



(12) 发明专利申请

(10) 申请公布号 CN 114556865 A

(43) 申请公布日 2022. 05. 27

(21) 申请号 202080070661.5

(22) 申请日 2020.09.28

(30) 优先权数据

10-2019-0124090 2019.10.07 KR

(85) PCT国际申请进入国家阶段日

2022.04.07

(86) PCT国际申请的申请数据

PCT/KR2020/013213 2020.09.28

(87) PCT国际申请的公布数据

W02021/071157 EN 2021.04.15

(71) 申请人 三星电子株式会社

地址 韩国京畿道

(72) 发明人 李圣嫻 金秀娟 金周泳 郑载勋

丁填杞

(74) 专利代理机构 北京市立方律师事务所

11330

专利代理师 谢玉斌

(51) Int.Cl.

H04L 9/32 (2006.01)

H04L 9/08 (2006.01)

H04L 9/06 (2006.01)

H04L 9/40 (2022.01)

G06F 21/64 (2013.01)

G06F 21/62 (2013.01)

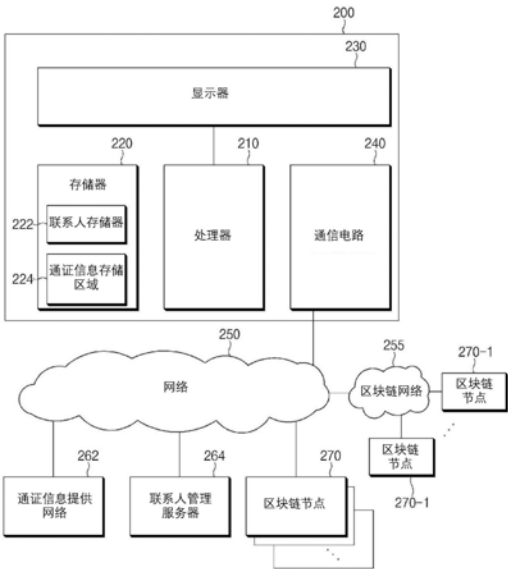
权利要求书2页 说明书29页 附图22页

(54) 发明名称

电子装置和使用该电子装置管理区块链地址的方法

(57) 摘要

提供了一种电子装置,所述电子装置使用私钥对区块链地址和与所述区块链地址相关联的第一信息执行数字签名,将作为执行所述数字签名的结果而获得的签名数据与所述区块链地址或所述第一信息中的至少一者相关联并存储,基于所存储的签名数据,使用与所述私钥相对应的公钥来执行对所述区块链地址和所述第一信息的认证,以及基于执行所述认证的结果,显示所述区块链地址和所述第一信息。



1. 一种电子装置,所述电子装置包括:
显示器;以及
至少一个处理器,所述至少一个处理器与所述显示器连接,
其中,所述至少一个处理器被配置为:
使用私钥对区块链地址和与所述区块链地址相关联的第一信息执行数字签名,
将作为执行所述数字签名的结果而获得的签名数据与所述区块链地址或所述第一信息中的至少一者相关联并存储,
基于所存储的签名数据,使用与所述私钥相对应的公钥来执行对所述区块链地址和所述第一信息的认证,以及
基于执行所述认证的结果,控制所述显示器显示所述区块链地址和所述第一信息。
2. 根据权利要求1所述的电子装置,其中,所述至少一个处理器还被配置为:
当所述认证失败时,在所述显示器上输出与所述失败相对应的信息。
3. 根据权利要求1所述的电子装置,其中,所述至少一个处理器还被配置为:
当所述认证成功时,控制所述显示器显示第二信息,该第二信息表示与所述区块链地址和所述第一信息之间的相关性相关联的可靠性。
4. 根据权利要求3所述的电子装置,其中,所述至少一个处理器还被配置为:
基于以下至少一个来确定所述可靠性:所述区块链地址与所述第一信息之间的映射关系是否被认证、所述第一信息所属的类别或关于所述区块链地址的交易历史的信息。
5. 根据权利要求3所述的电子装置,其中,所述至少一个处理器还被配置为:
当认证所述区块链地址的请求被生成时,输出所述区块链地址和所述第一信息;
接收将所述第一信息映射到所述区块链地址的批准命令;以及
响应于所述批准命令,将所述签名数据与所述区块链地址或所述第一信息中的至少一者相关联并存储。
6. 根据权利要求5所述的电子装置,其中,所述至少一个处理器还被配置为:
运行富操作系统和可信操作系统;
响应于所述请求,将所述第一信息和所述区块链地址从所述富操作系统的第一应用递送到所述可信操作系统的第二应用;
通过所述第二应用获得针对所述第一信息和所述区块链地址的所述批准命令;
响应于所述批准命令,通过所述可信操作系统的第三应用,使用所述私钥生成所述第一信息和所述第一区块链地址的签名数据;以及
通过所述第一应用将所述签名数据存储在该电子装置的存储器中。
7. 根据权利要求6所述的电子装置,
其中,所述第一应用包括数字钱包应用,
其中,所述第二应用是可信用户界面应用,并且
其中,所述第三应用是区块链可信应用。
8. 根据权利要求5所述的电子装置,其中,所述私钥被所述电子装置的用户用来执行区块链交易。
9. 根据权利要求5所述的电子装置,其中,所述至少一个处理器还被配置为:
执行对输入了所述批准命令的用户进行验证的用户认证过程。

10. 根据权利要求5所述的电子装置,

其中,所述第一信息包括确认用于通证交易的通证的通证信息,并且

其中,所述至少一个处理器被配置为:

将所述签名数据存储在该所述电子装置的存储器的通证信息存储区域中。

11. 根据权利要求10所述的电子装置,所述电子装置还包括:

通信电路,所述通信电路被配置为与所述电子装置外部的网络进行通信,

其中,所述至少一个处理器还被配置为:

经由所述通信电路从通证信息提供网络获得所述通证信息。

12. 根据权利要求5所述的电子装置,其中,在与所述区块链地址相关联的所述签名数据被存储在所述电子装置的存储器中的第一情况下,在所述显示器上输出的所述第二信息包括第一图像,在存在包括所述区块链地址的交易历史或所述第一信息满足预定条件的第二情况下,在所述显示器上输出的所述第二信息包括第二图像,在除所述第一情况和所述第二情况以外的第三情况下,在所述显示器上输出的所述第二信息包括第三图像。

13. 根据权利要求6所述的电子装置,其中,所述第一应用获得所述第一信息,所述第一信息包括由从所述富操作系统的用户应用获得的所述第一区块链地址表示的区块链交易目标的联系人信息。

14. 一种用于在电子装置中管理区块链地址的方法,所述方法包括:

使用私钥对区块链地址和与所述区块链地址相关联的第一信息执行数字签名;

将作为执行所述数字签名的结果而获得的签名数据与所述区块链地址或所述第一信息中的至少一者相关联并存储;

基于所存储的签名数据,使用与所述私钥相对应的公钥来执行对所述区块链地址和所述第一信息的认证;以及

基于执行所述认证的结果,在所述电子装置的显示器上显示所述区块链地址和所述第一信息。

15. 根据权利要求14所述的方法,

其中,显示所述区块链地址和所述第一信息包括:

生成或接收认证所述区块链地址的请求;以及

响应于所述请求,在所述显示器上输出所述区块链地址和所述第一信息,并且

其中,所述认证的执行包括:

接收将所述第一信息映射到所述区块链地址的批准命令,以及

响应于所述批准命令,基于所述私钥将通过对所述区块链地址和所述第一信息进行数字签名而获得的签名数据与所述区块链地址和所述第一信息相关联并存储。

电子装置和使用该电子装置管理区块链地址的方法

技术领域

[0001] 本公开涉及电子装置和用于使电子装置管理区块链地址的技术。

背景技术

[0002] 数字签名是一种用于防止电子文档或数字数据被篡改并确认生成该签名的实体的技术,该技术在基于信息和通信网络来交换电子文档或执行电子商务时使用。

[0003] 区块链技术被应用于各种领域,该技术针对通过参与区块链网络的参与者的协作而认证的交易生成区块,使得参与该区块链网络的参与者具有区块链形式的信息,该信息在将生成的区块与先前的区块连接之后被存储,并防止能够由一些用户生成的数据被伪造。区块链大致可分为公共区块链和私有区块链。公共区块链可以是被用作在没有中心化服务器的去中心化网络环境中维护安全性和完整性的技术。例如,区块链技术保持安全性和完整性,并用于电子货币或加密货币服务。

[0004] 区块链地址可用于处理基于区块链技术的交易。换言之,为了指定区块链交易的实体和目标,可以使用以预定格式配置的区块链地址。

[0005] 上述信息仅作为背景信息呈现,以帮助理解本公开。对于上述任何内容是否可作为本公开的现有技术应用,尚未做出任何决定,也未做出任何断言。

发明内容

[0006] 技术问题

[0007] 作为使用区块链技术的示例,Ethereum网络是一种区块链平台,其能够在参与区块链的参与者(例如,节点)生成区块之后执行区块中包括的智能合约。例如,在Ethereum平台中,参与区块链网络的参与节点(例如,Ethereum客户端)可以使用共识算法(例如,工作量证明(Proof of Work)、权益证明(Proof of Stake)、实际拜占庭容错(Practical Byzantine Fault Tolerance))来验证交易的有效性,并且可以基于验证的结果来批准交易。被批准的交易可以被包括在该区块中,并且可以与先前的区块一起被存储。例如,将批准的交易存储在区块中的方案可以被称为区块链技术。此外,可以使用区块链技术发送和接收加密货币。在此情况下,为了发送和接收加密货币,可以使用数字钱包。在此情况下,数字钱包可以提供能够管理用户信息和加密密钥的功能。

[0008] 当用户试图在区块链中发送加密货币时,区块链技术可以处理用于发送和接收加密货币的交易。例如,交易可以包括例如一个交易,“A向B发送100BTC”。区块链中的交易可以包括与发送加密货币的发送者、接收加密货币的接收者或者要发送的加密货币的数额相关联的信息。区块链系统和数字钱包可以使用数字签名算法来处理交易。区块链可以保证交易的合法性,即数字签名没有被伪造或篡改。区块链在生成交易时执行数字签名。例如,区块链可以为每笔交易逐一分配数字签名。此外,用于验证数字签名的公钥可以作为一组被包括。为了在区块链中生成交易,需要一对密钥和对应于该密钥的公钥。例如,电子装置可以通过非对称算法生成密钥和对应于密钥的公钥。非对称算法可以使用例如椭圆曲线数

字签名算法 (ECDSA) 来生成和使用超过256位的密钥。当使用交易时,电子装置可以使用私钥来执行数字签名,并且参与区块链网络的节点可以使用公钥来验证数字签名。验证数字签名的操作可以包括确定第三方(例如,黑客)是否伪造或篡改交易内容的操作、确定第三方是否通过盗用执行交易的操作,或确定交易是否由加密货币的授权所有者生成的操作。由节点验证的所有交易可以存储在区块链中,并且数字签名和公钥可以作为一组存储在每个交易中。为了处理交易,区块链可以使用在区块链系统中以预定格式形成的区块链地址(例如,通过组合数字、小写英文字母和大写英文字母获得的40个字符的HEX字符串)。换句话说,区块链系统可以基于区块链地址确认作为区块链交易的实体或目标的数字钱包。然而,因为区块链地址由用户可识别的无意义的长串组成,所以用户很难确认区块链交易的目标是否是用户想要的目标。因此,当包括在区块链地址中的一个字符不正确时,就有发生异常交易或不执行交易的风险。

[0009] 当区块链地址被外部攻击者进行黑客攻击时,存在关于与真实区块链地址的目标不同的目标的信息将被显示在电子装置上的风险。例如,区块链地址在电子装置上被显示为电子装置的用户的家庭成员。然而,当包括在真实交易数据中的区块链地址被外部攻击者改变为攻击者地址时,交易可能是相对于外部攻击者的地址而不是该用户的家庭成员而建立的。例如,用户可能会将加密货币汇给攻击者。作为这种攻击技术的黑客方法的示例,存在剪贴板劫持。剪贴板劫持是当用户将区块链地址复制到交易的目标项目中时,将在交易的目标项目中输入的地址改变为黑客的地址。在交易中途更改任何地址时,用户都需要详细确认输入的地址是否为正常地址,以防止产生错误的交易。

[0010] 区块链系统可以有主网络。参与区块链系统的参与者可以在主网络上使用加密货币(币)进行交易。通证(token)可以被用作能够表示区块链中的唯一价值的价值单位的币。通证可以被用作区块链中交易的交换手段。或者,通证可以用作对基于区块链的交易的认证的补偿。在主网络中,可以使用协议,使得用户使用核心加密货币(币)生成通证。例如,Ethereum平台可以使用ERC20协议向用户发布定制的通证。根据本公开的实施例,智能合约可以在区块链网络中运行。区块链网络的开发者可以通过智能合约额外地生成通证。例如,Ethereum中生成的通证可以由智能合约生成,并且可以由唯一的智能合约管理。

[0011] 对于基于通证的交易,因为关于交易接收者的信息还包括通证程序的地址信息和通证接收者的信息,所以存在更多的用户应当确认的项目。

[0012] 参与区块链网络的参与者(例如,企业、团体、个人等)可以使用区块链的协议来构建去中心化应用(Dapp),并且可以生成每个唯一的通证。例如,Ethereum的区块链系统可以使用作为通证协议的标准ERC-20来生成和管理通证。在此情况下,与通证相关联的区块链交易信息可以被提供给第三方(例如,企业、个人、团体等),并且电子装置可以获得区块链交易信息的内容。例如,对于Ethereum,电子装置可以通过分析和发布区块的站点(例如,以太网扫描)在线接收Ethereum的区块链系统中使用的通证的信息。

[0013] 因为关于通证的信息在递送信息的过程中被操纵,所以仅通过可信用户界面显示关于要交易的目标的信息可能不会增强交易的可靠性。

[0014] 本公开的各方面至少解决上述问题和/或缺点,并至少提供下述优点。因此,本公开的一个方面是提供一种电子装置和用于使电子装置管理区块链地址的技术。

[0015] 另外的方面将部分地在随后的描述中阐述,并且部分地将从描述中显而易见,或

者可以通过实践所呈现的实施例来学习。

[0016] 问题的解决方案

[0017] 根据本公开的一方面,提供了一种电子装置。所述电子装置包括:显示器;以及至少一个处理器,所述至少一个处理器与所述显示器连接。所述至少一个处理器可以被配置为:使用私钥对区块链地址和与所述区块链地址相关联的第一信息执行数字签名;将作为执行所述数字签名的结果而获得的签名数据与所述区块链地址和所述第一信息中的至少一者相关联并存储;基于所存储的签名数据,使用与所述私钥相对应的公钥来执行对所述区块链地址和所述第一信息的认证;以及基于执行所述认证的结果,控制所述显示器显示所述区块链地址和所述第一信息。

[0018] 根据本公开的另一方面,提供了一种电子装置。该电子装置包括:显示器;存储器,所述存储器将与区块链交易目标相关联的第一信息与区块链地址相关联并存储该第一信息;以及至少一个处理器,所述至少一个处理器与所述显示器和所述存储器连接。所述至少一个处理器可以被配置为:生成要被发送到区块链网络的区块链交易数据;基于包括在所述区块链交易数据中的所述区块链地址获得所述第一信息;基于私钥对所述区块链地址和所述第一信息执行认证;当所述认证有效时,输出所述区块链地址和所述第一信息;接收批准了所述区块链交易数据的用户输入;响应于所述用户输入,使用所述私钥对所述区块链交易数据执行数字签名;以及将数字签名后的区块链交易数据发送到所述区块链网络。

[0019] 根据本公开的另一方面,提供了一种方法。所述方法包括:使用私钥对区块链地址和与所述区块链地址相关联的第一信息执行数字签名;将作为执行数字签名的结果而获得的签名数据与区块链地址和第一信息中的至少一者相关联并存储;基于所存储的签名数据,使用与所述私钥相对应的公钥来执行对所述区块链地址和所述第一信息的认证;以及基于执行所述认证的结果,在所述电子装置的显示器上显示所述区块链地址和所述第一信息。

[0020] 根据本公开的另一方面,提供了一种方法。所述方法包括:将与区块链交易目标相关联的第一信息与区块链地址相关联并存储;生成要发送到区块链网络的区块链交易数据;基于包括在所述区块链交易数据中的所述区块链地址获得所述第一信息;基于私钥对所述区块链地址和所述第一信息执行认证;当所述认证有效时,输出所述区块链地址和所述第一信息;接收批准了所述区块链交易数据的用户输入;以及响应于所述用户输入,使用所述私钥对所述区块链交易数据执行数字签名。

[0021] 本公开的其他方面、优点和显著的特征将从以下详细描述中对于本领域的技术人员来说是显而易见的,并与附图一起使用,公开本公开的各种实施例。

[0022] 本发明的有益效果

[0023] 根据本公开中公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法来验证区块链地址,而无需用户确认区块链地址是否被正确输入,并且使用户容易地确认与地址相关联的信息。

[0024] 此外,根据本公开中公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以向用户提供熟悉的信息,并使用户容易地确认区块链地址。

[0025] 此外,根据本公开中公开的实施例,可以使用具有增强安全性的存储空间来存储与区块链地址相关联的信息。具有增强安全性的存储空间可以包括例如物理划分的可信空

间和逻辑划分的可信空间。例如,物理划分的可信空间可以具有存在于电子装置内部或外部的单独的存储空间。电子装置可以通过单独的可信应用或功能来访问物理可信空间。逻辑划分的可信空间可以是在一个存储空间(存储器)中与不可信区域逻辑地分离的可信区域。为了访问逻辑信任区,电子装置可以仅通过单独的信任应用或功能(例如,API)来访问信任区。例如,为了访问逻辑可信区域,可以运行单独的操作系统(例如,可信操作系统)。富操作系统可以请求可信操作系统访问逻辑可信区域。可信操作系统可以验证该请求,并且只有当该请求是正常请求时才可以访问逻辑可信区域。根据本公开的实施例,可信操作系统可以作为单独的操作系统或者其中包括在富操作系统的内核中的软件被虚拟划分的操作系统来运行。根据本公开的实施例,存储空间可以包括电子装置中的存储空间。例如,电子装置可以在一个存储器中存储通用数据,而无需单独划分信任区。具有增强安全性的存储空间可以控制对电子装置的至少部分存储区域的访问。例如,至少一部分存储区域可以是仅通过单独的可信操作系统和/或单独的可信内核可访问的可信存储区域。电子装置可以仅通过借助可信操作系统或可信内核的单独认证来访问存储在可信存储区域中的区块链地址或相关信息。或者,区块链地址和相关信息可以被加密,以便仅通过可信操作系统或可信区域中的密钥来解密,从而被存储在不可信区域中的存储空间中。提供电子装置和在电子装置中管理区块链地址的方法以执行附加认证,并且仅当附加认证完成时才执行区块链交易,以增强区块链交易的安全性。

[0026] 根据本公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以增强区块链地址的可用性,因为通过认证(例如,生物特征认证)使用了各种信息。

[0027] 根据本公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以在尽管用户改变了他或她的终端装置的情况下在交易中继续使用认证信息。例如,因为认证信息是在区块链网络中分发和存储的,所以在尽管改变了终端装置的情况下,用户可以从区块链网络获得和使用认证信息。

[0028] 此外,可以提供通过本公开直接或间接确定的各种效果。

附图说明

[0029] 通过结合附图进行的以下描述,本公开的某些实施例的上述和其他方面、特征和优点将更加明显,其中:

[0030] 图1是示出根据本公开实施例的网络环境中的电子装置的框图;

[0031] 图2是示出根据本公开实施例的电子装置的配置的框图;

[0032] 图3是示出根据本公开实施例的电子装置显示区块链地址的过程的流程图;

[0033] 图4是示出根据本公开实施例的在电子装置上显示区块链地址的验证画面的示意图;

[0034] 图5是示出根据本公开实施例的电子装置显示关于可靠性的信息的示意图;

[0035] 图6是示出根据本公开实施例的电子装置将区块链地址与第一信息相关联并存储的过程的流程图;

[0036] 图7是示出根据本公开实施例的显示在电子装置上的联系人应用正在运行的画面的示意图;

[0037] 图8是示出根据本公开实施例的基于联系人共享功能生成区块链地址认证请求的

示图；

[0038] 图9是示出根据本公开实施例的电子装置在区块链交易过程中接收区块链地址认证请求的示图；

[0039] 图10是示出根据本公开实施例的电子装置基于显示区块链交易历史的画面接收区块链地址认证请求的示图；

[0040] 图11是示出根据本公开实施例的电子装置显示区块链地址和第一信息的画面的示图；

[0041] 图12是示出根据本公开实施例的在电子装置执行用户认证过程的过程中显示的画面的示图；

[0042] 图13是示出根据本公开实施例的电子装置将区块链地址与另一信息相关联并存储的示图；

[0043] 图14是示出根据本公开实施例的电子装置结合另一信息存储区域区块链地址的示图；

[0044] 图15是示出根据本公开实施例的由电子装置操作的富操作系统和可信操作系统实现的富执行环境(REE)和可信执行环境(TEE)的框图；

[0045] 图16是示出根据本公开实施例的电子装置将区块链地址与签名数据相关联并存储的过程的信号序列图；

[0046] 图17是示出根据本公开实施例的电子装置对区块链交易数据执行数字签名的过程的流程图；

[0047] 图18是根据本公开实施例的基于存储在电子装置中的第一信息对区块链交易数据执行数字签名的信号序列图；

[0048] 图19是示出了根据本公开实施例的电子装置获得和存储通行证信息的过程的示图；

[0049] 图20是示出根据本公开实施例的电子装置基于异构操作系统输出区块链地址和第一信息的过程的流程图；

[0050] 图21是示出根据本公开实施例的电子装置中包括的应用、操作系统和内核的结构框图；

[0051] 图22是示出根据本公开实施例的使用电子装置配置的数字钱包的结构示图；

[0052] 图23是示出根据本公开实施例的由电子装置执行的过程的信号序列图。

[0053] 在所有附图中，相似的附图标记将被理解为指代相似的部件、组件和结构。

具体实施方式

[0054] 提供参考附图的以下描述以帮助全面理解由权利要求书及其等同形式限定的本发明的各种实施例。下述说明包括各种具体的细节，以协助理解，但这些细节被视为仅仅是示范性的。因此，本领域普通技术人员将认识到，在不脱离本公开的范围和精神的情况下，可以对本文所描述的各种实施例进行各种更改和修改。此外，为了清楚和简明，可能省略对公知功能和结构的描述。

[0055] 在权利要求书和以下的说明书中使用的术语和词汇不限于字面的含义，而是，这些术语和词汇仅仅是由发明人使用从而使得对本公开的理解变得清楚和一致。因此，本领域技术人员应当明白，以下对本公开的各种实施例的描述仅仅为了说明的目的，而不旨在

限制由所附权利要求及其等同形式所限定的本公开。

[0056] 应理解,除非上下文中另有明确指示,未指明数量的表述“一”、“该”和“所述”也包括多个所指对象。因此,例如对“组件表面”的引述包括对一个或更多个这种表面的引述。

[0057] 图1是示出根据本公开实施例的网络环境100中的电子装置101的框图。

[0058] 参照图1,网络环境100中的电子装置101可经由第一网络198(例如,短距离无线网络)与电子装置102进行通信,或者经由第二网络199(例如,长距离无线网络)与电子装置104或服务器108进行通信。根据本公开的实施例,电子装置101可经由服务器108与电子装置104进行通信。根据本公开的实施例,电子装置101可包括处理器120、存储器130、输入装置150、声音输出装置155、显示装置160、音频模块170、传感器模块176、接口177、触觉模块179、相机模块180、电力管理模块188、电池189、通信模块190、用户识别模块(SIM)196或天线模块197。在本公开的一些实施例中,可从电子装置101中省略所述部件中的至少一个(例如,显示装置160或相机模块180),或者可将一个或更多个其他部件添加到电子装置101中。在本公开的一些实施例中,可将所述部件中的一些部件实现为单个集成电路。例如,可将传感器模块176(例如,指纹传感器、虹膜传感器、或照度传感器)实现为嵌入在显示装置160(例如,显示器)中。

[0059] 处理器120可运行例如软件(例如,程序140)来控制电子装置101的与处理器120连接的至少一个其他部件(例如,硬件部件或软件部件),并可执行各种数据处理或计算。根据本公开的实施例,作为所述数据处理或计算的至少部分,处理器120可将另一部件(例如,传感器模块176或通信模块190)接收到的命令或数据加载到易失性存储器132中,对存储在易失性存储器132中的命令或数据进行处理,并将结果数据存储在非易失性存储器134中。根据本公开的实施例,处理器120可包括主处理器121(例如,中央处理器(CPU)或应用处理器(AP))以及与主处理器121在操作上独立的或者相结合的辅助处理器123(例如,图形处理单元(GPU)、图像信号处理器(ISP)、传感器中枢处理器或通信处理器(CP))。另外地或者可选择地,辅助处理器123可被适配为比主处理器121耗电更少,或者被适配为具体用于指定的功能。可将辅助处理器123实现为与主处理器121分离,或者实现为主处理器121的部分。

[0060] 在主处理器121处于未激活(例如,睡眠)状态时,辅助处理器123可控制与电子装置101(而非主处理器121)的部件之中的至少一个部件(例如,显示装置160、传感器模块176或通信模块190)相关的功能或状态中的至少一些,或者在主处理器121处于启用状态(例如,运行应用)时,辅助处理器123可与主处理器121一起来控制与电子装置101的部件之中的至少一个部件(例如,显示装置160、传感器模块176或通信模块190)相关的功能或状态中的至少一些。根据本公开的实施例,可将辅助处理器123(例如,图像信号处理器或通信处理器)实现为在功能上与辅助处理器123相关的另一部件(例如,相机模块180或通信模块190)的部分。

[0061] 存储器130可以存储由电子装置101的至少一个组件(例如,处理器120或传感器模块176)使用的各种数据。所述各种数据可包括例如软件(例如,程序140)以及针对与其相关的命令的输入数据或输出数据。存储器130可包括易失性存储器132或非易失性存储器134。

[0062] 可将程序140作为软件存储在存储器130中,并且程序140可包括例如操作系统(OS)142、中间件144或应用146。

[0063] 输入装置150可从电子装置101的外部(例如,用户)接收将由电子装置101的其他

部件(例如,处理器120)使用的命令或数据。输入装置150可包括例如麦克风、鼠标、键盘或数字笔(例如,手写笔)。

[0064] 声音输出装置155可将声音信号输出到电子装置101的外部。声音输出装置155可包括例如扬声器或接收器。扬声器可用于诸如播放多媒体或播放唱片的通用目的,接收器可用于呼入呼叫。根据本公开的实施例,可将接收器实现为与扬声器分离,或实现为扬声器的部分。

[0065] 显示装置160可向电子装置101的外部(例如,用户)视觉地提供信息。显示装置160可包括例如显示器、全息装置或投影仪以及用于控制显示器、全息装置和投影仪中的相应一个的控制电路。根据本公开的实施例,显示装置160可包括被适配为检测触摸的触摸电路或被适配为测量由触摸引起的力的强度的传感器电路(例如,压力传感器)。

[0066] 音频模块170可将声音转换成电信号,反之亦可。根据本公开的实施例,音频模块170可经由输入装置150获得声音,或者经由声音输出装置155或与电子装置101直接(例如,有线地)连接或无线连接的外部电子装置(例如,电子装置102)的耳机输出声音。

[0067] 传感器模块176可检测电子装置101的操作状态(例如,功率或温度)或电子装置101外部的环境状态(例如,用户的状态),然后产生与检测到的状态相应的电信号或数据值。根据本公开的实施例,传感器模块176可包括例如手势传感器、陀螺仪传感器、大气压力传感器、磁性传感器、加速度传感器、握持传感器、接近传感器、颜色传感器、红外(IR)传感器、生物特征传感器、温度传感器、湿度传感器或照度传感器。

[0068] 接口177可支持将用来使电子装置101与外部电子装置(例如,电子装置102)直接(例如,有线地)或无线连接的一个或多个特定协议。根据本公开的实施例,接口177可包括例如高清晰度多媒体接口(HDMI)、通用串行总线(USB)接口、安全数字(SD)卡接口或音频接口。

[0069] 连接端178可包括连接器,其中,电子装置101可经由所述连接器与外部电子装置(例如,电子装置102)物理连接。根据本公开的实施例,连接端178可包括例如HDMI连接器、USB连接器、SD卡连接器或音频连接器(例如,耳机连接器)。

[0070] 触觉模块179可将电信号转换成可被用户经由他的触觉或动觉识别的机械刺激(例如,振动或运动)或电刺激。根据本公开的实施例,触觉模块179可包括例如电机、压电元件或电刺激器。

[0071] 相机模块180可捕获静止图像或运动图像。根据本公开的实施例,相机模块180可包括一个或多个透镜、图像传感器、图像信号处理器或闪光灯。

[0072] 电力管理模块188可管理对电子装置101的供电。根据本公开的实施例,可将电力管理模块188实现为例如电力管理集成电路(PMIC)的至少部分。

[0073] 电池189可对电子装置101的至少一个部件供电。根据本公开的实施例,电池189可包括例如不可再充电的原电池、可再充电的蓄电池、或燃料电池。

[0074] 通信模块190可支持在电子装置101与外部电子装置(例如,电子装置102、电子装置104或服务器108)之间建立直接(例如,有线)通信信道或无线通信信道,并经由建立的通信信道执行通信。通信模块190可包括能够与处理器120(例如,应用处理器(AP))独立操作的一个或多个通信处理器,并支持直接(例如,有线)通信或无线通信。根据本公开的实施例,通信模块190可包括无线通信模块192(例如,蜂窝通信模块、短距离无线通信模块或全

球导航卫星系统 (GNSS) 通信模块) 或有线通信模块194 (例如, 局域网 (LAN) 通信模块或电力线通信 (PLC) 模块)。这些通信模块中的相应一个可经由第一网络198 (例如, 短距离通信网络, 诸如蓝牙、无线保真 (Wi-Fi) 直连或红外数据协会 (IrDA)) 或第二网络199 (例如, 长距离通信网络, 诸如蜂窝网络、互联网、或计算机网络 (例如, LAN或广域网 (WAN))) 与外部电子装置进行通信。可将这些各种类型的通信模块实现为单个部件 (例如, 单个芯片), 或可将这些各种类型的通信模块实现为彼此分离的多个部件 (例如, 多个芯片)。无线通信模块192可使用存储在用户识别模块196中的用户信息 (例如, 国际移动用户识别码 (IMSI)) 识别并验证通信网络 (诸如第一网络198或第二网络199) 中的电子装置101。

[0075] 天线模块197可将信号或电力发送到电子装置101的外部 (例如, 外部电子装置) 或者从电子装置101的外部 (例如, 外部电子装置) 接收信号或电力。根据本公开的实施例, 天线模块197可包括天线, 所述天线包括辐射元件, 所述辐射元件由形成在基底 (例如, 印刷电路板 (PCB)) 中或形成在基底上的导电材料或导电图案构成。根据本公开的实施例, 天线模块197可包括多个天线。在此情况下, 可由例如通信模块190 (例如, 无线通信模块192) 从所述多个天线中选择适合于在通信网络 (诸如第一网络198或第二网络199) 中使用的。通信方案的至少一个天线。随后可经由所选择的至少一个天线在通信模块190和外部电子装置之间发送或接收信号或电力。根据本公开的实施例, 除了辐射元件之外的另外的组件 (例如, 射频集成电路 (RFIC)) 可附加地形成为天线模块197的一部分。

[0076] 上述部件中的至少一些可经由外设间通信方案 (例如, 总线、通用输入输出 (GPIO)、串行外设接口 (SPI) 或移动工业处理器接口 (MIPI)) 相互连接并在其之间通信地递送信号 (例如, 命令或数据)。

[0077] 根据本公开的实施例, 可经由与第二网络199连接的服务器108在电子装置101和外部电子装置104之间发送或接收命令或数据。电子装置102和电子装置104中的每一个可以是与电子装置101相同类型的装置, 或者是与电子装置101不同类型的装置。根据本公开的实施例, 将在电子装置101运行的全部操作或一些操作可在外部电子装置102、外部电子装置104或服务器108中的一个或更多个运行。例如, 如果电子装置101应该自动执行功能或服务或者应该响应于来自用户或另一装置的请求执行功能或服务, 则电子装置101可请求所述一个或更多个外部电子装置执行所述功能或服务中的至少部分, 而不是运行所述功能或服务, 或者电子装置101除了运行所述功能或服务以外, 还可请求所述一个或更多个外部电子装置执行所述功能或服务中的至少部分。接收到所述请求的所述一个或更多个外部电子装置可执行所述功能或服务中的所请求的所述至少部分, 或者执行与所述请求相关的另外功能或另外服务, 并将执行的结果传送到电子装置101。电子装置101可在对所述结果进行进一步处理的情况下或者在不对所述结果进行进一步处理的情况下将所述结果提供作为对所述请求的至少部分答复。为此, 可使用例如云计算技术、分布式计算技术或客户机-服务器计算技术。

[0078] 区块链中使用的私钥和公钥可以基于非对称算法来生成。非对称加密算法可以使用一种加密算法, 例如Rivest-Shamir-Adleman (RSA)、椭圆曲线加密 (ECC) 或数字签名算法 (DSA)。对称加密算法具有彼此相同的加密密钥和解密密钥, 而非对称算法使用彼此不同的加密密钥和解密密钥。公钥可以是公开的, 并且可以被另一个用户访问。例如, 当发送者使用接收者的公钥执行加密时, 接收者可以使用私钥执行解密以确认所加密的内容。公钥可

用于数字签名。电子装置可以确认出公钥签名是使用特定的密钥做出的,并且可以知道公钥签名是由拥有私钥的人进行数字签名的。例如,用私钥加密的密文可以用相应的公钥解密。当通过使用私钥进行加密和签名来执行数字签名时,验证签名的设备可以使用公钥来执行解密。验证签名的设备可以将散列解密数据的值与散列发送数据的值进行比较,以执行签名认证。区块链可以使用利用这种私钥和公钥的签名。例如,私钥可以被用作用户用来生成交易的密码,并且可以被用来利用公钥生成区块链地址。例如,电子装置可以通过使用私钥的椭圆曲线算法生成公钥,并且可以通过哈希函数将生成的公钥生成能够在区块链中使用的地址。私钥可以用随机抽取的数字来配置。私钥可以生成256位数。私钥可以从根种子生成。根种子是能够从其中生成许多密钥和地址的缺省值。电子装置可以恢复通过根种子生成的密钥值。根种子可以使用助记单词序列。助记单词序列可以包括人可识别的单词。根据本公开的各种实施方式,根种子可以使用各种类型的种子。例如,根种子可以使用用十六进制数配置的种子,或者可以使用用12个单词的助记符配置的种子。在此情况下,助记符可以包括用户可识别的单词形式。在此情况下,根种子可以使用基于比特币改进提案(BIP)-39标准的助记符。可以基于BIP-39标准生成助记码和种子。可以通过使用包括在种子中的单词和盐(salt)值(例如,来自用户的代码输入)作为因子,使用密钥拉伸函数(key stretching function)来生成512位种子。密钥拉伸函数(例如,PBKDF2)可以使用两个因子值来输出某个(512位)值。例如,密钥拉伸函数可以使用散列算法(例如,HMAC-SHA512)重复散列两个因子值,并且可以生成最终输出值作为根种子。

[0079] 电子装置可以使用根种子生成私钥和公钥。例如,根种子可以从通过HMAC-SHA512函数生成的散列值中生成主私钥和主链码。512位散列值左边的256位可用作私钥,512位散列值右边的256位可用作链码。可以利用私钥和椭圆曲线函数来使用公钥。当在区块链中生成交易时,可以执行使用私钥和公钥的签名。例如,发送者针对交易编写交易消息,可以用发送者的私钥加密该消息,并且可以生成签名。生成的签名仅可以用公钥解密。生成的签名和交易消息可以一起在区块链上发送。在此情况下,可以一起释放公钥。验证数字签名的设备可以用公钥解密签名,并且可以将解密的签名与包括在交易中的消息进行比较。当签名与消息相同时,设备可以确定签名是用普通私钥加密的。根据本公开的实施例,电子装置可以利用用于交易的私钥对地址和与该地址相关联的附加信息进行数字签名,并且可以在其中存储签名的值、地址和附加信息。当用户想要生成交易时,电子装置可以一起显示附加信息,以更容易地向用户通知关于目的地地址的信息。为了确认存储在不信任区域中的地址、附加信息等不是伪造或篡改的,可以执行对数字签名的认证。根据本公开的实施例,电子装置可以请求在具有增强安全性的操作系统上运行的可信应用或者在不可信区域上运行的具有增强安全性的可信应用来确认签名。在此情况下,电子装置可以递送存储在不信任区域中的区块链地址、附加信息、交易的区块链地址或数字签名值中的至少一个。可信应用可以利用公钥来解密数字签名值,可以通过在解密的值中散列区块链地址来生成散列值,并且将生成的散列值与通过散列接收到的区块链地址而生成的散列值进行比较来认证签名。

[0080] 图2是示出根据本公开实施例的电子装置的配置的框图。

[0081] 参考图2,电子装置200(例如,图1的电子装置101)可以包括处理器210(例如,图1的处理器120)、存储器220(例如,图1的存储器130)、显示器230(例如,图1的显示设备160)、通信电路240(例如,图1的通信模块190中包括的通信电路)。根据本公开的实施例,处理器

210可以执行存储在存储器220中的指令。作为执行指令的结果,处理器210可以处理数据或者可以控制电子装置200的组件,使得电子装置200执行操作。

[0082] 根据本公开的实施例,存储器220可以存储第一信息。根据本公开的实施例,第一信息可以包括这样的信息,在该信息中电子装置200的用户可以指定关于区块链交易的目标的信息或者关于区块链交易的目的地址的信息。例如,第一信息可以包括联系人信息(更具体地,由第一区块链地址指示的区块链交易的目标的联系人信息)。例如,联系人信息可以包括姓名、电话号码或电子邮件地址。根据本公开的实施例,第一信息可以通过组合几条信息而打包的信息。例如,第一信息可以包括关于电子装置200的用户与区块链交易的目标之间的关系的消息。更具体地,第一信息可以使用包括在联系人信息中的组信息以“詹姆斯/朋友”或“詹姆斯/同事”的形式配置。电子装置200可以获得存储在多个数据库中的信息,以组合几条信息来配置信息。根据本公开的实施例,包括联系人信息的第一信息可以存储在联系人存储器222中。例如,联系人信息可以是包括在存储目标的电话号码的数据库中的信息,该信息被运行在电子装置200上的电话相关应用用来进行呼叫。根据本公开的实施例,电子装置200的各种应用可以使用存储在联系人存储器222中的信息来运行。例如,能够在电子装置200上运行的电子邮件应用可以使用包括在联系人存储器222中的用户名和电子邮件信息来发送电子邮件。

[0083] 例如,联系人信息可以包括:在电子装置200处使用输入装置(例如,图1的输入装置150)从用户接收的信息。又例如,联系人信息可以包括由电子装置200使用通信电路240通过网络250从与电子装置200交互工作的联系人管理服务器264获得的信息。又例如,联系人信息可以包括使用联系人共享功能从另一电子装置(例如,图1的电子装置102或电子装置104)接收到的信息。

[0084] 又例如,第一信息可以包括通证信息。根据本公开的实施例,包括通证信息的第一信息可以存储在存储器220的通证信息存储区域224中。通证信息存储区域224可以指在存储器220中形成的用于存储通证信息的空间。例如,通证信息可以包括指示通证类型以确认用于通证交易的通证的信息、由电子装置200使用输入装置(例如,图1的输入装置150)从用户接收的通证程序的地址信息,以及通证接收者的信息。又例如,通证信息可以包括由电子装置200使用通信电路240通过网络250从通证信息提供网络262接收到的信息。

[0085] 根据本公开的实施例,处理器210可以将第一区块链地址与第一信息相关联并存储在存储器220中。此外,处理器210可以在显示器230上向用户显示第一区块链地址和与第一区块链地址相关联的第一信息。例如,当电子装置200试图使用第一区块链地址生成区块链交易时,处理器210可以在显示器230上显示包括第一区块链地址的交易记录画面。电子装置200可以在包括第一区块链地址的交易记录画面上输出用于确认过去执行了多少次使用第一区块链地址的交易的信息。电子装置200可以响应于对交易记录画面的用户输入,执行用于执行针对第一区块链地址的交易(例如,向第一区块链地址发送加密货币)的数字签名。根据本公开的实施例,当没有交易记录时,电子装置200还可以执行用于确认第一区块链地址的附加操作,以验证地址的有效性。根据本公开的实施例,电子装置200可以经由外部服务器(例如,区块链地址认证服务器)获得关于第一区块链地址的信息。根据本公开的实施例,关于第一区块链地址的信息可以包括关于第一区块链地址的可靠性信息。例如,当第一区块链地址是授权机构的区块链地址时,其可以包括关于授权机构的信息。根据本公

开的实施例,当第一区块链地址是黑客使用的地址时,外部服务器可以向电子装置200提供具有关于其信息的第一区块链地址。在此情况下,电子装置200可以将第一区块链地址发送到外部服务器,并且可以响应于发送的第一区块链地址获得关于第一区块链地址的附加信息。电子装置200可以显示获得的附加信息以及第一区块链地址。

[0086] 电子装置200可以以各种方法获得第一区块链地址。例如,电子装置200可以捕获QR码的图像,并且可以基于通过解密QR码获得的信息来获得第一区块链地址。又例如,电子装置200可以读取第一区块链地址或用于通过NFC从近场通信(NFC)标签获得第一区块链地址的信息(例如,统一资源定位符(URL))。电子装置200可以获得第一区块链地址,并且可以执行用于附加认证(例如,个人身份号码(PIN)或生物特征认证)的认证过程,以执行第一区块链地址的数字签名。例如,使用生物特征认证的认证过程可以包括电子装置200获得用户的生物特征信息(例如,指纹或虹膜)并基于获得的生物特征信息执行认证的操作。根据本公开的实施例,当第一区块链地址的数字签名完成时,在显示第一区块链地址时,电子装置200可以输出指示用户被认证的附加信息(例如,可信标记或声音)。例如,电子装置200可以在显示器230上显示指示用户被认证的图像。根据本公开的实施例,取决于第一区块链地址是否被认证,电子装置200可以不同地显示另一图像。例如,当第一区块链地址未被认证时,电子装置200可以显示红色图标。当第一区块链地址被认证时,电子装置200可以显示绿色图标。根据本公开的实施例,取决于第一区块链地址是否被认证或者可靠性水平,电子装置200可以向用户显示不同的图像。

[0087] 例如,当第一信息包括用户名时,处理器210可以在显示器230上显示包括第一区块链地址的交易记录画面,使得电子装置200执行用于区块链交易的数字签名。根据本公开的实施例,处理器210可以确定与第一区块链地址和第一信息相关联的可靠性。根据本公开的实施例,处理器210可以在显示器230上输出指示所确定的可靠性的第二信息。根据本公开的实施例,第二信息可以以各种形式输出(例如,图形信息、音频信息、视频信息、振动信息等)。例如,当第二信息包括与可靠性相对应的图标时,该图标是图形信息,处理器210可以在显示器230上显示该图标。例如,当第一区块链地址的可靠性高时,处理器210可以显示第一图标,并且当第一区块链地址的可靠性低时,可以显示第二图标。

[0088] 处理器210可以基于认证用户的输入对区块链交易数据进行数字签名。通信电路240可以通过网络250将由处理器210数字签名的区块链交易数据发送到区块链网络255。发送到区块链网络的区块链交易数据可以通过至少一个区块链节点270认证。认证后的交易数据可被记录在包括在区块中的至少一个区块链节点270中。

[0089] 根据本公开的实施例,区块链系统可以包括根据区块链平台单独建立的区块链网络255。例如,基于私有区块链平台(如Ripple或Hyper Ledger)配置的区块链系统可以包括独立建立的区块链网络。区块链网络255可以只为认证的设备验证交易,并且可以配置能够生成/存储区块的区块链节点270-1。

[0090] 图3是示出根据本公开实施例的电子装置显示区块链地址的过程的流程图300。

[0091] 参考图3,在操作310中,电子装置200(例如,图2的处理器210)可以存储第一信息。例如,电子装置200可以运行能够管理联系人的应用,并且可以存储由使用该应用的用户使用输入装置(例如,图1的输入装置150)输入的信息。例如,能够管理联系人的应用可以是地址簿应用。电子装置200可以接收诸如电话号码、电子邮件地址或想要进行呼叫的用户的姓

名的信息,作为呼叫应用中的第一信息。电子装置200可以在图2的存储器220中存储用接收到的第一信息构建的数据库。又例如,电子装置200可以存储从使用通信电路240通过网络250与电子装置200交互工作的联系人管理服务器264获得的联系人信息。又例如,电子装置200可以使用联系人共享功能存储从另一个电子装置(例如,图1的外部电子装置102或外部电子装置104)接收到的信息。又例如,电子装置200可以存储从图2的通证信息提供网络262获得的信息。

[0092] 在操作320中,电子装置(例如,处理器210)可以将第一区块链地址与第一信息相关联并存储。根据本公开的实施例,在操作320,电子装置可以执行用户认证过程,用于验证用户是否是授权用户。此外,在操作320,电子装置可执行向认证的用户提供第一区块链地址和第一信息并从用户接收将第一区块链地址与第一信息相关联并存储的批准命令的操作。电子装置可以生成数据库,在该数据库中,第一区块链地址被映射到第一信息。电子装置可以管理将第一区块链地址和第一信息一起存储的数据库。电子装置可以基于用户的输入存储第一区块链地址和第一信息。例如,在确认了第一区块链地址并接收到批准将第一区块链地址映射到第一信息的输入时,电子装置可以执行将第一区块链地址与第一信息相关联的关联操作。根据本公开的实施例,电子装置可以验证第一区块链地址的有效性。电子装置可以将被验证为有效的第一区块链地址映射到第一信息。根据本公开的实施例,电子装置可以从电子装置的内部或外部获得将第一区块链地址映射到第一信息所额外需要的信息。电子装置可以基于对获得的信息的分析结果来执行将第一区块链地址映射到第一信息的操作。

[0093] 在操作330中,电子装置(例如,处理器210)可以确认用于显示第一区块链地址的事件是否发生。例如,电子装置可以接收选择第一区块链地址的用户输入,以生成用于发送加密货币的交易。在此情况下,电子装置可以确定发生了用于显示作为接收加密货币的目的地址的第一区块链地址的事件。

[0094] 在操作340,电子装置可以在显示器(例如,图2的显示器230)上显示第一区块链地址、第一信息和第二信息。用于显示第一区块链地址的事件例如可以是当生成用于发送区块链系统的加密货币的交易时,可以接收加密货币的接收者的第一区块链地址被输入到区块链交易记录输入画面。

[0095] 图4是示出了根据本公开的实施例的显示区块链地址、第一信息和第二信息的区块链交易确认画面400的示图。

[0096] 参考图4,电子装置可以显示包括区块链地址410、第一信息411和第二信息412的区块链交易确认画面400。

[0097] 根据本公开的实施例,第二信息可以是表示第一区块链地址或第一信息的可靠性的信息。例如,当第一区块链地址是用户先前生成交易的区块链地址时,电子装置可以将第一区块链地址确定为可靠地址,并且可以显示与所确定的可靠性相对应的第一信息。例如,当第一区块链地址被可靠的外部设备认证时,电子装置可以根据认证结果显示与第一区块链地址的可靠性相对应的第二信息。根据本公开的实施例,第二信息可以指示根据认证第一区块链地址的实体的可靠性信息。例如,可以基于电子装置是否认证了用户的第一区块链地址或者第一区块链地址是否通过外部设备认证来确定第二信息。根据本公开的实施例,当第一区块链地址无效时,电子装置可以输出包括表示第一区块链地址不可靠的图形

指示的第二信息。例如,当确定第一区块链地址是被黑客操纵的区块链地址时,或者当从外部获得表示第一区块链地址是黑客的地址的信息时,电子装置可以确定第一区块链地址不是有效地址。电子装置可以输出表示第一区块链地址不可靠的图形指示。

[0098] 例如,第二信息可以包括:表示可靠性具有从用户认证了第一区块链地址与第一信息相关联的水平信息,表示可靠性具有被预测为与用户相关联的目标的水平信息(例如,第一区块链地址被包括在用户的交易历史中),或者表示第一区块链地址不与可靠信息相关联的信息。根据本公开的实施例,第二信息可以以图形图像的形式输出。根据本公开的另一实施例,第二信息可以经由扬声器以声音的形式输出。根据本公开的另一实施例,电子装置可以向与电子装置连接的第二电子装置提供第二信息。例如,第二信息可以被发送到与便携式移动设备(第一电子装置)连接的用户另一智能手表(第二电子装置)。根据本公开的实施例,电子装置可以向外部服务器或至少一个外部区块链网络发送关于第一区块链的可靠性信息。

[0099] 图5是示出根据本公开实施例的与区块链地址一起显示的第二信息的示意图。

[0100] 参照图5,电子装置可以显示关于第一区块链地址的各种类型的第二信息。根据本公开的实施例,对于针对第一区块链地址与第一信息之间的映射关系完成用户的认证的第一种情况(例如,当与第一区块链地址和第一信息中的至少一个相关联并存储的签名数据有效时),电子装置可以显示表示高可靠性的第一图像(例如,图标510)。根据本公开的实施例,当关于第一区块链地址的用户的认证没有完成时,电子装置可以显示指示用户的认证没有完成的图标。根据本公开的实施例,当用户将第一区块链地址映射到第一信息时,电子装置可以显示表示高可靠性的图标510。

[0101] 又例如,参考图5,当存在针对第一区块链地址的正常区块链交易历史时(例如,第二种情况),电子装置可以显示第二图像(例如,图标520),该第二图像表示第一区块链地址结合第一信息具有中等水平的可靠性。又例如,参考图5,当存储在联系人存储器(例如,图2的联系人存储器222)中的包括第一区块链地址的联系人类别满足指定条件(例如,对于属于家庭类别的联系人)时,电子装置可以显示图标520,该图标520表示第一区块链地址结合第一信息具有中等水平的可靠性。或者,当映射到第一区块链地址的第一信息未被验证时,或者当不能确保第一区块链的可靠性时,电子装置可以显示第三图像(例如,表示第一区块链地址是未被确认的地址的图标530)。

[0102] 图6是示出根据本公开实施例的电子装置将区块链地址与第一信息相关联并存储的过程的流程图600。

[0103] 参考图6,在操作610中,电子装置(例如,处理器210)可以确认是否生成了针对第一区块链地址的区块链地址认证请求。

[0104] 当在操作610中生成了地址认证请求时,在操作620中,电子装置(例如,处理器210)可以在显示器(例如,图2的显示器230)上显示第一区块链地址和要与第一区块链地址相关联并被存储的第一信息。区块链地址认证请求可以意味着从用户认证在第一区块链地址与第一信息之间是否存在联系。根据实施例,区块链地址认证请求可以以各种方式实现。将参照图7至图9描述关于各种实施例的内容。

[0105] 当生成了地址认证请求时,在操作620中,电子装置(例如,处理器210)可以显示第一区块链地址和第一信息。根据本公开的实施例,当第一信息包括通证名称和通证符号(通

证信息)时,电子装置可以显示包括通证名称、通证符号、区块链地址和用户界面对象的画面。

[0106] 在操作630中,电子装置可以通过用户界面对象从确认联系人信息和区块链地址的用户接收批准命令。根据本公开的实施例,批准命令可以指示用户验证区块链地址和第一信息彼此映射,并且可以指请求将区块链地址与第一信息相关联并存储的用户输入。

[0107] 在图6的操作630中,电子装置可以通过用户界面对象从确认通证名称、通证符号、区块链地址的用户接收批准命令。通证可以指这样的对象,该对象将是作为基于区块链系统发布的区块链系统的用户之间的交易目标。

[0108] 根据本公开的实施例,电子装置可以执行验证输入批准命令的用户的用户认证过程。例如,在图6的操作630中输入批准命令之后,电子装置可执行用户认证过程。这里,实施例不限于此。这里,用户认证过程可以在图6所示的任何一个操作之前执行。当没有认证出用户是电子装置的授权用户时,作为执行用户认证过程的结果,电子装置可能无法继续进行图6所示的处理,或者可能停止图6所示的处理。

[0109] 作为用户认证过程的示例,电子装置可以从用户接收个人识别号(PIN)。

[0110] 作为用户认证过程的示例,电子装置可以包括从用户接收生物特征信息(例如,指纹或虹膜)并认证该生物特征信息的操作,作为用户认证过程。

[0111] 根据本公开的实施例,响应于批准命令向用户显示信息以及获得针对批准命令的用户输入的操作可以借助于电子装置中的独立可信操作系统或独立可信内核通过画面或指令来执行。

[0112] 根据本公开的实施例,当输入了批准命令时,在图6的操作640中,电子装置可基于私钥对第一区块链地址和第一信息执行数字签名。在说明书中,包括私钥和公钥的密钥对可以指基于区块链根种子生成的密钥对。例如,电子装置可以通过数字签名来生成签名数据,该数字签名基于关于通过组合第一区块链地址和第一信息获得的值的私钥。

[0113] 用于区块链交易的区块链地址(例如,区块链账户地址)可以基于区块链交易的每一方的私钥和对应于该私钥的公钥来生成。例如,许多基于区块链的加密货币从根种子导出用于确认加密货币账户的私钥和公钥。电子装置可以使用基于比特币改进建议(BIP)-32标准的算法来生成私钥和公钥。例如,在BIP-32标准中,从同一根种子导出的私钥和公钥可以总是以相同的方式生成。BIP-44标准定义了实现BIP-32标准的方案,并提出了5级分层确定性(HD)路径作为从根种子导出和获得私钥和公钥的方法。当相同的HD路径与相同的根种子一起使用时,理论上可以导出或获得所有的公钥。实现上述技术并确认加密货币账户被称为HD钱包。例如,钱包可被分类为非确定性钱包或确定性钱包。HD钱包已经被开发成在单个种子中生成各种密钥。HD钱包具有如树形结构生成的密钥。HD钱包可以以树形结构从父密钥生成子密钥,并且可以从子密钥生成孙密钥。理论上可以以这种方式无限制地生成密钥。可以使用HD钱包生成多个密钥,并且可以管理和使用各种区块链地址。根种子是能够从其中生成许多密钥和地址的缺省值。电子装置可以恢复属于整个HD钱包的密钥。电子装置可以使用助记单词序列来生成根种子。例如,为了生成根种子,电子装置可以从通过HMAC-SHA512函数生成的散列值中生成主私钥和主链码。根据实施例的电子装置可以使用512位散列值左边的256位作为私钥,并且可以使用512位散列值右边的256位作为链码。电子装置可以使用椭圆曲线函数从私钥获得公钥。电子装置可以使用根种子生成私钥和公钥,并且

可以使用公钥生成区块链地址。因为理论上很难复制和生成区块链地址,所以个人可以唯一地使用区块链地址。

[0114] 在图6的操作650中,电子装置(例如,处理器210)可以将第一区块链地址和第一信息中的至少一个与签名数据相关联并存储。根据本公开的实施例,将第一区块链地址和第一信息与签名数据相关联并存储的操作可以包括以数据库中包括的表格的形式将第一区块链地址、第一信息或签名数据存储于电子装置中包括的存储区域或可信存储区域中的操作。根据本公开的实施例,当访问第一区块链地址、第一信息或签名数据时,电子装置可以通过数据库获得信息。

[0115] 图7是示出根据本公开实施例的用于请求用户认证区块链地址的画面的示意图。

[0116] 参考图7,电子装置可以利用运行着联系人应用的画面700从用户接收针对区块链地址认证请求的用户输入。根据本公开的实施例,联系人应用不限于联系人,其通常可以包括能够显示区块链地址或第一信息的应用。例如,运行着联系人应用的画面700可以包括第一信息710和区块链地址720。根据本公开的实施例,运行着联系人应用的画面700还可以包括指示与区块链地址720相关联的区块链平台的信息730(例如,加密货币信息)、验证按钮740和用于与电子装置外部共享的共享按钮。依据将要使用区块链地址的区块链网络的类型,表示区块链平台的信息730可以是与区块链平台的名称(例如,Ethereum、Bitcoin等)相关联的信息。例如,对于Ethereum,可以显示Ethereum的加密货币单位ETH或与Ethereum相关联的图像(例如,象征Ethereum的标记)。当用户选择验证按钮740时,电子装置可以对第一信息710和区块链地址720执行区块链地址认证过程。根据本公开的实施例,区块链地址认证过程可以包括例如图6的操作620至650或图16的操作1064至1614。此外,当用户输入选择了共享按钮750时,电子装置可以向另一装置(例如,图1的外部电子装置102或外部电子装置104)发送在运行着联系人应用的画面700中包括的至少一些信息。根据本公开的实施例,区块链地址认证过程可以包括向外部设备(例如,区块链地址认证服务器)发送区块链地址信息并由外部设备执行认证的操作。根据本公开的实施例,区块链地址认证过程可以包括向电子装置外部的电子装置发送区块链地址信息并由外部电子装置执行认证的操作。

[0117] 图8是示出根据本公开实施例的用于共享区块链地址的画面的示意图。

[0118] 参照图8,电子装置可以显示包括区块链地址共享设置项811的联系人共享功能设置列表810。当根据对区块链地址共享设置项目811的用户输入选择联系人共享功能时,电子装置可以确定是否共享区块链地址。根据本公开的实施例,接收从启用了区块链地址共享功能的电子装置共享的联系人电子装置可以存储区块链地址以及联系人信息,并且可以显示联系人信息画面820,该联系人信息画面820显示区块链地址以及联系人信息。根据本公开的实施例,电子装置可以与显示在联系人信息画面820上的至少一个联系人共享关于区块链地址的信息,该联系人信息画面820被显示为共享区块链地址。根据本公开的实施例,当共享关于区块链地址的信息时,电子装置可以使用对应于相应联系人的电话号码、电子邮件、MAC地址、消息、NFC或蓝牙来发送关于区块链地址的信息。

[0119] 图9是示出根据本公开实施例的用于请求认证区块链地址的画面的示意图。

[0120] 参考图9,电子装置可以在区块链交易过程中接收区块链地址认证请求。例如,电子装置可以执行利用Ethereum向昵称Jane发送特定加密货币(例如,0.0103Ethereum)的交

易。在此情况下,电子装置可以认证接收加密货币的昵称Jane的区块链地址。根据本公开的实施例,电子装置可以显示交易信息输入画面910,用于输入生成区块链交易的信息。电子装置可以通过交易信息输入画面910接收区块链地址和第一信息911。交易信息输入画面910可以包括验证按钮912。当用户输入选择了验证按钮912时,电子装置可以根据区块链地址认证请求来执行处理,以显示信息确认画面920。根据本公开的实施例,信息确认画面920可以由在可信执行环境中执行的可信用户界面应用来执行。可信执行环境可以包括例如可信操作系统。为了加强安全性,可信执行环境可以包括需要单独的操作系统或功能来访问单独的可信存储器(例如,逻辑和物理可信存储器区域(信任区))的环境。可信执行环境可以包括这样的环境,其中电子装置将需要安全性的数据存储在物理上划分的存储器或逻辑上划分的存储器区域中,并限制仅通过单独的可信操作系统或功能来访问数据。当包括在信息确认画面920中的确认按钮921被选择时,电子装置可以将区块链地址与第一信息相关联并存储。

[0121] 根据本公开的实施例,电子装置可以通过区块链网络确认与区块链地址相关联的有效性。例如,当用户试图为区块链交易生成交易或者从先前的区块链地址簿中获取区块链地址列表时,电子装置可以通过区块链网络获得关于区块链地址的有效性信息。例如,当用于确定区块链地址有效性的单独的应用编程界面(API)被包括在区块链网络中时,电子装置可以通过远程过程调用(RPC)的API请求区块链网络以确定区块链地址的有效性。电子装置可以分析通过区块链网络(例如,MAIN NET)获得的信息,并且可以根据分析的信息向用户提供第二信息或第三信息。例如,电子装置或外部服务器可以通过区块链网络收集关于区块链地址的信息,并且可以基于所收集的信息存储关于区块链地址的第二信息或第三信息。根据本公开的实施例,区块链网络可以存储对应于区块链地址的交易信息,并且可以将交易信息提供给Java脚本对象符号(JSON)RPC格式API。web应用中的Java脚本代码可以使用JSON在web上递送信息。当使用JSON对象时,JSON对象可以包括一个数字、一个字符串和序列值。例如,JSON RPC对象可以用作基于Ethereum的各种应用发送和接收信息的对象。JSON可以是使用文本来递送数据对象的开放标准格式,RPC可以包括用于对等(P2P)网络之间的数据发送和接收的协议。例如,Ethereum可以基于JSON RPC在钱包中执行Ethereum网络之间的请求和接收。例如,对于Ethereum网络,电子装置可以通过ethGetTransactionCount(区块链地址,param)函数来确认与区块链地址相对应的交易内容。根据本公开的实施例,电子装置认证区块链地址的操作可以包括提供从区块链主网或外部服务器提供的附加信息以及向用户提供基于附加信息确定的各种用户界面的操作。

[0122] 图10是示出根据本公开实施例的用于将区块链地址映射到联系人信息的画面的示意图。

[0123] 参考图10,电子装置可以基于显示区块链交易历史的交易历史画面1010接收区块链地址认证请求。根据本公开的实施例,电子装置可以显示包括区块链地址1011和验证按钮1012的交易历史画面1010。当接收到来自在交易历史画面1010上确认区块链地址1011的用户的选择验证按钮1012的输入时,电子装置可以显示联系人信息列表画面1020,用于选择要与区块链地址1011相关联并存储的联系人信息。联系人信息列表画面1020可以包括例如存储在联系人存储器中的联系人列表。替代地,又例如,联系人信息列表画面1020可以包括基于输入到电子装置的关键字检索的联系人列表。根据本公开的实施例,为了配置联系

人信息列表画面1020,电子装置可以显示由电子装置的应用使用的联系人存储器中存储的联系人信息。根据本公开的实施例,电子装置可以过滤存储在联系人存储器中的联系人信息中能够与区块链地址相关联的信息,并且可以输出联系人列表,过滤的联系人信息首先显示在该联系人列表上。根据本公开的实施例,当提供联系人信息列表画面1020时,电子装置可以从外部获得与联系人信息相关联的数据,以生成联系人信息列表。根据图10所示的实施例,电子装置可以接收输入关键字“Jane”的用户输入,以将区块链地址映射到联系人信息。电子装置可以输出从存储在联系人存储器中的信息中检索输入的关键词“Jane”的结果。当在联系人信息列表画面1020上选择联系人信息时,电子装置可以根据区块链地址认证请求执行处理。

[0124] 图11是示出根据本公开实施例的用于将区块链地址映射到通行证信息的画面的示意图。

[0125] 参考图11,电子装置可以显示包括联系人信息1111、区块链地址1112和用户界面对象1113的画面1110。

[0126] 电子装置可以通过用户界面对象1113从确认联系人信息1111和区块链地址1112的用户接收批准命令。根据本公开的实施例,批准命令可以指示用户验证出区块链地址和第一信息相互映射,并且可以指请求将区块链地址1112与第一信息相关联并存储的用户输入。

[0127] 又例如,当第一信息包括通行证名称1121和通行证符号1122(通行证信息)时,电子装置可以显示包括通行证名称1121、通行证符号1122、智能联系人地址1123和用户界面对象1124的画面1120。电子装置可以通过用户界面对象1124从确认通行证名称1121、通行证符号1122和区块链地址1112的用户接收批准命令。

[0128] 图12是示出根据本公开的实施例的显示为使得用户认证区块链地址的画面的示意图。

[0129] 参考图12,电子装置可以向用户显示第一区块链地址和第一信息,并且可以接收批准映射两条信息的输入。在此情况下,为了接收批准映射两条信息的输入,电子装置可以输出请求批准的消息,并且可以使用个人标识号(PIN)或生物特征认证来认证用户。例如,电子装置可以显示包括用于接收PIN的PIN输入项1211的画面1210。电子装置可以基于输入的PIN来验证用户。又例如,电子装置可以从用户接收生物特征信息(例如,指纹信息、虹膜信息等)。根据本公开的实施例,电子装置可以显示包括向用户请求指纹输入的对象1221的画面1220。根据本公开的实施例,电子装置可以通过用户的指纹输入来执行认证。当用户的认证完成时,电子装置可以将区块链信息与第一信息相关联并存储。

[0130] 图13是示出根据本公开实施例的将区块链地址与第一信息相关联并存储的映射表1300的示意图。

[0131] 参考图13,电子装置可以将至少一个区块链地址1310与第一信息1320相关联并存储,该第一信息1320包括联系人信息(例如,联系人的昵称)和通过使用用户的私钥执行签名而获得的签名数据1330中的至少一个。

[0132] 图14是图示了根据本公开实施例的电子装置将区块链地址与另一信息相关联并存储的示意图1400。

[0133] 参考图14,电子装置可以将区块链地址1410与包括通行证名称1422和通行证符号1424

以及签名数据1430的通证信息相关联并存储。

[0134] 图15是示出根据本公开实施例的由电子装置操作的富执行环境(REE)和可信执行环境(TEE)的示意图。

[0135] 参考图15,电子装置1500的存储器可以虚拟地与由通常包括在电子装置中的操作系统运行的富用户应用可访问的REE分离,并且可以与仅由特别授权的软件模块可访问的TEE分离。根据本公开的实施例,特别授权的软件模块可以在TEE中运行。根据本公开的实施例,电子装置可以通过基于硬件的安全系统来控制对TEE的访问。例如,电子装置的存储器可以包括用户通常可访问的区域(REE)和虚拟实现的信任区(TEE)。根据本公开的实施例,可信内核可以是包括在富操作系统中的内核,但是单独具有增强的安全性。富操作系统可以以这样的方式实现,即向可信内核递送消息,并将可信内核基于递送的消息执行的结果递送给富操作系统。根据本公开的实施例,为了加强安全性,可信内核仅可由验证过的消息或允许的消息访问。根据本公开的实施例,可信操作系统或可信内核可以是安全性被单独加强的操作系统,其不同于富操作系统。

[0136] 电子装置1500可以运行具有多个安全级别的执行环境。

[0137] 多个执行环境可以包括例如REE 1510和TEE 1520。REE 1510可以是具有第一安全级别的第一执行环境。TEE 1520可以是具有与第一安全级别不同的(例如,更高)第二安全级别的第二执行环境。根据本公开的另一实施例,电子装置1500可以包括但不限于具有第三安全级别的附加的另一执行环境(例如,第三执行环境)。

[0138] 电子装置1500可以将操作系统(OS)划分成REE 1510和TEE 1520并运行。REE 1510可以由富OS(例如,不安全的OS)运行。TEE 1520可以由可信OS运行。例如,富操作系统可以是Android™ OS。例如,可信操作系统可以是Teegris™、QSEE™或Trustzone。可信OS可以独立于富OS,并且可以基于单独的资源运行,该单独的资源被配置为未授权的程序或应用不能访问的环境。

[0139] 根据本公开的实施例,TEE 1520中的电子装置1500可以基于在可信OS基础上运行的可信应用(TA)来加密数据。根据本公开的实施例,TEE 1520中的电子装置1500可以使用与不可信存储区域分离的单独的可信存储区域(例如,安全元件(SE)、eSE或eSIM)空间来执行加密以存储加密的信息,并且可以使得富OS和富应用(例如,数字钱包应用1512或用户应用(例如,联系人管理应用、金融应用、社交网络应用、消息应用、电子邮件应用等)1514或区块链应用1516)运行在富OS上,以不直接访问TEE 1520来安全地保护数据。TEE 1520中的电子装置1500不能通过在REE 1510上运行的应用直接加密和解密存储在TEE 1520中的数据。根据本公开的实施例,访问存储在TEE 1520中的数据的权利可以仅由在TEE 1520上运行的单独授权的应用来允许。

[0140] 电子装置1500可以在安全的TEE 1520中存储需要相对高的安全级别的数据,并且可以执行与该数据相关联的操作。根据本公开的实施例,TEE 1520可以基于在电子装置1500中提供的应用处理器(例如,图1的处理器120或图2的处理器210)上运行的富OS来操作,该富OS基于在制造电子装置1500的过程中确定的可靠硬件结构运行。例如,电子装置可以在制造电子装置的阶段使用硬件随机数生成器生成设备唯一硬件密钥(DUHK)。当基于唯一的硬件密钥将数据绑定到特定设备时,电子装置可以仅允许硬件加密模块访问电子装置。因此,可以增强电子装置的安全性。根据本公开的实施例,电子装置可以仅在TEE中使用

硬件密钥,其安全性得到加强。根据本公开的实施例,在电子装置的TEE上运行的特别授权的可信软件可以使用硬件密钥将数据存储存储在TEE中。

[0141] 根据本公开的另一实施例,TEE 1520可以是可由电子装置1500的应用处理器运行的可信OS访问的存储区域。需要安全的软件或硬件可以通过TEE 1520运行。根据本公开的实施例,电子装置1500可以通过硬件的物理分离或软件的逻辑分离来操作TEE 1520。例如,电子装置1500可以使用与不可信存储区域分离的单独的硬件存储器来配置TEE 1520。

[0142] 根据本公开的实施例,TEE 1520可以通过硬件约束与REE 1510分离。根据本公开的实施例,当REE 1510和TEE 1520通过硬件约束彼此分离时,TEE 1520可以被构造在单独的存储器中。根据本公开的实施例,TEE 1520可以是在处理器的至少一部分中实现的存储区域。根据本公开的实施例,TEE可以被构建在电子装置的外部存储器中,并且可以被配置为当与电子装置电连接或可操作地连接时,在电子装置中是可访问的。根据本公开的实施例,外部存储器可以包括可电连接到电子装置的SIM卡中包括的至少部分存储器。根据另一实施例,TEE 1520可以在逻辑上与REE 1510分离,以在相同的硬件(例如,存储器)上操作。根据本公开的实施例,电子装置可以在逻辑上将包括在电子装置中的物理存储器的至少一部分分类为不信任区(如REE),并且可以将物理存储器的至少另一个分类为信任区(TEE),以使用不信任区和信任区。

[0143] 在REE 1510上运行的至少一个应用(例如,数字钱包应用1512)可以使用被允许访问TEE 1520的API向在TEE 1520上运行的特别授权的软件递送数据或消息,或者可以接收与该消息相对应的响应。

[0144] 根据本公开的实施例,电子装置1500可以在REE 1510中运行数字钱包应用1512、用户应用1514和区块链应用1516。此外,电子装置1500可以在TEE 1520中运行各种软件。例如,电子装置1500可以运行可信用户界面应用1522和区块链可信应用1524。此外,电子装置1500可以具有有可在REE 1510中运行的应用访问的存储器(例如,联系人存储器1518)。

[0145] 根据本公开的实施例,电子装置1500可以将联系人信息存储在联系人存储器1518中,该联系人存储器1518使用电子装置1500中的存储器的一部分(例如,REE)来配置。联系人存储器1518可以是基于与联系人相关联的信息在电子装置1500中配置的数据库。这里,图15的联系人存储器1518可以利用存储了由电子装置1500的用户应用1514使用的数据的另一个数据库来代替。

[0146] 例如,电子装置1500可以运行用户应用1514,以将用户输入的联系人信息存储在联系人存储器1518中。又例如,存储在联系人存储器1518中的联系人信息可以是与存储在联系人服务器1540中的信息同步的信息。可以省略联系人服务器1540。

[0147] 根据本公开的实施例,用户应用1514可以是管理存储在联系人存储器1518中的联系人信息的地址簿应用。联系人管理应用可以被实现为各种类型的应用,诸如简单的地址簿管理应用、即时信使或社交媒体应用。

[0148] 根据本公开的实施例,数字钱包应用1512可以管理与用户的区块链地址相对应的私钥。此外,数字钱包应用1512可以管理在TEE 1520上运行的可信应用(例如,可信用户界面(TUI)应用1522或区块链可信应用(TA) 1524)。

[0149] 数字钱包应用1512可以接收区块链地址认证请求。例如,数字钱包应用1512可以接收对由用户应用1514显示的区块链地址和第一信息的区块链地址认证请求。根据本发明

的实施例,数字钱包应用1512可允许用户确认区块链地址和第一信息,且可允许电子装置1500显示用于接收将区块链地址映射到第一信息(例如,联系人信息)的批准命令的画面。为了在保持安全的环境中显示区块链地址和第一信息,数字钱包应用1512可以使用TUI应用1522显示区块链地址和第一信息。此外,为了安全地接收与区块链地址和第一信息相关联的用户输入,电子装置1500可以通过TUI应用1522接收用户输入。例如,电子装置1500可以通过TUI应用1522接收用于认证用户的认证信息(例如,PIN、指纹信息或虹膜信息),以批准将区块链地址映射到第一信息。接收到对区块链地址和第一信息的批准命令后,TUI应用1522可以将批准命令递送给数字钱包应用1512。

[0150] 接收到批准命令后,数字钱包应用1512可以向区块链TA 1524递送对区块链地址和第一信息的签名请求。区块链TA 1524可以基于用户的私钥对区块链地址和第一信息执行数字签名。区块链TA 1524可以将作为执行数字签名的结果而生成的签名数据递送给数字钱包应用1512。接收到签名数据后,数字钱包应用1512可以通过用户应用1514将第一信息、区块链地址和签名数据相关联并存储在联系人存储器1518中。

[0151] 区块链应用1516可以允许电子装置1500连接到建立区块链网络的区块链节点1530。此外,区块链应用1516可以写入要由电子装置1500发送到区块链网络的区块链交易数据。区块链应用1516可以向数字钱包应用1512递送包括所写入的区块链交易数据的签名请求。数字钱包应用1512可以从签名请求中获得和/或解析区块链交易的原始数据。数字钱包应用1512可以通过TUI应用1522显示包括在区块链交易数据中的交易记录。这里,数字钱包应用1512可以基于包括在区块链交易数据中的第二区块链地址(例如,接收者的区块链地址)来检索存储在联系人存储器1518中的信息。当联系人存储器中存在与第二区块链地址相匹配的区块链地址(第一区块链地址)时,电子装置可以将与区块链地址相关联的信息(第一信息、第二信息和签名数据)发送到TEE区,以通过TUI应用来显示。这里,电子装置可以使用基于TEE接收到的信息来确认数字签名是否有效。例如,电子装置可以使用私钥解密接收到的信息中由用户数字签名的值,并且可以将解密的值与接收到的第一信息和第一区块链地址值进行比较,以确认数字签名是否有效。根据本公开的实施例,当使用存储在TEE中的私钥来验证从REE递送到TEE的信息的数字签名的有效性时,电子装置可以向用户提供通过TUI应用1522接收到的信息(例如,第一区块链地址、第一信息或第二信息)以及包括在区块链交易数据中的交易记录。例如,当包括在区块链交易数据中的第二区块链地址与第一区块链地址相同时,数字钱包应用1512可以通过TUI应用1522显示与第一区块链地址相关联并存储的第一信息(例如,“Jane”)。

[0152] TUI应用1522可以从确认所显示信息的用户接收用于批准交易的附加输入。根据本公开的实施例,TUI应用1522可以通过生物特征认证(例如,指纹认证)可信应用1526来另外地执行生物特征认证。

[0153] TUI应用1522可以向数字钱包应用1512递送批准交易的输入。

[0154] 接收到批准交易的输入后,数字钱包应用1512可将第二区块链地址、区块链交易数据、基于第二区块链地址检索到的第一信息以及包括签名数据的签名请求递送给区块链TA 1524。区块链TA 1524可以确定第一区块链地址和第二区块链地址是否彼此相同。当第一区块链地址和第二区块链地址彼此不不同时,区块链TA 1524可能无法执行数字签名。区块链TA 1524可以对第二区块链地址和第一信息执行数字签名,并且可以将执行数字签名

的结果与从数字签名应用1512接收到的签名数据进行比较。当比较的结果是两个数据彼此不相同,因为存在存储在联系存储器1518中的数据将被外部攻击改变的可能性,所以区块链TA 1524可以向数字签名应用1512递送错误消息,而不对区块链交易数据执行数字签名。当对第二区块链地址和第一信息执行数字签名的结果与签名数据相同时,区块链TA 1524可以对区块链交易数据执行数字签名,并且可以将数字签名的区块链交易数据递送给数字签名应用1512。数字钱包应用1512可以通过区块链应用1516将数字签名的数据发送到区块链网络,从而执行交易。

[0155] 根据本公开的另一实施例,当与区块链地址相关联并存储的第一信息包括通行证信息时,图15的用户应用1514可以用通行证信息管理应用来替换。在此情况下,第一信息、区块链地址和签名数据可以被存储在存储器(例如,图1的存储器130)中的存储了通行证信息的通行证信息存储区域中。

[0156] 图16是示出根据本公开的实施例的电子装置将区块链地址与签名数据相关联并存储的过程的流程图1600。

[0157] 参考图16,在操作1601中,电子装置(例如,处理器120)可以通过联系人管理应用来存储第一信息。此外,在操作1602中,用户应用1514可以依据数字钱包应用1512的请求将第一信息递送给数字钱包应用1512。此外,根据本公开的实施例,在操作1602中,数字钱包应用1512可以接收第一信息以及区块链地址。或者,根据本公开的另一实施例,数字钱包应用1512可以通过正在运行数字钱包应用1512的画面接收将与第一信息相关联并存储的区块链地址。根据本公开的另一实施例,当数字钱包应用1512有权访问联系人存储器1518时,其可以直接获得第一信息。

[0158] 在操作1604中,数字钱包应用1512可以依据对数字钱包应用1512的用户输入来生成区块链地址认证请求,或者可以接收由另一个应用(例如,用户应用1514)生成的区块链地址认证请求。

[0159] 响应于区块链地址认证请求,在操作1606中,数字钱包应用1512可以将第一信息和区块链地址递送给TUI应用1522。在操作1608中,TUI应用1522可以在显示器上显示第一信息和区块链地址。在操作1609中,可信用户界面应用1522可以从用户接收将第一信息映射到区块链地址的批准命令。响应于批准命令,在操作1610中,TUI应用1522可以向区块链TA 1524递送对第一信息和区块链地址的签名请求。根据本公开的实施例,TUI应用1522可以通过数字钱包应用1512向区块链TA 1524递送签名请求。例如,TUI应用1522可以将针对所接收的批准命令的信息或消息递送给数字钱包应用1512,并且可以将针对区块链地址的签名请求和第一信息递送给区块链TA1524。

[0160] 在操作1612,响应于签名请求,区块链TA 1524可基于用户的私钥对区块链地址和第一信息执行数字签名,以生成签名数据。根据本公开的实施例,区块链TA 1524可以在执行数字签名之前执行用于认证用户的用户认证过程(例如,生物特征认证)。在操作1614中,区块链TA 1524可以将生成的签名数据递送给数字钱包应用1512(或用户应用1514)。接收到签名数据,数字钱包应用1512可以将签名数据与区块链地址和第一信息相关联并存储。根据本公开的实施例,数字钱包应用1512可以进一步存储表示区块链地址与第一信息之间的链接的可靠性的第二信息。

[0161] 根据本公开的实施例,区块链TA 1524可以将生成的签名数据、区块链地址或第一

信息中的至少一个存储在由区块链TA 1524运行的操作系统(例如,第二操作系统或可信操作系统)管理的存储区域中。根据本公开的实施例,区块链TA 1524可以将表示区块链地址与第一信息之间的链路的可靠性的第二信息存储在由区块链TA 1524运行的操作系统管理的存储区域(例如,TEE)中。

[0162] 图17是示出根据本公开的实施例的电子装置对区块链交易数据执行数字签名的过程的流程图1700。

[0163] 参考图17,在操作1710中,电子装置(例如,处理器120)可以生成或接收包括第二区块链地址的区块链交易数据。电子装置可以从交易数据中获得第二区块链地址。在操作1720中,电子装置可以基于第二区块链地址获得第一信息和签名数据。例如,电子装置可以基于第二区块链地址来确认与第二区块链地址相同的第一区块链地址是否存储在存储装置中。当确认了与第二区块链地址匹配的第一区块链地址时,电子装置可以检索与第一区块链地址相关联并存储的信息(例如,第一信息、数字签名值和第二信息)。例如,电子装置可以检索与第二区块链地址相关联并存储的数据。

[0164] 在操作1730中,电子装置可以基于私钥对第二区块链地址和第一信息执行数字签名。在操作1740中,电子装置可以将数字签名的值与在操作1720中获得的签名数据进行比较。当通过对第二区块链地址和第一信息执行数字签名获得的值与在操作1720中获得的签名数据不相同,在操作1755中,电子装置可显示表示数字签名没有正常执行的错误画面。根据本公开的另一实施例,电子装置可使用公钥对在操作1720中获得的签名数据进行解密。电子装置可以将解密的签名数据与第二区块链地址和第一信息进行比较,以验证数字签名值的有效性。

[0165] 当通过对第二区块链地址和第一信息执行数字签名获得的值与在操作1720获得的签名数据相同时,在操作1750中,电子装置可显示包括第一信息和关于交易数据中包括的交易记录的信息的交易内容画面。

[0166] 在操作1760中,电子装置可使用交易内容画面上的第一信息来确认交易目标,并可从确认用于交易目标的交易记录的用户来接收批准交易内容的用户输入。当接收到批准交易内容的用户输入时,在操作1770中,电子装置可以对区块链交易数据执行数字签名。电子装置可以将与区块链交易数据相对应的交易递送到区块链网络,以作为区块生成。

[0167] 图18是示出根据本公开实施例的基于存储在电子装置中的第一信息对区块链交易数据执行数字签名的过程的流程图1800。

[0168] 参照图18,在操作1801中,用户应用1514可将第一信息与第一区块链地址和用于第一区块链地址和第一信息的签名数据相关联并存储。例如,在执行图16所示的过程之后,用户应用1514可以依据数字钱包应用1512的请求,将第一信息与第一区块链地址和用于第一区块链地址和第一信息的签名数据相关联并存储。在操作1802中,区块链应用1516可以生成包括第二区块链地址的区块链交易数据。区块链应用1516可以发送通过与区块链网络交互产生的区块链交易数据。区块链应用1516可以与配置区块链网络的节点交互工作以生成交易。区块链应用1516可以是请求数字钱包执行交易签名的应用。根据本公开的实施例,区块链应用1516可以根据区块链的类型(例如,Ethereum、Bitcoin等)单独运行。例如,区块链应用1516可以生成用于处理向第二区块链地址汇款的区块链交易数据。在操作1804中,区块链应用1516可以向数字钱包应用1512请求用于区块链交易数据的签名。例如,区块链

应用1516可以将签名所需的数据递送给数字钱包应用1512,以生成区块链交易。在操作1806中,数字钱包应用1512可基于包括在区块链交易数据中的第二区块链地址向用户应用1514递送检索第一信息和签名数据的请求。根据本公开的实施例,数字钱包应用1512可以直接访问电子装置的数据以检索第一信息和签名数据。例如,当数字钱包应用1512有权访问电子装置的存储器时,其可以从存储的数据中确认与区块链地址相关联的第一信息和签名数据。

[0169] 当第二区块链地址与第一区块链地址相同时,在操作1808中,用户应用1514可以将与第一区块链地址相关联并存储的第一信息和签名数据递送给数字钱包应用1512。根据本公开的另一实施例,当用户应用1514在操作1808中将第一区块链地址相关联并存储的第一信息和签名数据递送给数字钱包应用1512时,数字钱包应用1512可以确定第二区块链地址是否与第一区块链地址相同。当第二区块链地址与第一区块链地址相同时,数字钱包应用1512可以执行操作1810。

[0170] 在操作1810中,数字钱包应用1512可以将对区块链交易数据的签名请求、第一信息和签名数据递送给区块链TA 1524。在操作1812中,区块链TA1524可以对区块链地址(第一区块链地址或第二区块链地址)和第一信息执行数字签名。在操作1813中,区块链TA 1524可以将作为执行数字签名的结果而生成的值与接收到的签名数据进行比较。

[0171] 当作为比较的结果,两个数据彼此相同时,在操作1814中,区块链TA 1524可以将对应于签名请求和第一信息的交易记录递送给TUI应用1522。对应于签名请求的交易记录可以是包括在请求签名的区块链交易数据中的交易记录。根据本公开的实施例,包括在区块链交易数据中的交易记录可以包括当产生区块链交易时能够使用的接收者的区块链地址、发送者的区块链地址、要交易的加密货币的类型或发送的加密货币的数额中的至少一个。根据本公开的实施例,区块链TA 1524可以通过数字钱包应用1512向TUI应用1522递送交易记录和第一信息。

[0172] 在操作1816中,TUI应用1522可以在显示器上输出包括交易记录和第一信息的交易内容画面。TUI应用1522可以接收批准与交易内容画面相对应的交易数据的签名的用户输入。根据本公开的实施例,TUI应用1522可以在接收批准用户输入的过程中执行接收用于认证用户的认证信息的用户认证过程(例如,生物特征认证、个人身份号码(PIN)等),该用户输入批准签名。用户认证过程可以包括例如输出图12所示的画面的操作、接收用于认证用户的认证信息的操作以及将输入的认证信息与用于用户注册的信息进行比较的操作。

[0173] 在操作1818中,响应于批准交易数据的签名的用户输入,TUI应用1522可以向区块链TA 1524递送继续进行针对交易数据的数字签名的请求。在操作1820中,区块链TA 1524可以基于用于区块链交易的用户的私钥对区块链交易数据执行数字签名。

[0174] 当在操作1822中数字签名的区块链交易数据被递送到数字钱包应用1512时,在操作1824中,数字钱包应用1512可以通过区块链应用1516将数字签名的区块链交易数据递送到区块链网络。

[0175] 图19是示出了根据本公开实施例的电子装置获得和存储通证信息的过程的示意图。

[0176] 根据本公开的实施例,电子装置可以从通证信息提供网络接收由通证信息提供系统验证了的多个通证信息。电子装置可以接收多个通证信息,并且可以通过一系列过程来认证多个通证信息。

[0177] 参考图19,电子装置可以显示包括用于接收经验证的通证信息的菜单项1912的功能画面1910。当用户选择用于接收经验证的通证信息的菜单项1912时,电子装置可以显示包括可接收的通证信息列表1922的通证列表画面1920。

[0178] 根据本公开的实施例,电子装置可以经由电子装置的通信电路向通证信息提供网络发送通证地址,以从通证信息提供网络获得通证信息。电子装置可以响应于所发送的通证地址获得通证信息(例如,通证名称或通证图标)。

[0179] 根据本公开的实施例,电子装置可以允许用户通过画面1931和1932顺序地认证每个通证信息,画面1931和1932顺序地显示关于从通证信息列表1922中选择出的通证的通证信息。

[0180] 例如,电子装置可以从外部获得与区块链地址相对应的通证信息,并且可以输出显示获得的通证信息的通证信息列表1922。电子装置可以接收选择在通证信息列表1922上的被映射到区块链地址的通证的用户输入。当基于用户输入选择通证时,电子装置可以通过画面1931和1932从用户接收顺序地认证每个通证信息的用户输入。当接收到认证通证信息的用户输入时,通证信息可以是要被映射到区块链地址和被存储的第一信息。这里,图19是,但不限于,用于描述实施例的示例。例如,电子装置可以在一个画面上显示所有的通证信息。又例如,电子装置可以根据用户的滚动输入来移动画面,使得用户确认每个通证信息。

[0181] 图20是示出根据本公开的实施例的电子装置基于异构操作系统输出区块链地址和第一信息的过程的流程图2000。

[0182] 参考图20,在操作2010中,电子装置可以基于第一操作系统(例如,富操作系统)接收区块链地址认证请求。例如,电子装置可以通过数字钱包应用或另一用户应用(例如,联系人应用)接收选择用于区块链地址和第一信息的验证按钮的用户输入。

[0183] 在操作2020中,响应于区块链地址认证请求,电子装置可以将与区块链地址认证请求相对应的区块链地址、第一信息和签名数据递送给第二操作系统(例如,可信操作系统)。

[0184] 在操作2030中,基于第二操作系统,电子装置可确定存储在第二操作系统中的区块链地址是否与在操作2020从第一操作系统发送的区块链地址相同。因为区块链地址是唯一的,所以电子装置可以使用区块链地址作为签名数据的索引。根据本公开的实施例,电子装置可以在由第二操作系统管理的存储器区域(例如,TEE)中存储认证的地址,并且可以限制对存储的地址的访问。例如,当用户认证图16中的区块链地址时,电子装置可以将认证的区块链数据、签名数据或第一信息中的至少一个存储在由第二操作系统管理的存储区域中。根据本公开的实施例,由第二操作系统管理的存储区域可以是电子装置中的区域,并且可以存储在电子装置外部的具有增强安全性的独立存储器中。根据本公开的实施例,由第二操作系统管理的存储器区域可以包括外部服务器。例如,电子装置可以将根据图16中的用户认证而认证的第一信息、区块链地址或签名数据中的至少一个发送到第三服务器,以通过第三服务器存储。

[0185] 当在操作2020中存储在第二操作系统中的区块链地址与在操作2030中从第一操作系统发送的区块链地址相同时,在操作2040中,电子装置可验证数字签名。例如,电子装置可以基于私钥对区块链地址和第一信息进行数字签名,并且可以将数字签名的值与在操

作2020中发送的签名数据进行比较。当作为比较的结果,数字签名的值与签名数据匹配时,电子装置可以确定数字签名有效。

[0186] 当验证数字签名有效时,在操作2050,电子装置可以基于第二操作系统在其显示器上显示区块链地址和第一信息。例如,电子装置可以在显示区块链地址的交易(例如,加密货币汇款)记录的画面上显示区块链地址和第一信息。根据本公开的实施例,电子装置还可以显示表示区块链地址和第一信息的可靠性的第二信息。

[0187] 图21是示出根据本公开实施例的电子装置中包括的应用、操作系统和内核的结构的框图。

[0188] 参考图21,根据实施例的电子装置可以被配置为包括富操作系统2110、应用2115、可信操作系统2120、可信应用2125和内核2130。

[0189] 应用2115可以基于富操作系统2110运行,并且可以基于可信应用2125应用。富操作系统2110和可信操作系统2120可以基于内核2130运行。例如,富操作系统2110和可信操作系统2120可以通过内核2130被分配应用2115或可信应用2125的运行所需的资源。

[0190] 图22是示出根据本公开实施例的使用电子装置配置的数字钱包的结构的示意图。

[0191] 根据本公开的实施例,电子装置可以包括基于富操作系统运行的数字钱包2210和可信操作系统2240。

[0192] 参照图22,根据实施例的数字钱包2210可以包括用户界面2211、状态控制器2216、供应管理器2217、交易编码器2219、区块链可信应用连接器2221、可信用户界面(UI)连接器2223和生物特征认证管理器2225。根据本公开的实施例,用户界面2211可以包括用于显示或处理用户的区块链交易所需的信息的模块(余额2212、交易2213、交换2214和设置2215)。

[0193] 根据本公开的实施例,状态控制器2216可以包括管理在电子装置中执行区块链交易的过程的最上层应用。状态控制器2216可以根据经由用户界面2211接收的请求(例如,种子的生成、种子的恢复或数字签名)来加载或卸载一个或多个可信应用。状态控制器2216可以将执行经由用户界面2211接收的请求的详细命令递送给可信应用。

[0194] 供应管理器2217可以在运行与数字钱包2210相关联的应用时执行完整性测试。例如,在执行用户注册过程的过程中(例如,关于条款和条件的协议或条款和条件的交换),供应管理器2217可以执行使用户执行指纹注册或PIN注册的操作。或者,当与区块链交易相关联的种子没有被存储时,供应管理器2217可以使电子装置输出种子生成画面。此外,供应管理器2217可以确定软件版本,并且可以更新软件。交易编码器2219可以管理区块链交易。交易编码器2219可以将未签名的交易数据转换成数字签名的交易数据。交易编码器2219可以生成封装有一个字节列的交易数据,以在区块链节点中接收。当数字签名由可信应用执行时,交易编码器2219可以根据区块链协议使用未被数字签名的交易数据、签名值和附加参数来封装数据。

[0195] 区块链可信应用连接器2221可以为数字钱包2210的区块链可信应用2241执行通信。可信UI连接器2223可以与可信UI可信应用2242通信。可信应用连接器(例如,区块链可信应用连接器2221或可信UI连接器2223)可以是对应于在可信操作系统2240中执行的可信应用的模块。可信应用连接器可以串行化或解串行化要递送给可信应用的命令。可信应用连接器可以接收执行递送给可信应用的命令的结果,并且可以将接收到的结果递送给可信应用连接器的更高模型。

[0196] 生物特征认证管理器2225可以与生物特征可信应用2243通信以执行生物特征认证。生物特征认证管理器2225可以向电子装置的生物特征认证服务递送认证请求。生物特征认证管理器2225可以将执行生物特征认证的结果递送给更高的模块。

[0197] 可信操作系统2240可以包括区块链可信应用2214、可信UI可信应用2242和生物特征可信应用2243。根据本公开的实施例，可信操作系统2240可以指用于控制对内核中特定可信区域的访问的单独的可信代码，而不是单独的操作系统。例如，存储在信任区域中的数据可以由信任代码加密，并且对存储在信任区域中的数据的访问可以被控制以增强安全性。根据本公开的实施例，可信操作系统2240可以与富操作系统分开运行，或者可以与富操作系统一起运行。可信操作系统2240可以是独立于内核级运行的功能。根据本公开的实施例，可信操作系统2240可以与富操作系统一起操作，而无需单独操作，并且可信UI可信应用2242和生物特征可信应用2243可以被包括在一个数字钱包2210中以进行操作。区块链可信应用2241可以根据数字钱包2210的请求来验证数字签名。根据本公开的实施例，区块链可信应用2241可以存储用于数字签名的私钥或公钥。

[0198] 可信UI可信应用2242可以在保持安全性的状态下显示区块链地址和第一信息，并且可以接收对所显示的安全性信息的用户输入。例如，当执行需要安全性的操作时，可以通过可信UI可信应用2242来显示UI。当用户单独执行生物特征认证时，可以通过生物特征认证可信应用2243来执行生物特征认证。

[0199] 根据本公开的实施例，电子装置可以基于特定时间段继续确认区块链账户。例如，在用户执行交易之前，电子装置可以通过电子装置可访问的网络周期性地确认区块链地址的有效性，并且可以更新改变的区块链地址。根据本公开的实施例，电子装置可以周期性地更新存储在电子装置中的区块链地址或个人信息。可以基于用户预设的周期或系统自动设置的周期来执行对信息的更新。根据本公开的实施例，当存储在电子装置中的区块链地址或个人信息被改变时，电子装置可以被配置为通过特定事件来更新信息。例如，电子装置可以接收关于区块链地址的信息，该地址被确定为黑客的账户或者用于黑客攻击。电子装置可以从外部电子装置接收与信息相关联的更新消息。响应于接收到的更新消息，电子装置可以用从区块链网络获得的区块链地址替换存储在电子装置中的区块链地址中与更新消息中包括的信息相匹配的区块链地址。根据本公开的实施例，关于区块链地址的有效性的信息可以用于确认交易信息、余额信息或者由可靠机构通过从区块链网络（例如，区块链主网络）提供的功能进行认证的结果。例如，为了确认区块链地址的有效性，电子装置可以通过从区块链主网络提供的功能来执行认证请求。区块链主网络可以向电子装置提供认证信息，该认证信息表示基于地址执行的确定有效性的结果。根据本公开的实施例，电子装置可以与周围的电子装置共享关于区块链账户地址的认证信息。例如，电子装置可以通过区块链主网络认证区块链地址的有效性，并且可以将认证的区块链地址和对应于区块链地址的信息递送给另一个电子装置。例如，电子装置可以将认证的区块链地址递送给与电子装置连接的智能手表，并且智能手表可以显示与区块链地址相关联的信息。

[0200] 图23是示出根据本公开实施例的由电子装置执行的过程的信号序列图2300。根据本公开的实施例，至少一个集成应用可以处理区块链应用、数字钱包应用、可信用户界面应用或区块链可信应用的操作。

[0201] 参照图23，在操作2301中，电子装置可以使用富应用2314将第一信息存储在存储

器中。例如,当富应用2314是联系人应用时,电子装置可以在存储器中存储与联系人信息(例如,电话号码)相关联的第一信息(例如,电话号码的所有者姓名)。

[0202] 在操作2303中,电子装置可以通过区块链应用2316获得区块链地址。在操作2305中,电子装置可以获得存储在存储器2318中的第一信息。例如,区块链应用2316可以包括使得电子装置显示存储在存储器2318中的联系人信息并接收在所显示的联系人信息中选择第一信息的用户输入的指令。

[0203] 根据本公开的实施例,在操作2307中,区块链应用2316可以使电子装置在电子装置的显示器上显示区块链地址和第一信息。在操作2309中,区块链应用2316可以获得针对用户关联并存储两条信息的认证或批准(例如,图16的操作1609)。根据本公开的实施例,在操作2311中,当用户执行认证时,电子装置可以利用在针对第一信息和区块链地址生成区块链交易时用于数字签名的私钥来执行数字签名。在操作2313中,电子装置可以将与数字签名的结果(例如,数字签名的值)相关联的数据(例如,第一信息或区块链地址)一起存储在存储器2318中。根据本公开的实施例,电子装置可以将第一信息、区块链地址或数字签名值存储在不可信存储区域或可信存储区域中。例如,不可信存储区域可以是图1的存储器130。例如,可信存储区域可以包括具有在逻辑上或物理上被划分的增强安全性的存储器。根据实施例,逻辑可信存储区域可以在逻辑上划分和设置不可信存储区域的一部分(例如,图1的存储器130)。例如,逻辑划分和设置可以包括这样的操作,其中电子装置将存储器的部分地址设置为可信区域,并且其中当存储或读取信息时,对相应存储区域的访问仅由单独的应用、单独的应用编程界面(API)或单独的功能或可信操作系统来执行。

[0204] 在操作2315和2317中,电子装置可以获得区块链地址和第一信息。在操作2319中,电子装置可以向用户提供区块链地址和第一信息。根据本公开的实施例,电子装置可以一起显示区块链地址和第一信息,或者可以一起显示区块链地址、第一信息或与区块链地址的可靠性相关联的第二信息(例如,图形信息)。

[0205] 根据本公开的实施例,当生成区块链交易时,电子装置可以确认区块链交易中包括的目的地的区块链地址(例如,第二区块链地址)是否存储在存储器(2318)中。例如,当第二区块链地址对应于存储在存储器2318中的第一区块链地址时,电子装置可以对与第一区块链地址相关联并存储的第一信息和第二区块链地址执行数字签名(例如,使用生成区块链交易时使用的私钥的数字签名),并且可以将作为执行数字签名的结果而获得的数字签名值与存储在存储器中的数字签名值进行比较。例如,当作为执行数字签名的结果而获得的数字签名值与存储在存储器中的数字签名值相同时,电子装置可以在显示器上显示与第二区块链地址相关联的第一信息。

[0206] 根据各种实施例的电子装置可以是各种类型的电子装置之一。电子装置可包括例如便携式通信装置(例如,智能电话)、计算机装置、便携式多媒体装置、便携式医疗装置、相机、可穿戴装置或家用电器。根据本公开的实施例,电子装置不限于以上所述的那些电子装置。

[0207] 应该理解的是,本公开的各种实施例以及其中使用的术语并不意图将在此阐述的技术特征限制于具体实施例,而是包括针对相应实施例的各种改变、等同形式或替换形式。对于附图的描述,相同的参考标号可用来指代相同或相关的元件。将理解的是,与术语相应的单数形式的名词可包括一个或更多个事物,除非相关上下文另有明确指示。如这里所使

用的,诸如“A或B”、“A和B中的至少一个”、“A或B中的至少一个”、“A、B或C”、“A、B和C中的至少一个”以及“A、B或C中的至少一个”的短语中的每一个短语可包括在与所述多个短语中的相应一个短语中一起列举出的项的任一项或所有可能组合。如这里所使用的,诸如“第1”和“第2”或者“第一”和“第二”的术语可用于将相应部件与另一部件进行简单区分,并且不在其他方面(例如,重要性或顺序)限制所述部件。将理解的是,在使用了术语“可操作地”或“通信地”的情况下或者在不使用术语“可操作地”或“通信地”的情况下,如果一元件(例如,第一元件)被称为“与另一元件(例如,第二元件)结合”、“结合到另一元件(例如,第二元件)”、“与另一元件(例如,第二元件)连接”或“连接到另一元件(例如,第二元件)”,则意味着所述一元件可与所述另一元件直接(例如,有线地)连接、与所述另一元件无线连接、或经由第三元件与所述另一元件连接。

[0208] 如这里所使用的,术语“模块”可包括以硬件、软件或固件实现的单元,并可与其他术语(例如,“逻辑”、“逻辑区块”、“部分”或“电路”)可互换地使用。模块可以是适配为执行一个或更多个功能的单个集成部件或者是该单个集成部件的最小单元或部分。例如,根据本公开的实施例,可以以专用集成电路(ASIC)的形式来实现模块。

[0209] 可将在此阐述的各种实施例实现为包括存储在存储介质(例如,内部存储器136或外部存储器138)中的可由机器(例如,电子装置101)读取的一个或更多个指令的软件(例如,程序140)。例如,在控制器的控制下,所述机器(例如,电子装置101)的处理器(例如,处理器120)可在使用或无需使用一个或更多个其他部件的情况下调用存储在存储介质中的所述一个或更多个指令中的至少一个指令并运行所述至少一个指令。这使得所述机器能够操作于根据所调用的至少一个指令执行至少一个功能。所述一个或更多个指令可包括由编译器产生的代码或能够由解释器运行的代码。可以以非暂时性存储介质的形式来提供机器可读存储介质。其中,术语“非暂时性”仅意味着所述存储介质是有形装置,并且可能不包括信号(例如,电磁波),但是该术语并不在数据被半永久性地存储在存储介质中与数据被临时存储在存储介质中之间进行区分。例如,“非暂时性存储介质”可以包括临时存储数据的缓冲器。

[0210] 根据本公开的实施例,可在计算机程序产品中包括和提供根据本公开的各种实施例的方法。计算机程序产品可作为产品在销售者与购买者之间进行交易。可以以机器可读存储介质(例如,紧凑盘只读存储器(CD-ROM))的形式来发布计算机程序产品(可下载的app),或者可经由应用商店(例如,PlayStore™)在线发布(例如,下载或上传)计算机程序产品,或者可直接在两个用户装置(例如,智能电话)之间分发(例如,下载或上传)计算机程序产品。如果是在线发布的,则计算机程序产品中的至少部分可以是临时产生的,或者可将计算机程序产品中的至少部分至少临时存储在机器可读存储介质(诸如制造商的服务器、应用商店的服务器或转发服务器的存储器)中。

[0211] 根据本公开的各种实施例,上述部件中的每个部件(例如,模块或程序)可包括单个实体或多个实体。根据本公开的各种实施例,可省略上述部件中的一个或更多个部件,或者可添加一个或更多个其他部件。可选择地或者另外地,可将多个部件(例如,模块或程序)集成为单个部件。在此情况下,根据本公开的各种实施例,该集成部件可仍旧按照与所述多个部件中的相应一个部件在集成之前执行一个或更多个功能相同或相似的方式,执行所述多个部件中的每一个部件的所述一个或更多个功能。根据本公开的各种实施例,由模块、程

序或另一部件所执行的操作可顺序地、并行地、重复地或以启发式方式来执行,或者所述操作中的一个或多个操作可按照不同的顺序来运行或被省略,或者可添加一个或多个其他操作。

[0212] 根据本公开中公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法来验证区块链地址,而无需用户确认区块链地址是否被正确输入,并且使用户容易地确认与地址相关联的信息。

[0213] 此外,根据本公开中公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以向用户提供熟悉的信息,并使用户容易地确认区块链地址。

[0214] 此外,根据本公开中公开的实施例,可以使用具有增强安全性的存储空间来存储与区块链地址相关联的信息。具有增强安全性的存储空间可以包括例如物理划分的可信空间和逻辑划分的可信空间。例如,物理划分的可信空间可以具有存在于电子装置内部或外部的单独的存储空间。电子装置可以通过单独的可信应用或功能来访问物理可信空间。逻辑划分的可信空间可以是在一个存储空间(存储器)中与不可信区域逻辑分离的可信区域。为了访问逻辑信任区,电子装置可以仅通过单独的信任应用或功能(例如,API)来访问信任区。例如,为了访问逻辑可信区域,可以运行单独的操作系统(例如,可信操作系统)。富操作系统可以请求可信操作系统访问逻辑可信区域。可信操作系统可以验证该请求,并且只有当该请求是正常请求时才可以访问逻辑可信区域。根据本公开的实施例,可信操作系统可以作为单独的操作系统或者其中包括在富操作系统的内核中的软件被虚拟划分的操作系统来操作。根据本公开的实施例,存储空间可以包括电子装置中的存储空间。例如,电子装置可以在一个存储器中存储通用数据,而无需单独划分信任区。具有增强安全性的存储空间可以控制对电子装置的至少部分存储区域的访问。例如,至少一个部分存储区域可以是仅通过单独的可信操作系统和/或单独的可信内核可访问的可信存储区域。电子装置可以仅通过借助可信操作系统或可信内核的单独认证来访问存储在可信存储区域中的区块链地址或相关信息。或者,区块链地址和相关信息可以被加密,以便仅通过可信操作系统或可信区域中的密钥来解密,从而被存储在不可信区域中的存储空间中。提供电子装置和在电子装置中管理区块链地址的方法以执行附加认证,并且仅当附加认证完成时才执行区块链交易,以增强区块链交易的安全性。

[0215] 根据本公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以增强区块链地址的可用性,因为通过认证(例如,生物特征认证)使用了各种信息。

[0216] 根据本公开的实施例,提供了电子装置和用于在电子装置中管理区块链地址的方法,以在尽管用户改变了他或她的终端装置的情况下在交易中继续使用认证信息。例如,因为认证信息是在区块链网络中分发和存储的,所以在尽管改变了终端装置的情况下,用户可以从区块链网络获得和使用认证信息。

[0217] 此外,可以提供通过本公开直接或间接确定的各种效果。

[0218] 虽然已经参考本发明的各种实施例示出和描述了本发明,但是本领域技术人员将理解,在不脱离由所附权利要求及其等同物限定的本发明的精神和范围的情况下,可以在其中进行形式和细节上的各种改变。

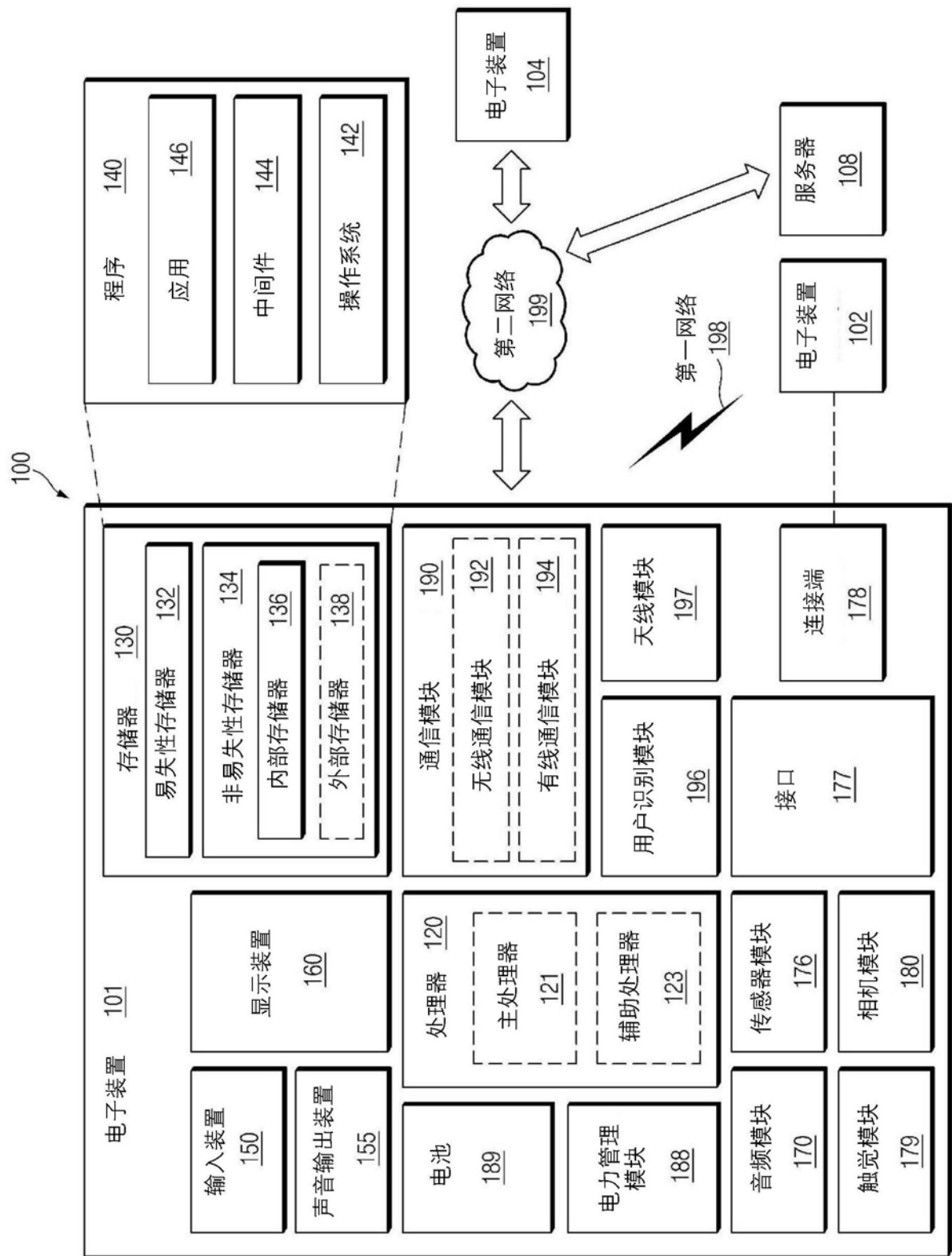


图1

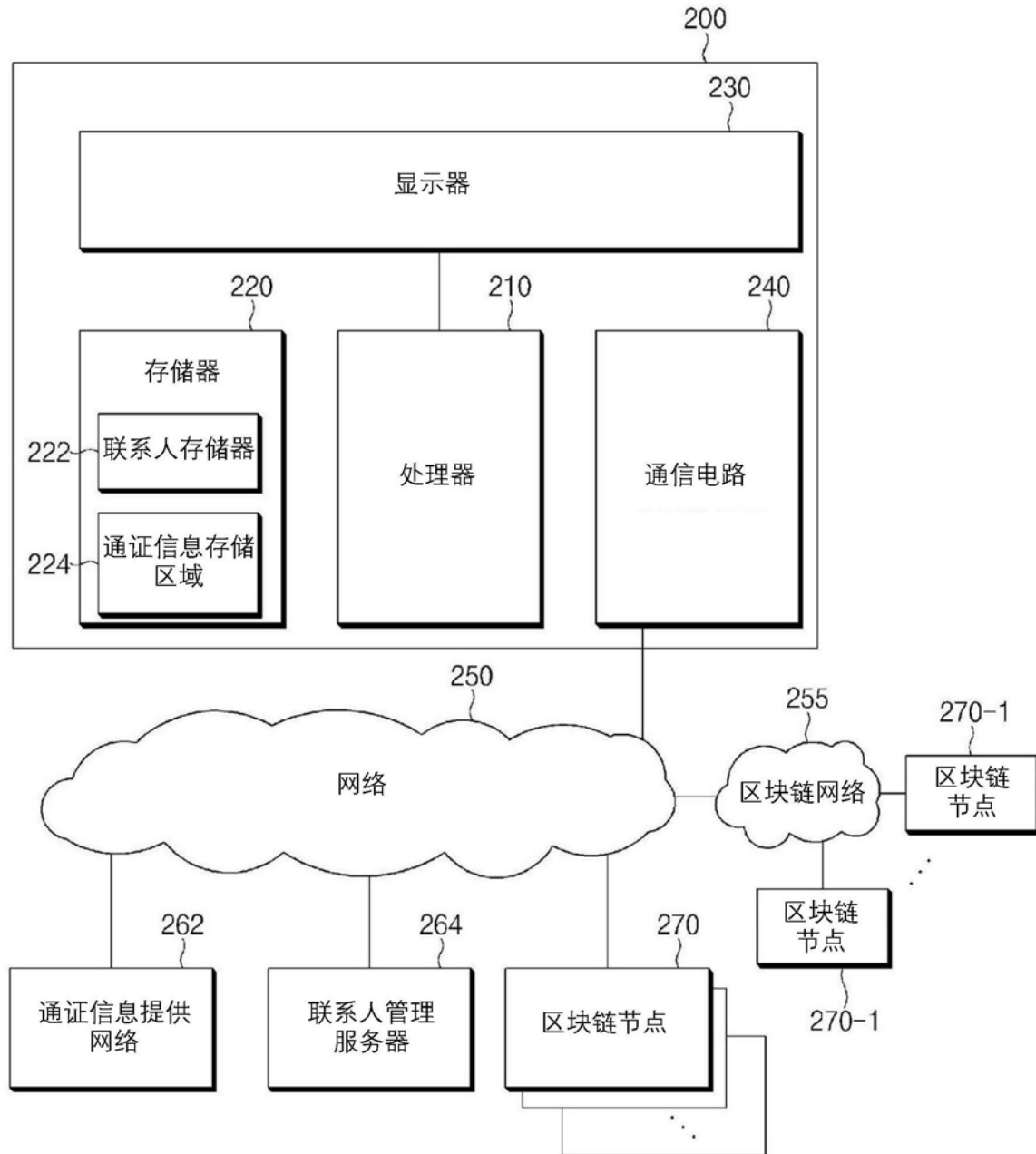


图2

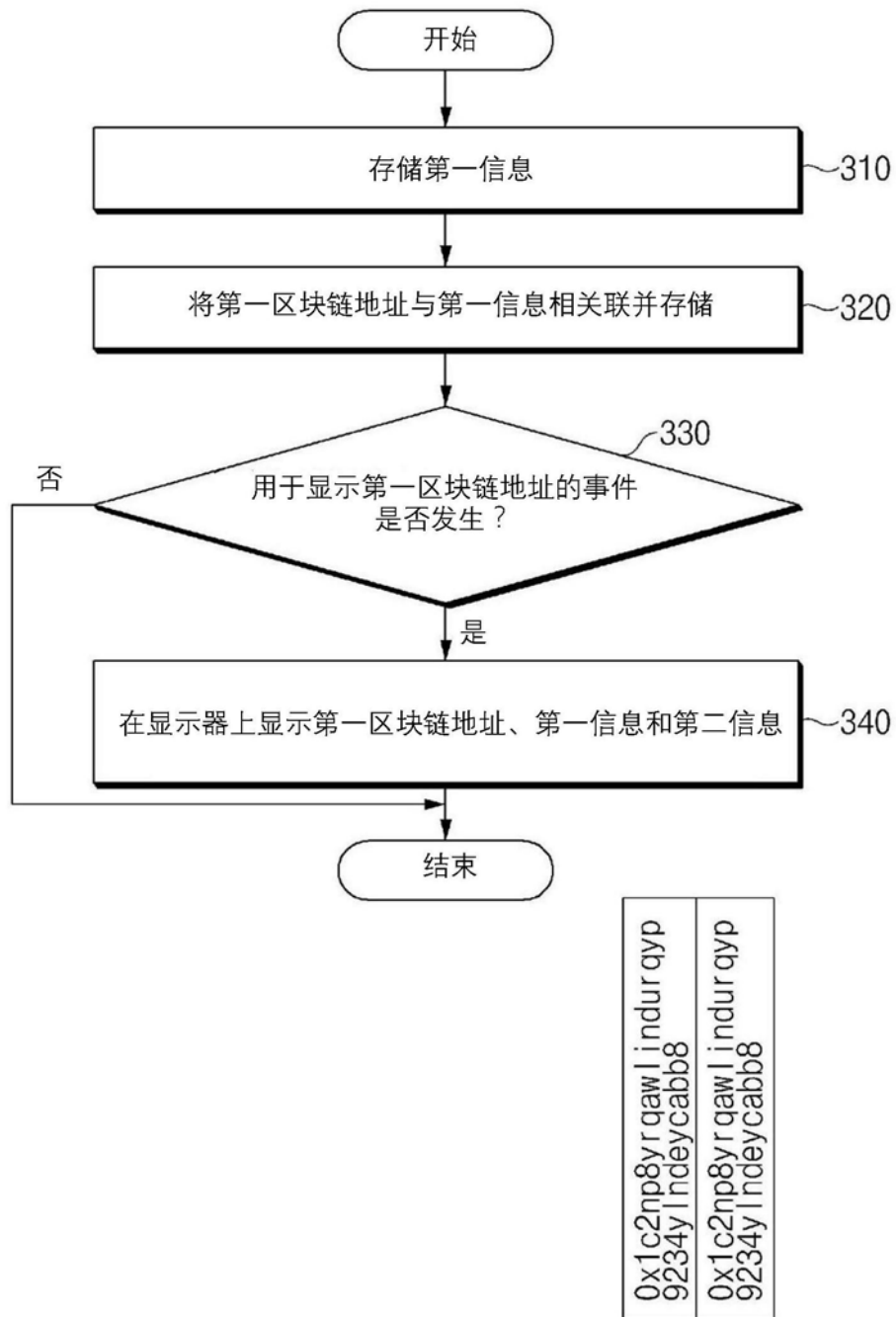


图3

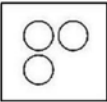
400

☐ 交易确认

在确认此交易之前，请确保以下细节正确

Om  go 币

OMG



智能联系人地址
0xd26114cd6EE289AccF82350c8d8487fedB8A0C07

数额

0.01 ETH

天然气价格

0.000000022 ETH

最高天然气价格

0.000462 ETH

类型

ERC20

传送

接收者地址

411
昵称：Jane
组：家庭

412


410
0x3f5ce5fbfe3e0af3971dd833d26ba9b5c936f0be

通证数额

32

确认

图4

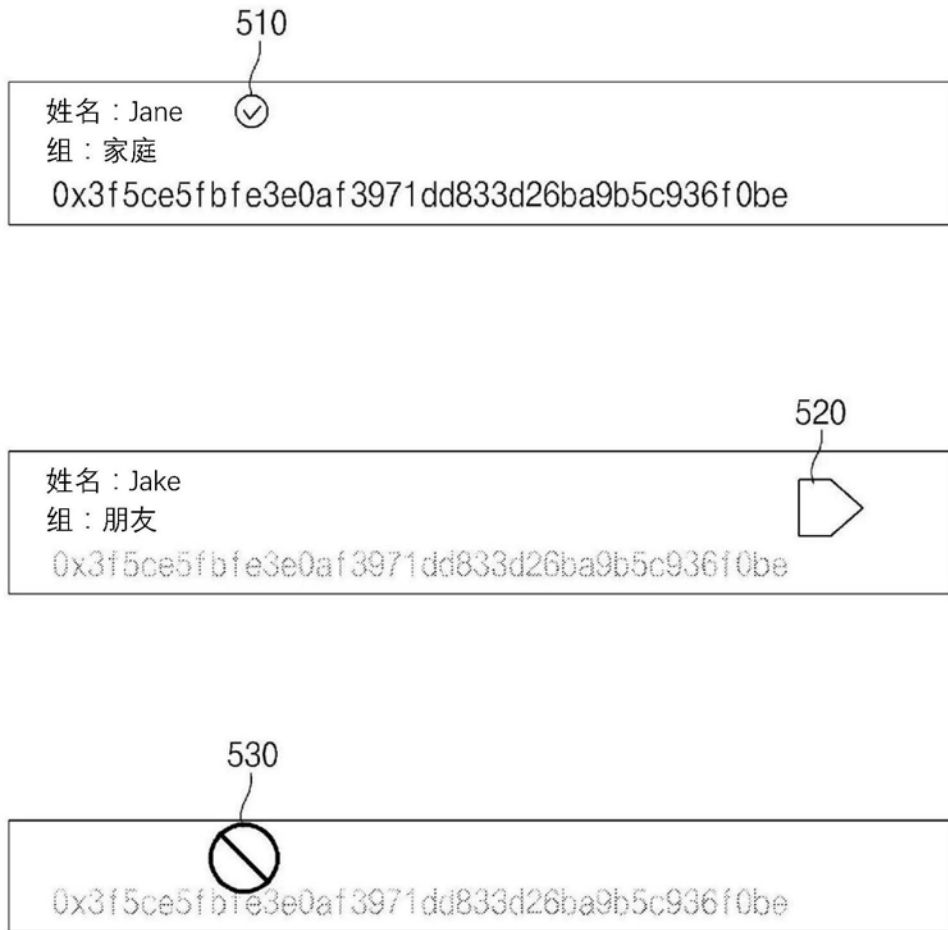


图5

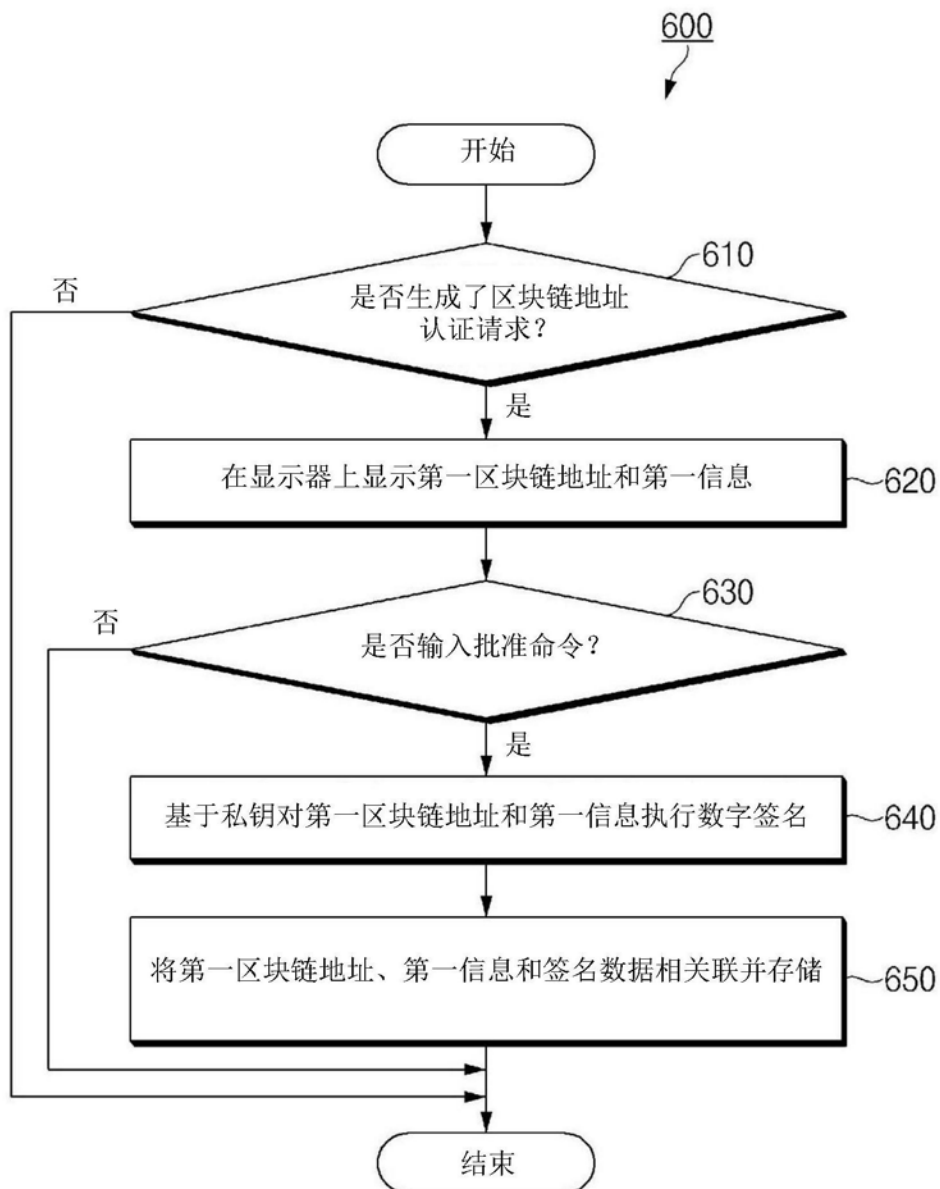


图6



图7

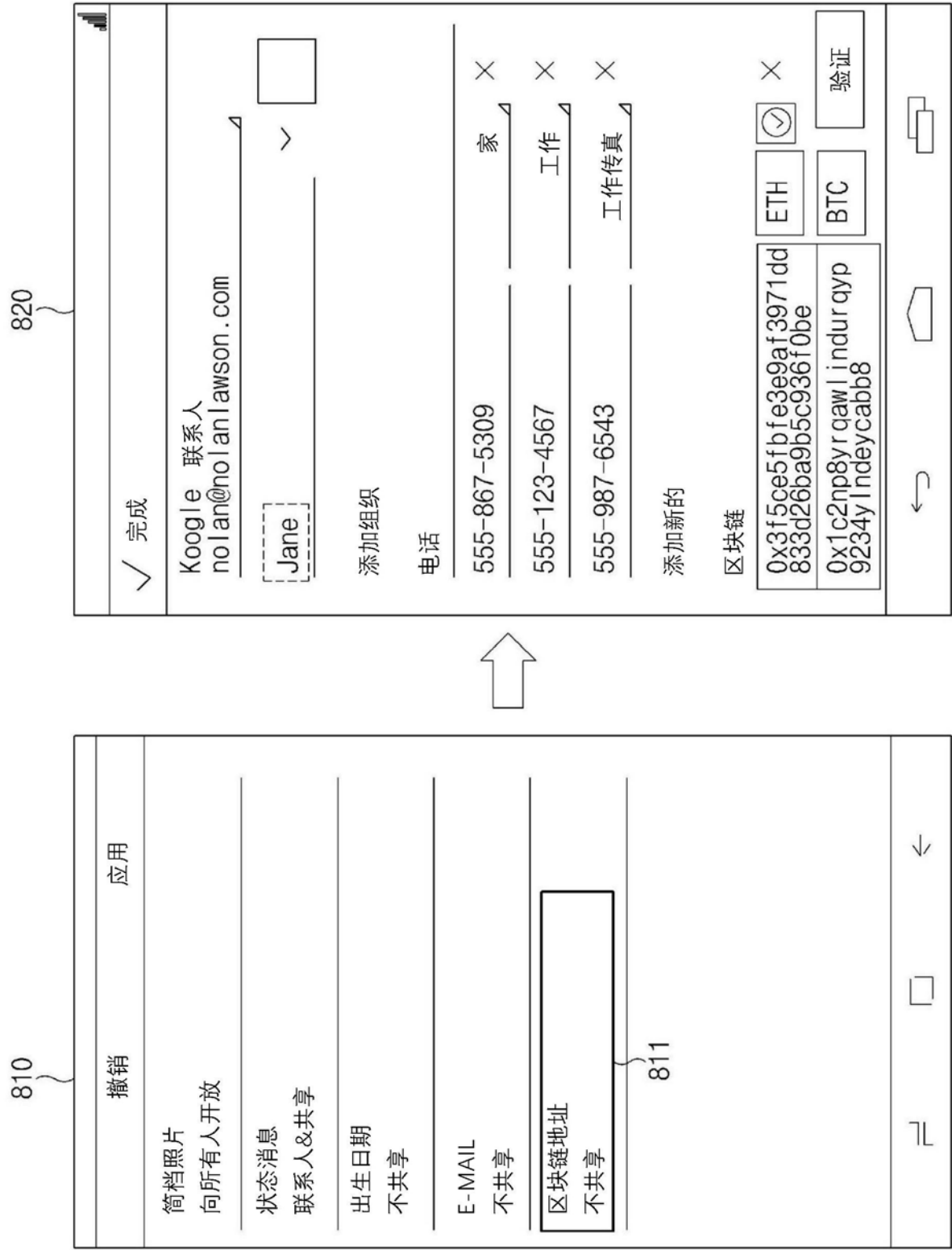


图8

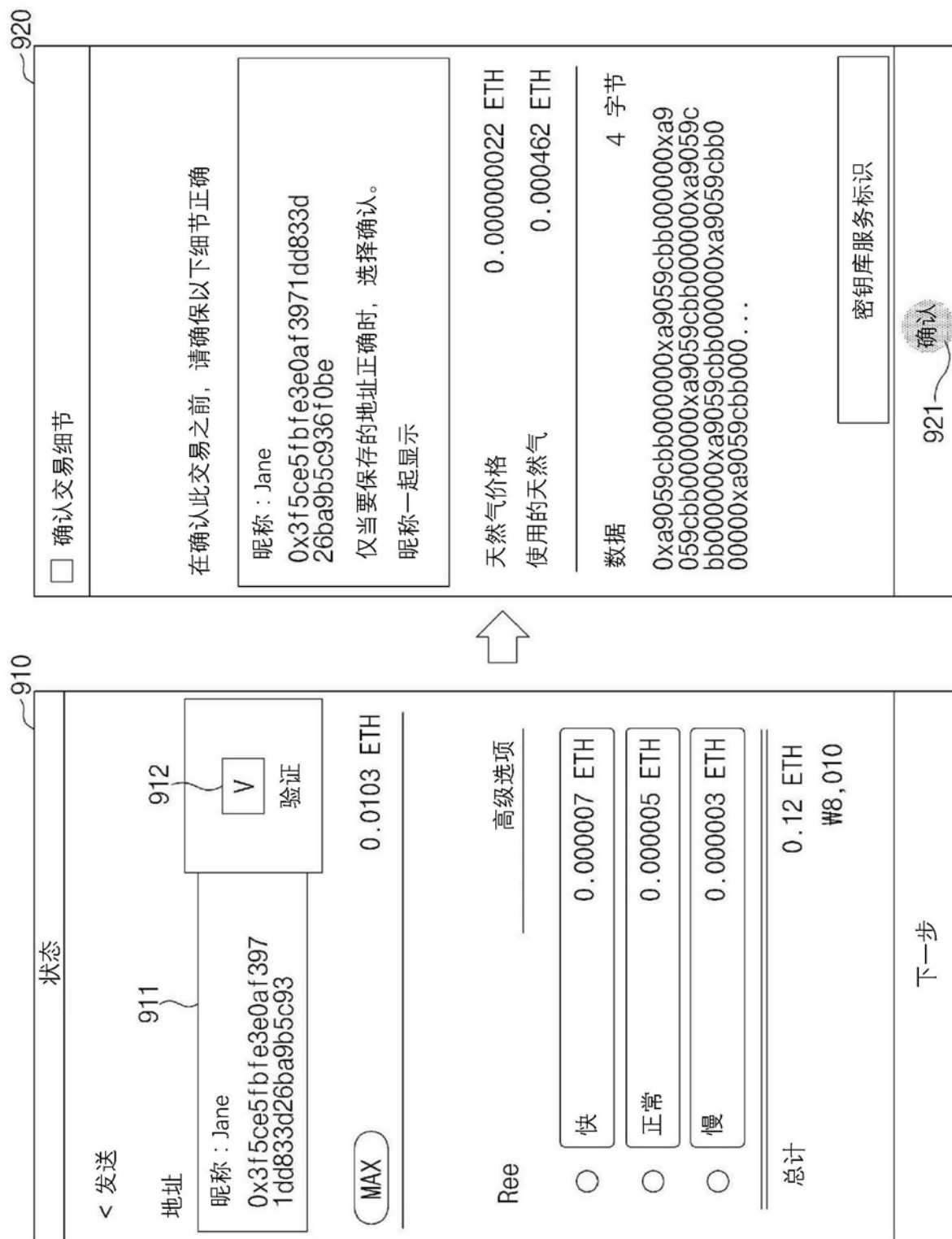


图9

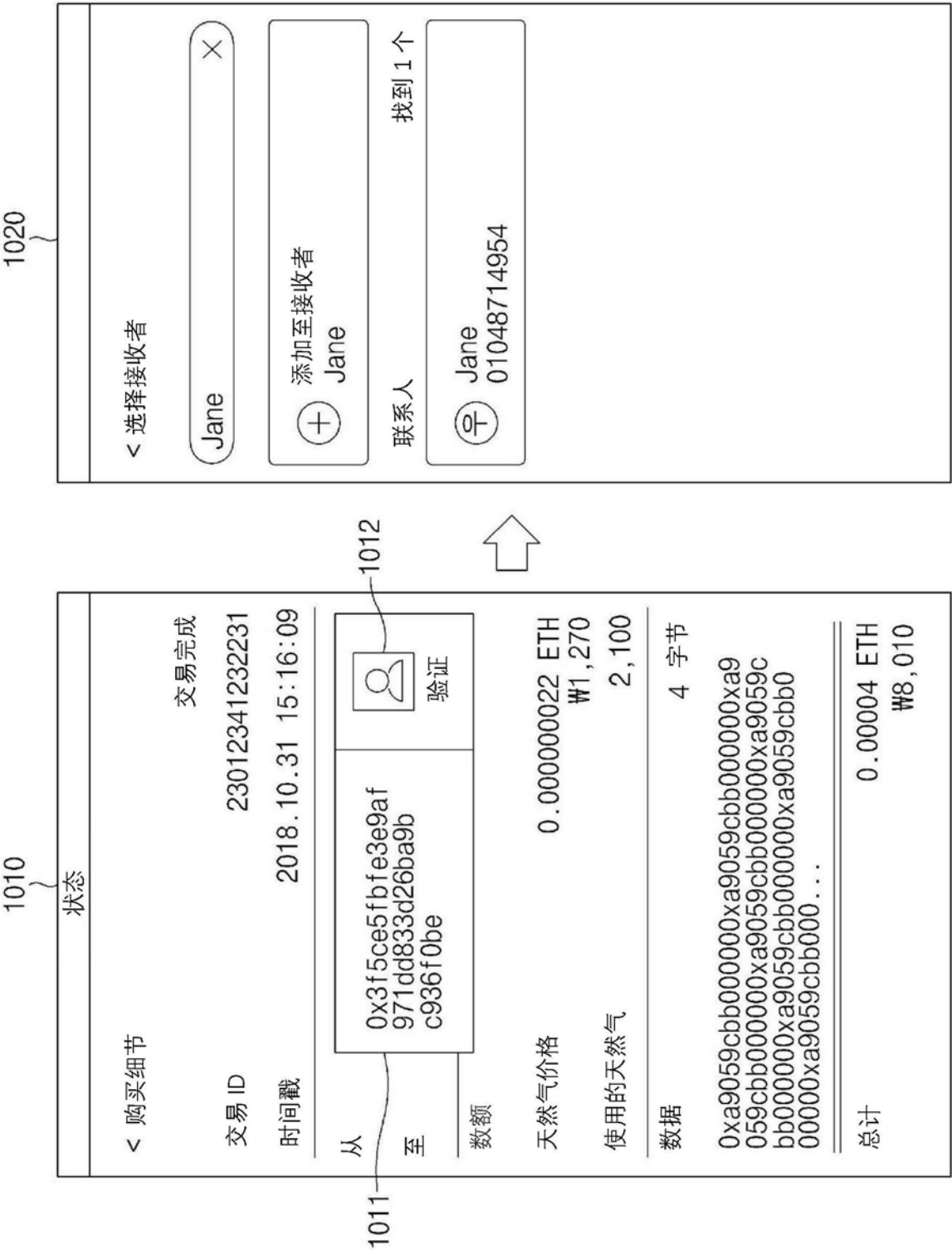


图10

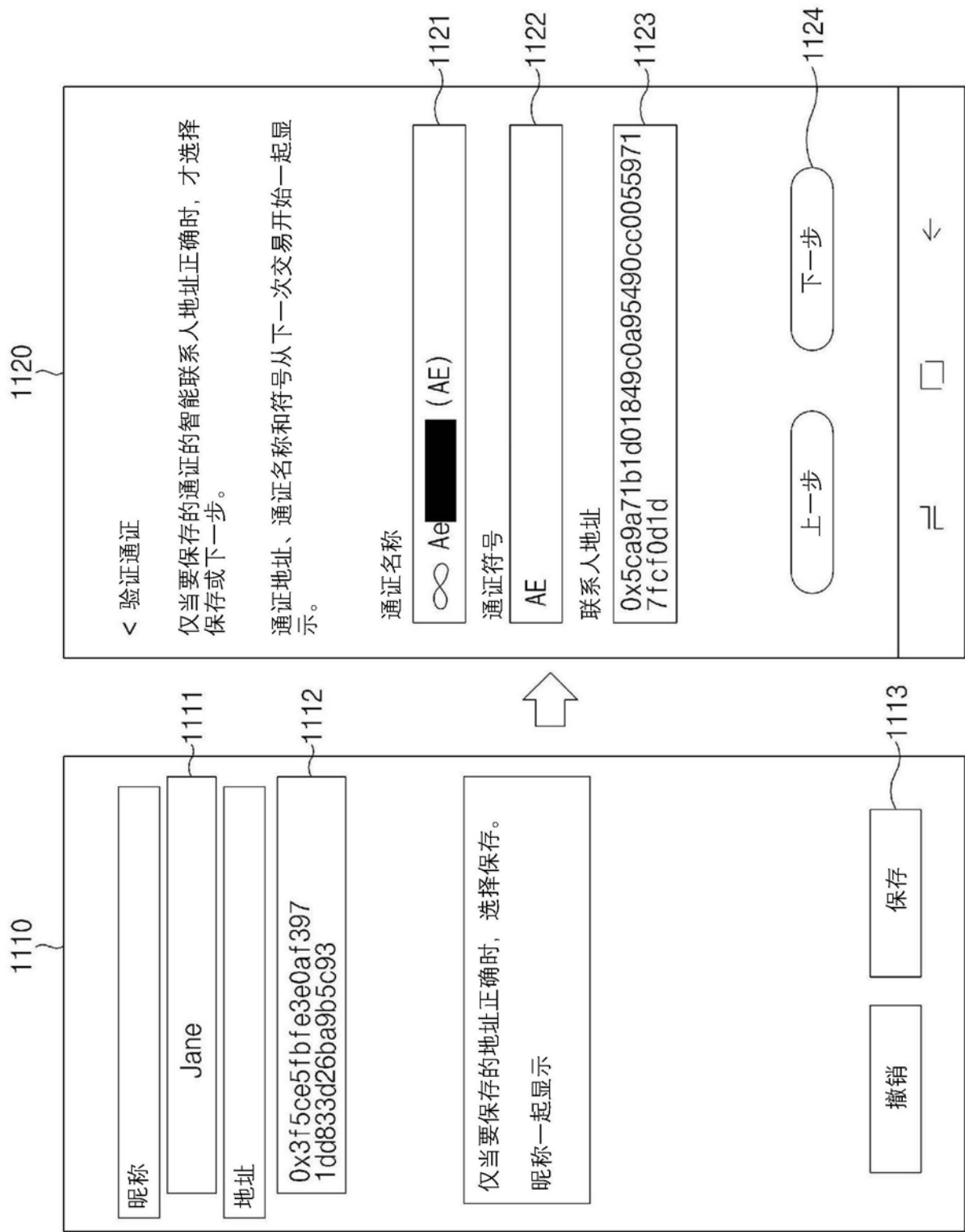


图11

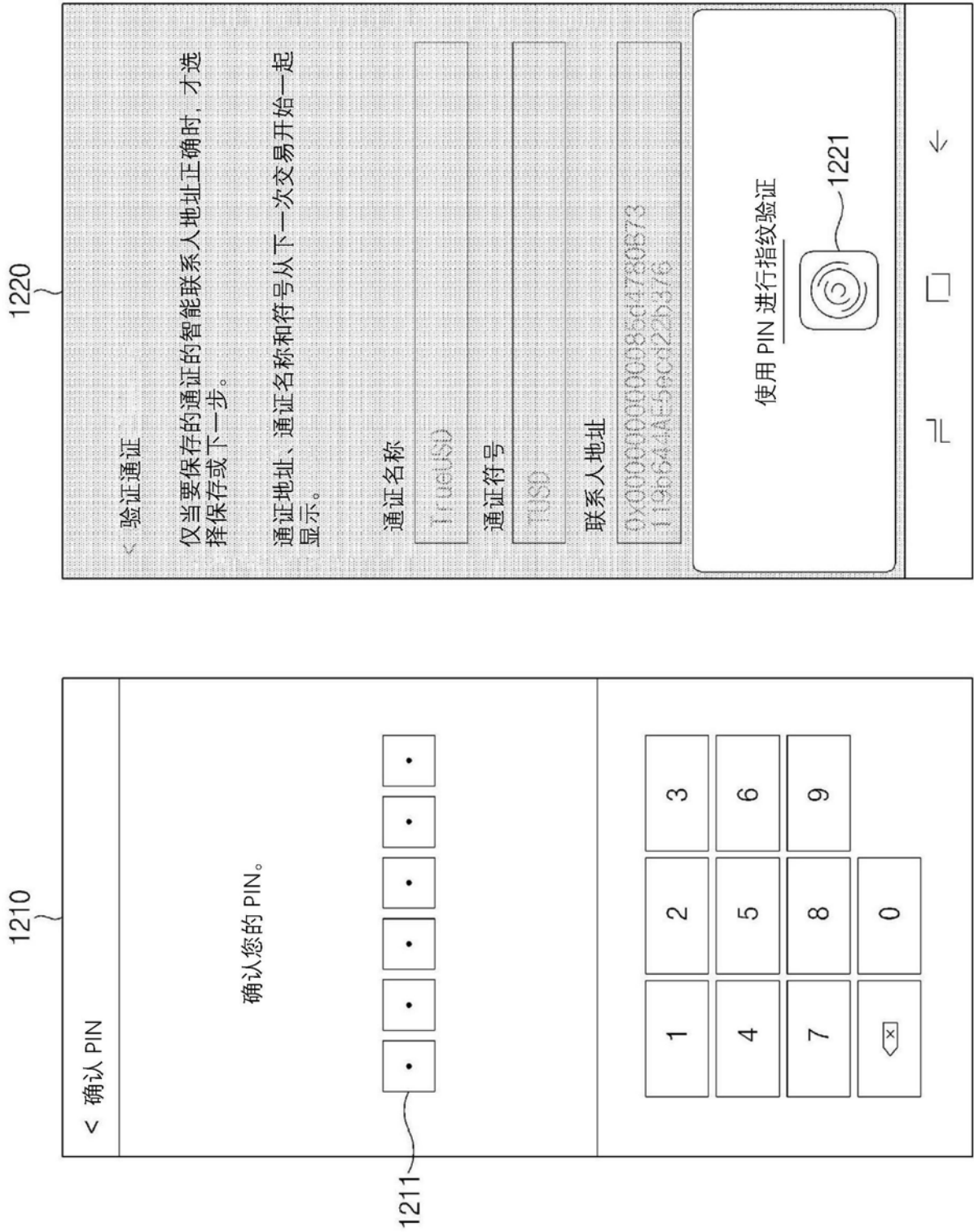


图12

1300
↓

1310	1320	1330
区块链地址	第一信息	签名数据
0xa8015df165e7f53d491d c7ed35013031ad25034	My Mother	0x2434d7f6d9744b21123e2e2dfb3b3ef 825110f7bcc7ff75cd99f56d99100af
0xe4c77dee303ea989aacff 21104dd358ea7ad7380	Alice	0x67e61aa1ba05e41355e1221aaf1451992 825110f7bcc7ff75cd99f56d99100af
0x05ee546c1a62f90d7acbff d6d846c9c54c7cf94c	Bob	0x16741086892edf937892c99b92beb8aef 53ef4117df316b633fb8d160448c34e
0x3f5ce5fbfe3e9af397dd8 33d26ba9b5c936f0be	Jimmy	0x16741086892edf937892c99b92beb8aef 53ef4117df316b633fb8d160448c
0xb5a5f22694352c15b0032 3844ad545abb2b11028	Bob	0xbd040615653c1ee3f3d0a220a79588032 7af77070a9ef2824093d91afedaf396
0x2ef09b25efee21565e51f 2dd033260fd5637bc2c	Charles	0x526089d0fd0d1b514b1366a44206e016 06e900dc167516a0f109a48c46930877

图13

1410		1422		1424		1430	
区块链地址		通证名称		符号		签名数据	
0xd26114cd6EE289AccF82350c8d8487fedB8A0C07		Om [REDACTED] GO		OMG		0xbe0bb396c506a0f979f535a43a50bd645158ee77cc88d41d6de9a73476b4b0c0	
0x9f8f72aa9304c8b593d555f12ef6589cc3a579a2		Ma [REDACTED]		MKR		0x0718f0f79b42805c4453919fdbd6521e3f8f5078acf27e6be7d95ea06405cdf1	
0xb5a5f22694352c15b00323844ad545abb2b11028		IC [REDACTED]		ICX		0xc26b7ed77b22dd3704433befa82ac518a49d2c78aa653137f5555ad25a9fa225	

图14

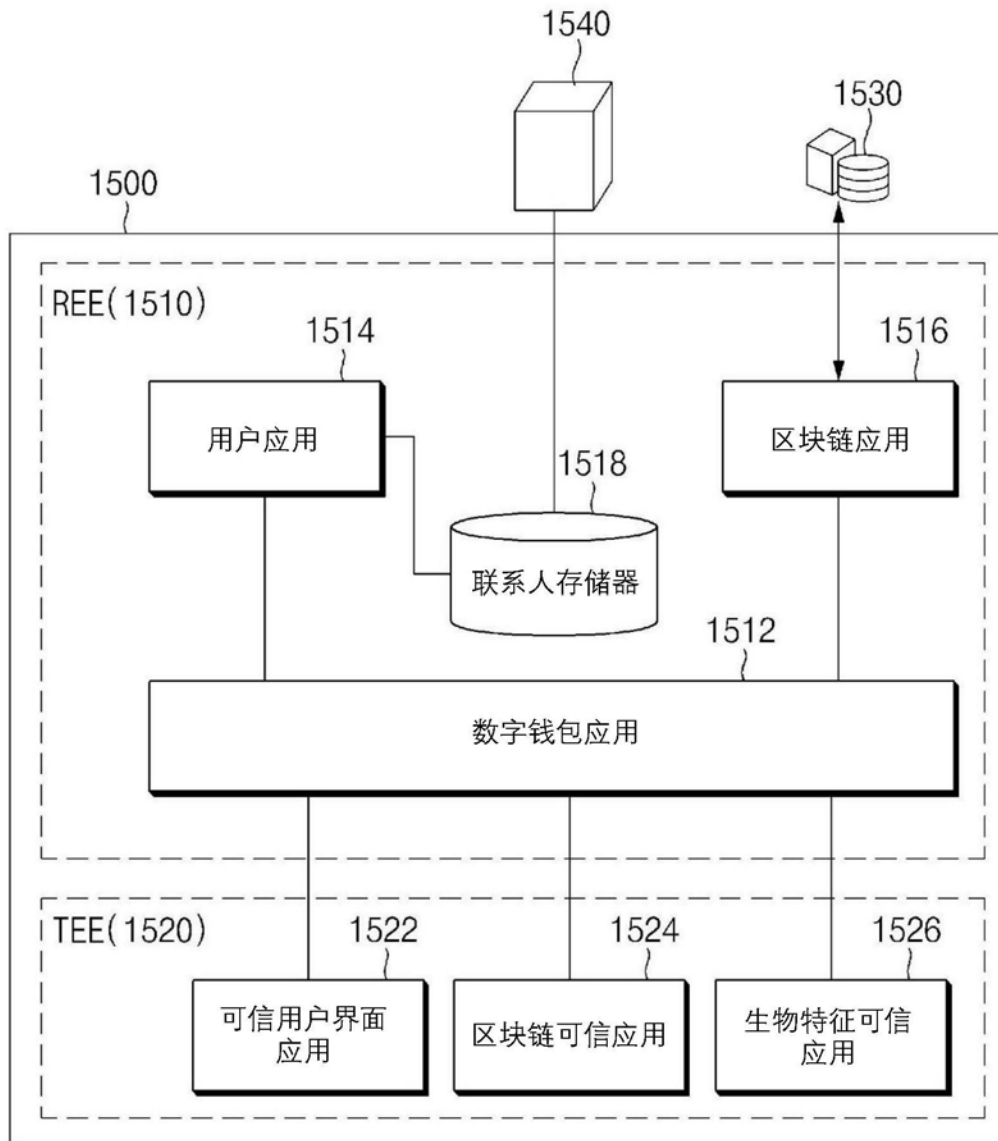


图15

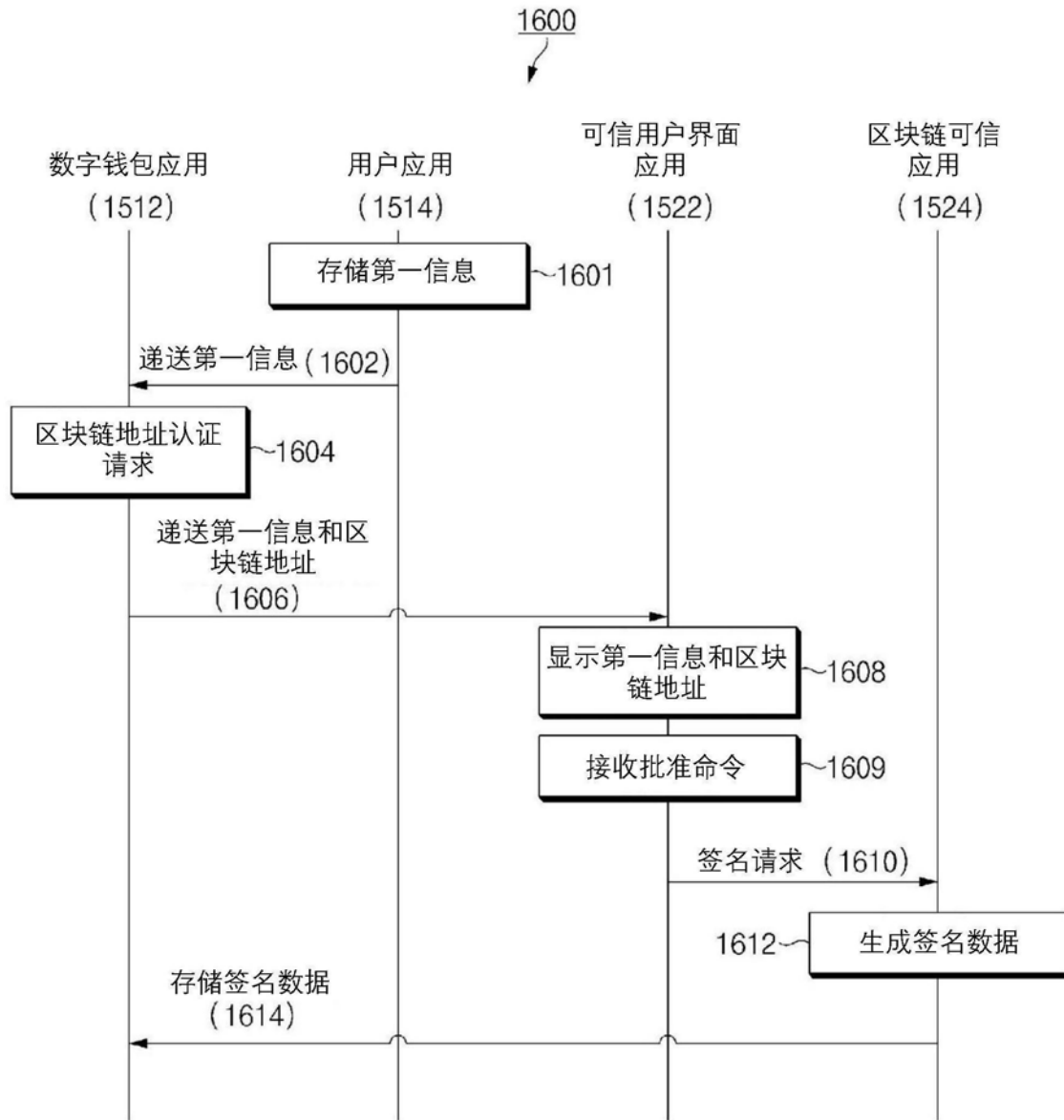


图16

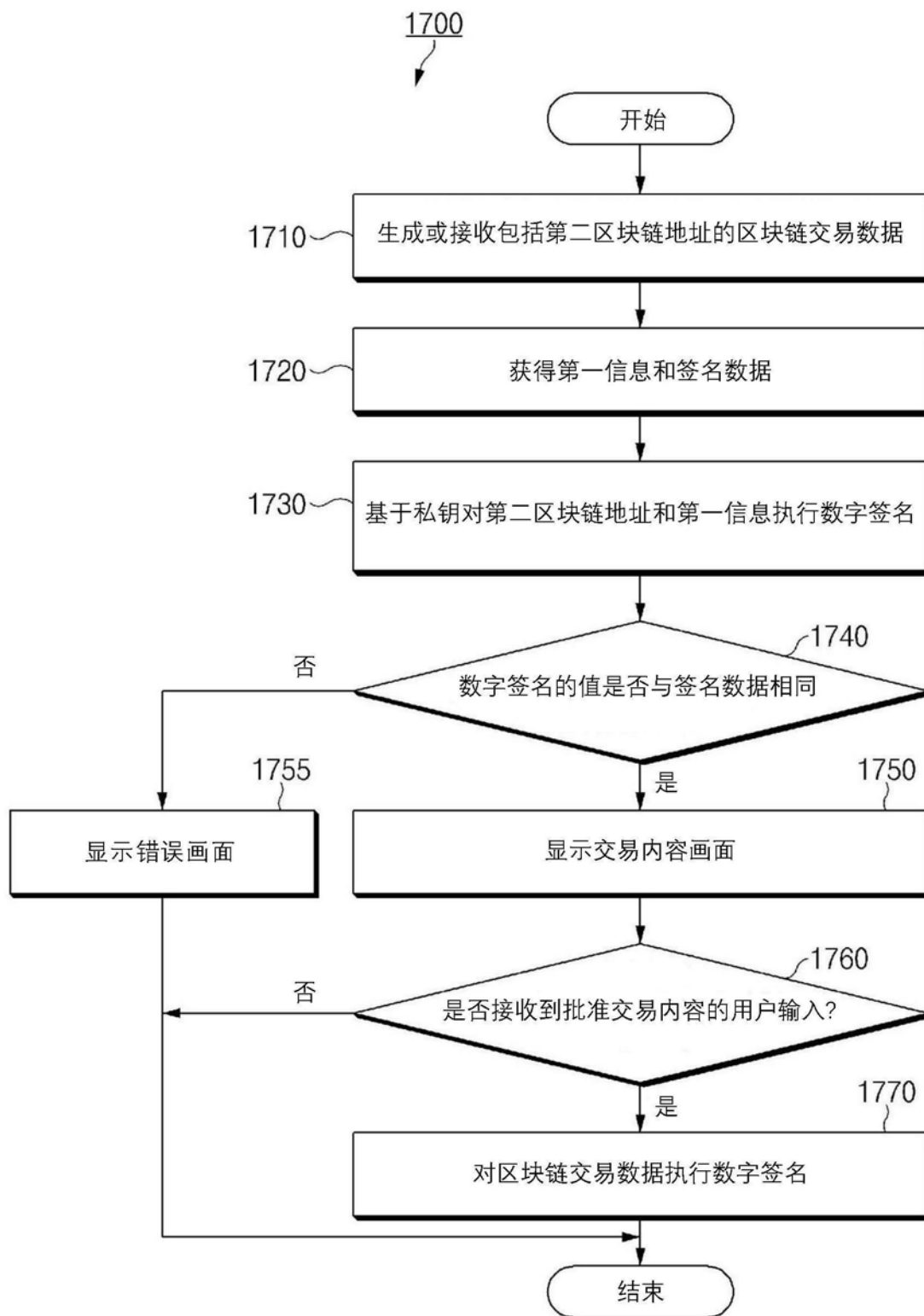


图17

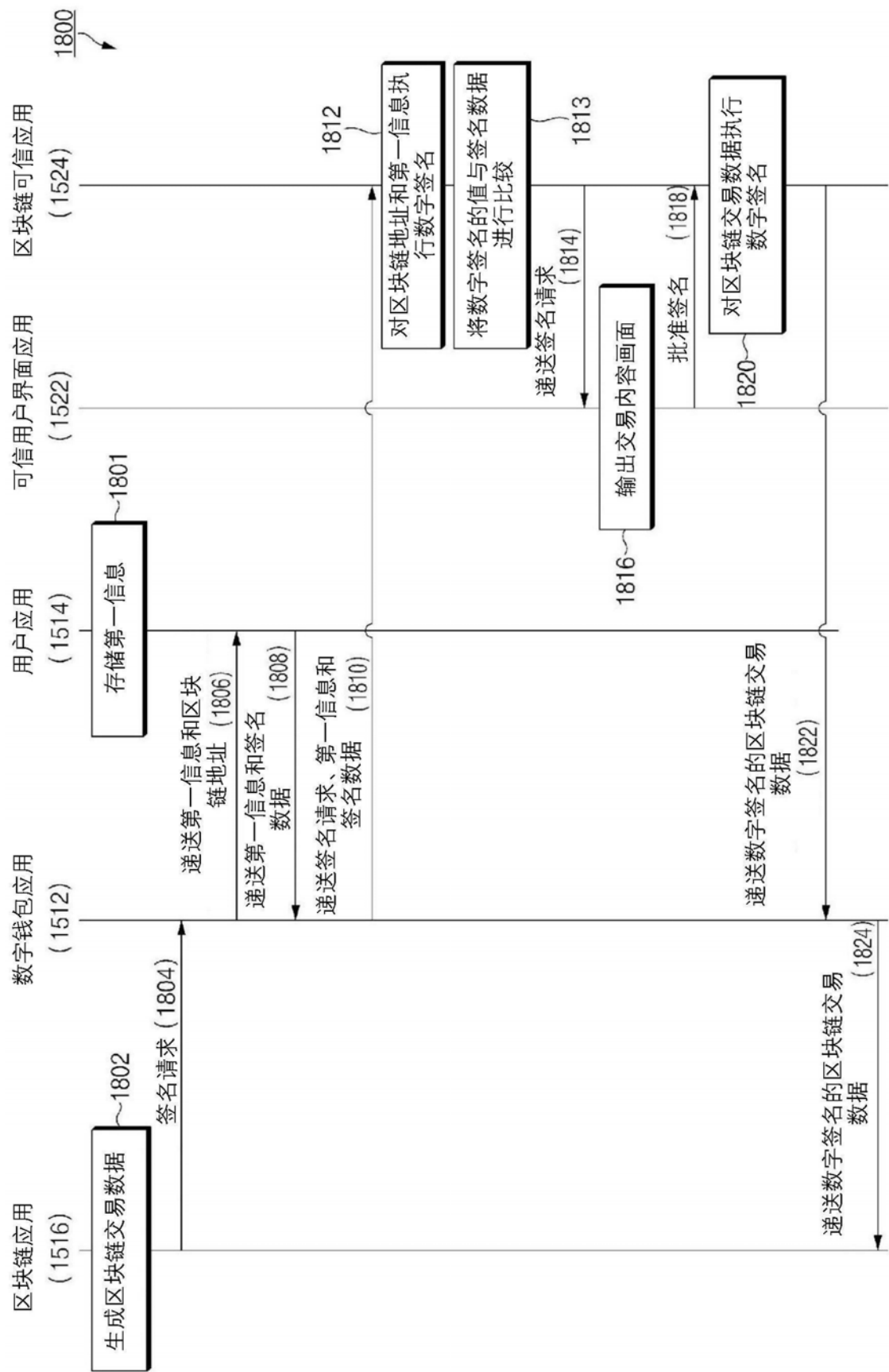


图18

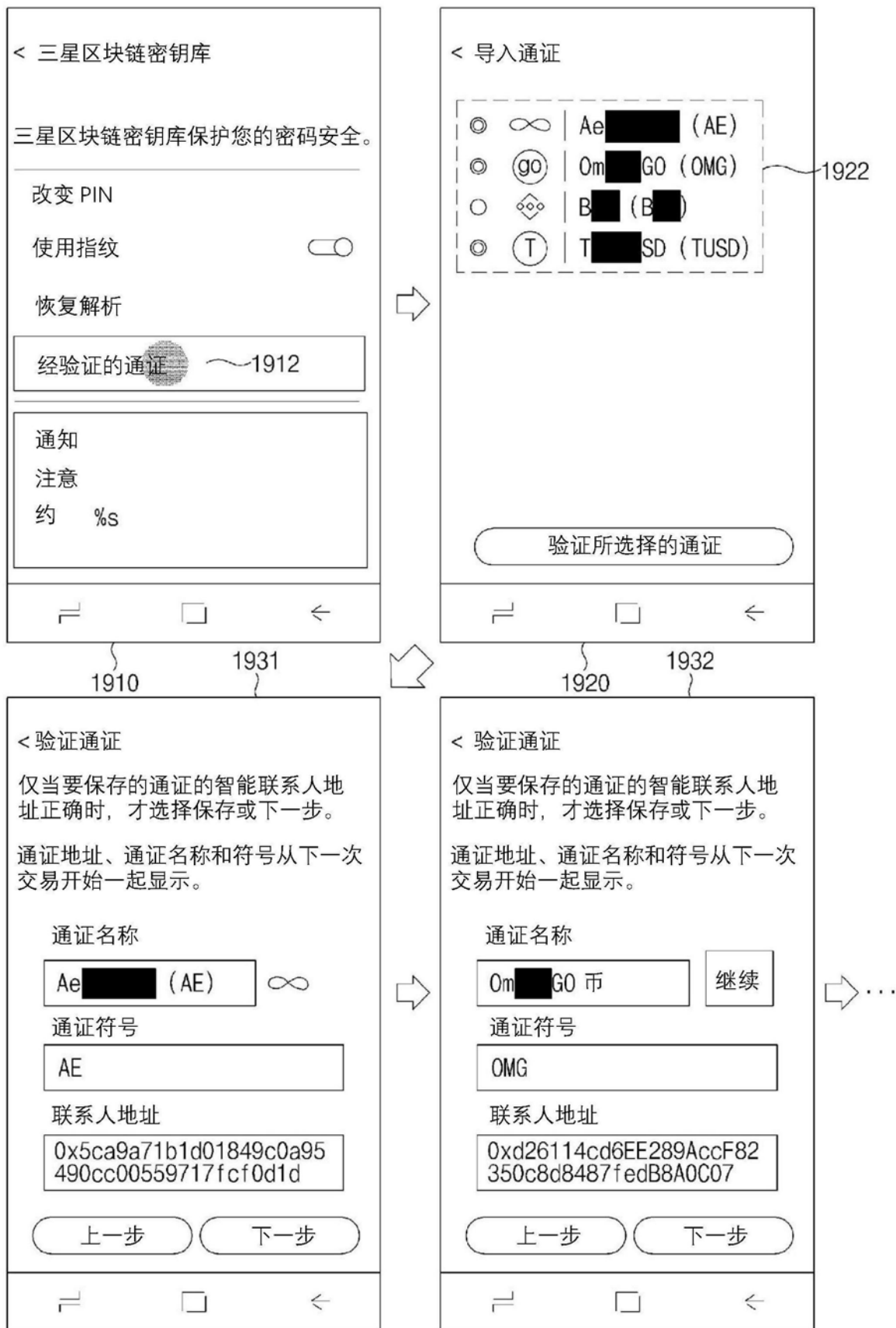


图19

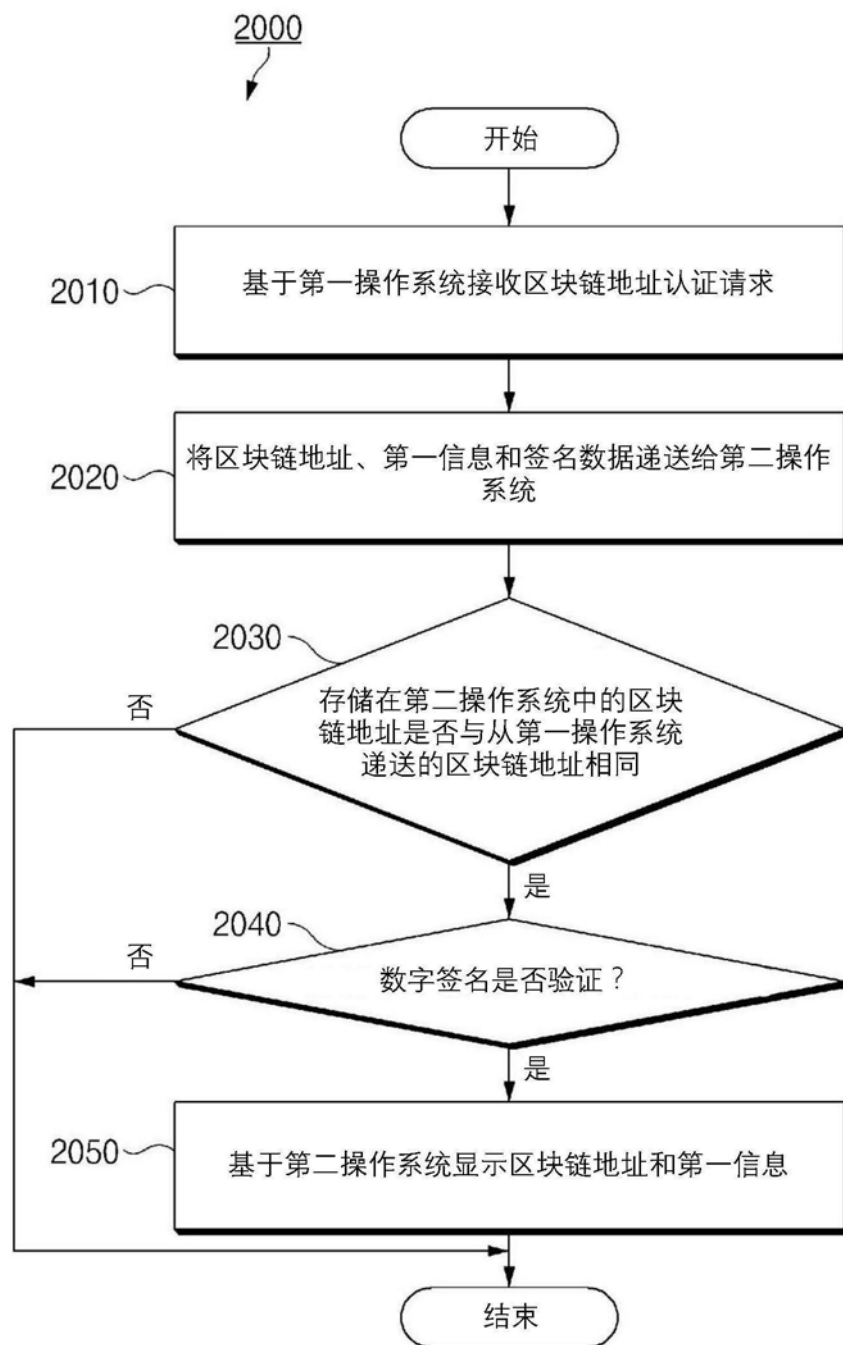


图20

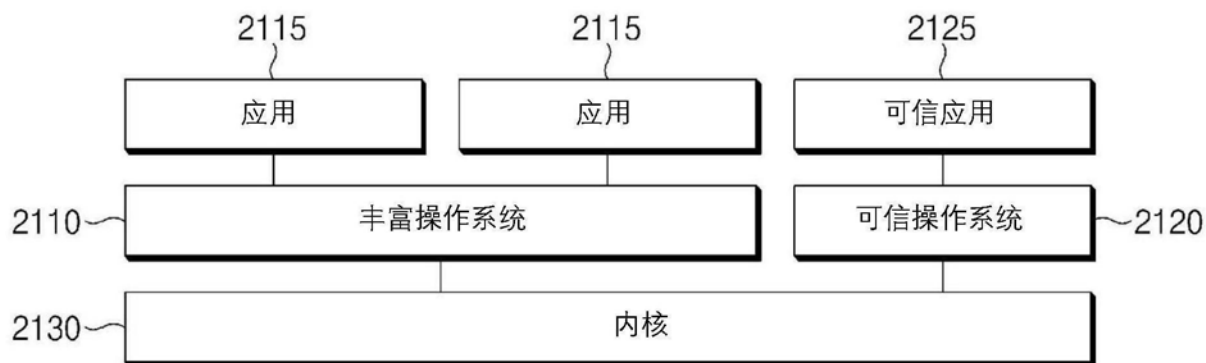


图21

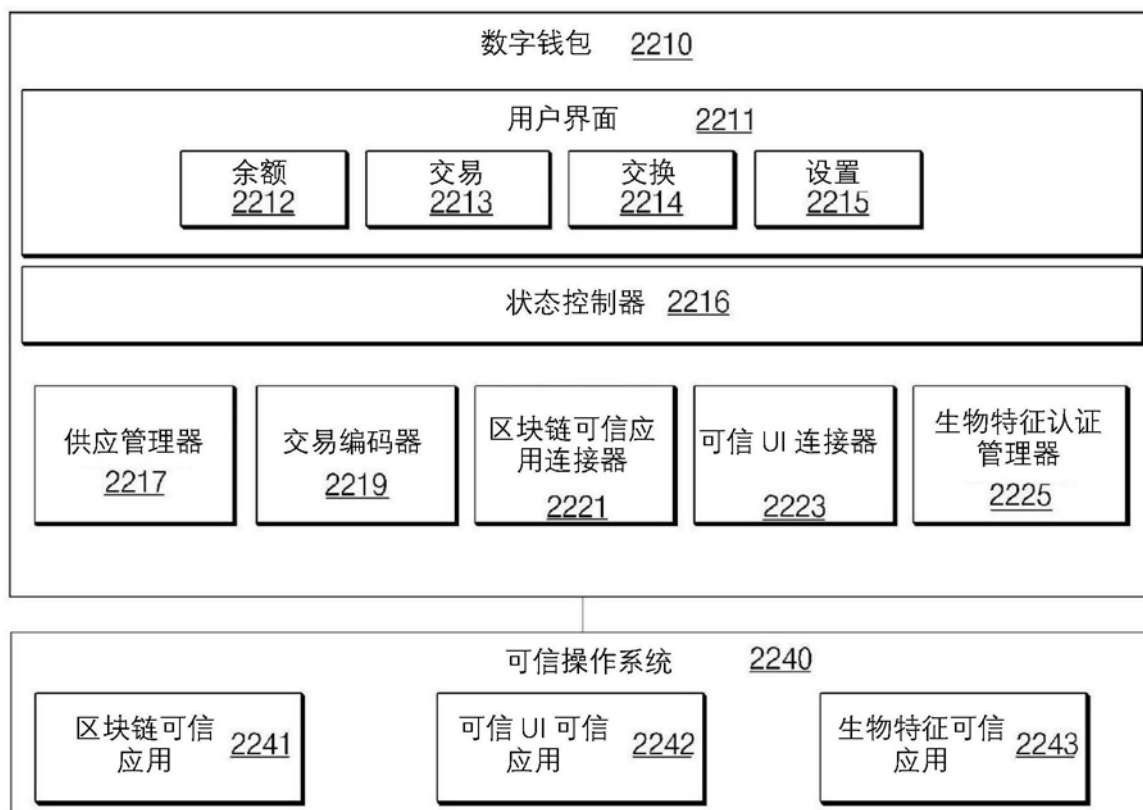


图22

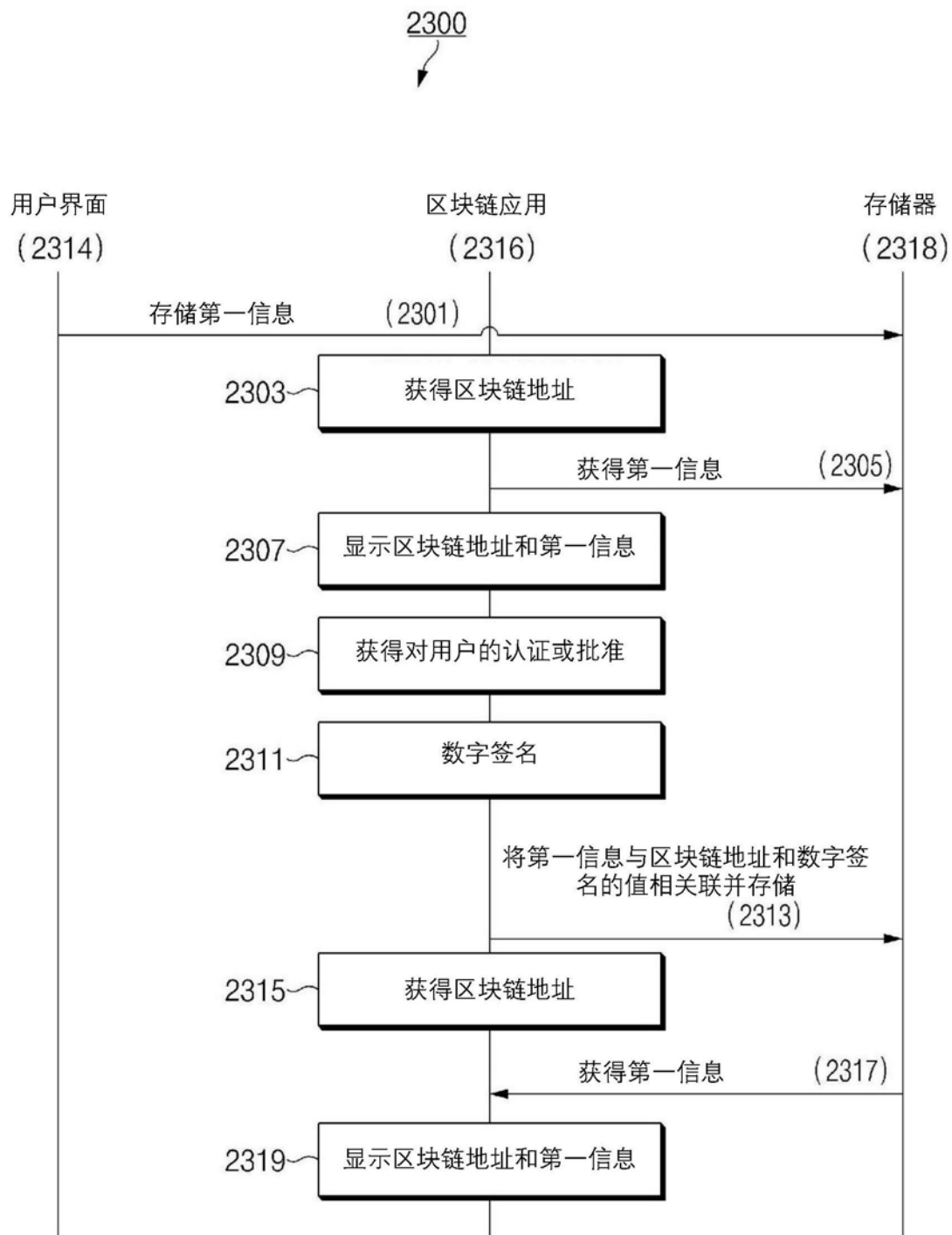


图23