效公钥；以及确定公共记录包括记录发送方设备的发送方公钥。

[0666] 在第210方面，根据方面209所述的方法，其中，使用发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对。

[0667] 在第211方面，根据方面203-210中任一方面所述的方法进一步包括使处理平台向恶意用户设备的黑名单添加记录发送方设备。

[0668] 在第212方面，公开了一种用于验证加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从记录发送方设备接收发送方个体记录，其中，发送方个体记录包括记录内容、发送方公钥、接收方公钥和发送方个体记录的发送方签名，其中，使用发送方私钥创建发送方签名，其中，发送方公钥和发送方私钥形成发送方公钥加密对，并且其中，在从记录接收方设备接收到内容请求并识别记录接收方设备之后由记录发送方设备发送个体记录；确定发送方个体记录无效而不一定与处理平台通信；创建接收方个体记录，其中，接收方个体记录包括发送方个体记录、恶意记录认可和接收方个体记录的接收方签名，其中，使用记录接收方设备的接收方私钥创建接收方签名，并且其中，接收方公钥和接收方私钥形成接收方公钥加密对；并向处理平台发送接收方个体记录。

[0669] 在第213方面，根据方面212所述的方法，其中，确定发送方个体记录是无效的包括检测具有多个接收方的发送方克隆或检测分叉。

[0670] 在第214方面，根据方面213所述的方法，其中，检测具有多个接收方的发送方克隆包括：确定发送方公钥是记录发送方设备的发送方公钥；并且确定接收方公钥不是记录接收方设备的公钥。

[0671] 在第215方面，根据方面213所述的方法，其中检测分叉包括：确定发送方公钥不是记录发送方设备的公钥，确定记录接收方设备的公钥不在发送方个体记录中，并确定接收方公钥不是记录接收方设备的公钥。

[0672] 在第216方面，根据方面214-215中任一方面所述的方法，其中，使用发送方私钥创建发送方签名，并且其中，发送方公钥和发送方私钥形成发送方公钥加密对。

[0673] 在第217方面，根据方面212-216中任一方面所述的方法，进一步包括使处理平台向恶意用户设备的黑名单添加记录发送方设备。

[0674] 在第218方面，公开了一种用于验证加密签名记录的方法。该方法在硬件处理器的

控制下执行，并且包括：从记录接收方设备接收接收方个体记录，其中，接收方个体记录包括发送方个体记录、仅用于处理的认可，以及接收方个体记录的接收方签名，其中，发送方个体记录包括记录内容、发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，其中，使用发送方私钥创建发送方签名，其中，发送方公钥和发送方私钥形成发送方公钥加密对，其中，在从记录发送方设备接收到发送方个体记录并使用发送方公钥验证发送方个体记录而不一定与处理平台通信之后，由记录接收方设备创建接收方个体记录，其中，使用记录接收方设备的接收方私钥创建接收方签名，并且其中，接收方公钥和接收方私钥形成接收方公钥加密对；确定接收方个体记录无效；并且拒绝如记录内容所指示地执行记录接收方设备。

[0675] 在第219方面，根据方面218所述的方法，其中，确定接收方个体记录是无效的包括检测接收方克隆或检测重影。

[0676] 在第220方面，根据方面219所述的方法，其中，发送方个体记录包括记录标识符，其中，发送方公钥是记录发送方设备的发送方公钥，其中，发送方私钥是记录发送方设备的发送方私钥，以及其中，检测接收方克隆包括确定个体记录包括发送方公钥并且在接收接收方个体记录之前已经接收到记录标识符。

[0677] 在第221方面，根据方面220所述的方法，其中，确定个体记录包括发送方公钥并且在接收接收方个体记录之前已经接收到记录标识符包括：保持先前接收的个体记录的记录标识符，其中记录发送方设备的发送方公钥作为先前接收的个体记录的发送方公钥；以及确定发送方个体记录的记录标识符不在先前接收的个体记录的记录标识符中，其中记录发送方设备的发送方公钥作为先前接收的个体记录的发送方公钥。

[0678] 在第222方面，根据方面219-221中任一方面所述的方法，其中，检测重影包括：确定发送方公钥是无效公钥。

[0679] 在第223方面，根据方面222所述的方法，其中，确定发送方公钥是无效公钥包括：维护有效发送方公钥；以及确定有效的发送方公钥包括发送方个体记录的发送方公钥。

[0680] 在第224方面，根据方面218-223中任一方面所述的方法，进一步包括：如果检测到接收方克隆，则向恶意用户的黑名单添加记录发送方设备；如果检测到重影，则向恶意用户的黑名单添加记录接收方设备。

[0681] 在第225方面，公开了一种验证加密签名记录的方法。该方法在硬件处理器的控制下执行，并且包括：从记录接收方设备接收接收方个体记录，其中，接收方个体记录包括发送方个体记录、认可和接收方个体记录的接收方签名，其中，认可是恶意记录认可或仅用于处理的认可，其中，发送方个体记录包括记录内容、记录发送方设备的发送方公钥、记录接收方设备的接收方公钥，以及发送方个体记录的发送方签名，以及其中，使用记录发送方设备的发送方私钥创建发送方签名，其中，发送方公钥和发送方私钥形成发送方公钥加密对；确定接收方个体记录无效；并确定接收方个体记录无效的原因。

[0682] 在第226方面，根据方面225所述的方法，其中，确定接收方个体记录无效的的原因包括使用布尔分析确定接收方个体记录无效的原因。

[0683] 在第227方面，根据方面225所述的方法，其中，确定接收方个体记录无效的原因包括使用模糊判定确定接收方个体记录无效的原因，包括：保持记录发送方设备作为任何个体记录无效的第一原因的第一概率；保持记录接收方设备作为任何个体记录无效的第二原

因的第二概率;通过将第一概率乘以第三概率来更新记录发送方设备作为任何个体记录无效的第一原因的第一概率,其中,第三概率是记录发送方设备或记录接收方设备作为接收方个体记录无效的原因的概率;通过将第二概率乘以第三概率来更新记录接收方设备作为任何个体记录无效的第二原因的第二概率;以及如果第一概率大于第二概率,则确定接收方个体记录无效的原因是记录发送方设备,或如果第二概率大于第一概率,则确定接收方个体记录无效的原因是记录接收方设备。

[0684] 在第228方面,根据方面227所述的方法,进一步包括向恶意用户设备的黑名单添加接收方个体记录无效的原因。

[0685] 在第229方面,公开了一种计算机系统。该计算机系统包括:硬件处理器;具有存储在其上的指令的非暂态存储器,该指令当由处理器执行时,使处理器执行方面203-228中任一方面的方法。

[0686] 在第230方面,根据方面229所述的计算机系统,其中,计算机系统是移动设备。

[0687] 在第231方面,根据方面230所述的计算机系统,其中,移动设备是可穿戴显示系统。

[0688] 加密签名数字支票的安全交换-(多个)金融机构

[0689] 在第232方面,公开了一种用于安全地交换加密签名的数字支票的方法。该方法在硬件处理器的控制下执行,并且包括:从收款方设备接收认可的数字支票,其中,认可的数字支票包括原始数字支票和认可的数字支票的收款方签名,其中,在从收款方接收到支付请求并识别收款方设备后由,付款方创建原始数字支票,其中,原始数字支票包括支付金额、付款方公钥、收款方公钥和原始数字支票的付款方签名,其中,使用付款方设备的付款方私钥创建付款方签名,其中,付款方公钥和收款方公钥形成收款方公钥加密对,其中,在从付款方设备接收到原始数字支票并使用付款方公钥验证原始数字支票而不一定与处理平台通信之后,由收款方设备创建认可的数字支票,其中,收款方设备使用收款方私钥创建收款方签名,并且其中,收款方公钥和收款方公钥形成收款方公钥加密对;验证认可的数字支票;并使得向收款方提供支付金额的支付。

[0690] 在第233方面,根据方面232所述的方法,其中,支付请求包括收款方公钥和请求的金额,并且其中,支付金额与请求的金额相关。

[0691] 在第234方面,根据方面232-233中任一方面所述的方法,其中,识别收款方设备包括执行伙伴标识,其中,伙伴标识包括内容授权、敲击、物理指示、波束成形、在先布置、粗略验证,或其任何组合。

[0692] 在第235方面,根据方面232-234中任一方面所述的方法,其中,原始数字支票进一步包括支票标识符。

[0693] 在第236方面,根据方面235所述的方法,其中,支票标识符是单调递增的数字。

[0694] 在第237方面,根据方面232-236中任一方面所述的方法,其中,从付款方设备接收原始数字支票包括直接或通过中间设备经由短程链路从付款方设备接收原始数字支票。

[0695] 在第238方面,根据方面237所述的方法,其中,短程链路是对等通信链路。

[0696] 在第239方面,根据方面232-238中任一方面所述的方法,其中,认可的数字支票进一步包括仅用于存款的认可、查询认可、恶意支票认可或其任何组合。

[0697] 在第240方面,根据方面232-239中任一方面所述的方法,其中,在由付款方设备接

收付款方的验证信息之后创建原始数字支票，并且其中，在收款方设备接收到收款方的认证信息之后，创建认可的数字支票。

[0698] 在第241方面，根据方面232-240中任一方面所述的方法，其中，验证原始数字支票包括：使用付款方公钥来确定使用付款方私钥创建付款方签名；并使用收款方公钥来确定使用收款方私钥创建收款方签名。

[0699] 在第242方面，根据方面232-241中任一方面所述的方法，进一步包括向付款方设备和收款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥。

[0700] 在第243方面，根据方面232-241中任一方面所述的方法，进一步包括：向付款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥；并使付款方设备向收款方设备提供公共分类帐。

[0701] 在第244方面，根据方面232-241中任一方面所述的方法，进一步包括：向收款方设备提供公共分类帐，其中，公共分类帐包括付款方公钥和收款方公钥；并使收款方设备向付款方设备提供公共分类帐。

[0702] 在第245方面，根据方面242-244中任一方面所述的方法，其中，公共分类帐进一步包括公共分类帐签名，其中，使用处理平台的处理平台私钥来创建公共分类帐签名，该方法进一步包括使用处理平台的处理平台公钥验证公共分类帐而不一定与处理平台通信，其中，处理平台公钥和处理平台私钥形成处理平台的公钥加密对，并且其中，验证公共分类帐包括使用处理平台公钥来确定使用处理平台私钥创建公共分类帐签名。

[0703] 在第246方面，根据方面242-245中任一方面所述的方法，进一步包括：从公共分类帐生成中央分类帐，其中，中央分类帐包括付款方设备的付款方帐户和收款方设备的收款方帐户，其中，付款方帐户包括付款方公钥和付款方帐户的帐户余额，并且其中，收款方帐户包括收款方公钥和收款方帐户的帐户余额。

[0704] 在第247方面，根据方面246所述的方法，使得向收款方提供支付金额的支付包括：使得确定付款方账户具有足够的余额对支付金额进行支付；使付款方账户借记支付金额；并使收款方帐户贷记支付金额。

[0705] 在第248方面，根据方面247所述的方法，其中，使付款方帐户借记支付金额包括指示第一金融机构借记付款方帐户支付金额，并且其中，使收款方帐户贷记支付金额包括指示第一金融机构借记付款方账户支付金额。

[0706] 在第249方面，根据方面247所述的方法，其中，使付款方帐户借记支付金额包括指示第一金融机构借记付款方帐户支付金额，并且其中，使收款方帐户贷记支付金额包括指示第二金融机构借记付款方账户支付金额。

[0707] 在第250方面，根据方面247-249中任一方面所述的方法，进一步包括：从收款方设备接收从收款方账户转出资金的请求，其中，从收款方账户转出资金的请求包括转出金额和转出方法，其中，转出方法是自动清算所(ACH)转账、电汇或发送实物支票；使收款方账户借记转出金额；并使得使用转出方法发送转出金额。

[0708] 在第251方面，根据方面250所述的方法，进一步包括：使收款方账户借记转移费用，其中，费用与转出金额成比例或固定。

[0709] 在第252方面，根据方面251所述的方法，进一步包括：从收款方设备接收从收款方账户转入资金的请求，其中，从收款方账户转入资金的请求包括转入金额和转入方法，其

中，转入方法是自动清算所(ACH)转移、电汇或发送实物支票；使收款方账户借记转入金额；并使得使用转入方法发送转入金额。

[0710] 在第253方面，根据方面252所述的方法，进一步包括：使收款方帐户借记转移费用，其中，费用与转入金额成比例或固定。

[0711] 在第254方面，根据方面246-253中任一方面所述的方法，其中使得向收款方提供支付金额的支付包括：使得确定付款方账户的余额不足以对支付金额进行支付；使得向付款方账户借记余额不足的费用；并向过失列表添加付款方设备。

[0712] 在第255方面，根据方面246-254中任一方面所述的方法，其中，原始数字支票进一步包括源账户，其中，使得向收款方提供支付金额的支付包括：使得从源帐户接收到支付金额；并使的向收款方帐户贷记支付金额。

[0713] 在第256方面，根据方面232-255中任一方面所述的方法，其中，原始数字支票包括费用分摊策略。

[0714] 在第257方面，根据方面232-256中任一方面所述的方法，其中，原始数字支票包括交易类型。

[0715] 在第258方面，根据方面257所述的方法，其中，交易类型包括支票类型交易、借记类型交易、信用卡类型交易、ACH类型交易或其组合。

[0716] 系统和设备

[0717] 在第259方面，公开了一种系统。该系统包括存储可执行指令的非暂态计算机可读存储器；以及由可执行指令编程的一个或多个硬件处理器，以执行方面1-259中任一方面的方法。

[0718] 在第260方面，公开了一种可穿戴显示系统。可穿戴显示系统包括显示器；存储可执行指令的非暂态计算机可读存储介质；以及由可执行指令编程的一个或多个硬件处理器，以执行方面1-259中任一方面的方法。

[0719] 结论

[0720] 在此描述和/或在附图中描绘的过程、方法和算法中的每一个可以由一个或多个物理计算系统、硬件计算机处理器、专用电路和/或被配置为执行具体和特定计算机指令的电子硬件执行的代码模块体现，并且完全或部分自动地体现。例如，计算系统可以包括用特定计算机指令编程的通用计算机(例如，服务器)或专用计算机、专用电路等。代码模块可以被编译并链接到可执行程序中，安装在动态链接库中，或者可以用解释性编程语言编写。在一些实施方式中，特定操作和方法可以由特定于给定功能的电路执行。

[0721] 此外，本公开的功能的某些实施方式在数学上、计算上或技术上足够复杂，以使得专用硬件或一个或多个物理计算设备(利用适当的专用可执行指令)对于执行功能可能是必需的，例如，由于所涉及的计算量或复杂性或基本上实时提供结果。例如，视频可以包括许多帧，每个帧具有数百万个像素，并且需要专门编程的计算机硬件来处理视频数据以在商业上合理的时间量内提供期望的图像处理任务或应用。此外，服务提供者104的处理平台124可以与数千或数百万个用户设备116a、116b进行电子通信，并且被配置为基本上在许多情况下或当用户设备116a、116b与处理平台124进行电子通信时实时地处理数十万、数百万或数亿个加密签名记录的交换。

[0722] 代码模块或任何类型的数据可以存储在任何类型的非暂态计算机可读介质上，诸

如物理计算机存储装置，包括硬盘驱动器、固态存储器、随机存取存储器(RAM)、只读存储器(ROM)、光盘、易失性或非易失性存储装置，它们的组合和/或类似物。方法和模块(或数据)还可以作为生成的数据信号(例如，作为载波或其它模拟或数字传播信号的一部分)在各种计算机可读传输介质(包括基于无线的和基于有线的/基于电缆的介质)上发送，并且可以采用多种形式(例如，作为单个或多路复用模拟信号的一部分，或者作为多个离散数字分组或帧)。所公开的过程或过程步骤的结果可以持久地或以其它方式存储在任何类型的非暂态有形计算机存储器中，或者可以经由计算机可读传输介质传送。

[0723] 在此描述和/或在附图中描绘的流程图中的任何过程、块、状态、步骤或功能应当理解为可能表示代码模块、代码段或代码部分，其包括用于实施特定功能(例如，逻辑或算术)或过程中的步骤的一个或多个可执行指令。各种过程、块、状态、步骤或功能可以与在此提供的说明性示例组合、重新排列、添加、删除、修改或以其它方式改变。在一些实施例中，附加或不同的计算系统或代码模块可以执行在此描述的一些或全部功能。在此描述的方法和过程也不限于任何特定序列，并且与其相关的块、步骤或状态可以以适当的其它顺序执行，例如，以串行、并行或以一些其它方式。可以向所公开的示例实施例添加任务或事件或从中删除任务或事件。此外，在此描述的实施方式中的各种系统组件的分离是出于说明性目的，并且不应被理解为在所有实施方式中都需要这种分离。应当理解，所描述的程序组件、方法和系统通常可以一起集成在单个计算机产品中或打包成多个计算机产品。许多实施方式变化都是可能的。

[0724] 可以在网络(或分布式)计算环境中实施过程、方法和系统。网络环境包括企业范围的计算机网络、内联网、局域网(LAN)、广域网(WAN)、个人局域网(PAN)、云计算网络、众包计算网络、因特网、基于云的网络和万维网。网络可以是有线或无线网络、基于卫星或气球的网络，或任何其它类型的通信网络。

[0725] 本公开的系统和方法各自具有若干创新方面，其中没有一个单独地对在此公开的期望属性负责或要求。上述各种特征和过程可以彼此独立地使用，或者可以以各种方式组合。所有可能的组合和子组合都旨在落入本公开的范围内。对本领域技术人员来说，对本公开中描述的实施方式的各种修改是显而易见的，并且在不脱离本公开的精神或范围的情况下，在此定义的一般原理可以应用于其它实施方式。因此，权利要求不旨在限于在此所示的实施方式，而是与符合本公开，在此公开的原理和新颖特征的最宽范围相一致。

[0726] 在单独实施方式的情境中在本说明书中描述的某些特征也可以在单个实施方式中组合实施。相反，在单个实施方式的情境中描述的各种特征也可以单独地或以任何合适的子组合在多个实施方式中实施。此外，尽管上面的特征可以描述为以某些组合起作用并且甚至最初如此声明，但是在一些情况下可以从组合中切除来自所要求保护的组合的一个或多个特征，并且所要求保护的组合可以针对子组合或子组合的变体。对于每个和所有实施例，没有必要或不可或缺的单个特征或特征组。

[0727] 除非另有说明或者在所使用的情境中以其它方式理解，否则在此使用的条件语言，诸如“能够”、“可”、“可能”、“可以”、“例如”等通常旨在传达某些实施例包括某些特征、元件和/或步骤，而其它实施例不包括某些特征、元件和/或步骤。因此，这种条件语言通常不旨在暗示对于一个或多个实施例以任何方式需要特征、元素和/或步骤，或者一个或多个实施例必须包括用于决定(无论是否有作者输入或提示)在任何特定实施例中包括或将要

执行这些特征、元件和/或步骤的逻辑。术语“包括”、“包含”、“具有”等是同义的并且以开放式方式包含使用，并且不排除附加元件、特征、动作、操作等。此外，术语“或”在其包含意义上使用(而不是在其独有意义上)，使得当以例如连接元素列表使用时，术语“或”表示列表中的一个、一些或全部元素。另外，除非另有说明，否则本申请和所附权利要求中使用的冠词“一”、“一个”和“该”应理解为表示“一个或多个”或“至少一个”。

[0728] 如在此所使用的，指代项目列表中的“至少一个”的短语是指那些项目的任何组合，包括单个成员。例如，“A、B或C中的至少一个”旨在涵盖:A、B、C、A和B、A和C、B和C，以及A、B和C。除非另有明确说明，否则诸如短语“X、Y和Z中的至少一个”的联合语言在上下文中被理解为通常用于表示项目、术语等可以是X、Y或Z中的至少一个。因此，这种联合语言通常不旨在暗示某些实施例需要X中的至少一个、Y中的至少一个和Z中的至少一个各自存在。

[0729] 类似地，尽管可以以特定顺序在附图中描绘操作，但应认识到，不需要以所示的特定顺序或按顺序执行这些操作，或者执行所有示出的操作，以实现期望的结果。此外，附图可以以流程图的形式示意性地描绘一个或多个示例过程。然而，未示出的其它操作可以包含在示意性示出的示例方法和过程中。例如，可以在任何所示操作之前、之后、同时或之间执行一个或多个附加操作。另外，可以在其它实施方式中重新排列或重新排序操作。在某些情况下，多任务处理和并行处理可能是有利的。此外，上述实施方式中的各种系统组件的分离不应被理解为在所有实施方式中都需要这种分离，并且应当理解，所描述的程序组件和系统通常可以在单个软件产品中集成在一起或者被打包到多种软件产品。另外，其它实施方式在以下权利要求的范围内。在一些情况下，权利要求中记载的动作可以以不同的顺序执行并且仍然实现期望的结果。以下权利要求通过引用明确地并入本具体说明书中作为本公开的另外方面。

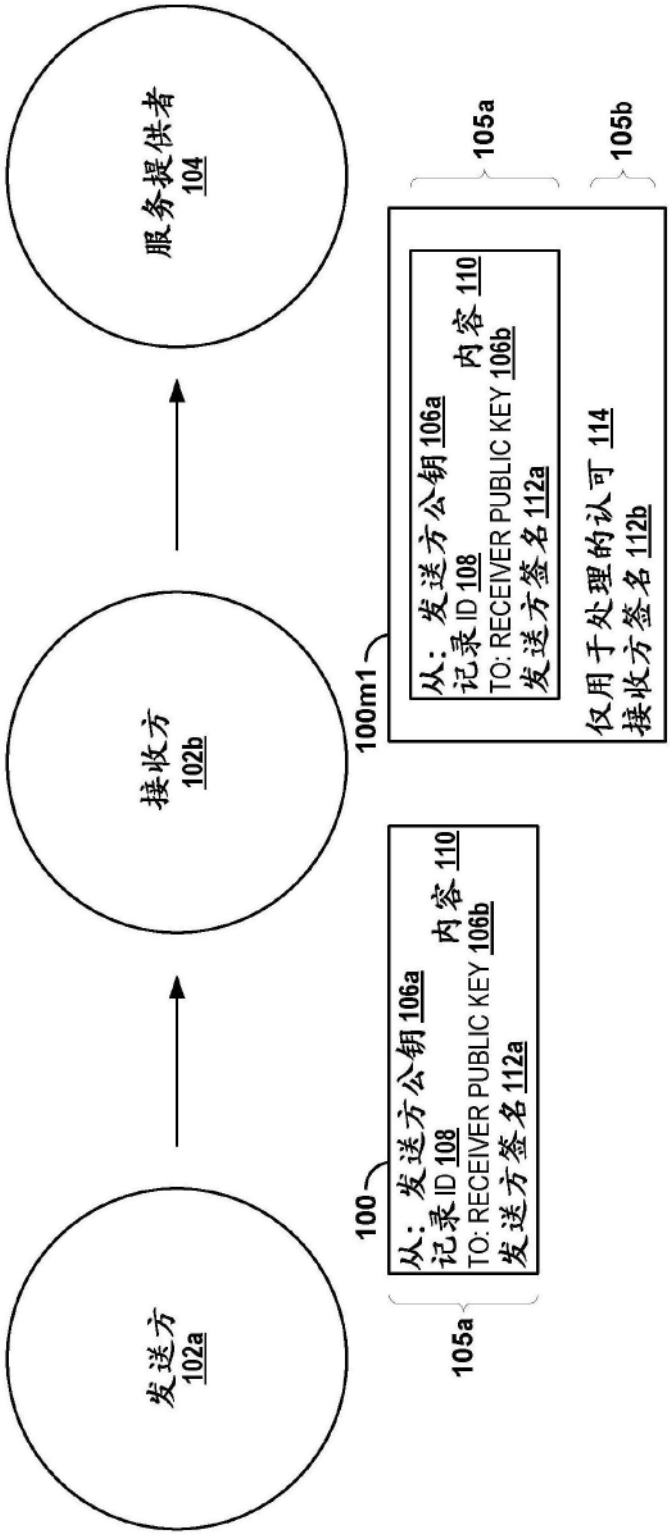

发送方
102a
接收方
102b
服务提供者
104
100
从：发送方公钥 106a
记录 ID 108
内容 110
TO: RECEIVER PUBLIC KEY 106b
发送方签名 112a
105a
100m1
从：发送方公钥 106a
记录 ID 108
内容 110
TO: RECEIVER PUBLIC KEY 106b
发送方签名 112a
仅用于处理的认可 114
接收方签名 112b
105a
105b

图1A

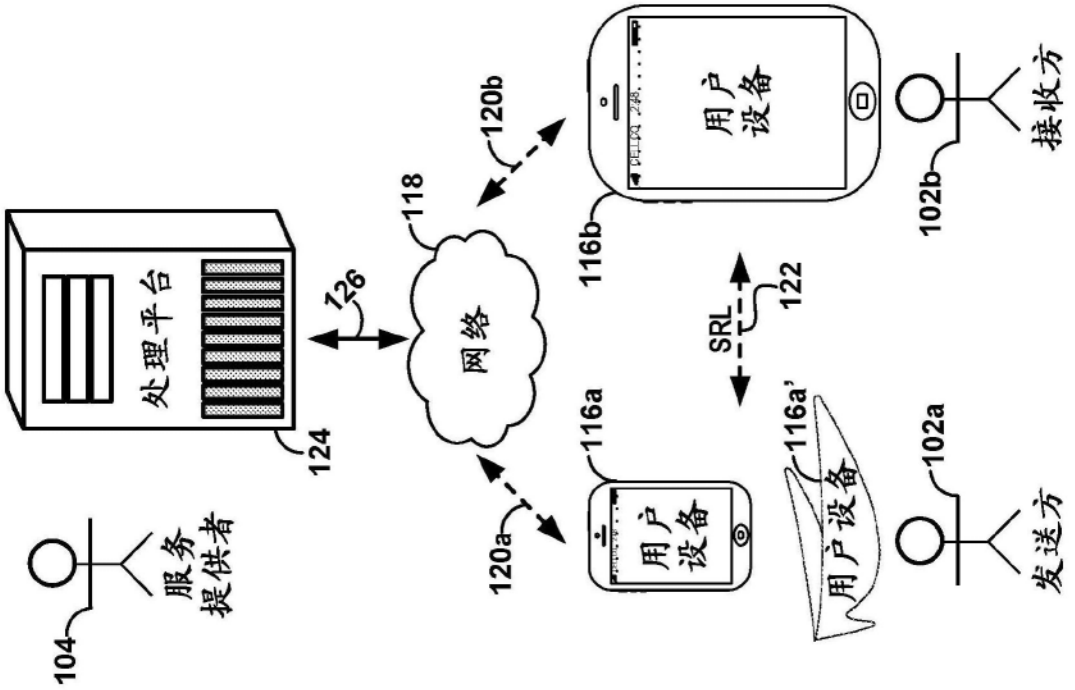

处理平台
124
126
网络
118
120b
120a
116b
116a
116a'
用户设备
用户设备
用户设备
SRL
122
102b
接收方
102a
发送方
104
服务提供者

图1B

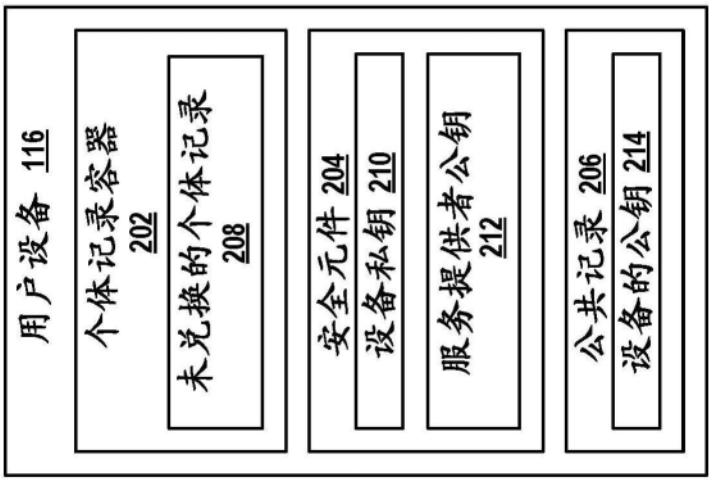

用户设备 116
个体记录容器 202
未兑换的个体记录 208
安全元件 204
设备私钥 210
服务提供者公钥 212
公共记录 206
设备的公钥 214

图2

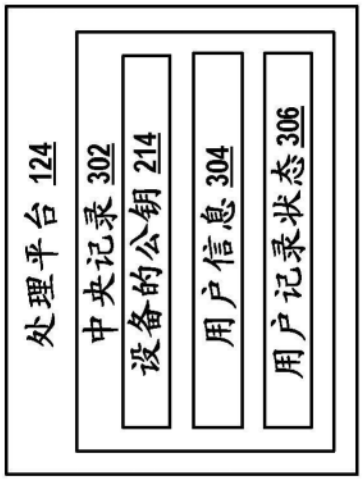


图3

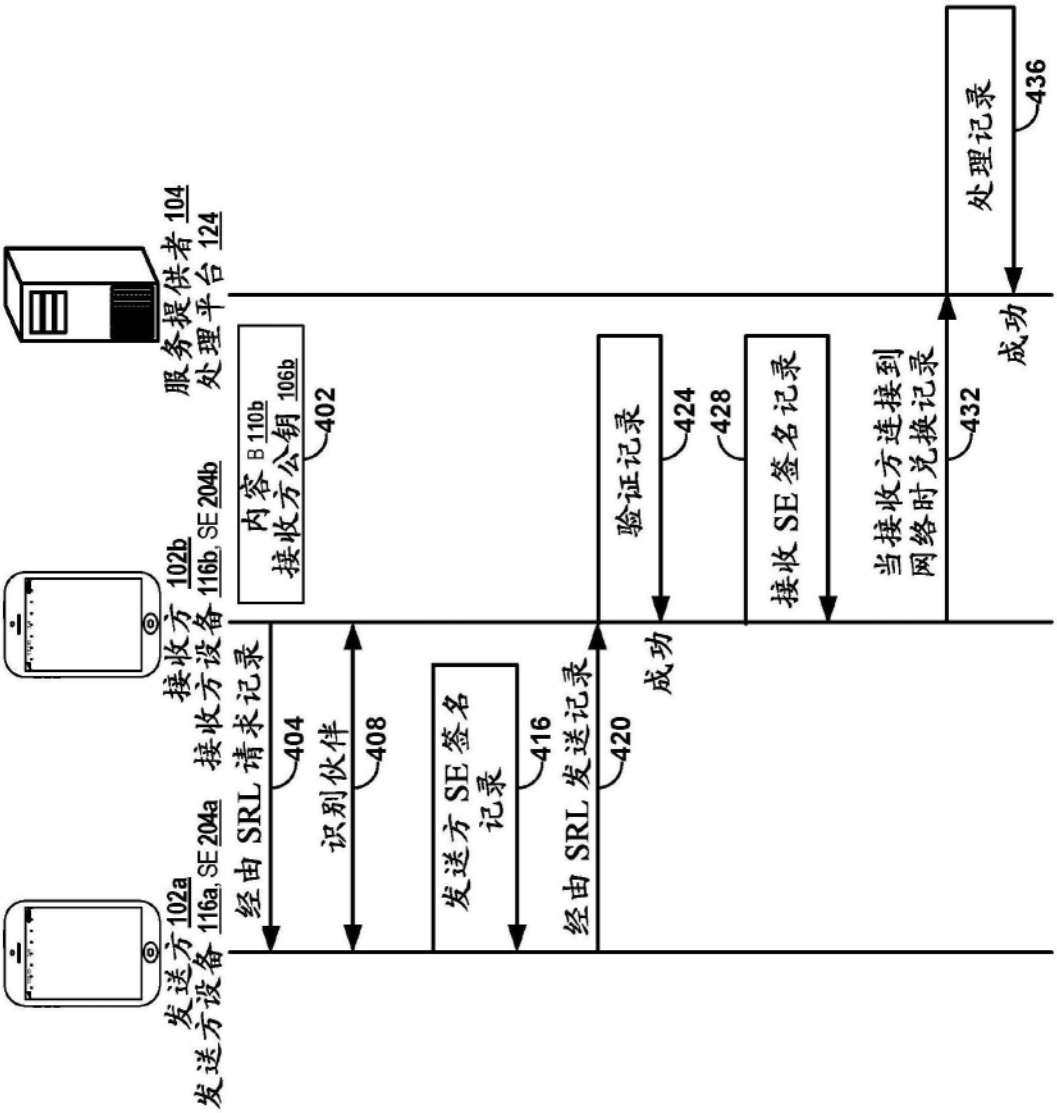

发送方设备 102a
116a, SE 204a
接收方设备 102b
116b, SE 204b
服务提供者处理平台 104
124
内容 B 110b
接收方公钥 106b
402
经由 SRL 请求记录
404
识别伙伴
408
发送方 SE 签名记录
416
经由 SRL 发送记录
420
成功
验证记录
424
接收 SE 签名记录
428
当接收方连接到网络时兑换记录
432
成功
处理记录
436

图4

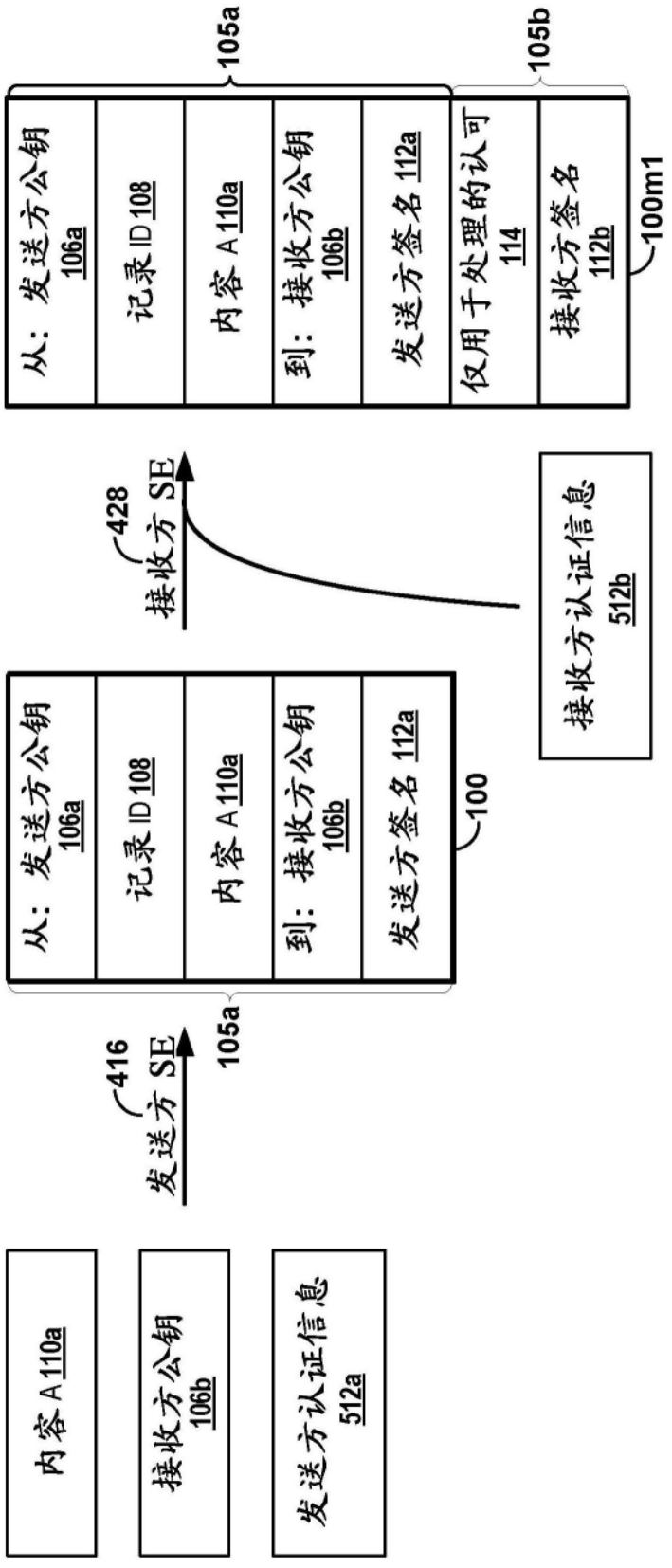

105a
105b
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方公钥 106b
发送方签名 112a
仅用于处理的认可 114
接收方签名 112b
100m1
428
接收方 SE
接收方认证信息 512b
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方公钥 106b
发送方签名 112a
100
416
发送方 SE
105a
内容 A 110a
接收方公钥 106b
发送方认证信息 512a

图5

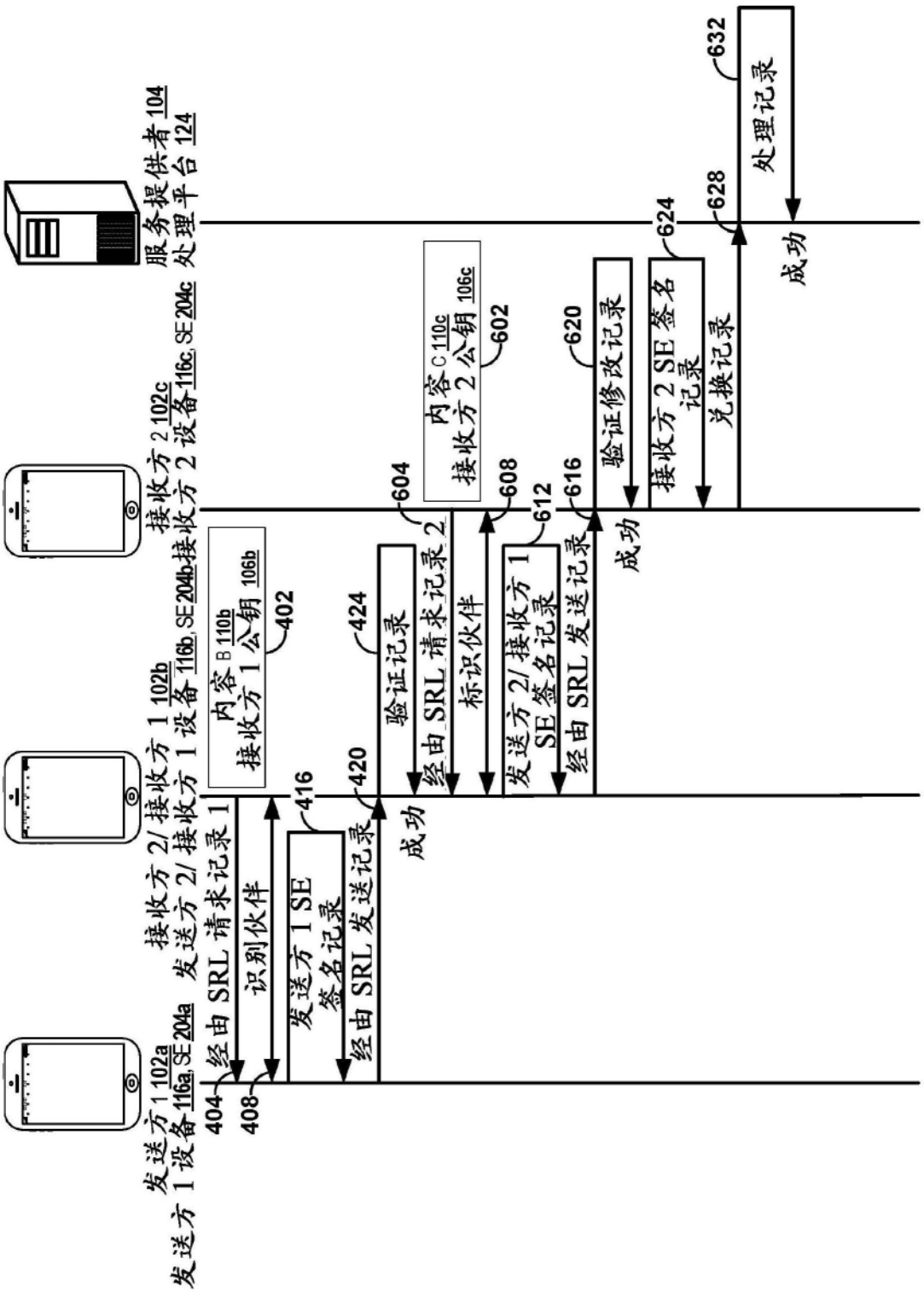

发送方 1 设备 116a, SE 204a 102a
接收方 2/ 发送方 2/ 接收方 1 设备 116b, SE 204b 102b
接收方 2 设备 116c, SE 204c 102c
服务提供者处理平台 124 104
404
经由 SRL 请求记录 1
识别伙伴
408
402
内容 B 110b
接收方 1 公钥 106b
416
发送方 1 SE 签名记录
420
经由 SRL 发送记录
成功
424
验证记录
604
经由 SRL 请求记录 2
标识伙伴
608
602
内容 C 110c
接收方 2 公钥 106c
612
发送方 2/ 接收方 1 SE 签名记录
616
经由 SRL 发送记录
成功
620
验证修改记录
624
接收方 2 SE 签名记录
628
兑换记录
632
处理记录
成功

图6

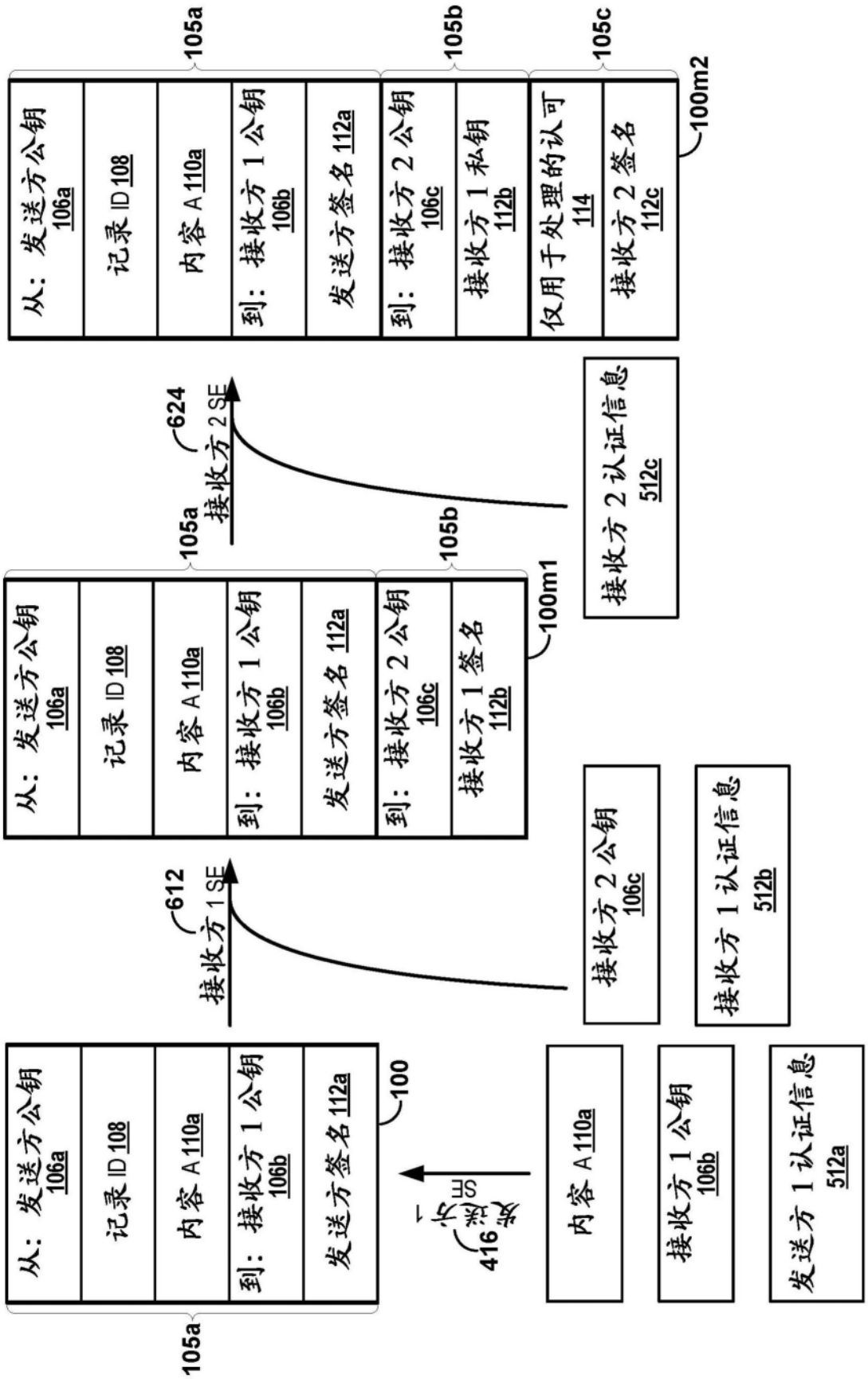

从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
105a
100
416 发送
内容 A 110a
接收方 1 公钥 106b
发送方 1 认证信息 512a
612 接收方 1 SE
接收方 2 公钥 106c
接收方 1 认证信息 512b
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
到：接收方 2 公钥 106c
接收方 1 签名 112b
105a
105b
100m1
624 接收方 2 SE
接收方 2 认证信息 512c
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
到：接收方 2 公钥 106c
接收方 1 私钥 112b
仅用于处理的认可 114
接收方 2 签名 112c
105a
105b
105c
100m2

图7

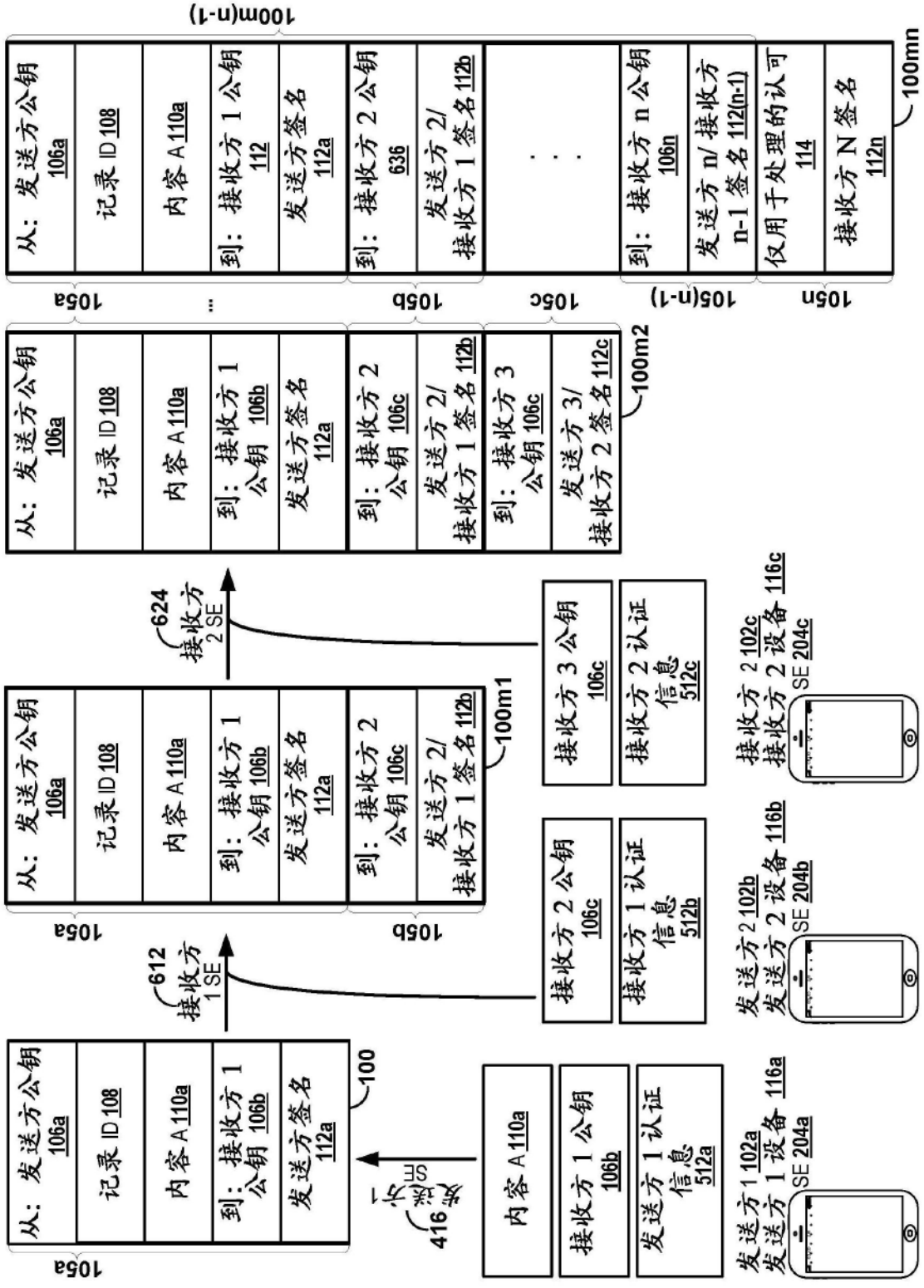

从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
100
105a
416 发送方 1 设备 SE 204a
发送方 1 102a
内容 A 110a
接收方 1 公钥 106b
发送方 1 认证信息 512a
116a
612 接收方 1 SE
到：接收方 2 公钥 106c
发送方 2/ 接收方 1 签名 112b
100m1
105b
发送方 2 102b
发送方 2 设备 SE 204b
接收方 2 公钥 106c
接收方 1 认证信息 512b
116b
624 接收方 2 SE
到：接收方 3 公钥 106c
发送方 3/ 接收方 2 签名 112c
100m2
接收方 2 102c
接收方 2 设备 SE 204c
接收方 3 公钥 106c
接收方 2 认证信息 512c
116c
105c
105(n-1)
到：接收方 n 公钥 106n
发送方 n/ 接收方 n-1 签名 112(n-1)
100m(n-1)
105n
仅用于处理的认可 114
接收方 N 签名 112n
100mn

图8

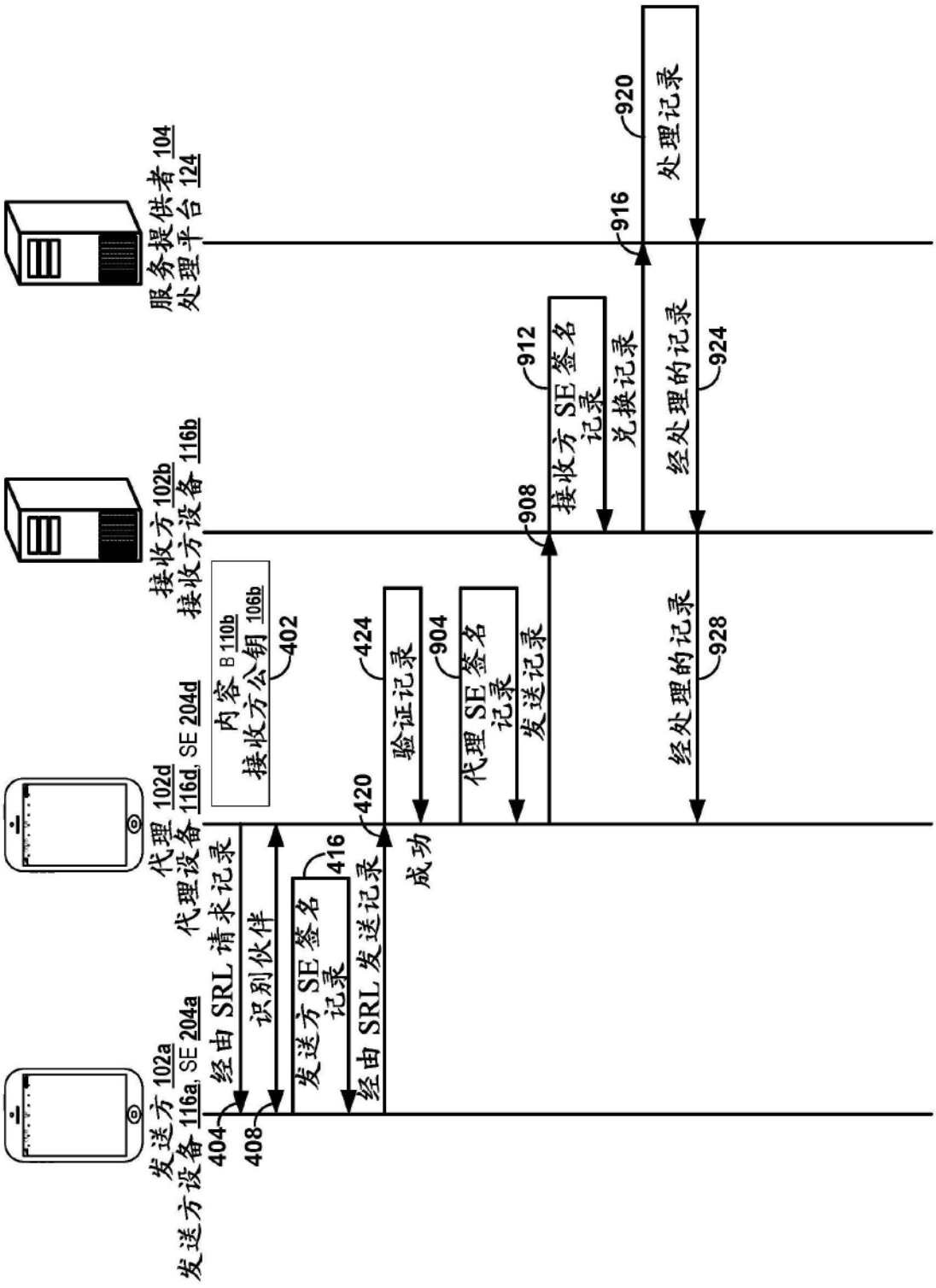

发送方 102a
发送方设备 116a, SE 204a
代理 102d
代理设备 116d, SE 204d
接收方 102b
接收方设备 116b
服务提供者 104
处理平台 124
404
经由 SRL 请求记录
408
识别伙伴
内容 B 110b
接收方公钥 106b
402
420
发送方 SE 签名记录
416
经由 SRL 发送记录
424
验证记录
成功
904
代理 SE 签名记录
发送记录
908
912
接收方 SE 签名记录
兑换记录
916
920
处理记录
924
经处理的记录
928
经处理的记录

图9

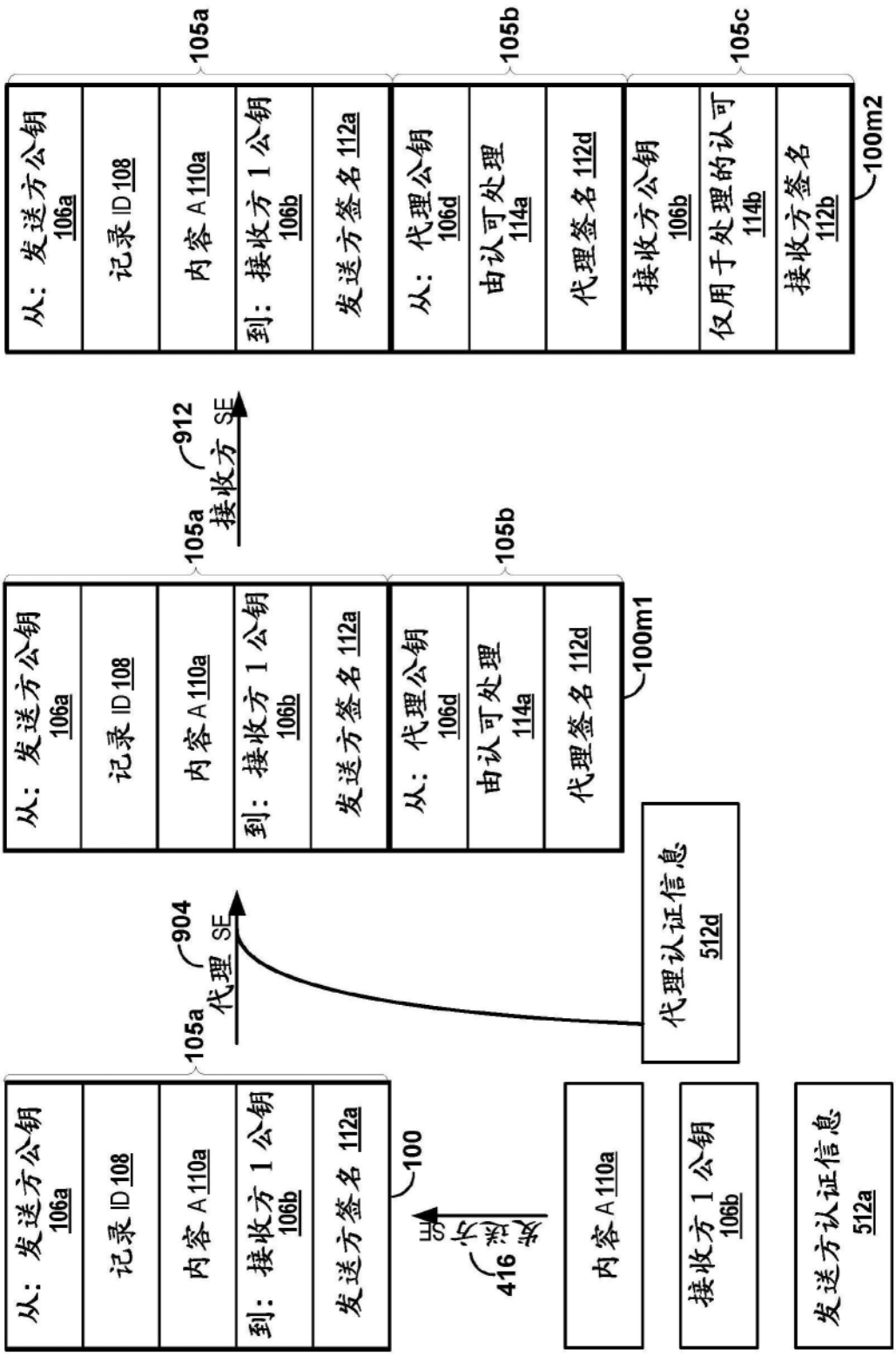

105a
105b
105c
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
从：代理公钥 106d
由认可处理 114a
代理签名 112d
接收方公钥 106b
仅用于处理的认可 114b
接收方签名 112b
100m2
912
接收方 SE
105a
105b
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
从：代理公钥 106d
由认可处理 114a
代理签名 112d
100m1
904
代理 SE
105a
代理认证信息 512d
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
100
416
内容 A 110a
接收方 1 公钥 106b
发送方认证信息 512a

图10

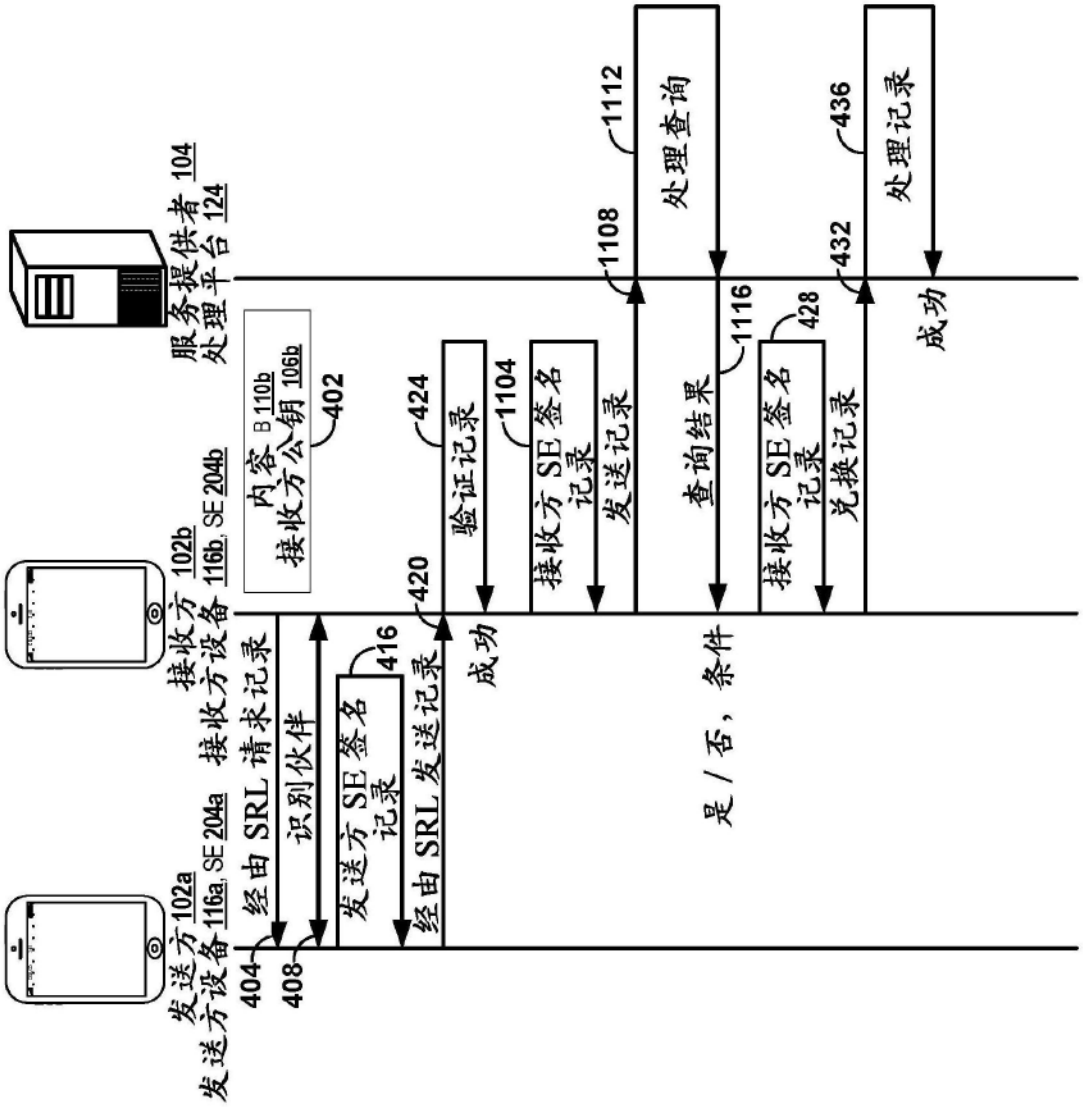

发送方设备 102a, 116a, SE 204a
接收方设备 102b, 116b, SE 204b
服务提供者处理平台 104, 124
404
经由 SRL 请求记录识别伙伴
408
内容 B 110b
接收方公钥 106b
402
发送方 SE 签名记录
416
经由 SRL 发送记录
420
验证记录
424
成功
接收方 SE 签名记录
1104
发送记录
1108
处理查询
1112
查询结果
1116
是 / 否，条件
接收方 SE 签名记录
428
兑换记录
432
处理记录
436
成功

图11

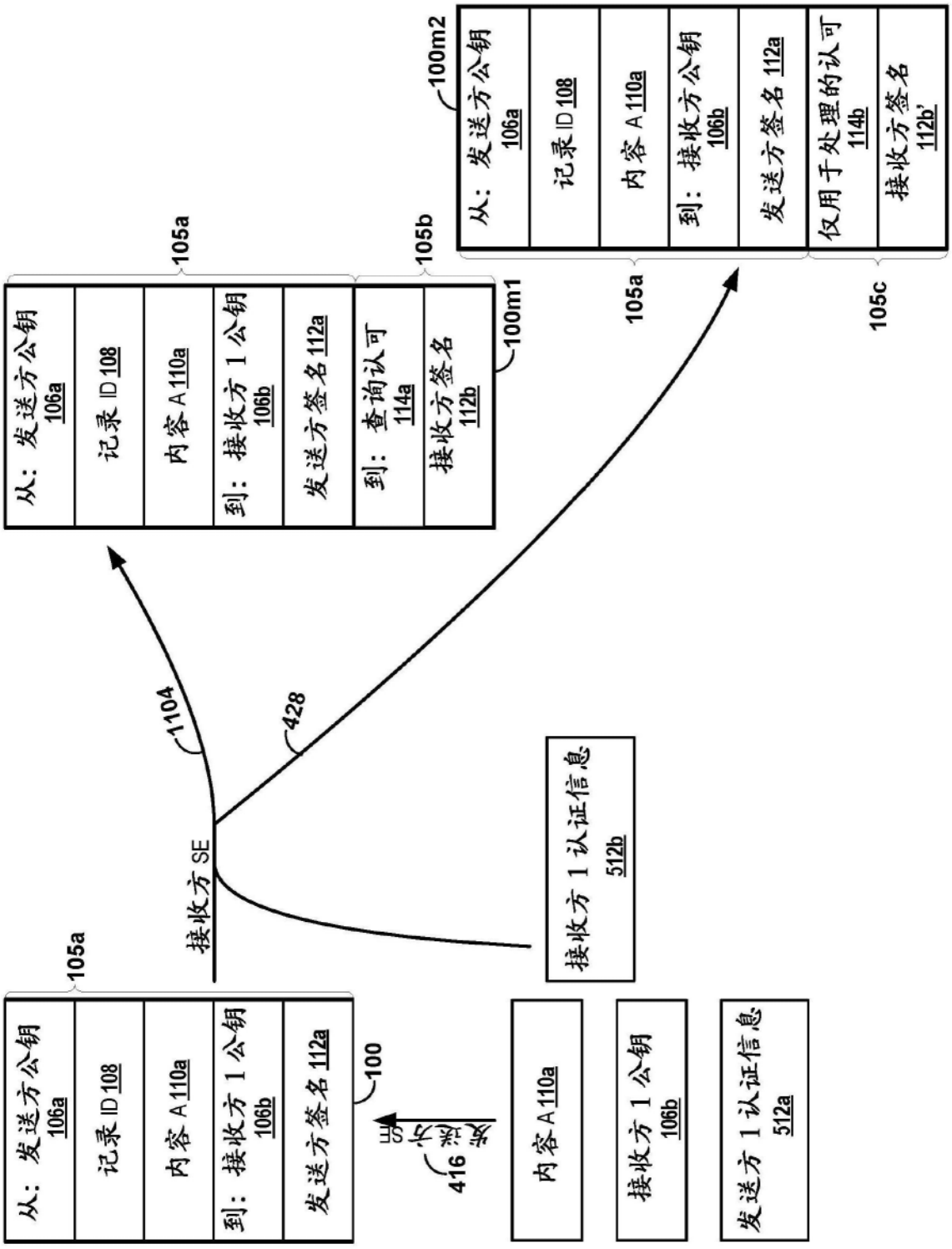

从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方 1 公钥 106b
发送方签名 112a
105a
100
416
内容 A 110a
接收方 1 公钥 106b
发送方 1 认证信息 512a
接收方 SE
1104
428
接收方 1 认证信息 512b
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：查询认可 114a
接收方签名 112b
105b
100m1
从：发送方公钥 106a
记录 ID 108
内容 A 110a
到：接收方公钥 106b
发送方签名 112a
仅用于处理的认可 114b
接收方签名 112b'
100m2
105a
105c

图12

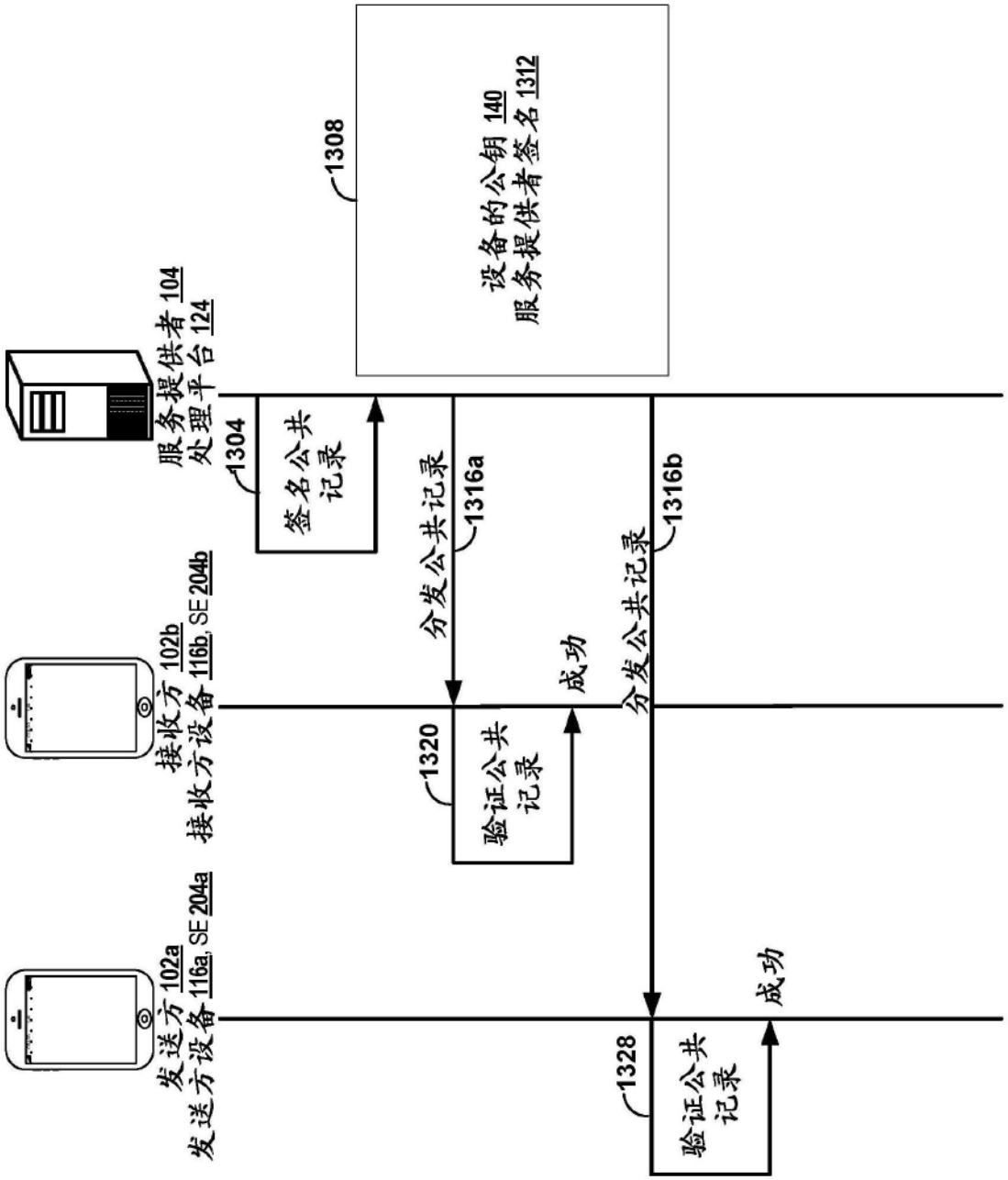

1308
设备的公钥 140
服务提供者签名 1312
服务提供者 104
处理平台 124
1304
签名公共记录
分发公共记录
1316a
分发公共记录
1316b
接收方 102b
接收方设备 116b, SE 204b
成功
1320
验证公共记录
发送方 102a
发送方设备 116a, SE 204a
成功
1328
验证公共记录

图13

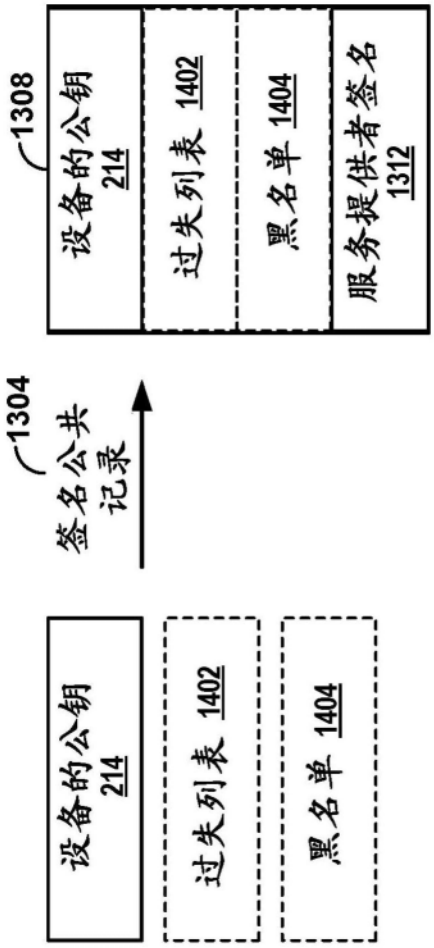

1308
设备的公钥 214
过失列表 1402
黑名单 1404
服务提供者签名 1312
1304
签名公共记录
设备的公钥 214
过失列表 1402
黑名单 1404

图14

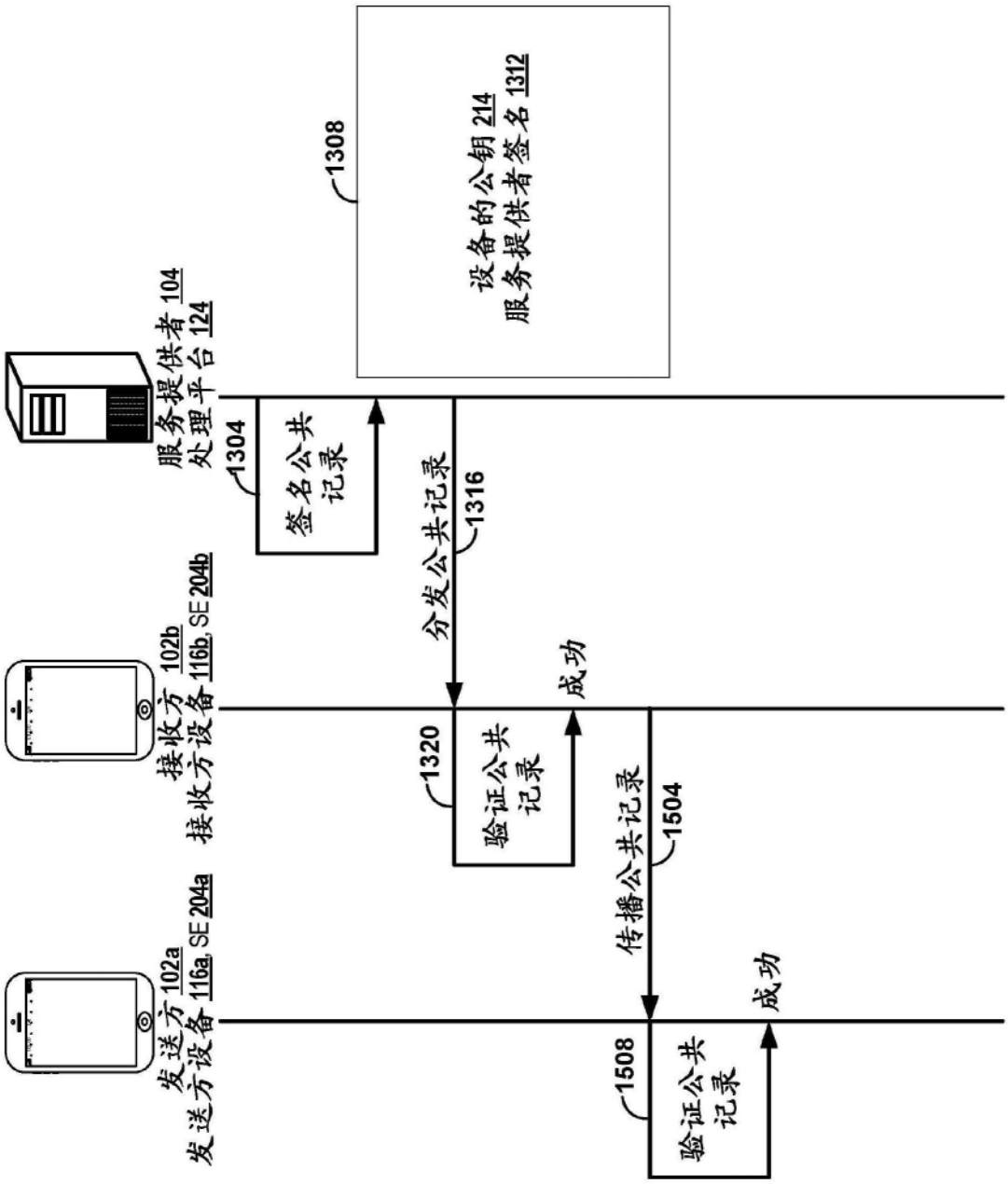

1308
设备的公钥 214
服务提供者签名 1312
服务提供者 104
处理平台 124
1304
签名公共记录
分发公共记录
1316
接收方 102b
接收方设备 116b, SE 204b
成功
1320
验证公共记录
传播公共记录
1504
发送方 102a
发送方设备 116a, SE 204a
成功
1508
验证公共记录

图15

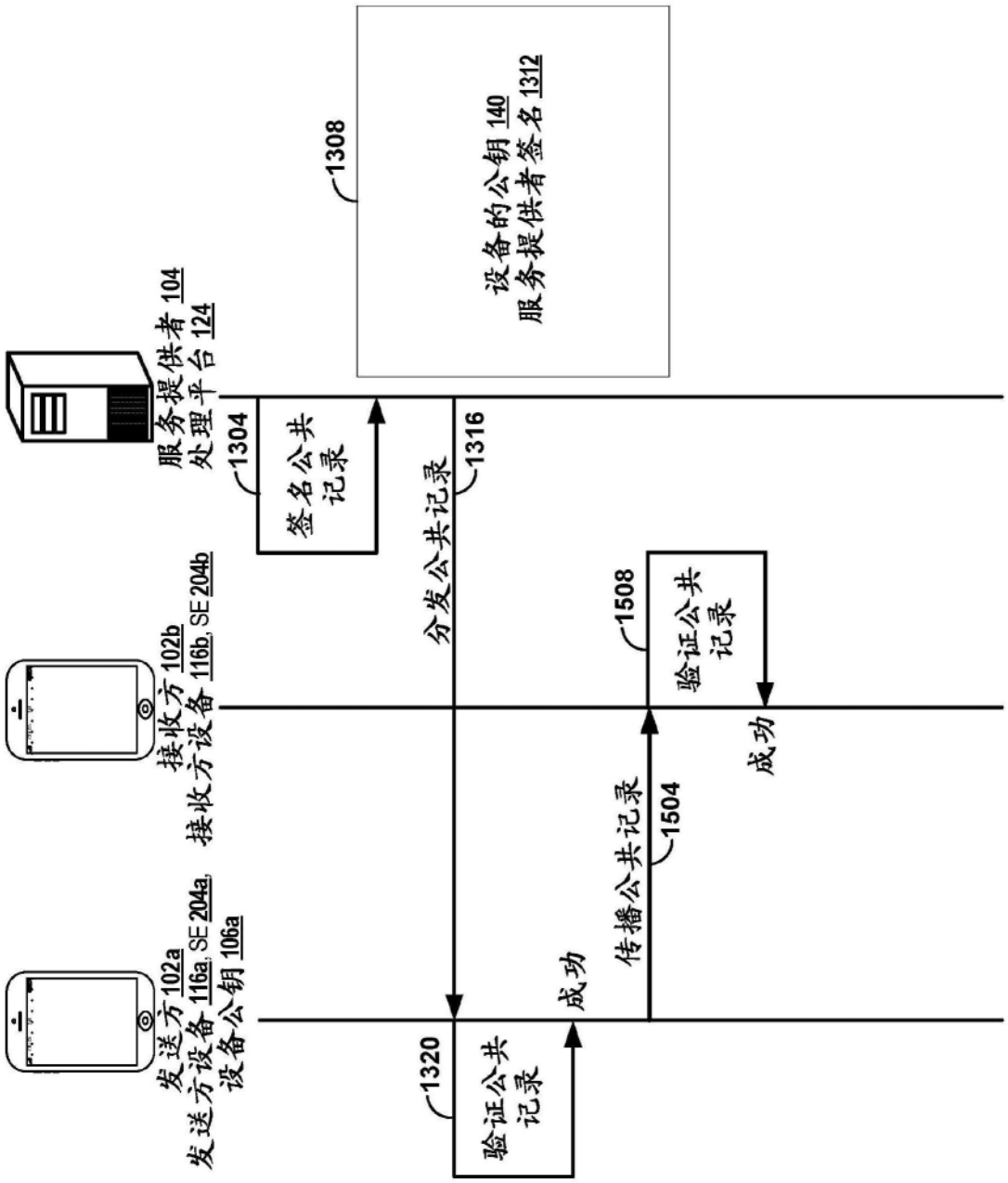

设备的公钥 140
服务提供者签名 1312
1308
服务提供者 104
处理平台 124
1304
签名公共记录
1316
分发公共记录
1508
验证公共记录
成功
接收方 102b
接收方设备 116b, SE 204b
1504
传播公共记录
成功
发送方 102a
发送方设备 116a, SE 204a,
设备公钥 106a
1320
验证公共记录

图16

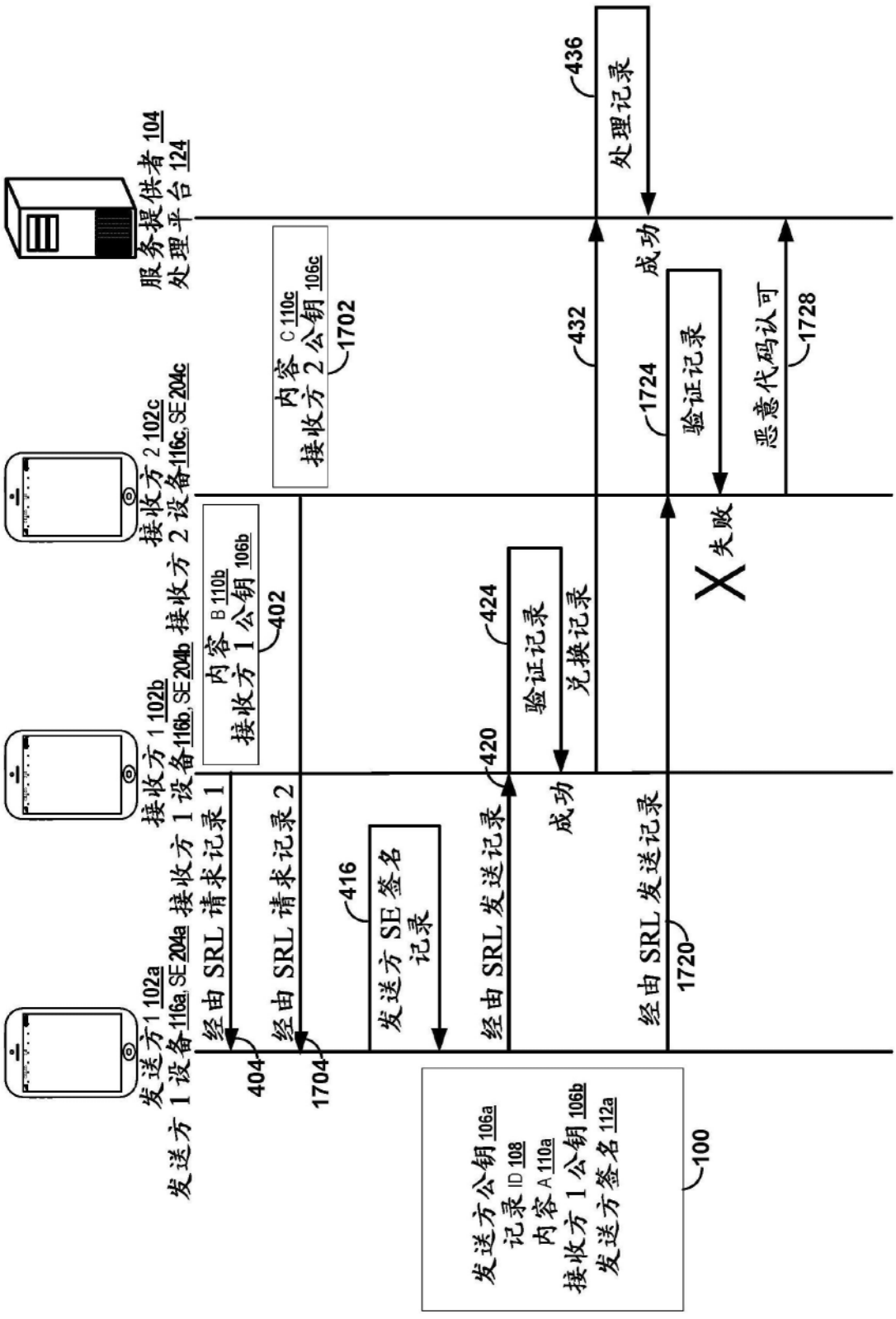

发送方1 102a
发送方 1 设备116a, SE204a
接收方 1 102b
接收方 1 设备116b, SE204b
接收方 2 102c
接收方 2 设备116c, SE204c
服务提供者 104
处理平台 124
经由 SRL 请求记录 1
404
经由 SRL 请求记录 2
1704
发送方 SE 签名记录
416
内容 B 110b 接收方 1 公钥 106b
402
内容 C 110c 接收方 2 公钥 106c
1702
经由 SRL 发送记录
420
验证记录
兑换记录
424
成功
经由 SRL 发送记录
1720
处理记录
436
成功
432
验证记录
1724
失败
恶意代码认可
1728
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方 1 公钥 106b
发送方签名 112a
100

图17

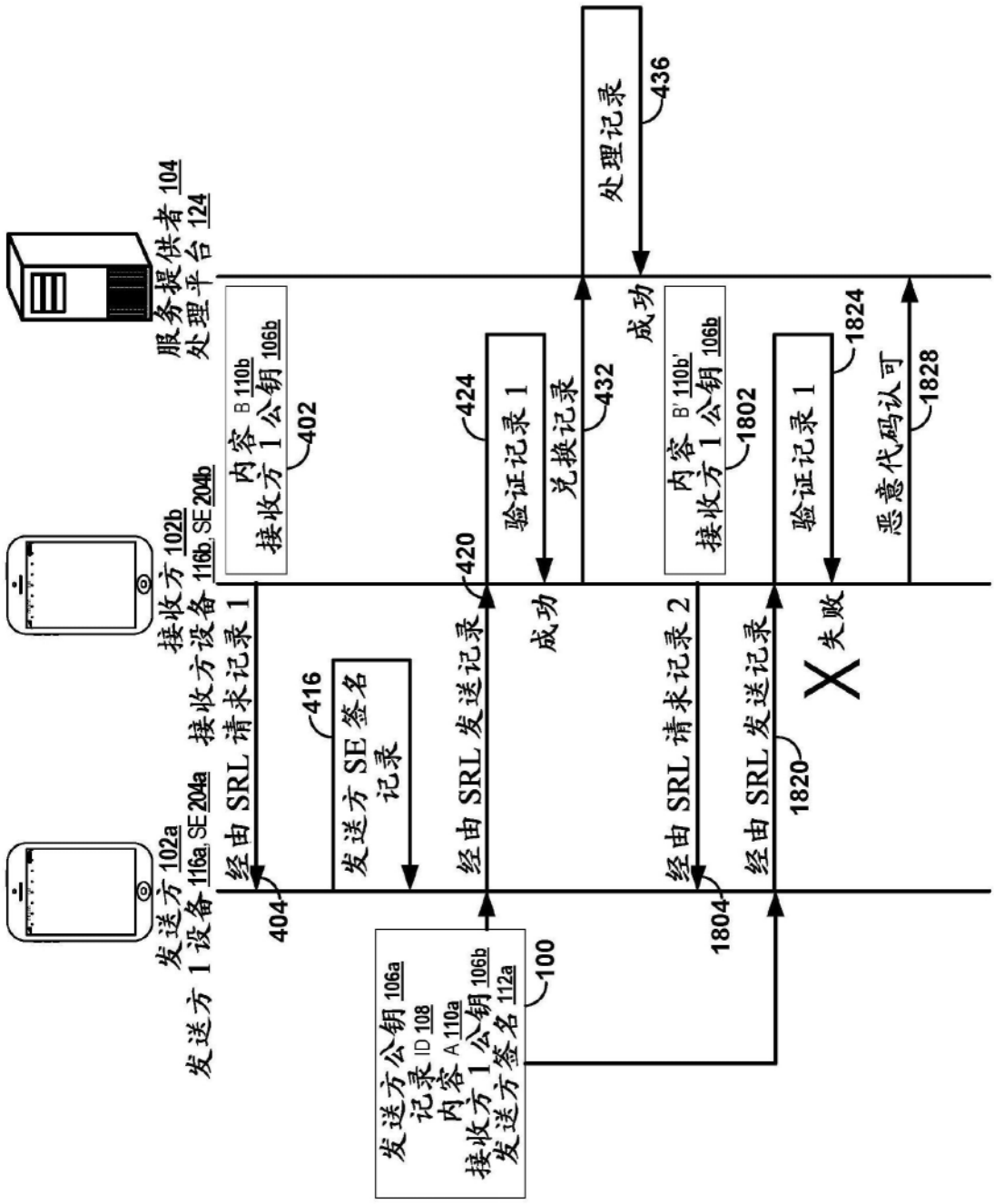

服务提供者 104
处理平台 124
处理记录
436
接收方 102b
接收方设备 116b, SE 204b
内容 B 110b
接收方 1 公钥 106b
402
验证记录 1
424
兑换记录
432
成功
内容 B' 110b'
接收方 1 公钥 106b
1802
验证记录 1
1824
恶意代码认可
1828
发送方 102a
发送方 1 设备 116a, SE 204a
接收方 SRL 请求记录 1
404
发送方 SE 签名记录
416
经由 SRL 发送记录
420
成功
经由 SRL 请求记录 2
1804
经由 SRL 发送记录
1820
失败
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方 1 公钥 106b
发送方签名 112a
100

图18

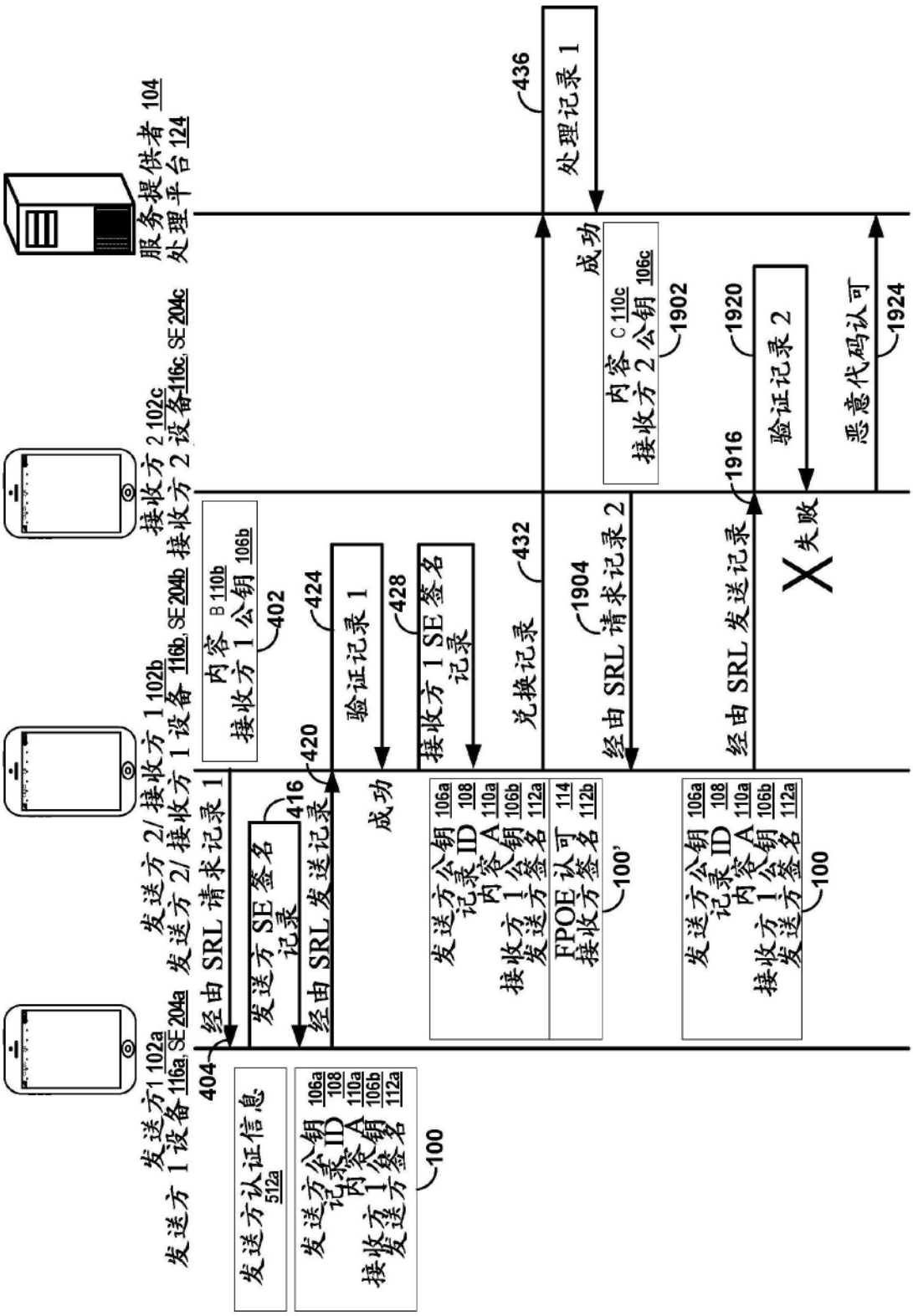

发送方1 102a
发送方 1 设备 116a, SE 204a
发送方认证信息 512a
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方 1 公钥 106b
发送方签名 112a
100
404
经由 SRL 请求记录 1
发送方 2/ 接收方 1 102b
发送方 2/ 接收方 1 设备 116b, SE 204b
发送方 SE 签名记录 416
经由 SRL 发送记录 420
接收方 2 102c
接收方 2 设备 116c, SE 204c
内容 B 110b
接收方 1 公钥 106b
402
成功
验证记录 1 424
接收方 1 SE 签名记录 428
兑换记录 432
经由 SRL 请求记录 2 1904
FPOE 认可 114
接收方签名 112b
100'
服务提供者 104
处理平台 124
处理记录 1 436
成功
内容 C 110c
接收方 2 公钥 106c
1902
1916
经由 SRL 发送记录
失败
1920
验证记录 2
恶意代码认可 1924

图19

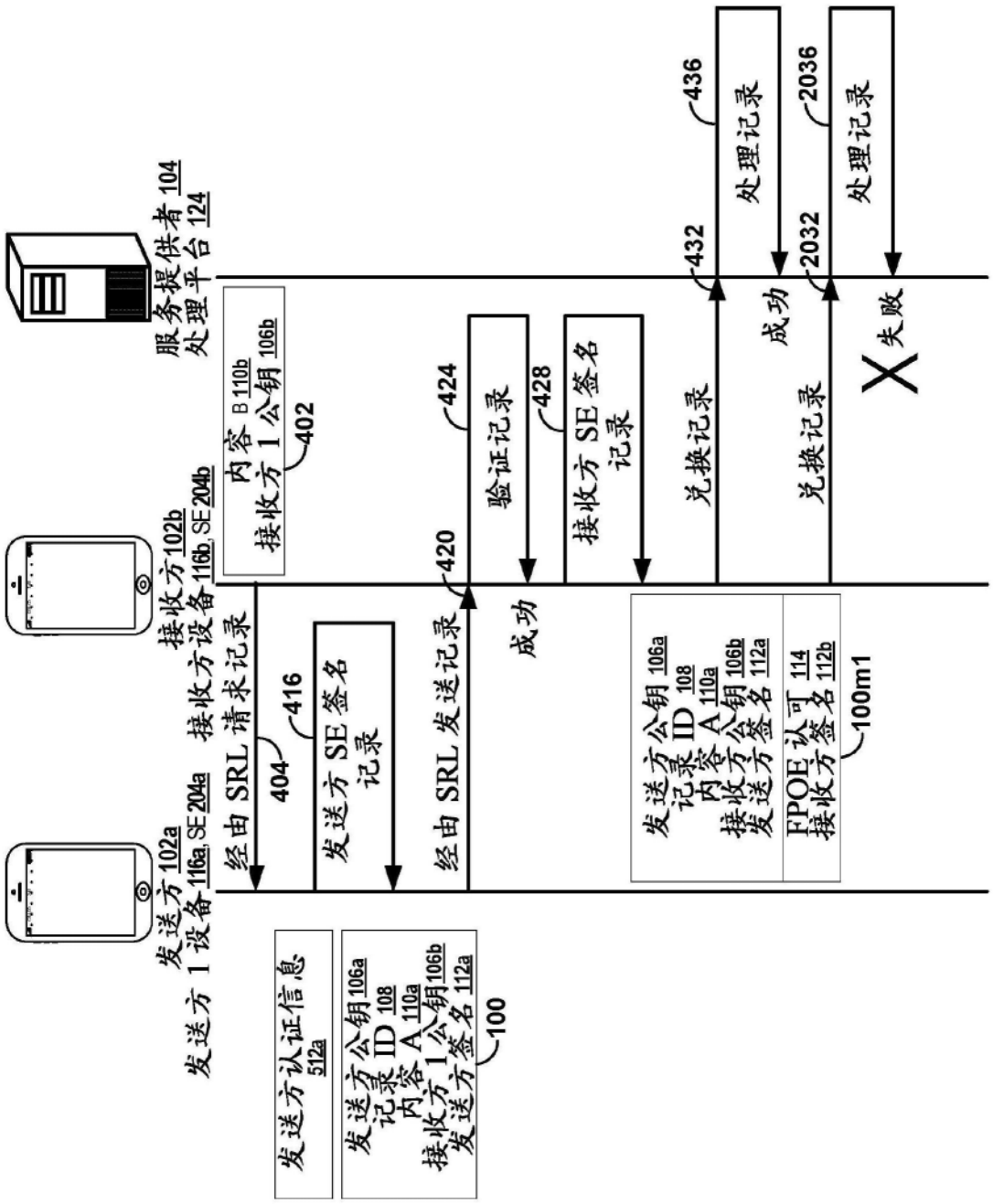

发送方 1 设备 116a, SE 204a
接收方 102b
接收方设备 116b, SE 204b
服务提供者 104
处理平台 124
经由 SRL 请求记录
404
416
发送方 SE 签名记录
经由 SRL 发送记录
420
424
验证记录
428
接收方 SE 签名记录
成功
内容 B 110b
接收方 1 公钥 106b
402
432
兑换记录
436
处理记录
成功
2032
兑换记录
2036
处理记录
失败
发送方认证信息 512a
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方 1 公钥 106b
发送方签名 112a
100
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方公钥 106b
发送方签名 112a
FPOE 认可 114
接收方签名 112b
100m1

图20

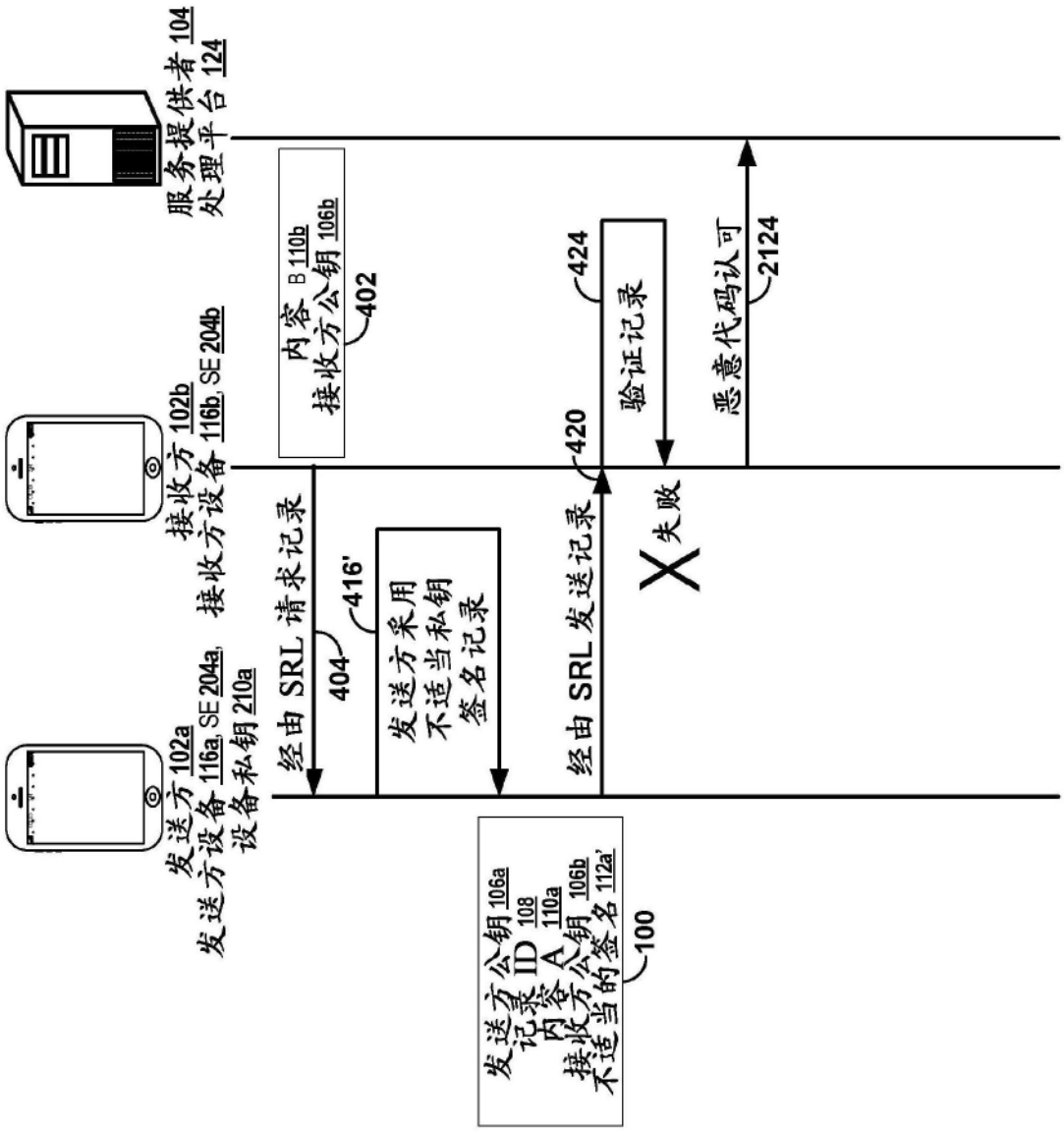

服务提供者 104
处理平台 124
接收方 102b
接收方设备 116b, SE 204b
发送方 102a
发送方设备 116a, SE 204a,
设备私钥 210a
内容 B 110b
接收方公钥 106b
402
经由 SRL 请求记录
404
416'
发送方采用
不适当私钥
签名记录
420
424
验证记录
失败
恶意代码认可
2124
经由 SRL 发送记录
发送方公钥 106a
记录 ID 108
内容 A 110a
接收方公钥 106b
不适当的签名 112a'
100

图21

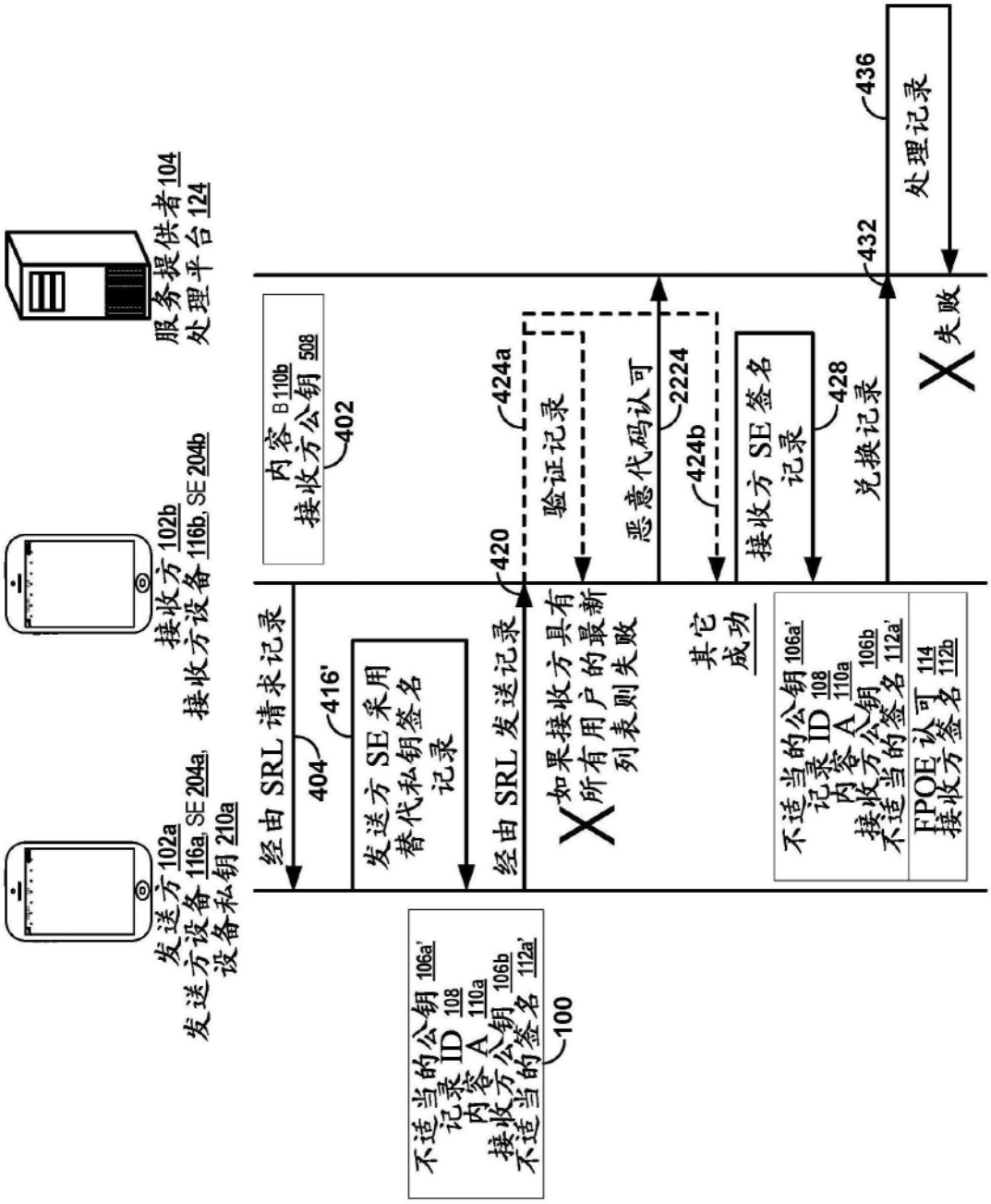

发送方 102a
发送方设备 116a, SE 204a,
设备私钥 210a
接收方 102b
接收方设备 116b, SE 204b
服务提供者 104
处理平台 124
内容 B 110b
接收方公钥 508
402
经由 SRL 请求记录
404
416'
发送方 SE 采用
替代私钥签名
记录
420
424a
验证记录
恶意代码认可
2224
424b
接收方 SE 签名
记录
428
兑换记录
432
处理记录
436
失败
经由 SRL 发送记录
如果接收方具有
所有用户的最新
列表则失败
其它
成功
不适当的公钥 106a'
记录 ID 108
内容 A 公钥 110a
接收方公钥 106b
不适当的签名 112a'
100
FPOE 认可 114
接收方签名 112b

图22

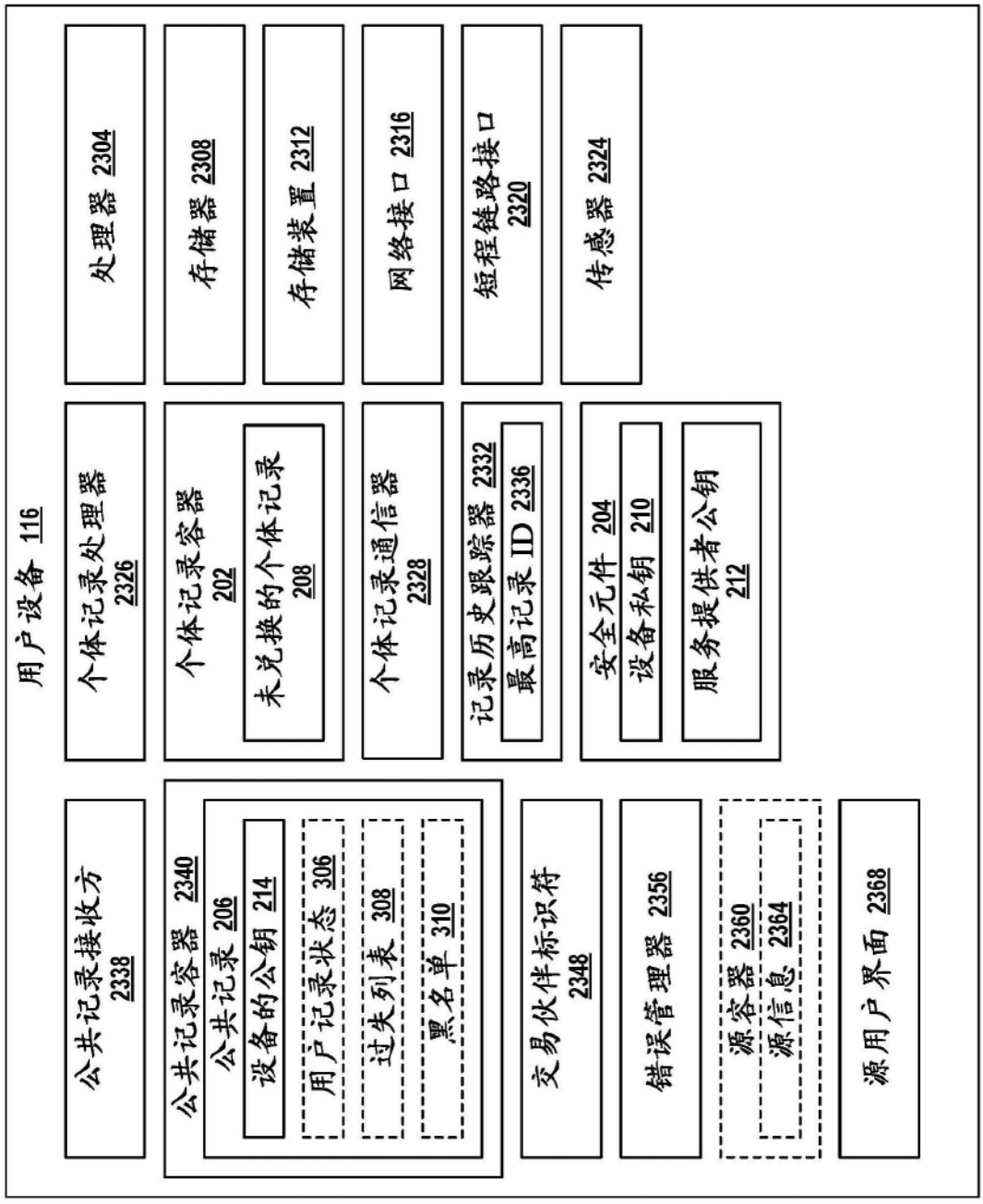

用户设备 116
处理器 2304
存储器 2308
存储装置 2312
网络接口 2316
短程链路接口 2320
传感器 2324
个体记录处理器 2326
个体记录容器 202
未兑换的个体记录 208
个体记录通信器 2328
记录历史跟踪器 2332
最高记录 ID 2336
安全元件 204
设备私钥 210
服务提供者公钥 212
公共记录接收方 2338
公共记录容器 2340
公共记录 206
设备的公钥 214
用户记录状态 306
过失列表 308
黑名单 310
交易伙伴标识符 2348
错误管理器 2356
源容器 2360
源信息 2364
源用户界面 2368

图23

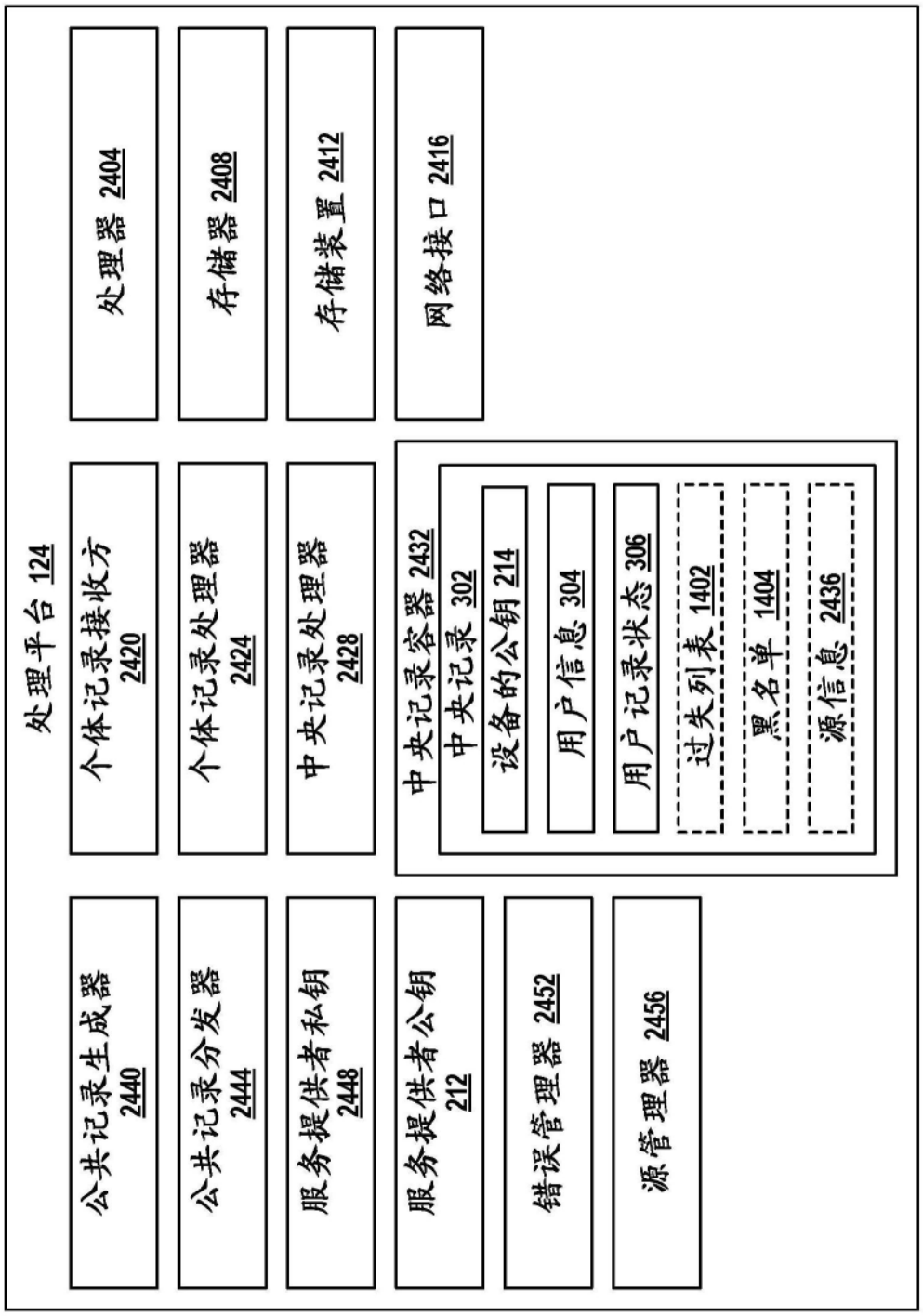

处理平台 124
处理器 2404
存储器 2408
存储装置 2412
网络接口 2416
个体记录接收方 2420
个体记录处理器 2424
中央记录处理器 2428
中央记录容器 2432
中央记录 302
设备的公钥 214
用户信息 304
用户记录状态 306
过失列表 1402
黑名单 1404
源信息 2436
公共记录生成器 2440
公共记录分发器 2444
服务提供者私钥 2448
服务提供者公钥 212
错误管理器 2452
源管理器 2456

图24

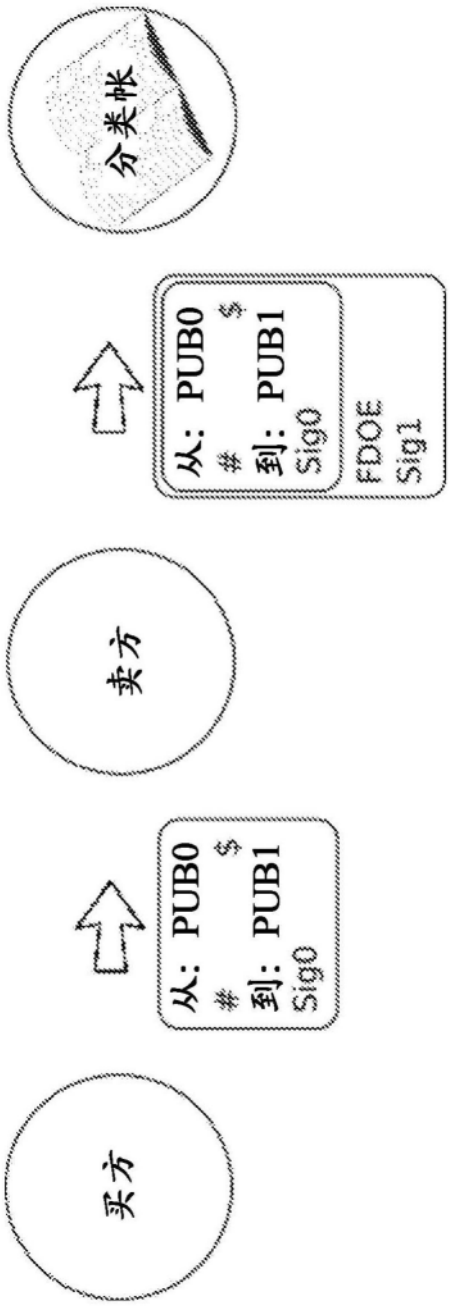


图25

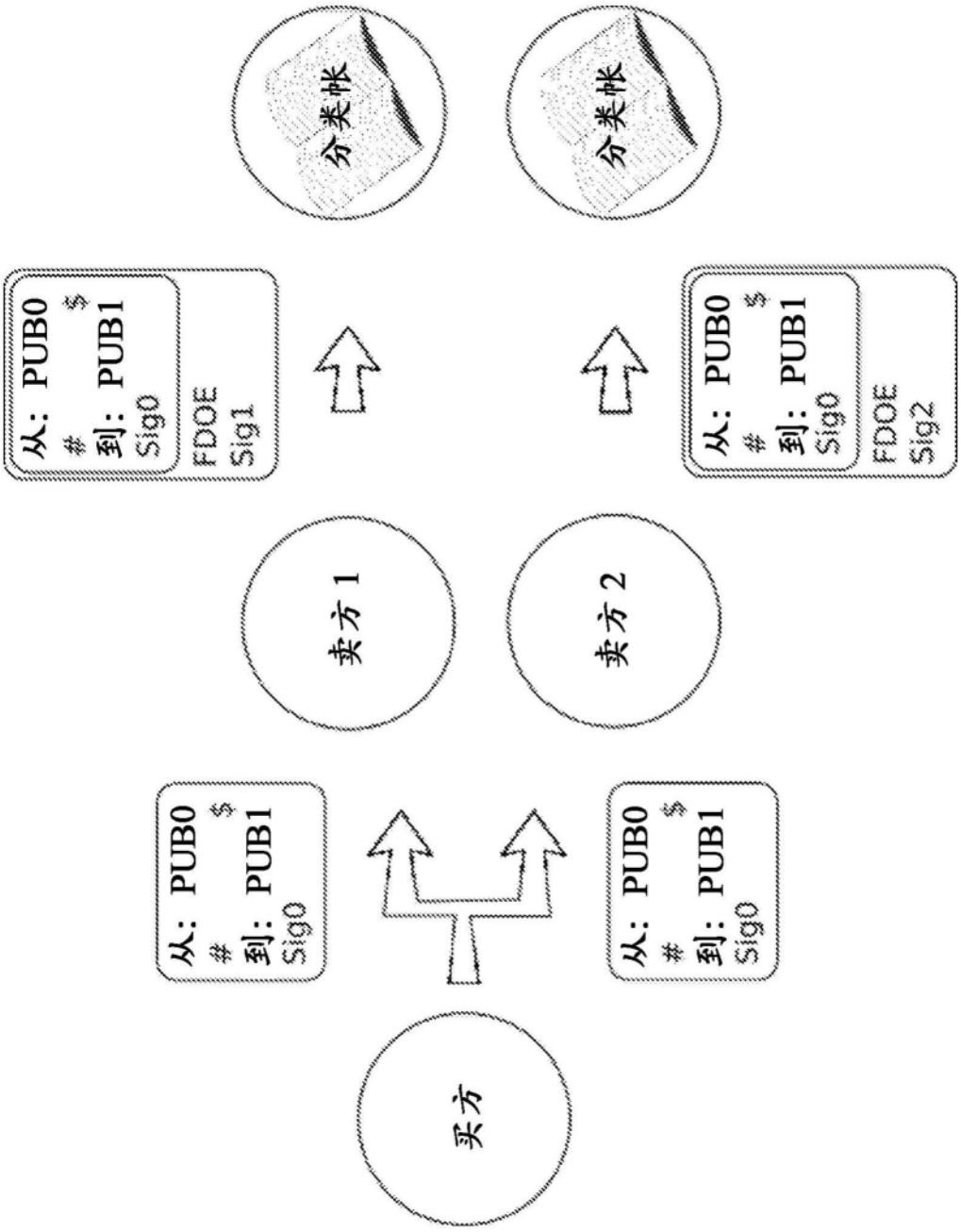

分类帐
分类帐
从: PUB0
$
#
到: PUB1
Sig0
FDOE
Sig1
从: PUB0
$
#
到: PUB1
Sig0
FDOE
Sig2
卖方 1
卖方 2
从: PUB0
$
#
到: PUB1
Sig0
从: PUB0
$
#
到: PUB1
Sig0
买方

图26

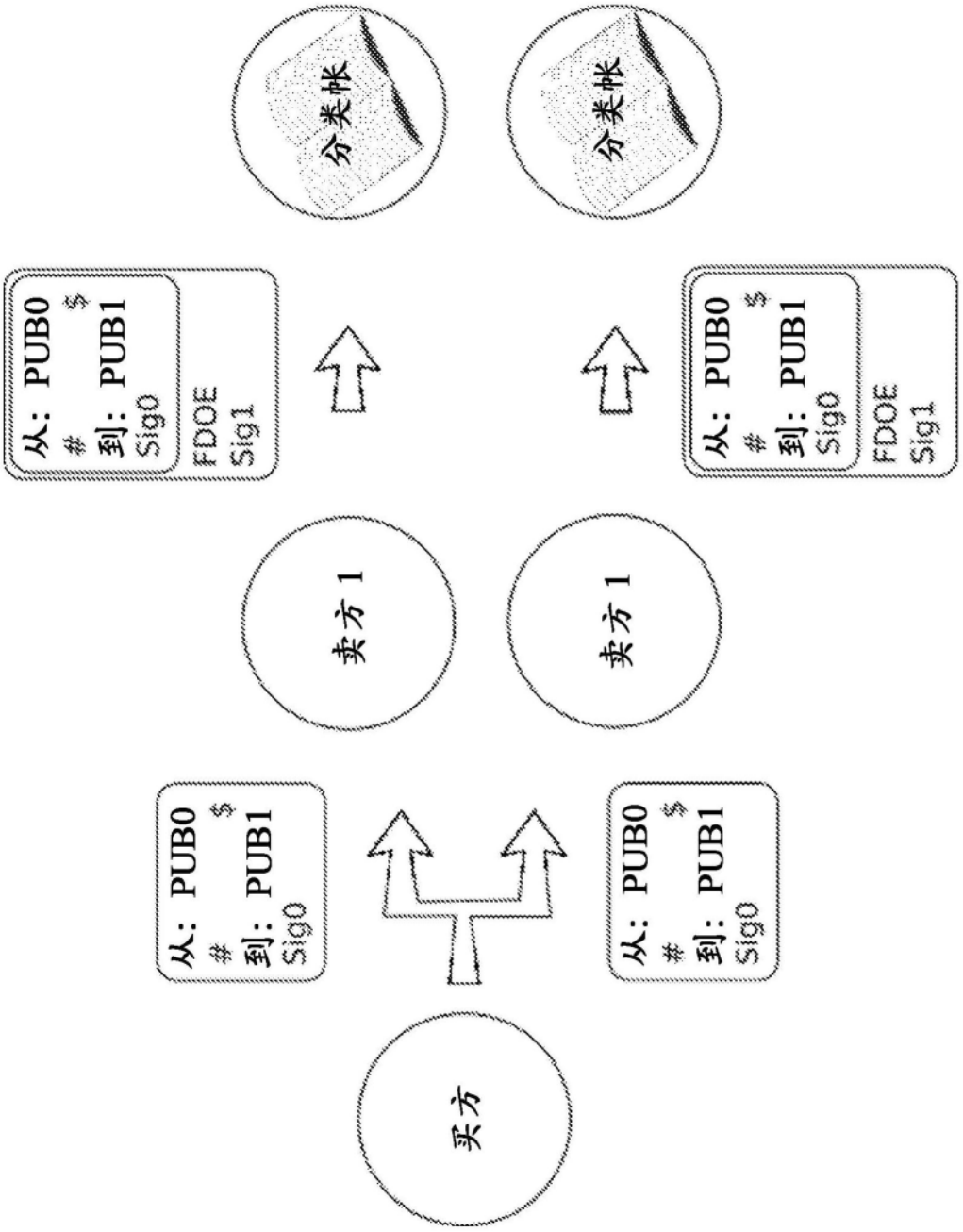

分类帐
分类帐
从: PUB0
#
到: PUB1
Sig0
FDOE
Sig1
从: PUB0
#
到: PUB1
Sig0
FDOE
Sig1
卖方 1
卖方 1
从: PUB0
#
到: PUB1
Sig0
从: PUB0
#
到: PUB1
Sig0
买方

图27

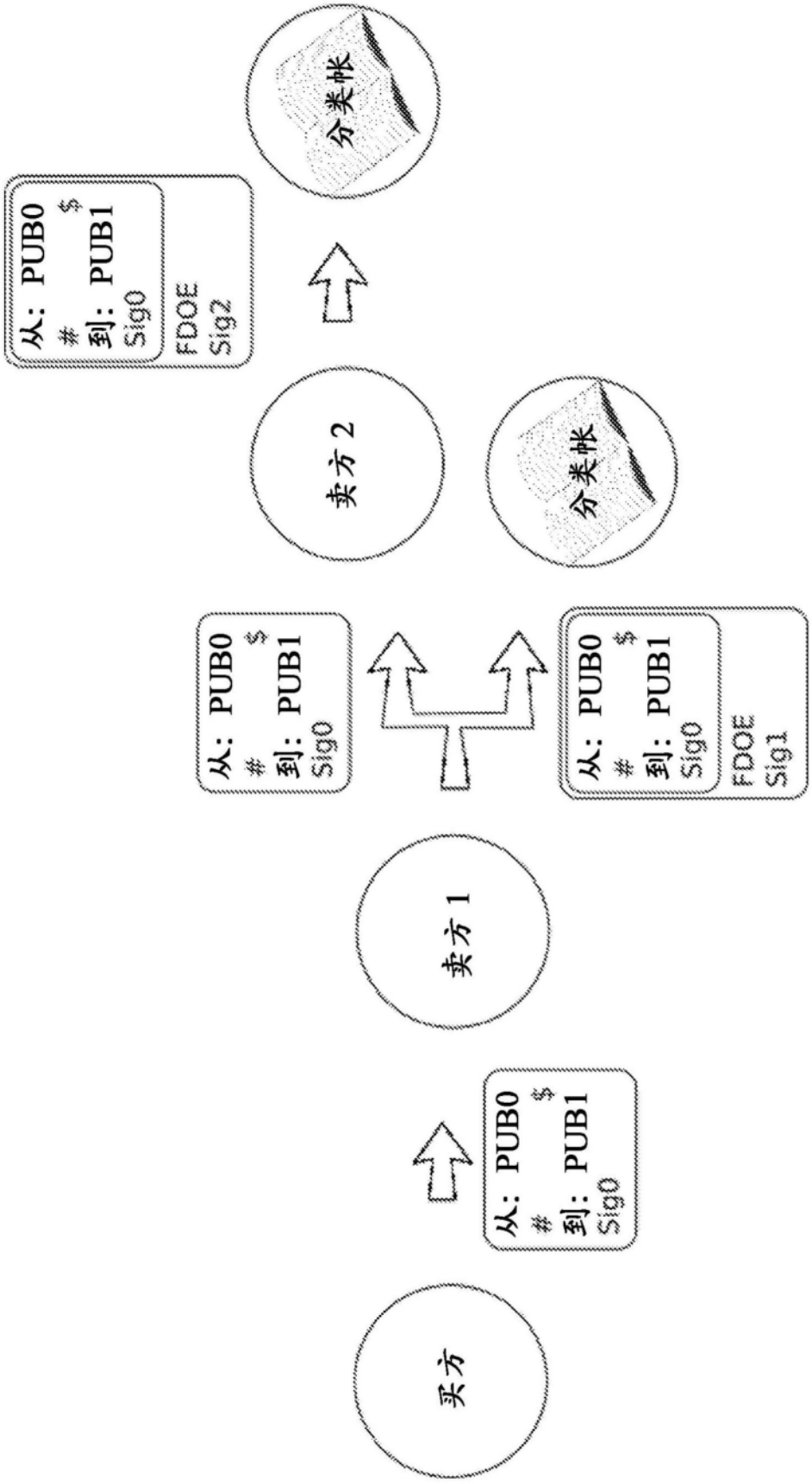

买方
从: PUB0
$
到: PUB1
Sig0
卖方 1
从: PUB0
$
到: PUB1
Sig0
从: PUB0
$
到: PUB1
Sig0
FDOE
Sig1
分类帐
卖方 2
从: PUB0
$
到: PUB1
Sig0
FDOE
Sig2
分类帐

图28

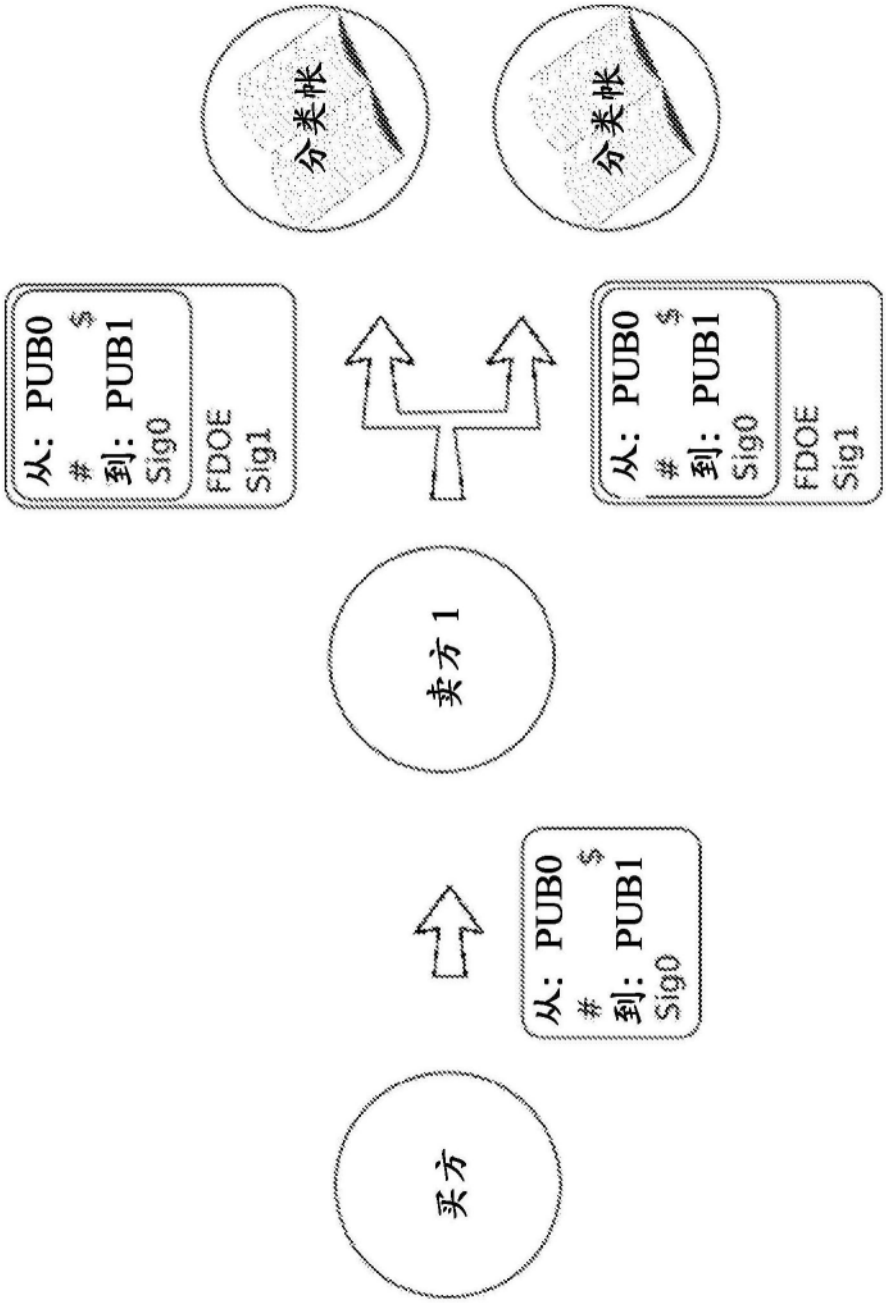

分类帐
分类帐
从: PUB0
$
#
到: PUB1
Sig0
FDOE
Sig1
从: PUB0
$
#
到: PUB1
Sig0
FDOE
Sig1
卖方 1
从: PUB0
$
#
到: PUB1
Sig0
买方

图29

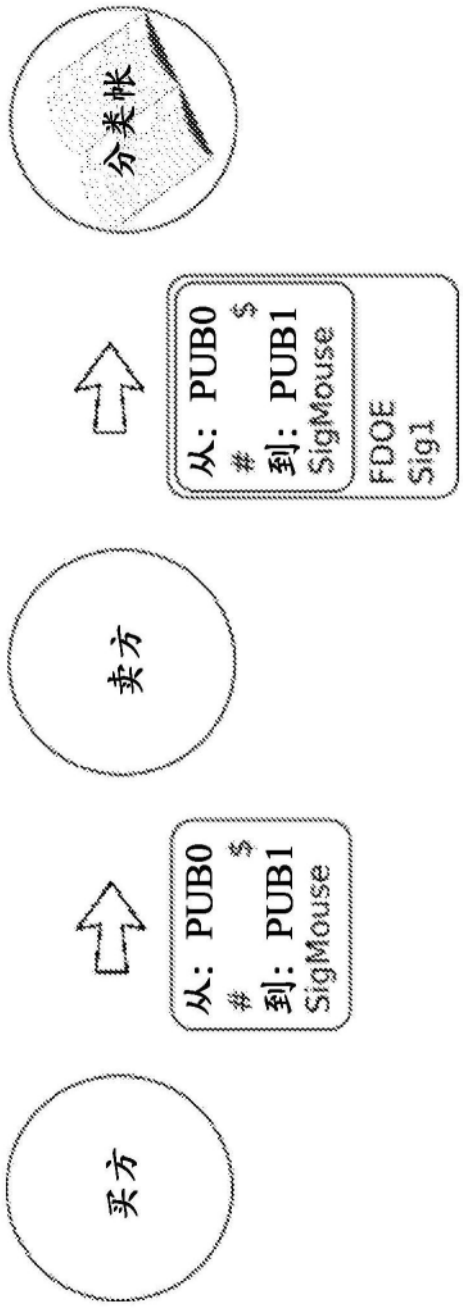

分类帐
从: PUB0 $
到: PUB1
SigMouse
FDOE
Sig1
卖方
从: PUB0 $
到: PUB1
SigMouse
买方

图30

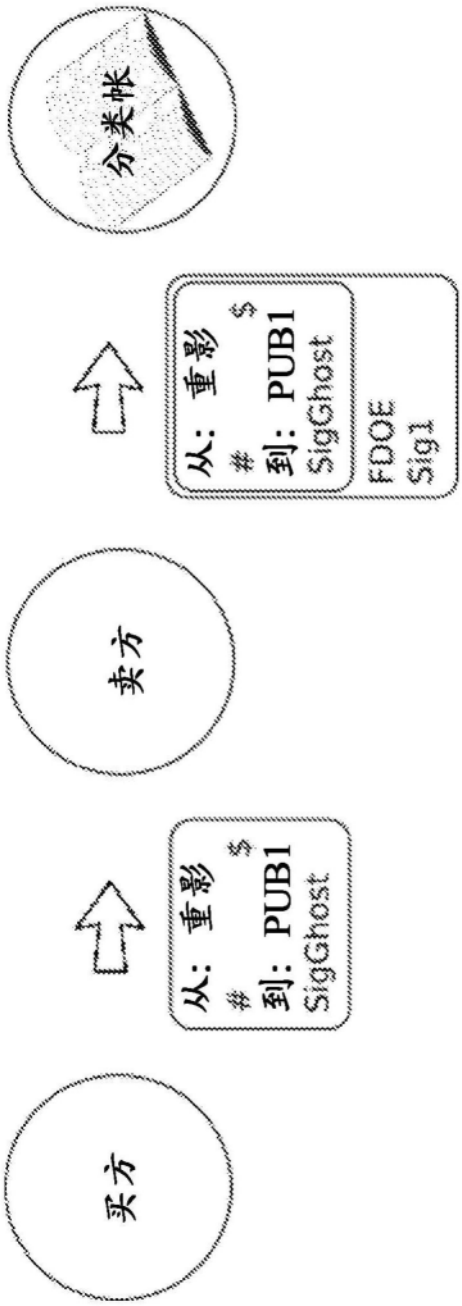


图31

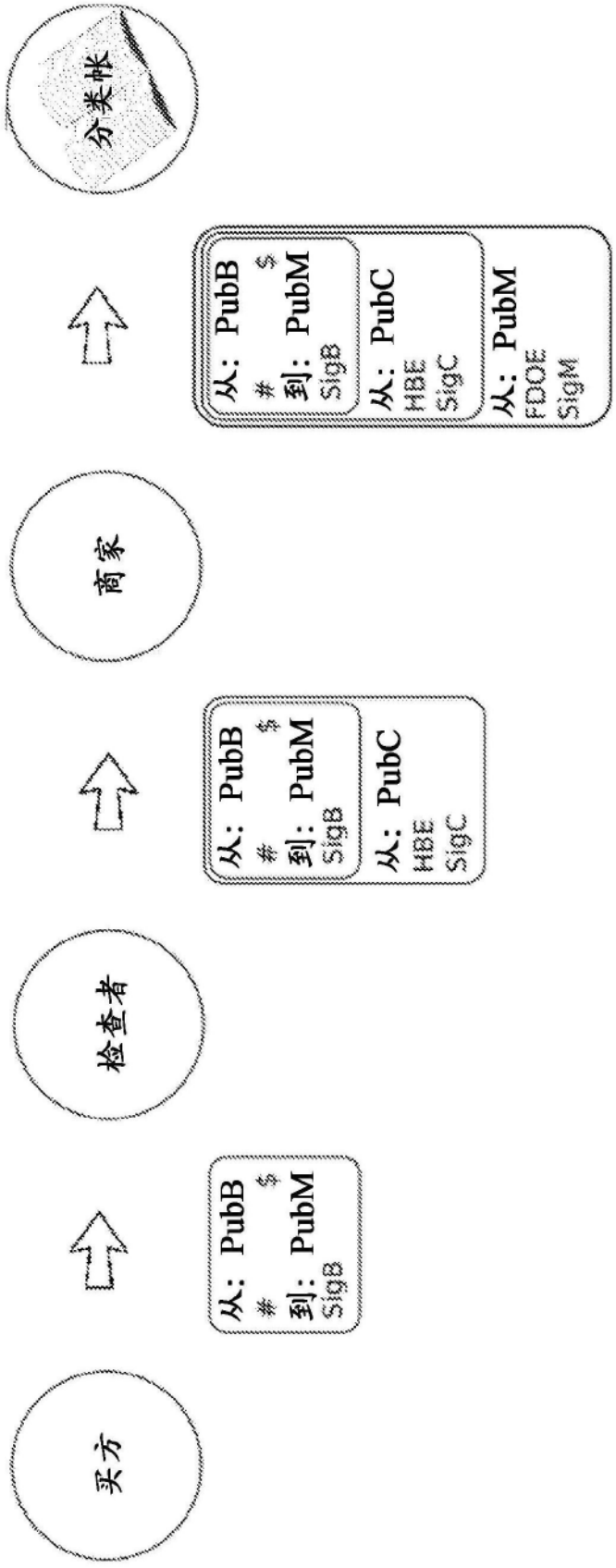


图32

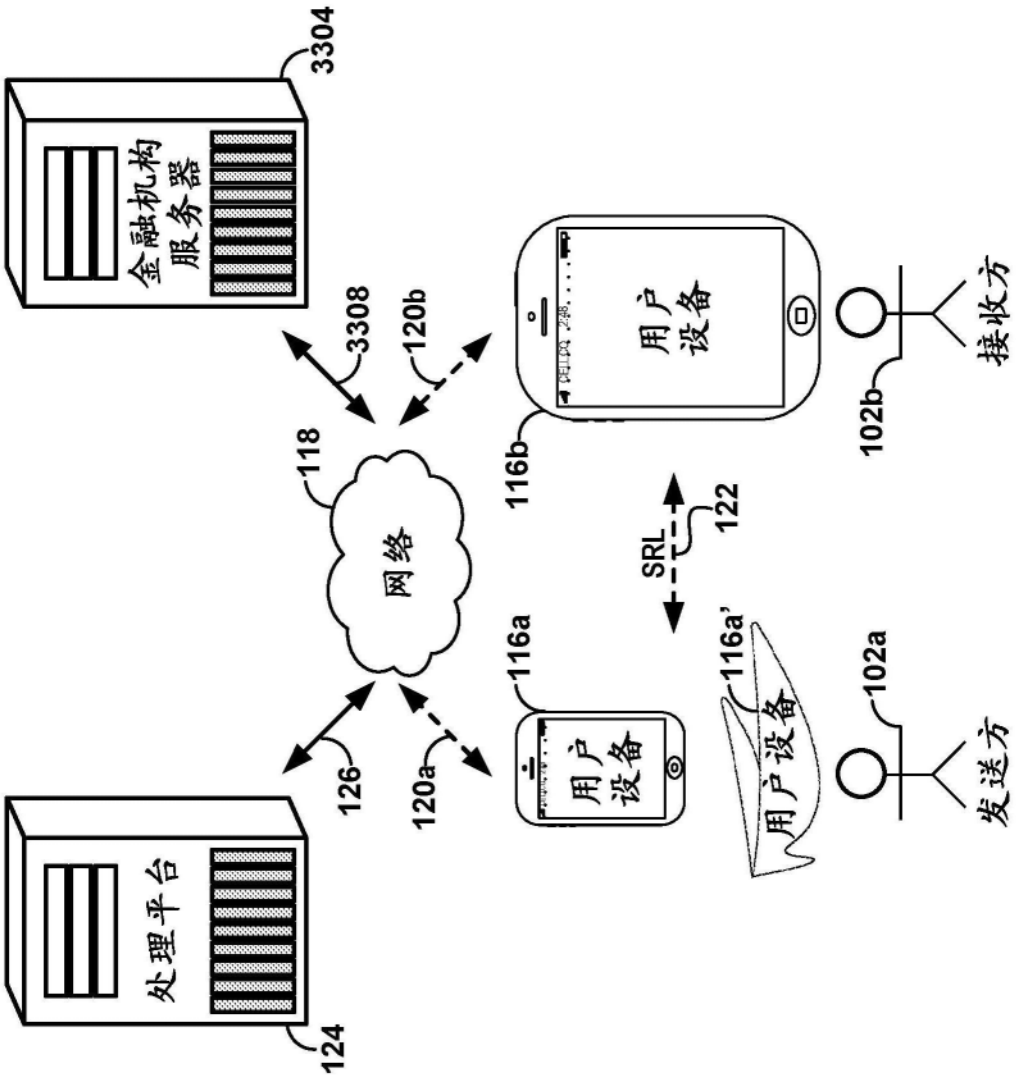

3304
金融机构服务器
3308
120b
118
网络
116b
用户设备
102b
接收方
SRL
122
126
120a
116a
用户设备
116a'
用户设备
102a
发送方
处理平台
124

图33A

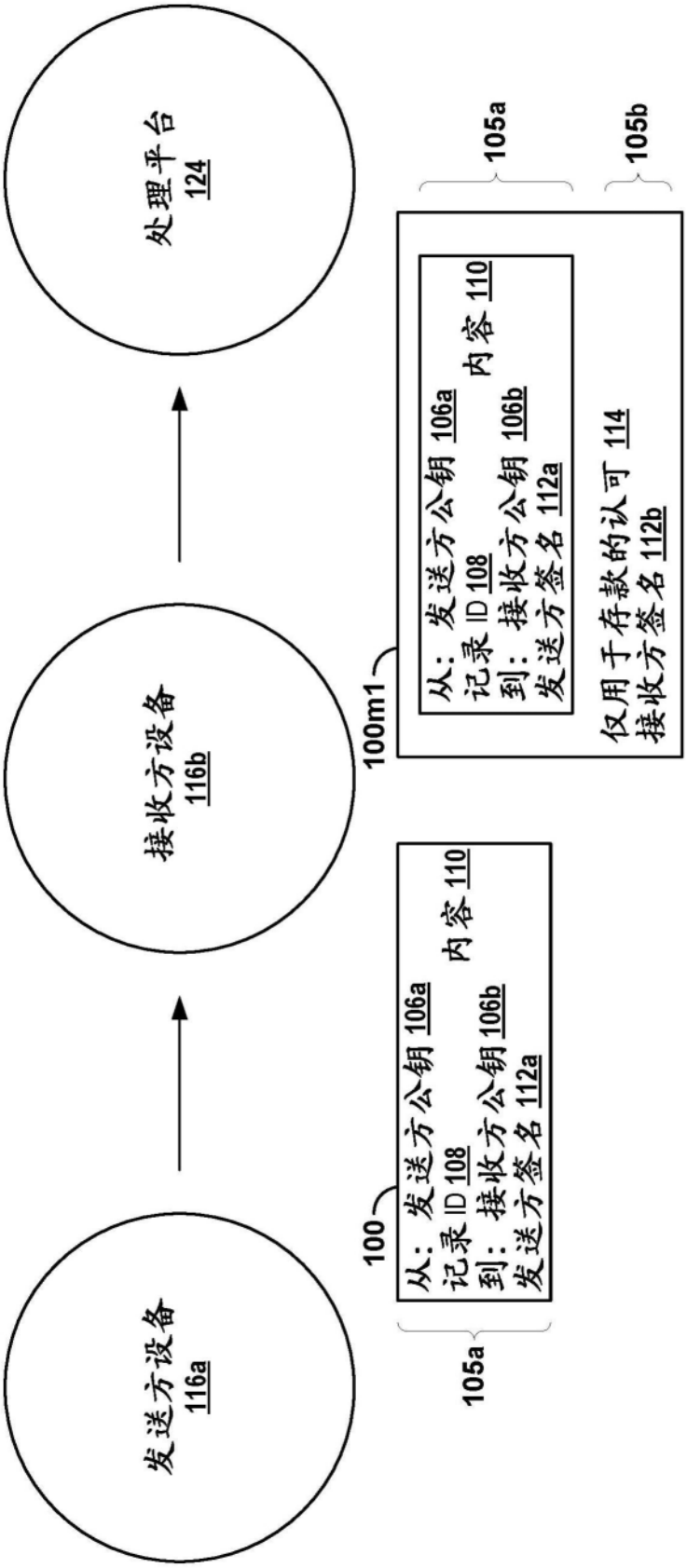

发送方设备
116a
接收方设备
116b
处理平台
124
100
从：发送方公钥 106a
记录 ID 108
到：接收方公钥 106b
发送方签名 112a
内容 110
105a
100m1
从：发送方公钥 106a
记录 ID 108
到：接收方公钥 106b
发送方签名 112a
内容 110
仅用于存款的认可 114
接收方签名 112b
105a
105b

图33B

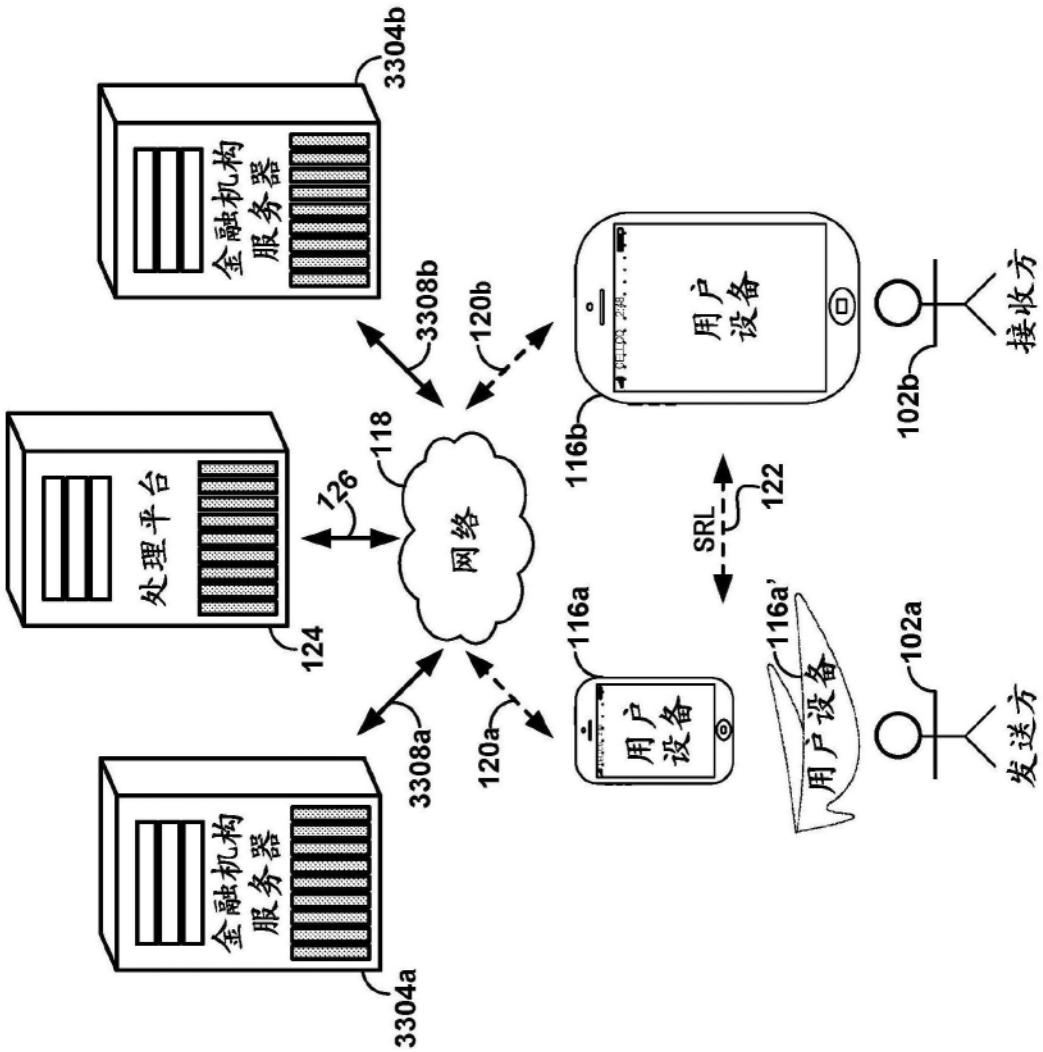

金融机构服务器
3304b
处理平台
124
网络
118
126
3308b
120b
3308a
120a
116b
用户设备
SRL
122
116a
116a'
用户设备
用户设备
102b
接收方
102a
发送方
金融机构服务器
3304a

图33C

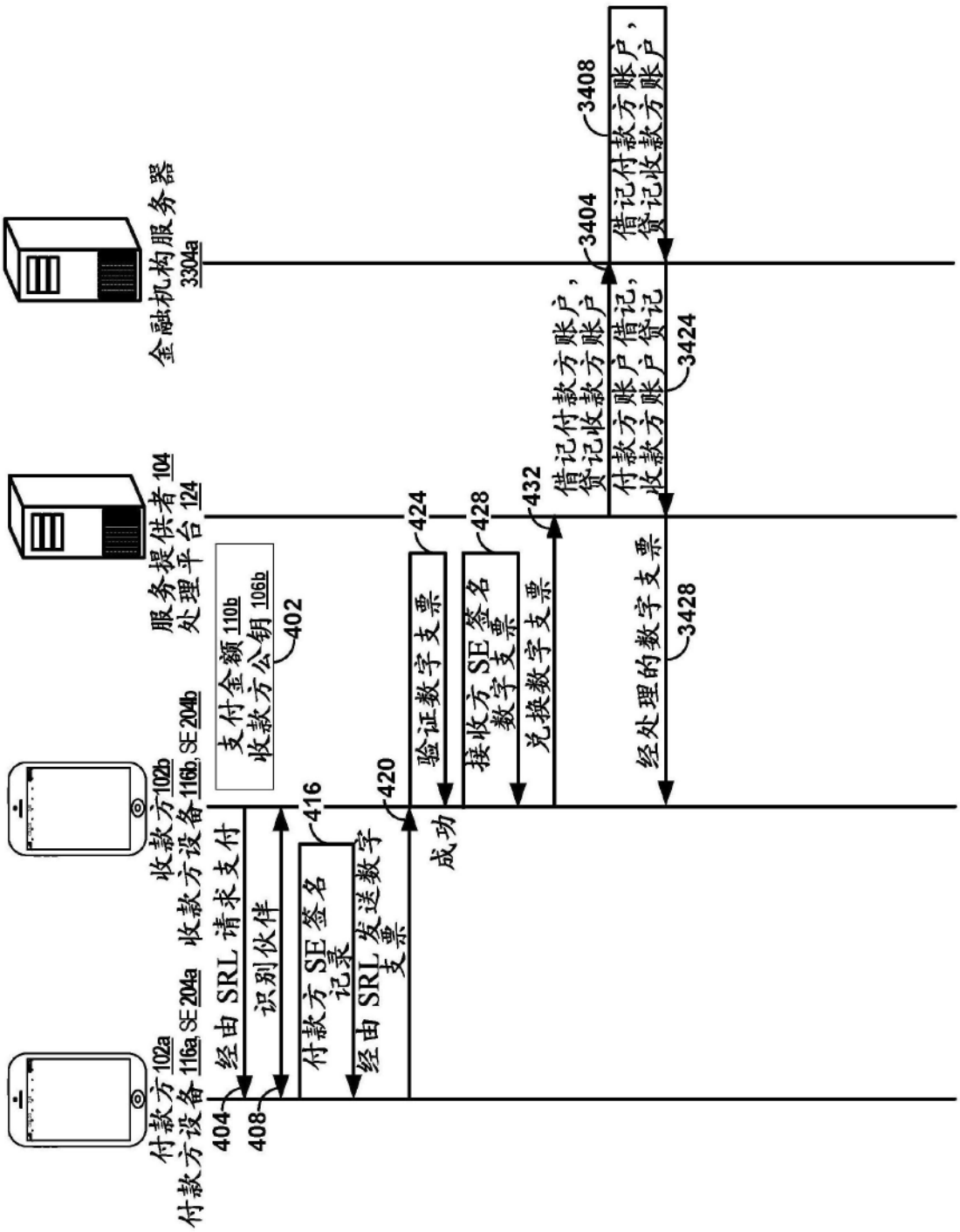

付款方 102a
付款方设备 116a, SE 204a
收款方 102b
收款方设备 116b, SE 204b
服务提供者 104
处理平台 124
金融机构服务器 330a
404
经由 SRL 请求支付
408
识别伙伴
402
支付金额 110b
收款方公钥 106b
416
付款方 SE 签名记录
420
经由 SRL 发送数字支票
424
验证数字支票
成功
428
接收方 SE 签名数字支票
432
兑换数字支票
3404
借记付款方账户，贷记收款方账户
3408
借记付款方账户，贷记收款方账户
3424
付款方账户借记，收款方账户贷记
3428
经处理的数字支票

图34A

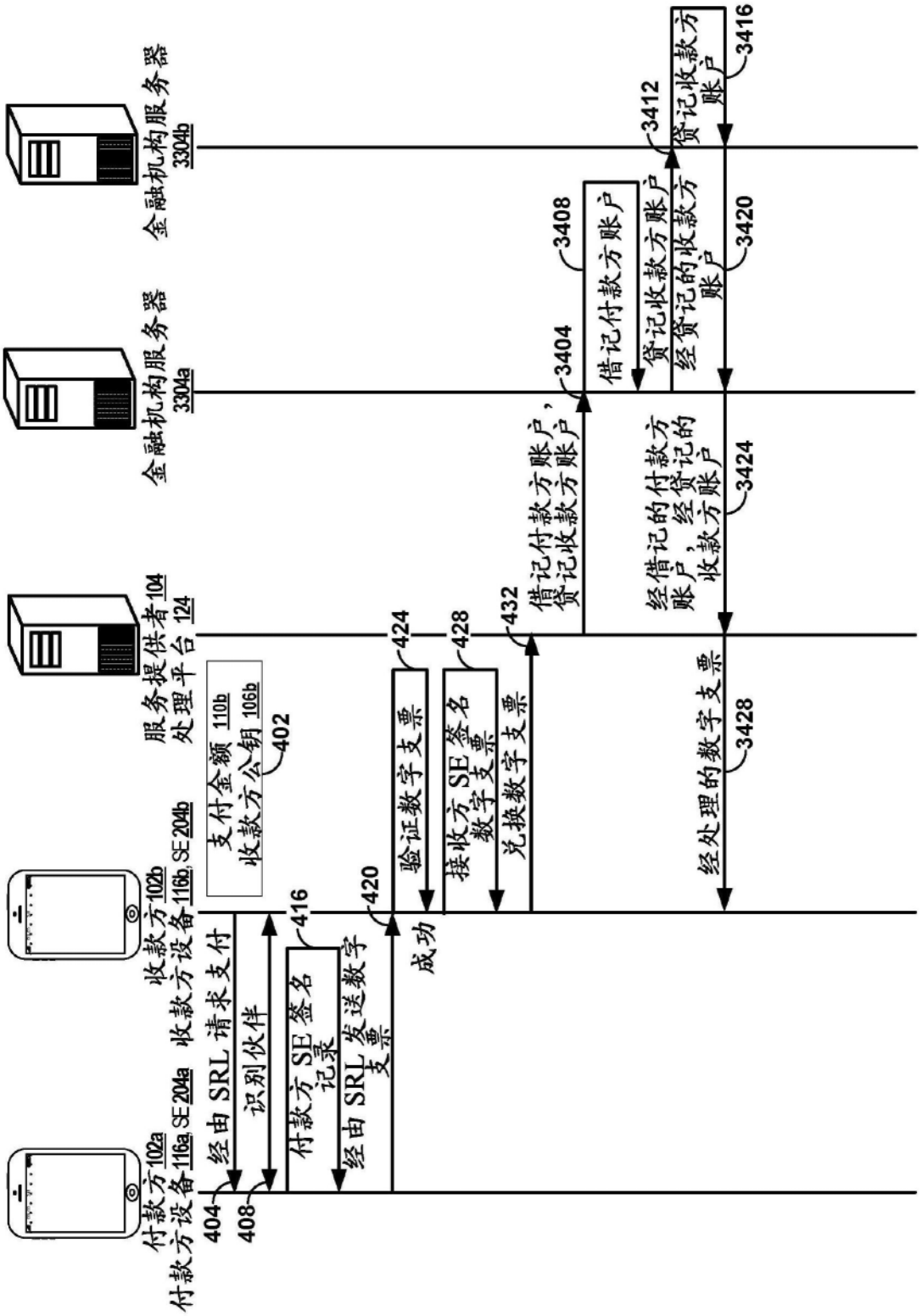

付款方设备 102a
付款方 116a
SE 204a
收款方设备 102b
收款方 116b
SE 204b
服务提供者处理平台 104 124
金融机构服务器 3304a
金融机构服务器 3304b
404
经由 SRL 请求支付
识别伙伴
408
402
支付金额 110b
收款方公钥 106b
416
付款方 SE 签名记录
经由 SRL 发送数字支票
420
成功
424
验证数字支票
428
接收方 SE 签名数字支票
兑换数字支票
432
借记付款方账户，贷记收款方账户
3404
借记付款方账户
3408
贷记收款方账户
3412
贷记收款方账户
3416
经贷记的收款方账户
3420
经借记的付款方账户，经贷记的收款方账户
3424
经处理的数字支票
3428

图34B

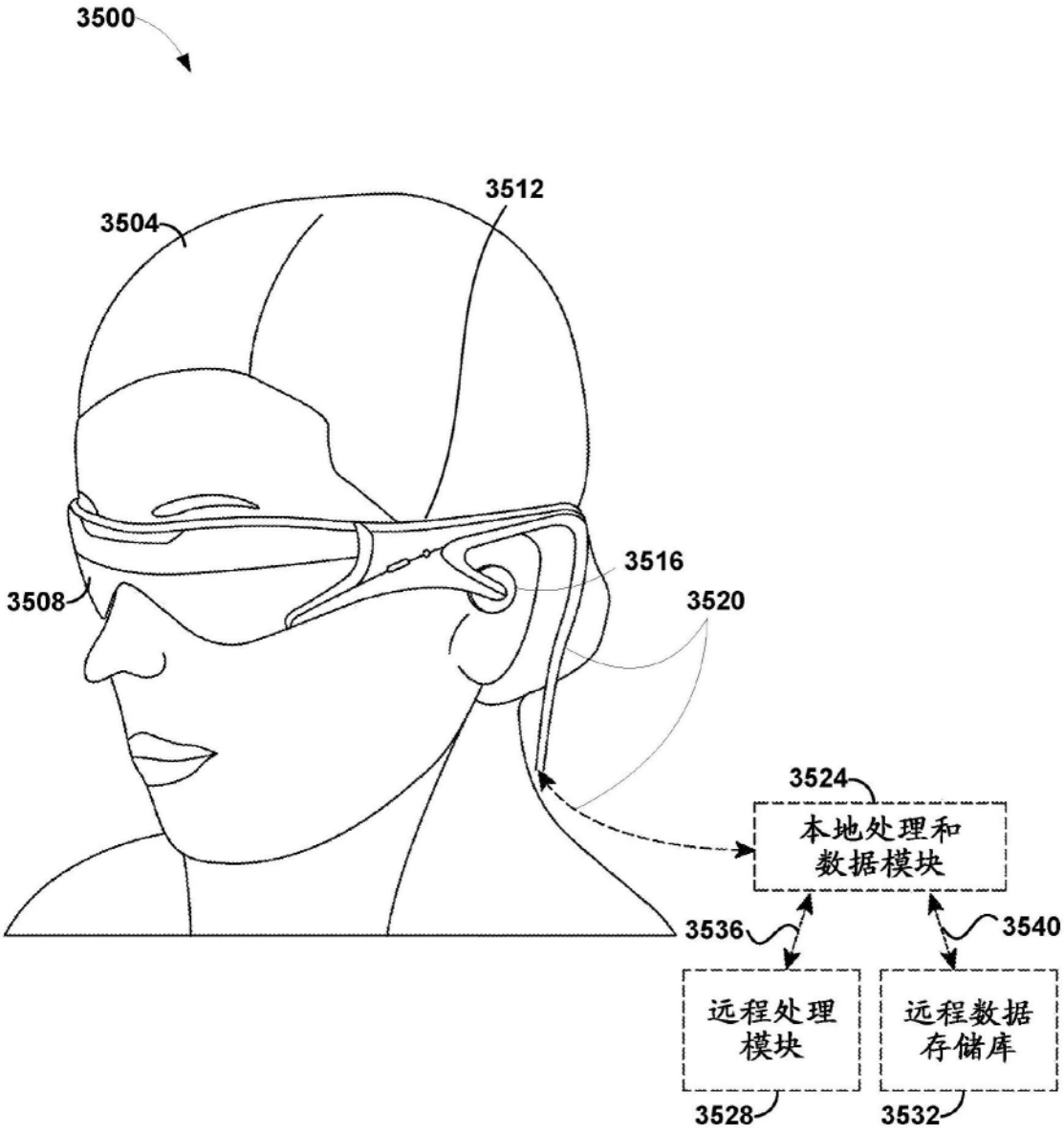

3500
3512
3504
3516
3508
3520
3524
本地处理和
数据模块
3536
3540
远程处理
模块
远程数据
存储库
3528
3532

图35