(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108764869 A
(43)申请公布日 2018.11.06

(21)申请号 201810521416.6

(22)申请日 2018.05.28

(71)申请人 北京比特大陆科技有限公司
地址 100192 北京市海淀区奥北科技园25号楼2层

(72)发明人 张理 付红勋

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)

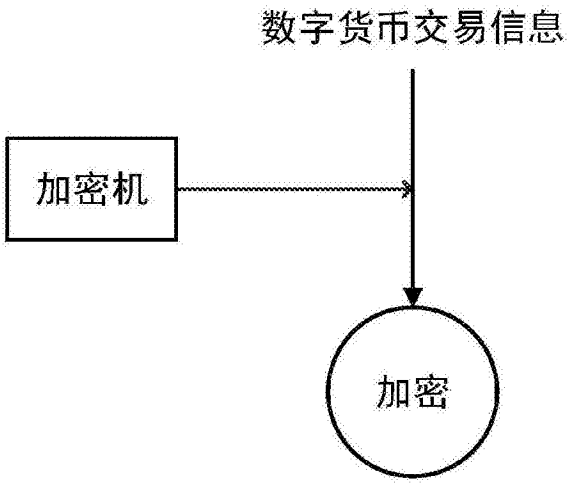
权利要求书2页 说明书5页 附图9页

(54)发明名称

一种实现交易信息加密的方法和装置

(57)摘要

本申请提供了一种实现数字货币交易信息加密的方法和装置，以利用加密机实现数字货币交易信息的加密。本申请还提供了一种电子设备，包括：至少一个处理器；以及与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行时，使所述至少一个处理器执行上述的实现数字货币交易信息加密的方法。



CN 108764869 A

1.一种实现数字货币交易信息加密的方法,其特征在于,包括:利用加密机实现数字货币交易信息的加密。

2.根据权利要求1所述的方法,其特征在于,所述利用加密机实现数字货币交易信息的加密包括:利用在所述加密机中生成的用于数字货币的密钥对所述数字货币交易信息进行加密。

3.根据权利要求2所述的方法,其特征在于,

所述密钥包括私钥;

所述加密的方式包括:利用所述私钥对所述数字货币交易信息进行加密。

4.根据权利要求2所述的方法,其特征在于,还包括:根据数字货币加密算法生成所述密钥。

5.根据权利要求4所述的方法,其特征在于,

所述密钥包括私钥;

生成所述密钥的方式包括:根据所述数字货币加密算法生成所述私钥。

6.根据权利要求5所述的方法,其特征在于,

所述密钥还包括公钥;

生成所述密钥的方式还包括:根据所述数字货币加密算法生成与所述私钥配对的所述公钥。

7.根据权利要求4至6任一项所述的方法,其特征在于,还包括:预设所述数字货币加密算法。

8.根据权利要求7所述的方法,其特征在于,预设所述数字货币加密算法包括:在所述加密机的加密算法库中添加用于加密数字货币的加密算法。

9.根据权利要求4所述的方法,其特征在于,所述数字货币加密算法包括椭圆曲线数字签名算法ECDSA。

10.根据权利要求2至9任一项所述的方法,其特征在于,还包括:执行对所述密钥的管理。

11.根据权利要求10所述的方法,其特征在于,所述管理包括以下至少之一:

对所述密钥的存储;

对所述密钥的分发;

对所述密钥的销毁。

12.根据权利要求1至11任一项所述的方法,其特征在于,所述方法在所述加密机中执行。

13.根据权利要求1所述的方法,其特征在于,还包括以下至少之一:

接收所述数字货币交易信息;

发送加密后的所述数字货币交易信息。

14.一种实现数字货币交易信息加密的装置,其特征在于,用于:利用加密机实现数字货币交易信息的加密。

15.根据权利要求14所述的装置,其特征在于,包括加密模块,用于:利用在所述加密机中生成的用于数字货币的密钥对所述数字货币交易信息进行加密。

16.根据权利要求15所述的装置,其特征在于,

所述密钥包括私钥；

所述加密模块用于：利用所述私钥对所述数字货币交易信息进行加密。

17.根据权利要求15所述的装置，其特征在于，还包括密钥生成模块，用于：根据数字货币加密算法生成所述密钥。

18.根据权利要求17所述的装置，其特征在于，

所述密钥包括私钥；

所述密钥生成模块用于：根据所述数字货币加密算法生成所述私钥。

19.根据权利要求18所述的装置，其特征在于，

所述密钥还包括公钥；

所述密钥生成模块还用于：根据所述数字货币加密算法生成与所述私钥配对的所述公钥。

20.根据权利要求17至19任一项所述的装置，其特征在于，所述密钥生成模块还用于：预设所述数字货币加密算法。

21.根据权利要求20所述的装置，其特征在于，所述密钥生成模块用于：在所述加密机的加密算法库中添加用于加密数字货币的加密算法。

22.根据权利要求21所述的装置，其特征在于，所述数字货币加密算法包括ECDSA。

23.根据权利要求15至22任一项所述的装置，其特征在于，还包括密钥管理模块，用于：执行对所述密钥的管理。

24.根据权利要求23所述的装置，其特征在于，所述密钥管理模块用于执行以下至少之一：

对所述密钥的存储；

对所述密钥的分发；

对所述密钥的销毁。

25.根据权利要求14至24任一项所述的装置，其特征在于，所述装置设置于所述加密机中。

26.根据权利要求25所述的装置，其特征在于，所述加密机为硬件安全模块HSM。

27.根据权利要求14至26任一项所述的装置，其特征在于，还包括接收模块和发送模块中至少之一；

其中，所述接收模块用于：接收所述数字货币交易信息；

所述发送模块用于：发送加密后的所述数字货币交易信息。

28.一种电子设备，其特征在于，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行时，使所述至少一个处理器执行权利要求1-13任一项所述的方法。

一种实现交易信息加密的方法和装置

技术领域

[0001] 本申请涉及数据处理技术领域，例如涉及一种实现数字货币交易信息加密的方法和装置。

背景技术

[0002] 目前，在使用数字货币(例如加密货币)进行交易时，为了保证交易安全性，可以通过交易所完成交易，或使用冷热钱包方案。

发明内容

[0003] 本公开实施例提供了一种实现数字货币交易信息加密的方法，包括：利用加密机实现数字货币交易信息的加密。

[0004] 本公开实施例还提供了一种实现数字货币交易信息加密的装置，用于：利用加密机实现数字货币交易信息的加密。

[0005] 本公开实施例还提供了一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为执行上述的实现数字货币交易信息加密的方法。

[0006] 本公开实施例还提供了一种计算机程序产品，所述计算机程序产品包括存储在计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述的实现数字货币交易信息加密的方法。

[0007] 本公开实施例还提供了一种电子设备，包括：

[0008] 至少一个处理器；以及

[0009] 与所述至少一个处理器通信连接的存储器；其中，

[0010] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行时，使所述至少一个处理器执行上述的实现数字货币交易信息加密的方法。

附图说明

[0011] 一个或多个实施例通过与之对应的附图进行示例性说明，这些示例性说明和附图并不构成对实施例的限定，附图中具有相同参考数字标号的元件表示为类似的元件，附图不构成比例限制，并且其中：

[0012] 图1为本公开实施例的实现数字货币交易信息加密的方法示意图；

[0013] 图2为本公开实施例的对数字货币交易信息进行加密的方法示意图；

[0014] 图3为本公开实施例的对数字货币交易信息进行加密的又一方法示意图；

[0015] 图4为本公开实施例的生成密钥的方法示意图；

[0016] 图5为本公开实施例的预设数字货币加密算法的方法示意图；

[0017] 图6为本公开实施例的执行密钥管理的方法示意图；

[0018] 图7为本公开实施例的收发数字货币交易信息的方法示意图；

[0019] 图8为本公开实施例的实现数字货币交易信息加密的装置示意图；

[0020] 图9为本公开实施例的对数字货币交易信息进行加密的装置示意图；

[0021] 图10为本公开实施例的对数字货币交易信息进行加密的又一装置示意图；

[0022] 图11为本公开实施例的生成密钥的装置示意图；

[0023] 图12为本公开实施例的预设数字货币加密算法的装置示意图；

[0024] 图13为本公开实施例的执行密钥管理的装置示意图；

[0025] 图14为本公开实施例的收发数字货币交易信息的装置示意图；以及

[0026] 图15为本公开实施例提供的电子设备的结构示意图。

[0027] 附图标记：

1：加密机；10：实现数字货币交易信息加密的装置；20：加密模块；30：密钥生成模块；40：加密算法库；50：密钥管理模块；60：接收模块；70：发送模块；80：交易生成系统；90：交易发布系统。

具体实施方式

[0028] 为了能够更加详尽地了解本公开实施例的特点与技术内容，下面结合附图对本公开实施例的实现进行详细阐述，所附附图仅供参考说明之用，并非用来限定本公开实施例。在以下的技术描述中，为方便解释起见，通过多个细节以提供对所披露实施例的充分理解。然而，在没有这些细节的情况下，一个或多个实施例仍然可以实施。在其它情况下，为简化附图，熟知的结构和装置可以简化展示。

[0029] 参见图1，本公开实施例提供了一种实现数字货币交易信息加密的方法，包括：利用加密机实现数字货币交易信息的加密。

[0030] 参见图2，所述利用加密机实现数字货币交易信息的加密，可以包括：利用在所述加密机中生成的用于数字货币的密钥对所述数字货币交易信息进行加密。

[0031] 参见图3，所述密钥可以包括私钥；所述加密的方式可以包括：利用所述私钥对所述数字货币交易信息进行加密。

[0032] 参见图4，可以根据数字货币加密算法生成所述密钥。

[0033] 作为一个实施例，在所述密钥包括私钥的情况下，生成所述密钥的方式可以包括：根据所述数字货币加密算法生成所述私钥。

[0034] 作为一个实施例，所述密钥还可以包括公钥；生成所述密钥的方式还可以包括：根据所述数字货币加密算法生成与所述私钥配对的所述公钥。

[0035] 参见图5，可以预设所述数字货币加密算法。

[0036] 作为一个实施例，预设所述数字货币加密算法，可以包括：在所述加密机的加密算法库中添加用于加密数字货币的加密算法。例如：在所述加密机的加密算法库中添加用于执行所述数字货币加密算法的代码。

[0037] 作为一个实施例，也可以在其它位置预设所述数字货币加密算法，只要能够成功获取、使用所述数字货币加密算法即可。

[0038] 作为一个实施例，所述数字货币加密算法可以包括椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm,ECDSA)。

[0039] 作为一个实施例，所述ECDSA可以基于椭圆曲线密码学(Elliptic curve cryptography,ECC)曲线实现；所述ECC曲线可以包括Secp256k1曲线等。

[0040] 参见图6,可以执行对所述密钥的管理。

[0041] 作为一个实施例,对所述密钥的管理可以包括以下至少之一:

[0042] 对所述密钥的存储;

[0043] 对所述密钥的分发;

[0044] 对所述密钥的销毁。

[0045] 其中,可以将所述密钥保存在加密机中;还可以将所述密钥备份到存储服务器中。可以在受到非法入侵或其它预设条件满足时主动或被动地删除所述密钥。

[0046] 作为一个实施例,上述的实现数字货币交易信息加密的方法可以在加密机中执行。

[0047] 参见图7,可以执行如下操作中至少之一:

[0048] 接收所述数字货币交易信息;例如:接收来自交易生成系统的所述数字货币交易信息;

[0049] 发送加密后的所述数字货币交易信息;例如:将加密后的所述数字货币交易信息发送到交易发布系统,由交易发布系统将加密后的所述数字货币交易信息发布到点对点(P2P)网络中。

[0050] 参见图8,本公开实施例还提供了一种实现数字货币交易信息加密的装置10,用于:利用加密机1实现数字货币交易信息的加密。

[0051] 参见图9,所述装置10可以包括加密模块20,用于:利用在所述加密机1中生成的用于数字货币的密钥对所述数字货币交易信息进行加密。

[0052] 参见图10,所述密钥可以包括私钥;所述加密模块20可以用于:利用所述私钥对所述数字货币交易信息进行加密。

[0053] 参见图11,所述装置10还可以包括密钥生成模块30,用于:根据数字货币加密算法生成所述密钥。

[0054] 作为一个实施例,在所述密钥包括私钥的情况下,所述密钥生成模块30可以用于:根据所述数字货币加密算法生成所述私钥。

[0055] 作为一个实施例,所述密钥还可以包括公钥;所述密钥生成模块30还可以用于:根据所述数字货币加密算法生成与所述私钥配对的所述公钥。

[0056] 参见图12,所述密钥生成模块30还可以用于:预设所述数字货币加密算法。

[0057] 作为一个实施例,所述密钥生成模块30可以用于:在所述加密机1的加密算法库40中添加用于加密数字货币的加密算法。例如:在所述加密机1的加密算法库40中添加用于执行所述数字货币加密算法的代码。

[0058] 作为一个实施例,也可以在其它位置预设所述数字货币加密算法,只要能够成功获取、使用所述数字货币加密算法即可。

[0059] 作为一个实施例,所述数字货币加密算法可以包括ECDSA。

[0060] 作为一个实施例,所述ECDSA可以基于ECC曲线实现;所述ECC曲线可以包括Secp256k1曲线等。

[0061] 参见图13,所述装置10还可以包括密钥管理模块50,用于:执行对所述密钥的管理。

[0062] 作为一个实施例,所述密钥管理模块50可以用于执行以下至少之一:

[0063] 对所述密钥的存储；

[0064] 对所述密钥的分发；

[0065] 对所述密钥的销毁。

[0066] 其中，可以将所述密钥保存在加密机1中；还可以将所述密钥备份到存储服务器中。可以在受到非法入侵或其它预设条件满足时主动或被动地删除所述密钥。

[0067] 作为一个实施例，所述装置10可以设置于加密机1中。

[0068] 作为一个实施例，所述加密机1可以为硬件安全模块(Hardware Security Module，HSM)。

[0069] 参见图14，所述装置10还可以包括接收模块60和发送模块70中至少之一；

[0070] 其中，所述接收模块60可以用于：接收所述数字货币交易信息；例如：接收来自交易生成系统80的所述数字货币交易信息；

[0071] 所述发送模块70可以用于：发送加密后的所述数字货币交易信息；例如：将加密后的所述数字货币交易信息发送到交易发布系统90，由交易发布系统90发布加密后的所述数字货币交易信息(例如，发布到P2P网络中)。

[0072] 本公开实施例还提供了一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令设置为执行上述实施例的实现数字货币交易信息加密的方法。

[0073] 本公开实施例还提供了一种计算机程序产品，所述计算机程序产品包括存储在计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述实施例的实现数字货币交易信息加密的方法。

[0074] 上述的计算机可读存储介质可以是暂态计算机可读存储介质，也可以是非暂态计算机可读存储介质。

[0075] 本公开实施例还提供了一种电子设备，其结构如图15所示，电子设备150包括：

[0076] 至少一个处理器(processor)151，图15中以一个处理器151为例；和存储器(memory)152，还可以包括通信接口(Communication Interface)153和总线154。其中，处理器151、通信接口153、存储器152可以通过总线154完成相互间的通信。通信接口153可以用于信息传输。处理器151可以调用存储器152中的逻辑指令，以执行上述实施例的实现数字货币交易信息加密的方法。

[0077] 此外，上述的存储器152中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。

[0078] 存储器152作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序，如本公开实施例中的方法对应的程序指令/模块。处理器151通过运行存储在存储器152中的软件程序、指令以及模块，从而执行功能应用以及数据处理，即实现上述方法实施例中的实现数字货币交易信息加密的方法。

[0079] 存储器152可包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序；存储数据区可存储根据终端设备的使用所创建的数据等。此外，存储器152可以包括高速随机存取存储器，还可以包括非易失性存储器。

[0080] 本公开实施例的实现数字货币交易信息加密的方案，提高了涉及数字货币的交易的安全性。

[0081] 本公开实施例的技术方案可以以软件产品的形式体现出来，该计算机软件产品存

储在一个存储介质中，包括一个或多个指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本公开实施例所述方法的全部或部分步骤。而前述的存储介质可以是非暂态存储介质，包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等多种可以存储程序代码的介质，也可以是暂态存储介质。

[0082] 当用于本申请中时，虽然术语“第一”、“第二”等可能会在本申请中使用以描述各元件，但这些元件不应受到这些术语的限制。这些术语仅用于将一个元件与另一个元件区别开。比如，在不改变描述的含义的情况下，第一元件可以叫做第二元件，并且同样第，第二元件可以叫做第一元件，只要所有出现的“第一元件”一致重命名并且所有出现的“第二元件”一致重命名即可。第一元件和第二元件都是元件，但可以不是相同的元件。

[0083] 本申请中使用的用词仅用于描述实施例并且不用于限制权利要求。如在实施例以及权利要求的描述中使用的，除非上下文清楚地表明，否则单数形式的“一个”(a)、“一个”(an)和“所述”(the)旨在同样包括复数形式。类似地，如在本申请中所使用的术语“和/或”是指包含一个或一个以上相关联的列出的任何以及所有可能的组合。另外，当用于本申请中时，术语“包括”(comprise)及其变型“包括”(comprises)和/或包括(comprising)等指陈述的特征、整体、步骤、操作、元素，和/或组件的存在，但不排除一个或一个以上其它特征、整体、步骤、操作、元素、组件和/或这些的分组的存在或添加。

[0084] 所描述的实施例中的各方面、实施方式、实现或特征能够单独使用或以任意组合的方式使用。所描述的实施例中的各方面可由软件、硬件或软硬件的结合实现。所描述的实施例也可以由存储有计算机可读代码的计算机可读介质体现，该计算机可读代码包括可由至少一个计算装置执行的指令。所述计算机可读介质可与任何能够存储数据的数据存储装置相关联，该数据可由计算机系统读取。用于举例的计算机可读介质可以包括只读存储器、随机存取存储器、CD-ROM、HDD、DVD、磁带以及光数据存储装置等。所述计算机可读介质还可以分布于通过网络联接的计算机系统中，这样计算机可读代码就可以分布式存储并执行。

[0085] 上述技术描述可参照附图，这些附图形成了本申请的一部分，并且通过描述在附图中示出了依照所描述的实施例的实施方式。虽然这些实施例描述的足够详细以使本领域技术人员能够实现这些实施例，但这些实施例是非限制性的；这样就可以使用其它的实施例，并且在不脱离所描述的实施例的范围的情况下还可以做出变化。比如，流程图中所描述的操作顺序是非限制性的，因此在流程图中阐释并且根据流程图描述的两个或两个以上操作的顺序可以根据若干实施例进行改变。作为另一个例子，在若干实施例中，在流程图中阐释并且根据流程图描述的一个或一个以上操作是可选的，或是可删除的。另外，某些步骤或功能可以添加到所公开的实施例中，或两个以上的步骤顺序被置换。所有这些变化被认为包含在所公开的实施例以及权利要求中。

[0086] 另外，上述技术描述中使用术语以提供所描述的实施例的透彻理解。然而，并不需要过于详细的细节以实现所描述的实施例。因此，实施例的上述描述是为了阐释和描述而呈现的。上述描述中所呈现的实施例以及根据这些实施例所公开的例子是单独提供的，以添加上下文并有助于理解所描述的实施例。上述说明书不用于做到无遗漏或将所描述的实施例限制到本公开的精确形式。根据上述教导，若干修改、选择适用以及变化是可行的。在某些情况下，没有详细描述为人所熟知的处理步骤以避免不必要地影响所描述的实施例。

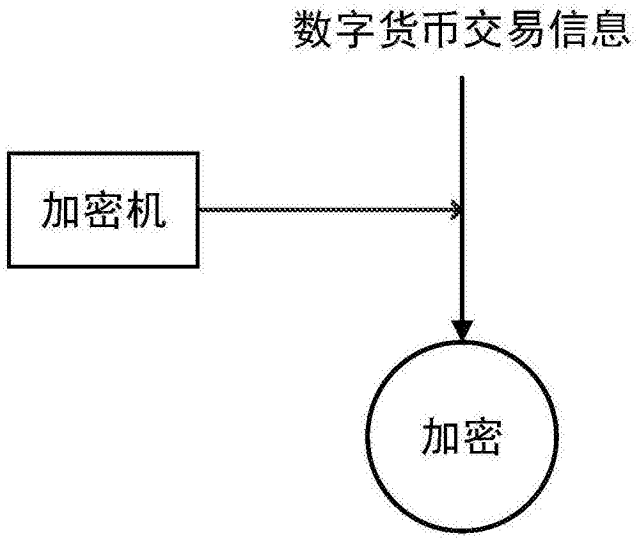


图1

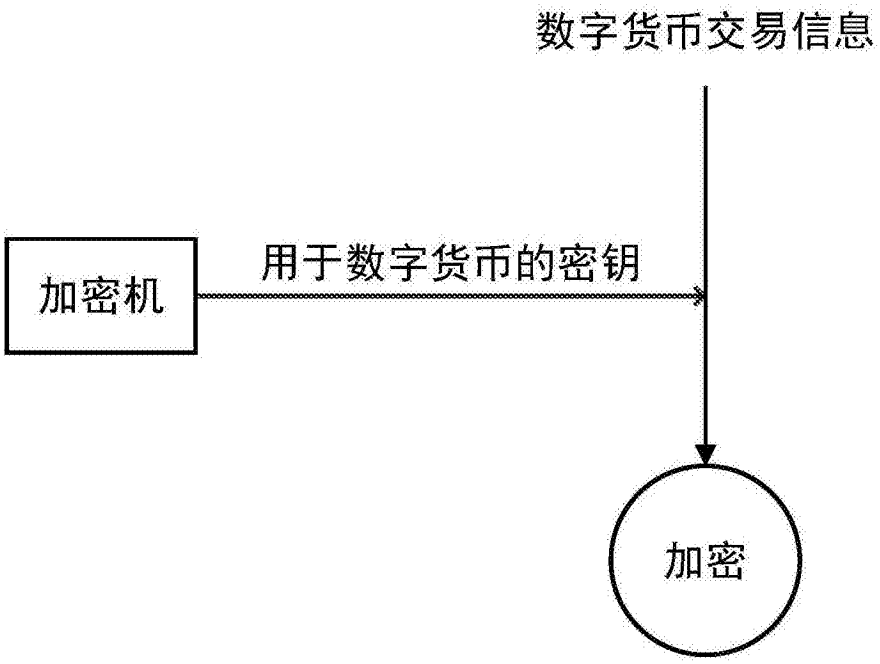


图2

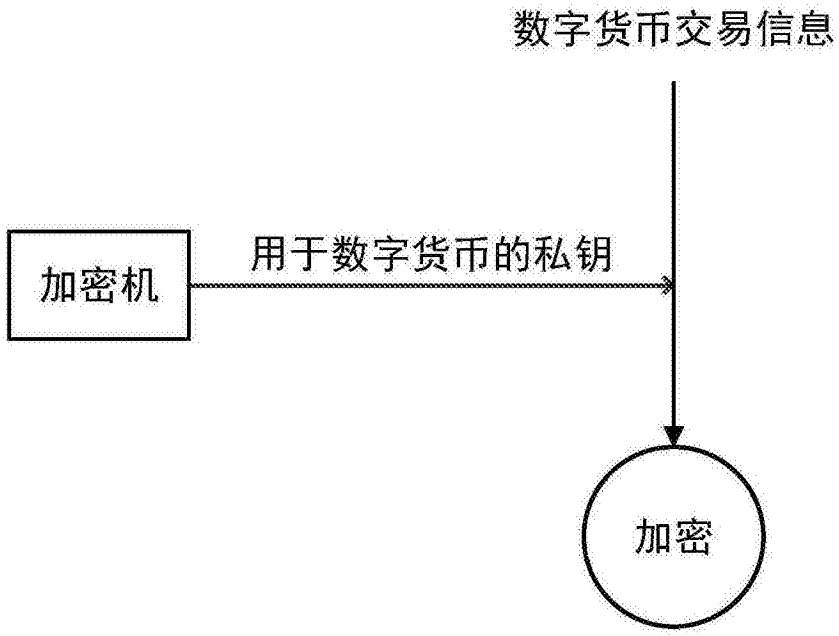


图3

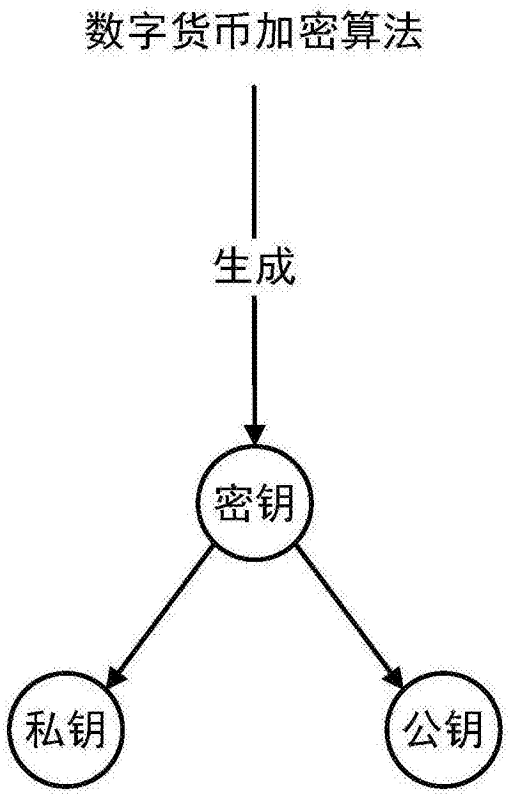


图4

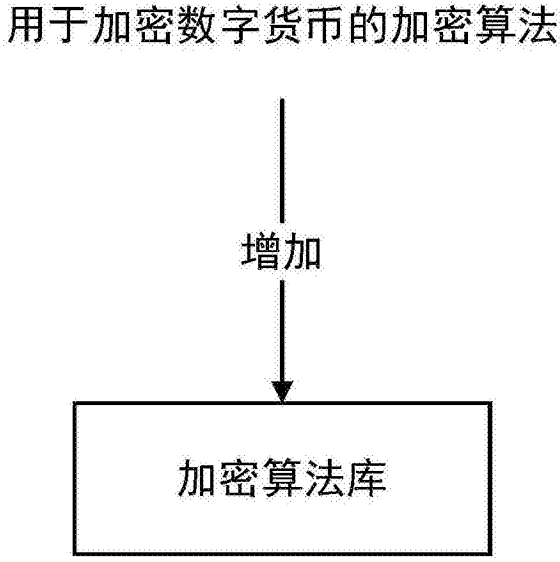


图5

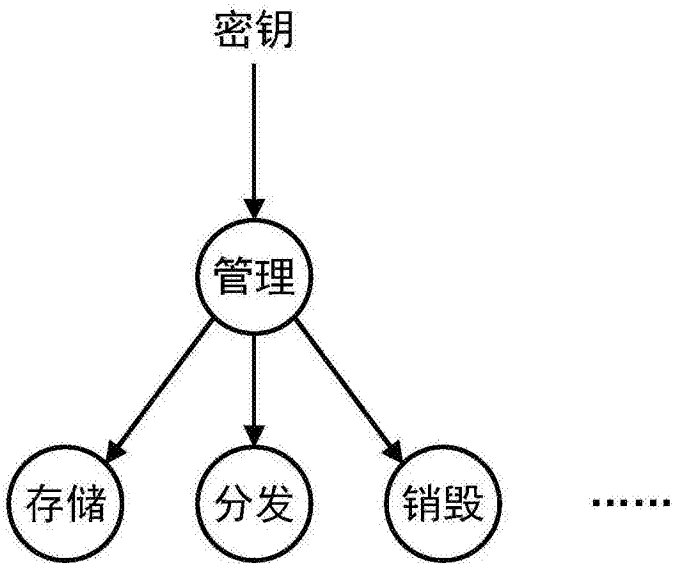


图6

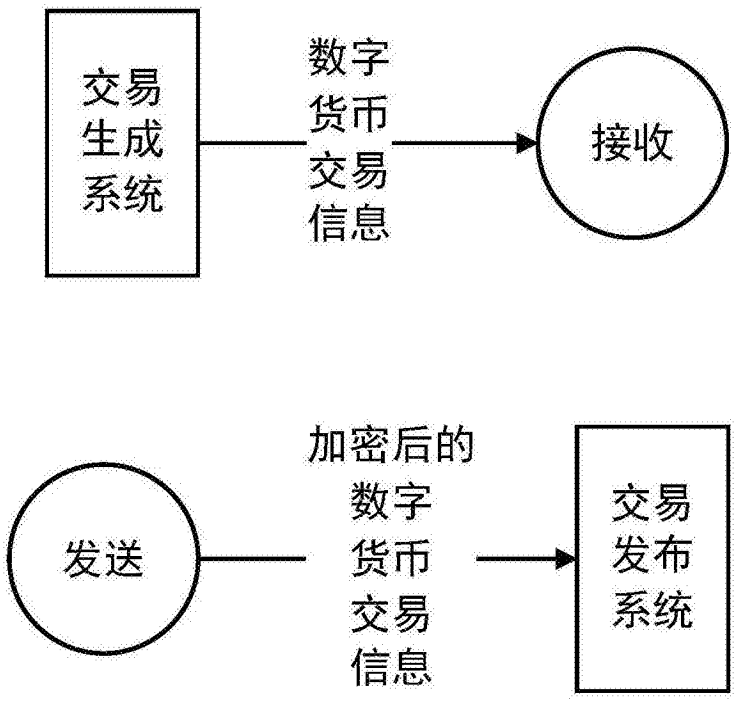

交易生成系统
数字货币交易信息
接收
发送
加密后的数字货币交易信息
交易发布系统

图7

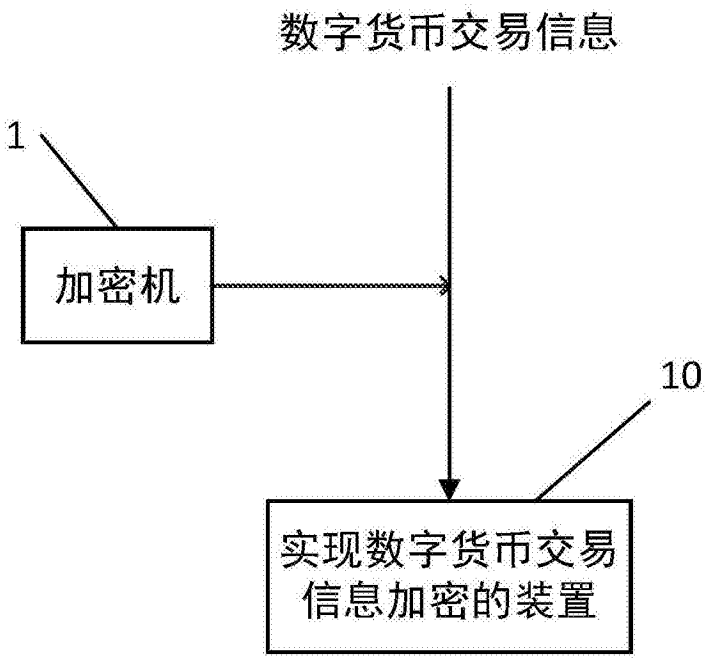

数字货币交易信息
1
加密机
10
实现数字货币交易信息加密的装置

图8

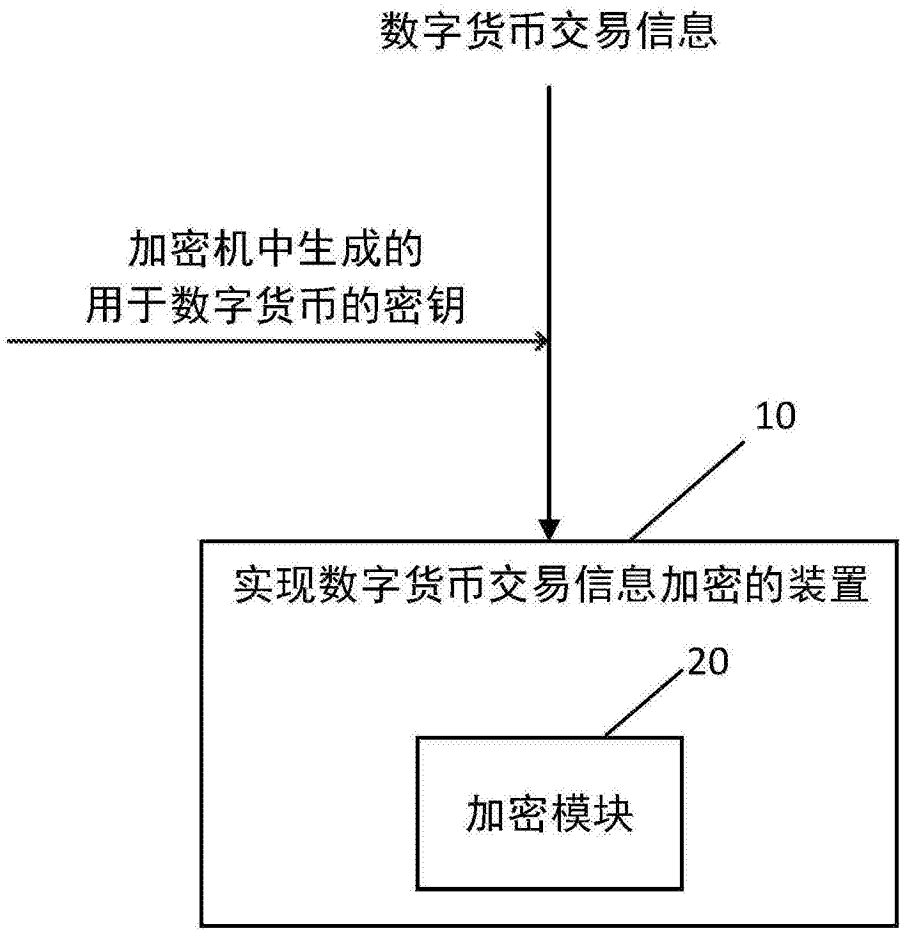


图9

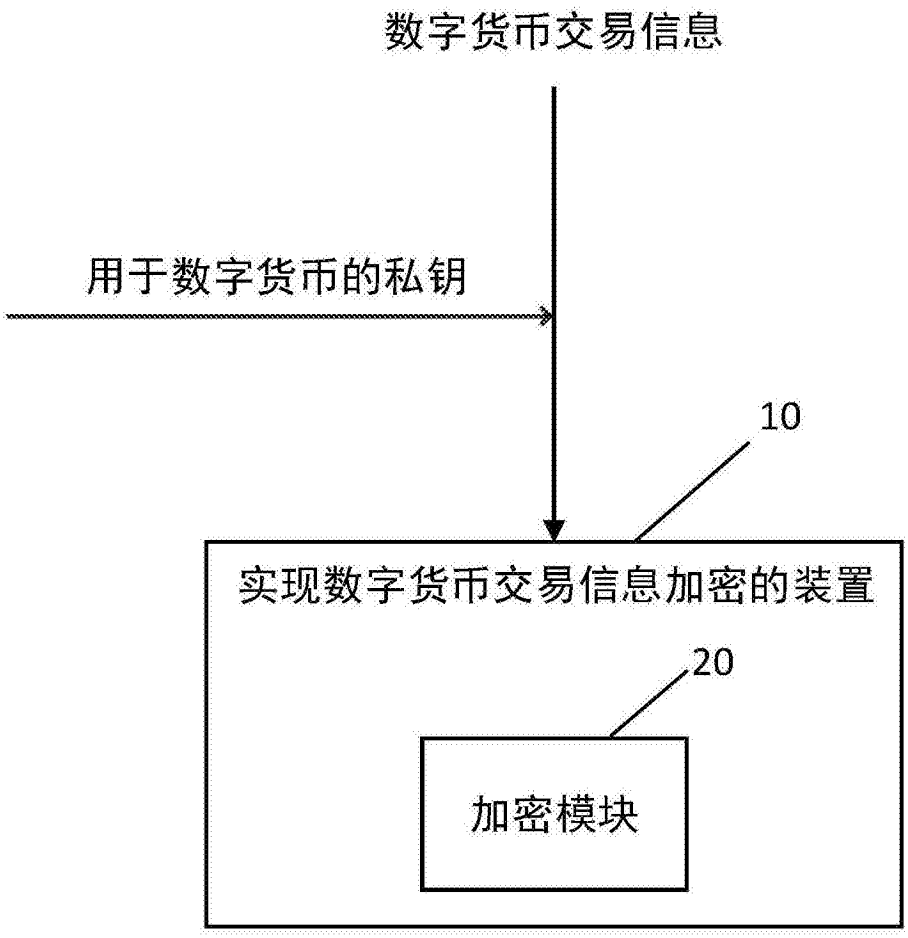


图10

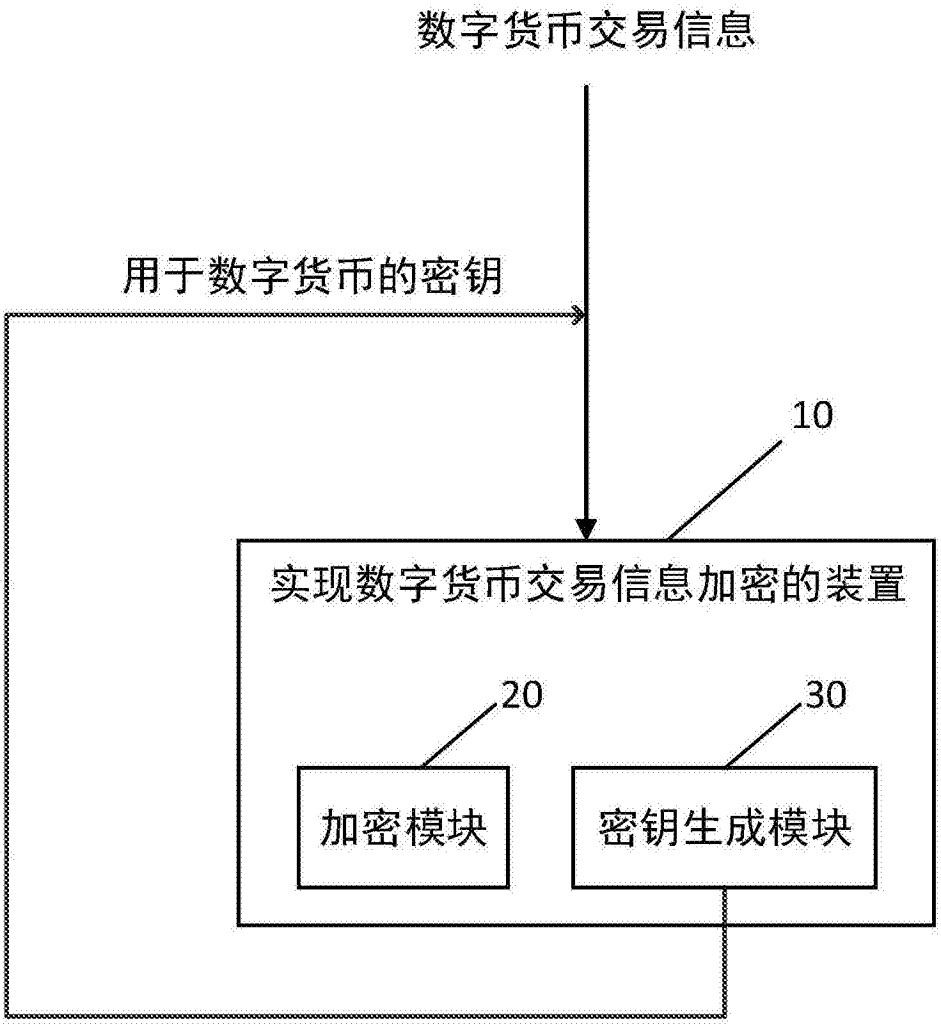


图11

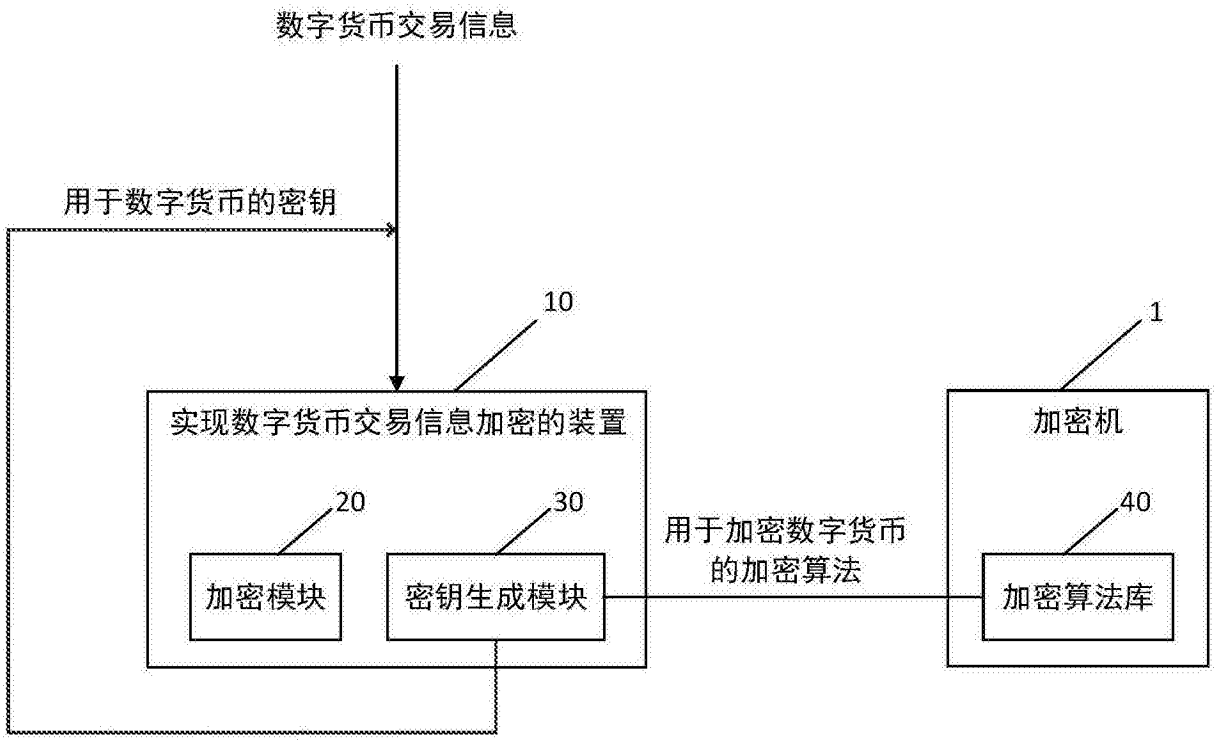

数字货币交易信息
用于数字货币的密钥
10
1
实现数字货币交易信息加密的装置
加密机
20
30
40
加密模块
密钥生成模块
用于加密数字货币的加密算法
加密算法库

图12

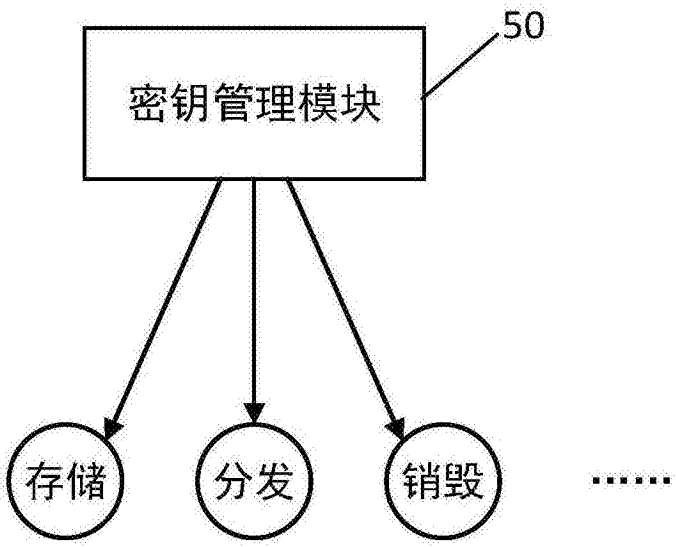

50
密钥管理模块
存储
分发
销毁
……

图13

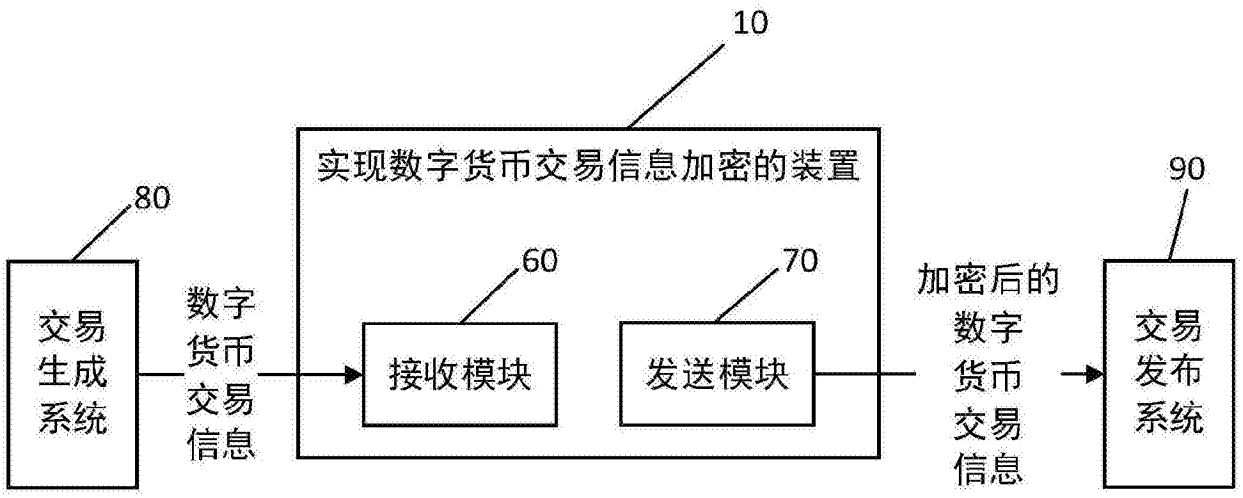

10
实现数字货币交易信息加密的装置
80
交易生成系统
数字货币交易信息
60
接收模块
70
发送模块
加密后的数字货币交易信息
90
交易发布系统

图14

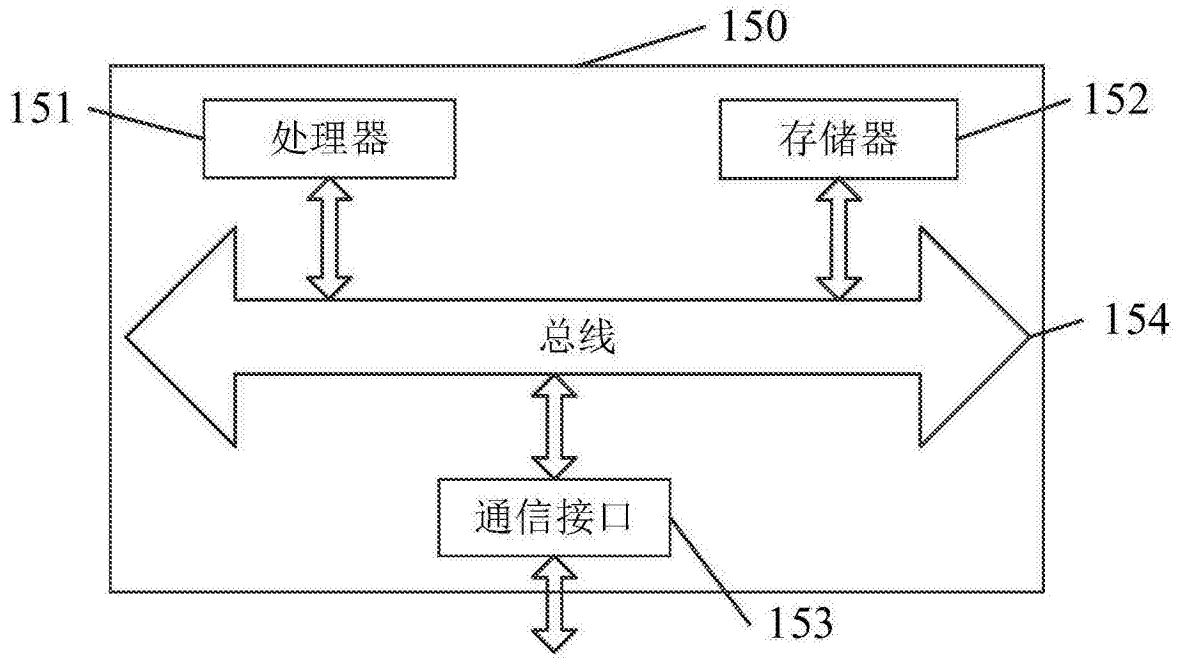

150
151
处理器
存储器
152
总线
154
通信接口
153

图15