(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 107851252 B
(45)授权公告日 2022.07.19

(21)申请号 201680030320.9
(22)申请日 2016.05.25
(65)同一申请的已公布的文献号
申请公布号 CN 107851252 A
(43)申请公布日 2018.03.27
(30)优先权数据
62/166,515 2015.05.26 US
(85)PCT国际申请进入国家阶段日
2017.11.24
(86)PCT国际申请的申请数据
PCT/US2016/034130 2016.05.25
(87)PCT国际申请的公布数据
WO2017/027082 EN 2017.02.16
(73)专利权人 缇零知识产权有限责任公司
地址 美国纽约州
(72)发明人 A·威尔金斯 E·N·费什
T·N·拉森
(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 金红莲 钱慰民
(51)Int.Cl.
G06Q 20/38(2006.01)
(56)对比文件
US 2009177591A1 ,2009.07.09
CN 1328675 A,2001.12.26
CN 102609841 A,2012.07.25
CN 102801710 A,2012.11.28
CN 1399756 A,2003.02.26
CN 101860548 A,2010.10.13
CN 1439138 A,2003.08.27
CN 1320877 A,2001.11.07
CN 102938120 A,2013.02.20
CN 1366263 A,2002.08.28
WO 2014063937 A1,2014.05.01
CN 101819614 A,2010.09.01
US 2013268772A1 ,2013.10.10
审查员 侯鹏

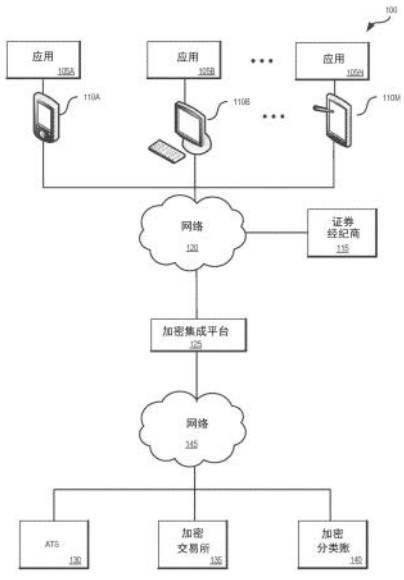
权利要求书4页 说明书18页 附图11页

(54)发明名称

使用加密技术在交易中对意向进行模糊

(57)摘要

本文所描述的方法和系统通过对订单进行模糊直到执行并且通过使用数字分类账指定所述订单的优先级来防止交易者利用订单意向和硬件解决方案推进他们的订单位置。如在此所描述的,使用一系列加密密钥对,可以创建、匹配并且执行交易的一方,而直到所述交易完成之后才对公共记录进行记录和维护而不进行模糊(即,未公开透明)。



CN 107851252 B

1.一种非暂态计算机可读存储介质,包括一组指令,所述指令在由一个或多个处理器执行时使得机器:

接收用于经由交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单,

创建已委托订单交易,所述已委托订单交易识别与所述订单相关联的数据,

使用与第一编址账户相关联的第一至少一个证书对与所述订单相关联的所述数据进行加密以创建经加密订单,其中,与所述第一编址账户相关联的所述第一至少一个证书受所述交易系统控制;

使用与第二编址账户相关联的第二至少一个证书对所述已委托订单交易进行加密签名,以便将所述已委托订单交易传送至所述第一编址账户;

通过所述交易系统利用与所述第一编址账户相关联的另外的至少一个证书对所述经加密订单进行解密以创建未经加密的订单;

将未经加密的所述订单与第二订单进行匹配,以便对所述至少一个其他数字交易品的至少第一部分进行交易;并且

通过从所述第一编址账户将所述至少一个数字交易品的第二部分加密传送并且将所述至少一个其他数字交易品的所述至少第一部分加密传送至与客户相关联的第三编址账户来执行第一交易。

2.如权利要求1所述的非暂态计算机可读存储介质,其中,所述一组指令在由所述一个或多个处理器执行时进一步使得所述机器:

以未经加密格式生成所述第一交易的已执行交易数据;

判定所述订单是否已经由所述第一交易完成;并且

当所述订单已经由所述第一交易完成时,向分布式分类账发送用于以所述未经加密格式来记录所述第一交易的所述已执行交易数据的请求。

3.如权利要求2所述的非暂态计算机可读存储介质,其中,所述一组指令在由所述一个或多个处理器执行时进一步使得所述机器:

当所述订单尚未由所述第一交易完成时,等待直到所述订单已经由所述第一交易和随后交易完成;以及

在所述订单已经由所述第一交易和所述随后交易完成之后:向所述分布式分类账发送用于以所述未经加密格式来记录所述第一交易和所述随后交易中的每一次交易的所述已执行交易数据的请求。

4.一种用于交易系统的计算机化方法,包括:

接收用于经由所述交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单;

创建已委托订单交易,所述已委托订单交易识别与所述订单相关联的数据;

使用与第一编址账户相关联的第一至少一个证书对与所述订单相关联的所述数据进行加密,其中,与所述第一编址账户相关联的所述第一至少一个证书受所述交易系统控制;

使用与第二编址账户相关联的第二至少一个证书对所述已委托订单交易进行加密签名;以及

经由被记录到分布式分类账的记录来验证所述订单已经被完成,其中,所述记录包括

采用未经加密格式的与所述订单相关联的至少第一已执行交易的已执行交易数据，其中，采用所述未经加密格式的所述已执行交易数据直到所述订单已经被完成才会被记录。

5.如权利要求4所述的计算机化方法，进一步包括：

向所述分布式分类账发送用于记录具有经加密数据的所述已委托订单交易的请求，其中，所述分布式分类账为所述订单指定优先级。

6.如权利要求4所述的计算机化方法，进一步包括：

在所述订单已经由所述交易系统验证、解密、匹配和执行之后，将所述至少一个其他数字交易品接收到第三编址账户中。

7.如权利要求4所述的计算机化方法，进一步包括：

在接收到用于对所述至少一个数字交易品进行交易的所述订单之后，验证所述至少一个数字交易品与第三编址账户相关联；以及

当所述至少一个数字交易品与所述第三编址账户相关联时，创建委托交易以便将所述至少一个数字交易品加密传送至所述第一编址账户，

其中，创建所述已委托订单交易进一步包括在所述已委托订单交易中引用所述委托交易以便防止在第二已委托订单交易中引用所述至少一个数字交易品。

8.如权利要求4所述的计算机化方法，其中，所述至少一个数字交易品包括数字证券或基金的数字表示，其中，所述数据包括以下各项中的一项或多项：所述至少一个数字交易品的身份、购入或卖出所述至少一个数字交易品的价格以及购入或卖出所述至少一个数字交易品的数量。

9.一种加密集成系统，包括：

至少一个处理器；以及

至少一个计算机可读存储介质，其上存储有指令，所述指令在由所述至少一个处理器执行时使得所述加密集成系统：

接收用于经由交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单；

创建已委托订单交易，所述已委托订单交易识别与所述订单相关联的数据；

使用与第一编址账户相关联的第一至少一个证书对与所述订单相关联的所述数据进行加密，其中，与所述第一编址账户相关联的所述第一至少一个证书受所述交易系统控制；

使用与第二编址账户相关联的第二至少一个证书对所述已委托订单交易进行加密签名；并且

经由被记录到分布式分类账的记录来验证所述订单已经被完成，其中，所述记录包括采用未经加密格式的与所述订单相关联的至少第一已执行交易的已执行交易数据，其中，采用所述未经加密格式的所述已执行交易数据直到所述订单已经被完成才会被记录。

10.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

向所述分布式分类账发送用于记录具有经加密数据的所述已委托订单交易的请求，其中，所述分布式分类账为所述订单指定优先级。

11.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

在所述订单已经由所述交易系统验证、解密、匹配和执行之后，将所述至少一个其他数字交易品接收到第三编址账户中。

12.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

在接收到用于对所述至少一个数字交易品进行交易的所述订单之后，验证所述至少一个数字交易品与第三编址账户相关联；并且

当所述至少一个数字交易品与所述第三编址账户相关联时，创建委托交易以便将所述至少一个数字交易品加密传送至所述第一编址账户，

其中，在由所述至少一个处理器执行时使得所述加密集成系统创建所述已委托订单交易的所述指令进一步使得所述加密集成系统：在所述已委托订单交易中引用所述委托交易以防止在第二已委托订单交易中引用所述至少一个数字交易品。

13.一种用于交易系统的计算机化方法，包括：

将经加密订单接收到第一客户委托编址账户中以便对至少一个数字交易品进行交易以交换至少一个其他数字交易品；

通过所述交易系统使用与所述第一客户委托编址账户相关联的第一至少一个证书对所述经加密订单进行解密以创建未经加密的订单；

将未经加密的所述订单与第二订单进行匹配，以便对所述至少一个数字交易品的至少一部分进行交易；

通过从所述第一客户委托编址账户将所述至少一个数字交易品的所述至少一部分加密传送并且将所述至少一个其他数字交易品的至少其他部分加密传送至第一客户文件夹编址账户来执行第一交易；以及

当未经加密的所述订单已经被完成时，向用于进行记录的分布式分类账发送所述第一交易的已执行交易数据以便允许对未经加密的所述订单和所述交易进行第三方验证，所述已执行交易数据包括采用未经加密格式的来自未经加密的所述订单的数据。

14.如权利要求13所述的计算机化方法，其中，将所述经加密订单记录到所述分布式分类账，所述分布式分类账基于在所述分布式分类账处的接收时间来为所述经加密订单指定优先级，并且其中，将未经加密的所述订单与所述第二订单进行匹配是基于所述优先级进行的。

15.如权利要求13所述的计算机化方法，进一步包括：使用证券经纪商账户的证书来验证所述经加密订单的发送者，其中，所述证书为公钥。

16.如权利要求13所述的计算机化方法，进一步包括：通过加密传送所述至少一个数字交易品的第二部分来执行第二交易，其中，所述已执行交易数据包括来自所述交易和所述第二交易两者的数据。

17.一种交易系统，包括：

至少一个处理器；以及

至少一个计算机可读存储介质，其上存储有指令，所述指令在由所述至少一个处理器执行时使得所述交易系统：

将经加密订单接收到第一客户委托编址账户中以便对至少一个数字交易品进行交易以交换至少一个其他数字交易品；

使用与所述第一客户委托编址账户相关联的第一至少一个证书对所述经加密订单进行解密以创建未经加密的订单；

将未经加密的所述订单与第二订单进行匹配，以便对所述至少一个数字交易品的至少一部分进行交易；

通过从所述第一客户委托编址账户将所述至少一个数字交易品的所述至少一部分加密传送并且将所述至少一个其他数字交易品的至少其他部分加密传送至第一客户文件夹编址账户来执行第一交易；并且

当未经加密的所述订单已经被完成时，向用于进行记录的分布式分类账发送所述第一交易的已执行交易数据以便允许对未经加密的所述订单和所述交易进行第三方验证，所述已执行交易数据包括采用未经加密格式的来自未经加密的所述订单的数据。

18.如权利要求17所述的交易系统，其中，将所述经加密订单记录到所述分布式分类账，所述分布式分类账基于接收时间为所述经加密订单指定优先级，并且其中，将未经加密的所述订单与所述第二订单进行匹配是基于所述优先级进行的。

19.如权利要求17所述的交易系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述交易系统：使用证券经纪商账户的证书来验证所述经加密订单的发送者，其中，所述证书为公钥。

20.如权利要求17所述的交易系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述交易系统：通过加密传送所述至少一个数字交易品的第二部分来执行第二交易，其中，所述已执行交易数据包括来自所述交易和所述第二交易两者的数据。

使用加密技术在交易中对意向进行模糊

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年5月26日提交的名称为“Obfuscation of intent in transactions using cryptographic Techniques(使用加密技术在交易中对意向进行模糊)”的美国临时申请号62/166,515的优先权,所述美国临时申请出于所有目的通过引用以其全文结合在此。

技术领域

[0003] 本公开的各个实施例总体上涉及交易。更具体地,本公开的各个实施例涉及使用分布式技术和加密(“crypto”)技术来在交易中混淆意向的系统和方法。

背景技术

[0004] 抢先交易(front-running)是一种预料即将到来的交易对证券价格的影响并且使用这种信息来影响证券价格的投资策略。在抢先交易中,交易者将刚好在另一个交易者进行使股票向可预测的方向移动的证券持仓之前持仓。当个人交易者刚好在大型机构针对股票下订单(从而导致股票价格快速上涨)前买入股票份额时,发生抢先交易的示例。关于机构订单的信息可以通过监控出价并在市场上进行询问来获得。例如,当订单仅部分地在一个交易所被完成时,可以揭示交易者在其他交易所的交易意向,允许其他投资者基于某次交易对股票价格的可预测影响来使用这种信息得以获利。

[0005] 本技术克服了现有交易系统的这种以及其他限制,并提供了从以下说明中对本领域技术人员将更加清楚的其他益处。

附图说明

[0006] 将通过使用附图来描述和解释本公开的实施例,在附图中:

[0007] 图1根据本公开的各实施例展示了基于网络的操作环境的示例;

[0008] 图2根据本公开的一个或多个实施例展示了加密集成平台中的一组组件;

[0009] 图3根据本公开的一个或多个实施例展示了对订单意向进行模糊直到订单被执行的过程;

[0010] 图4根据本公开的一个或多个实施例图解式地展示了使用对订单的意向进行模糊直到订单被执行的过程的代表性示例;

[0011] 图5根据本公开的一个或多个实施例图解式地展示了用于第三方对订单意向和优先级进行验证的过程的代表性示例;

[0012] 图6是流程图,根据本公开的一个或多个实施例展示了用于对订单的意向进行模糊直到订单被执行的过程;

[0013] 图7是流程图,根据本公开的一个或多个实施例从加密集成平台的角度展示了用于对订单的意向进行模糊直到订单被执行的过程;

[0014] 图8是流程图,根据本公开的一个或多个实施例从交易系统的角度展示了用于对

订单的意向进行模糊直到订单被执行的过程；

[0015] 图9至图10是简图，根据本公开的一个或多个实施例一起展示了对订单的意向进行模糊直到订单被执行的过程；以及

[0016] 图11展示了计算机系统的示例，本公开的一些实施例可以与所述计算机系统一起使用。

具体实施方式

[0017] 本公开的各个实施例总体上涉及买入和卖出证券的交易。更具体地，本公开的各个实施例涉及使用分布式技术和加密(“crypto”)技术对订单意向进行混淆以用于买入或卖出数字交易品的系统和方法。

[0018] 现在，诸如加密交易所(“crypto exchanges”)和替代性交易系统(“ATS”)等多种交易所交易同一证券。当由于订单很大和/或由于证券通常不会以高交易量进行交易而导致订单仅部分地在一个交易所被完成时，在执行交易(也就是说，完成交易)之前能够揭示交易者在其他交易所的交易意向。这种信息可以被其他人恶意地利用以影响证券的价格(即，抢先交易)。例如，高频交易平台(即，使用强大的计算机来快速地交易大量订单的程序交易平台)使用复杂的算法基于市场状况来分析多个市场并且执行订单。这些算法被设计用于留意以下信号：所述信号关于在一个交易所中的订单以及然后在订单被完成用于买入或卖出证券前到下一个交易所进行的竞争，由此影响证券的价格。通常，使用具有最快执行速度的计算机的交易者比使用具有较低执行速度的计算机的交易者获利更高。

[0019] 举例说明了当交易系统变慢时抢先交易和高频交易的影响。使用分类账或区块链来记录交易的交易系统依赖于分布式节点网络。分布式节点网络与可以较缓慢的分类账或区块链进行通信，使得投资者易于受到对他们的订单的预先执行的公开可获得意向的利用的影响。

[0020] 因此，当前系统具有如下的挑战：(1)当关于订单的信息可用时，交易者可能试图去影响市场价格，并且(2)由于订单优先级由在交易所处而不是在订单的创建处接收的订单来决定，可以承担得起最好的硬件并且可以将其算法定位为最接近交易所的交易者可以在先于他们的订单提交的订单前面抢占先机的环境，这种环境创造了一种不公平的优势。

[0021] 当前用于防止抢先交易(例如，暗池交易)的解决方案尚且不足。暗池交易是电子ATS，类似于可以在其中对交易进行匹配的股票交易所。不同于股票交易所，暗池交易中的订单是“暗的”，意味着订单的大小和价格并未透露给其他参与者。然而，暗池交易仅仅限制订单的可视性，而非掩盖信息(即，对暗池的所有者仍具有可视性)。缺乏透明度使得暗池交易易于发生其所有者可能的利益冲突以及一些高频交易者的掠夺性的交易行为。

[0022] 本文所描述的方法和系统防止交易者使用由于信息并未被模糊而允许交易者恶意地使用信息的硬件和软件解决方案。如在此描述的，使用一系列加密密钥对，可以创建、匹配并且执行交易的一方，而直到所述交易完成之后才对公共记录进行记录和维护而不进行模糊(即，还未公开透明)。分布式分类账可以记录并且指定订单的优先级。为了本公开的目的，“对订单意向进行模糊/混淆”、“对订单的意向进行模糊/混淆”、“对意向进行模糊/混淆”等等意味着对关于订单的信息进行模糊，从而使得无法推断出交易者的意向。

[0023] 在加密(“crypto”)交易所(例如，交易数字交易品的交易所)上所交易的用于交易

数字交易品的订单(例如,数字资产、数字负债、商品、数字证券、证券的数字利息、加密货币、资金的数字表示(比如代用货币、现金、现金等价物))可以被接收到传统系统中并且通过集成系统和交易平台(比如加密集成平台)进行处理。加密集成平台(除其他项以外)允许证券经纪商向加密交易所(例如,交易数字交易品的交易所)开放传统交易系统并允许证券发行者进行证券的公开发售并且引导公众在二手市场交易中交易这些证券。在这样做时,加密集成平台使用用于在证券经纪商、ATS与交易所(例如,财务信息交换(Financial Information eXchange)协议)之间进行交易和通信的协议来取得消息(例如,订单),并且变换消息,从而使得可以使用密码技术完善交易。例如,加密集成平台接收订单以便对来自证券经纪商的数字交易品进行交易并将所述订单转化成加密订单。

[0024] 可以使用加密技术(比如,公钥密码技术和双向加密)将经由交易系统(比如,加密交易所和ATS)交易的数字交易品传送至其他所有者。公钥密码技术需要密钥对,其中,这两个密钥在数学上相互联系。一个密钥是在对等网络内的节点之间自由共享的公钥。另一密钥是不与公众共享的私钥。公钥用于对明文进行加密并验证数字签名。私钥用于对密文进行解密并对交易进行数字签名。可以用发送者的私钥对交易消息进行数字签名从而认证发送者的身份。然后,可以使用发送者的公钥对发送者的经数字签名的交易消息进行解密,从而验证发送者发起了所述交易。

[0025] 数字交易品的所有权可以基于由网络节点所维持的分布式分类账中的所有权表项。分布式分类账(例如,用于比特币的区块链)针对每一数字交易品的所有权的每次变更记录表项并且可以与密钥对在数学上相互联系。为了卖出数字资产或数字负债,可以将(例如,数据包或其他数据结构中的)交易消息广播给对等网络上的节点。可以用卖者的私钥对交易消息进行签名,并且交易消息可以包括如数字资产或数字负债的产权链的历史、正传送的份额或商品的数量以及基于购买者公钥的地址等信息。当网络中大部分节点承认发送者具有正确的产权链,将所有权变更给购买者并更新分类账以标示交易。在数字交易品被卖出或订购之前,买者或卖者可能希望对交易保密以防止其他人使用影响数字交易品的价格的信息。

[0026] 在本文中描述的技术的实施方式中,至少三个密钥对是相关的并且与以下三个编址账户相关联:由加密集成平台控制的客户文件夹账户;由一个或多个交易系统(例如,交易所、ATS)控制的客户委托账户;以及由加密集成系统控制的证券经纪商密钥对。通常,由客户持有并且不委托至订单的数字交易品与客户文件夹账户相关联。委托至订单以及已委托订单交易的数字交易品与客户委托账户相关联,从而使得客户委托账户起到代管契约的作用。非委托订单与证券经纪商账户相关联。这些账户中的每个账户被用于对数字交易品进行交易并且更具体地用于当交易数字交易品时对订单意向进行模糊。为了本公开的目的,“编址账户(addressed account)”与“数字账户(digital account)”、“数字钱包(digital wallet)”、“注册表(registry)”、“客户文件夹/委托钱包(customer portfolio/committed wallet)”以及“钱包(wallet)”意思相同。

[0027] 在本公开的实施例中,接收来自证券经纪商的用于在交易系统(比如,ATS或加密交易所)上买卖数字交易品的订单。可以通过交易平台(比如,加密集成平台)接收来自证券经纪商的订单。

[0028] 当加密集成平台接收到交易时,所述加密集成平台可以检查被记录在分布式分类

账上的客户文件夹账户的余额，以确保数字交易品与客户的文件夹账户相关联。如果交易中所涉及的数字交易品与客户的文件夹账户相关联，则加密集成平台可以对交易进行加密签名，以便将与所述交易相关联的数字交易品传送至使用客户的文件夹账户的私钥的客户委托账户，从而创建委托交易。如所讨论的，客户委托账户由交易系统控制。

[0029] 然后，所述加密集成平台进一步创建包括来自订单的数据的已委托订单交易并且引用所述委托交易。加密集成平台使用交易系统的公钥对交易进行加密。在分布式分类账上记录订单(包括对已委托交易的引用)。对订单进行加密并且将其发布到分布式分类账导致订单被模糊(除了对交易所来说)，也就是说，公众可以看到订单的存在但是不能看到订单的内容。在一些实施例中，使用证券经纪商的私钥对订单进行签名(例如，对交易进行授权)，所述私钥可以由交易系统用来确保订单被授权。分布式分类账可以基于由交易系统所接收的订单的时间来指定订单的优先级。在其他实施方式中，分布式分类账可以基于由证券经纪商接收订单的时间来指定优先级。

[0030] 一旦交易系统接收经加密订单，所述交易系统利用交易系统的私钥对订单数据进行解密，并且可以利用证券经纪商的公钥(如果相关)对证券经纪商的签名进行验证。当已经基于订单的优先级定位到可能匹配的订单，交易系统(或者在一些实施例中，加密集成平台)验证数字交易品可用于交易并通过将数字交易品(例如，资金、数字资产/负债)放置到相应的客户文件夹账户中来即刻清算和结算交易。在订单已经被执行之后，公布订单明细。第三方可以通过利用交易系统的公钥对经执行订单进行再加密并将经再加密的订单与原始订单进行对比来验证经执行订单。在一些实施例中，可以部分完成订单。可以在执行之后公布已执行交易的明细，订单意向的明细(例如，所述订单的尚未被完成的剩余部分)在ATS/交易所接收整个订单已被完成的消息之前将不被发布。

[0031] 对订单的意向进行模糊的益处包括消除抢先交易和高频交易。附加益处是创建交易记录，在订单已被执行之后，公众方可以从分类账中重建所述交易记录。在当前系统中，交易者依靠交易系统内的数据源来维护订单。如果交易系统发生故障，则订单将会丢失。然而，使用本文所描述的方法和系统，所述订单被记录在分布式分类账上，从而提供订单记录。此外，对交易进行加密签名保证了认证、授权、和溯源。

[0032] 尽管本公开主要使用本文中所描述的技术讨论了对数字交易品进行交易，本文所描述的技术还可以在交易完成前交易意向应为独立的其他情境中使用。例如，本文所描述的方法和系统可以用于在拍卖完成前对拍卖出价进行模糊。另外，提供博彩服务的系统可以使用所描述的技术来对信息(比如投注或彩票号码)进行模糊。

[0033] 在此所介绍的技术可以被具体化为专用硬件(例如电路系统)、被适当地编程具有软件和/或固件的可编程电路系统、或专用电路系统与可编程电路系统的组合。因此，实施例可以包括具有存储在其上的指令的机器可读介质，所述指令可以用来对计算机(或其他电子设备)进行编程从而执行过程。机器可读介质可以包括例如：软盘、光盘、压缩盘只读存储器(CD-ROM)、磁光盘、只读存储器(ROM)、随机存取存储器(RAM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)、磁卡或光卡、闪速存储器、或者适用于存储电子指令的其它类型的媒体/机器可读介质。在上下文允许的情况下，使用单数或复数形式的词汇还可以分别包括复数或单数形式，并且为简洁起见在本文中不进行区分。

[0034] 图1展示了基于网络的操作环境100的示例，本公开的一些实施例可以用于所述基

于网络的操作环境中。如图1中所展示的，操作环境100包括在一个或多个计算设备110A至110M(比如移动设备、移动电话、平板计算机、移动媒体设备、移动游戏设备、基于车辆的计算机、专用终端、公共终端、台式或膝上计算机、自助服务终端等)上运行的应用105A至105N。在一些实施例中，用于执行比如生成订单和检查账户余额等操作的应用105A至105N可以存储在计算设备上或可以远程地存储。这些计算设备可以包括用于通过经网络120连接至加密集成平台125和证券经纪商115来接收和发送流量的机制。

[0035] 计算设备110A至110M被配置成经由网络120与证券经纪商115和加密集成平台125通信。在一些实施例中，计算设备110A至110M可以检索或向加密集成平台125提交信息，并运行具有加密集成平台125和证券经纪商115所检索的自定义内容的一个或多个应用。例如，计算设备110A至110M各自可以执行浏览器应用或自定义客户端从而使能计算设备110A至110M与加密集成平台125和证券经纪商115之间的交互。

[0036] 证券经纪商115是从事为其自己的账户或代表其客户交易资产(例如，证券、共同基金份额等)的生意的实体(即，自然人、公司、或其他组织)。在代表客户执行交易订单时，所述实体充当经纪人。在为其自己的账户执行交易时，所述实体充当商人。证券经纪商115可以从计算设备110A至110M接收订单或创建其自己的订单。证券经纪商115可以经由网络120将订单传达至加密集成平台125。每个证券经纪商可以具有用于对消息进行签名的密钥对。这种密钥对可以由交易系统(比如，ATS 130或加密交易所135)用于证明所述交易被证券经纪商授权(即，如果证券经纪商使用其私钥对交易进行签名，则ATS 130或加密交易所135可以使用证券经纪商的公钥进行验证)。在一些实施例中，证券经纪商115给予加密集成平台125使用代表证券经纪商115的证券经纪商115私钥的权限。

[0037] 加密集成平台125可以在一个或多个服务器上运行并且可用于对订单进行模糊并且对数字交易品进行交易。在一些实施例中，并且如图2所展示的，加密集成平台125包括加密适配器215、加密桥220、和加密匹配组件225。加密集成平台125通过网络145与一个或多个ATS 130、加密交易所135、和加密分类账140通信地耦合。

[0038] 网络120和网络145可以是同一网络或者可以是单独的网络，并且可以是局域网和/或广域网的任何组合，使用有线和/或无线通信系统。或者网络120或者网络145可以是或者可以使用协议/技术中的任意一项或多项：以太网、IEEE 802.11或WiFi、全球微波互联接入(WiMAX)、蜂窝电信(例如，3G、4G、5G)、CDMA、电缆、数字用户线(DSL)等。类似地，网络120和网络145上使用的联网协议可以包括：多协议标签交换(MPLS)、传输控制协议/互联网协议(TCP/IP)、用户数据报协议(UDP)、超文本传输协议(HTTP)、简单邮件传送协议(SMTP)和文件传送协议(FTP)。可以使用包括超文本标记语言(HTML)或可扩展标记语言(XML)的技术、语言和/或格式表示在网络120和网络145上交换的数据。另外，使用常规加密技术(比如安全套接层(SSL)、传输层安全(TLS)、和互联网协议安全性(IPsec))可以对所有或部分链路进行加密。

[0039] ATS 130是通过匹配买者和卖者来找到交易的相关方的非交易所交易系统。ATS 130是传统股票交易所的替代物。ATS 130的示例包括电子通信网络(ECN)、交叉网络、暗池交易、和短期拆借市场。ATS 130接收来自加密集成平台125的经数字签名的订单，找到用于对数字交易品进行交易的可能买入/卖出订单匹配，并维持记录着所述订单状态的订单状态簿。

[0040] 加密交易所135是对数字交易品进行交易的交易所。加密交易所135接收来自加密集成平台125的经数字签名的加密交易(例如,订单、取消)。在一些实施例中,加密交易所135可以对订单进行解密、匹配和执行,包括将数字交易品传送至客户的文件夹账户。

[0041] 出于本说明书的目的,针对交易系统的订单可能被模糊。诸如加密交易所135和ATS 130(被称为"交易系统"、"ATS 130"、"加密交易所135"、"ATS"、"加密交易所"或者"交易所")的交易系统可以参与如本文中所描述的加密技术。ATS 130具有相关联的密钥对。ATS 130的密钥对的公钥由加密集成平台125使用,具体地由加密桥220使用以用于加密订单。在一些实施例中,ATS 130控制由客户所拥有的密钥对(客户委托钱包的密钥对),ATS使用密钥对以便在订单已完成前保存数字交易品。另外,在优选实施例中,ATS 130具有每个授权的证券经纪商115的公钥。ATS 130中数字交易品的所有权可以记录在一个或多个分布式分类账(比如加密分类账140)上。ATS 130可以从分类账中读取经加密订单,所述分类账引用已委托交易并且可以利用其私钥对订单进行解密。而且,如果交易由证券经纪商的私钥进行签名,则ATS 130可以通过利用证券经纪商公钥验证证券经纪商的签名来验证交易被授权。

[0042] 在一些实施例中,可以存在完成竞争去匹配交易的多个匹配的ATS 130或者加密交易所135,而非多个用户的订单去往一个交易所。所述交易可以由"n"个授权方中的一个授权方进行解码,而非由一个ATS或者加密交易所135进行签名以便对所述订单进行解密。

[0043] 优选地,在将订单公布前,应该完成整个订单。如果所述订单跨越多次交易(例如,订单是100份并且其需要两次交易来完成订单),则每次交易可以引用原始订单标识符。ATS可以经由匹配组件和分布式分类账保持跟踪交易标识符并且检测订单已完全完成。在订单被完成之后,则ATS可以将订单意向发布到分类账。

[0044] 加密分类账140记录经济交易,比如出售数字资产来交换资金。加密分类账140每个单位地变化。例如,比特币使用被称为区块链的分布式公共分类账。当加密分类账140从加密集成平台125接收到用正确密钥签名的交易并且所述交易经网络节点验证时,加密分类账140通过记录交易(例如,在区块中向区块链确保交易)将资产移至适当的编址账户(例如,数字钱包)。加密分类账140接收由证券经纪商的私钥进行签名并且由加密桥220进行加密的订单并且然后基于共识算法指定所述订单的优先级订单。

[0045] 各数据存储设备可以用于管理对数字证券、客户信息、和其他数据的存储和访问。所述数据存储设备可以是分布式数据存储设备,比如加密分类账140。所述数据存储设备可以是具有被集成对象的集合的数据储存库,使用数据库模式中定义的类别模拟所述被集成对象。数据存储设备可以进一步包括可以存储数据的平面文件。加密集成平台125和/或其他服务器可以收集和/或访问来自数据存储设备的数据。

[0046] 图2根据本公开的一个或多个实施例展示了加密集成平台125内的一组组件。根据图2中所示的实施例,加密集成平台125可以包括存储器205、一个或多个处理器210、加密适配器215、加密桥220、和加密匹配组件225。连同其他模块、应用、和/或组件一起,其他实施例可以包括这些模块和组件中的一些、全部、或没有一个。仍然还,一些实施例可以将这些模块和组件中的两个或更多个并入单个模块和/或将这些模块中的一个或多个的功能的一部分与不同模块相关联。例如,在一个实施例中,加密桥220和加密匹配组件225可以被组合成单个组件。

[0047] 存储器205可以是用于存储信息的任何设备、机构、或被填充的数据结构。根据本公开的一些实施例，存储器205可以是或包括例如任何类型的易失性存储器、非易失性存储器、和动态存储器。例如，存储器205可以是随机存取存储器、存储器存储设备、光学存储器设备、磁性介质、软盘、磁带、硬盘驱动器、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)、压缩盘、DVD等。根据一些示例，存储器205可以包括一个或多个磁盘驱动器、闪盘驱动器、一个或多个数据库、一个或多个表格、一个或多个文件、本地高速缓存存储器、处理器高速缓存存储器、关系数据库、平面数据库等。另外，本领域技术人员将理解可以被用作存储器205的许多用于存储信息的附加设备和技术。

[0048] 存储器205可以用来存储在(多个)处理器210上运行一个或多个应用或模块的指令。例如，在一个或多个实施例中，存储器205可以用来容纳执行加密适配器215、加密桥220、和加密匹配组件225的功能所需的指令中的全部或部分。

[0049] 加密适配器

[0050] 加密适配器215充当证券经纪商与交易所之间的接口。加密适配器215来自证券经纪商115并且在一些实施例中直接从计算设备110A至110M接收交易数字资产的订单。订单被加密适配器215以证券经纪商115常用的常规协议/格式(例如，FIX消息)接收。加密适配器215将所述订单转换为加密交易。加密适配器215与加密桥220通信从而从交易所向证券经纪商提供市场数据。加密适配器215还通过存储证券经纪商所提供的客户标识符并生成具有两个单独的密钥的编址账户对来集成新客户。这两个密钥对用来创建与客户标识符相关联的两个编址账户。

[0051] 两个编址账户都表示数字账户或者数字钱包。第一编址账户(被称为客户文件夹钱包(customer portfolio wallet)、客户文件夹账户(customer portfolio account)或者客户文件夹编址账户(customer portfolio addressed account))存储未委托用于买入或卖出订单的数字交易品。在一些实施例中，与客户标识符相关联的客户拥有客户文件夹钱包的密钥对，但授权加密适配器215使用用于交易的密钥对。在其他实施例中，加密适配器215或第三方拥有客户文件夹钱包。第二编址账户(其可以可互换地或者被称为客户委托钱包(customer committed wallet)、客户委托账户(customer committed account)或者客户委托账户编址账户(customer committed addressed account))存储客户在尚未完成的买入或卖出订单中已放置的数字交易品(例如，“委托的”资产或资金)。在一些实施例中，加密适配器215或者拥有客户委托钱包的密钥或者被授权使用客户委托钱包的密钥。在一些实施例中，交易系统控制客户委托钱包的密钥。在这种情况下，交易系统充当代管契约账户，其中资金或资产由第三方(交易所)控制并且当达成协议的条款时，数字交易品被发放到其新的账户。

[0052] 加密适配器215还控制与证券经纪商相关联的编址账户的密钥对。在一些实施例中，证券经纪商编址账户的私钥用于对订单进行签名。交易所之后可以验证所述订单通过使用证券经纪商的公钥来验证所述证券经纪商的签名而被授权。

[0053] 密适配器215可以接收订单消息，所述订单消息包括来自证券经纪商的与客户标识符相关联的买入、卖出、或取消订单。如果所述订单是买入订单，则订单消息指示证券经纪商具有用于交易的资金存款。因此，加密适配器215发出来自客户的现金正被专门结算交易的证券经纪商持有的表示(例如，数字负债、代用货币、来自证券经纪商的IOU)。在一些实

施例中，可以经由加密货币交易将资金从证券经纪商的编址账户发送至客户文件夹钱包。

[0054] 加密适配器215针对包括用于将数字交易品从源账户(即，客户文件夹钱包)向目的账户(即，委托钱包)传送的信息的订单创建委托交易(即，用于在ATS或加密交易所买入或卖出数字交易品的交易)，并且利用客户文件夹钱包的私钥对委托交易进行签名。委托交易可以包括数字资产或代用货币、客户标识符、和/或委托钱包的公钥。在交易由加密适配器215签名并且数字交易品的所有权由网络节点验证之后，完成向客户委托钱包传送代用货币并且创建已委托交易。

[0055] 加密适配器215进一步创建包括订单的已委托订单交易并且引用所述委托交易。加密适配器215将所述已委托交易订单路由至加密桥220，所述加密桥利用交易所的公钥来验证所述交易并且对所述订单进行加密。加密适配器215还创建了执行报告并将其传递给证券经纪商，从而告知证券经纪商所述订单待完成。加密适配器215从加密匹配组件225接收由加密适配器215转发至证券经纪商的执行报告。在一些实施例中，每个证券经纪商115具有专用加密适配器。加密适配器215可以进一步通过以下方式来验证订单已经被执行：通过检查分布式分类账，以便判定所述订单中所涉及的数字交易品是否与客户文件夹账户相关联。

[0056] 加密桥

[0057] 加密桥220从加密适配器215接收针对交易所处的市场数据的请求。加密桥220对来自加密交易所的信息进行聚集并充当路由器以对交易中涉及的证券定位市场中的最好价格。加密桥220可以通过监视加密分类账来聚集数据，从而通过订阅公共分类账上可见的订单信息来生成订单簿的当前快照。加密桥220通过监测不同的分布式分类账并维护跨交易所和分布式分类账的市场数据的当前状态来进一步为证券经纪商提供单个接口。交易所可以具有不同的分布式分类账。例如，可以使用各个分布式分类账，并且这些分布式分类账可以具有伴随不同相关联密钥的不同应用编程接口。加密桥220存取来自所有分布式分类账的数据并向证券经纪商提供一种标准格式的数据。这种信息对ATS判定订单是否被完成而言是有用的，尤其在涉及多个交易所时。

[0058] 加密桥220接收来自加密适配器215的订单并且验证订单是否正确。加密桥220还利用交易所的公钥对订单进行加密(其引用所述已委托交易)。多于一个订单可以被包含在已委托交易中，只要订单的总量不超过交易量。通常，交易量包括在订货时可支付的任何费用(例如，佣金、交易费)。加密桥220然后与分布式分类账进行通信，以便将经加密订单记录到分类账。

[0059] 加密匹配组件

[0060] 加密匹配组件225从ATS或者交易所接收匹配请求，所述ATS或者交易所识别可能匹配的两个委托订单(即，其中资产/资金已经被传送至客户委托钱包的订单)。匹配请求包括每个已委托交易的订单标识符。加密匹配组件225将订单标识符映射至彼此的客户委托钱包。加密匹配组件225从加密分类账请求委托钱包的余额，从而保证：从卖出方，数字资产可用且被委托用于交易，并且从买入方，资金可用并且被委托用于交易。加密匹配组件225将所述请求响应进行匹配并将所述交易对方散列包括在内。加密匹配组件225然后通过使用交易对方散列(为彼此)从委托钱包扣除并存入客户文件夹钱包来结算并清算交易。

[0061] 加密匹配组件225可以充当交易所的所有订单的订单簿，记录订单的状态(例如，

部分完成、完全完成、取消、到期)。加密匹配组件225然后将明文执行报告记录到分类账,并且以现有的证券经纪商的格式将执行报告返回到证券经纪商115。例如,在已经执行交易之后,加密匹配组件225(或者ATS/交易所)可以将交易记录到分布式分类账,表明X份是以Y美元买下的。当加密匹配组件225已经检测到整个订单已经被完成,加密匹配组件225(或者ATS/交易所)将订单(包括订单意向)记录至分布式分类。在一些实施例中,加密匹配组件225的功能可以通过一个或多个ATS或加密交易所来完成和/或加密匹配组件225可以向ATS/交易所提供订单信息以便记录到分类账。

[0062] 图3展示了对订单意向进行模糊直到订单被执行的过程。接收操作302从证券经纪商接收用于买入或者卖出一个或多个数字交易品的订单。加密操作304使用交易系统的公钥对订单数据进行加密。加密集成平台(或者在一些实施例中,证券经纪商)创建已委托订单交易并利用创建操作306中的证券经纪商的私钥对已委托订单交易进行签名。已委托订单交易可以将订单传送至受交易所控制的委托钱包,从而挂起对订单的取消或结算。在记录操作310中,已委托订单交易(包括经加密订单数据)然后被记录到的分布式分类账。此时,第三方(即,不能读取交易所的私钥的任何人)可以看到交易的存在但是不能看到交易的明细。分布式分类账可以指定订单的优先级。

[0063] 接下来,在验证操作312中,交易所可以通过使用证券经纪商的公钥来验证所述证券经纪商的签名从而判定所述订单是否被授权。解密操作314使用交易所的私钥对订单数据进行解密。匹配操作316按照由分布式分类账指定的优先级对订单进行匹配。结算操作318对交易进行结算,并且可以包括交易对方散列和明文订单信息。包括明文(例如,未加密的、可读的)订单信息的交易在记录操作320中被记录到分类账中,并且被发布。在一些实施例中,只有当加密匹配组件确认整个订单已经被完成时才会发布订单的明文。在确认操作322中,加密集成平台可以通过读取或查询分布式分类账以检查客户文件夹钱包的内容从而确认订单已被完成(或部分完成)。

[0064] 图4图解式地展示了使用对订单意向进行模糊直到订单被执行的过程的代表性示例400。出于本示例的目的,假设第一客户向第一证券经纪商提交了以$100/份卖出10份X的订单(操作402)。第二客户向第二证券经纪商提交了另外两个订单,包括以$100/份买入的10份X的订单和以$50/份买入的20份A的订单(操作404)。

[0065] 在优选实施例中,加密适配器和加密桥一起创建已委托订单交易,所述已委托订单交易在交易完成前被模糊。通常,加密适配器创建交易并且加密桥提供在加密适配器与加密分类账之间的接口。

[0066] 订单被发送至在证券经纪商处的加密适配器进行处理(操作406、408)。加密适配器通过在证券经纪商处的加密适配器将订单从传统协议(例如,FIX)转化成加密订单。如果数字交易品(例如,卖出订单的数字资产、买入订单的资金/代用货币/加密货币)尚未与第一和第二客户的文件夹钱包相关联,加密适配器(或证券经纪商)将数字交易品从不同的账户(例如,加密使用证券经纪商的私钥)传送至对应的客户的文件夹钱包。

[0067] 接下来,加密适配器通过利用客户的文件夹钱包的对应客户私钥对已委托订单交易进行签名来将数字交易品从第一和第二客户的文件夹钱包传送至第一和第二客户的委托钱包中。将数字交易品传送至客户委托钱包确保了数字交易品将不会用于其他交易。在一些实施例中,在对已委托交易进行签名以便将数字交易品传送至客户委托钱包之前,加

密适配器通过利用加密分类账(或分布式分类账)确认所有权来验证数字交易品事实上由对应的客户所拥有。

[0068] 然后,加密适配器创建两个已委托订单交易(每一个客户一个):委托_ID 999(Commit_ID 999)和委托_ID 1000(Commit_ID 1000)。委托_ID 999包括以$100/份卖出10份X的订单并且委托_ID 1000包括以$100/份买入10份X以及以$50/份买入20份A的订单。每个已委托订单交易可以具有与已委托订单交易相关联的多于一个的订单,只要与订单相关联的总量未超过已委托订单交易的量(例如,订单_ID=1并且订单_ID=2都与委托_ID=1000相关联,其中,总量为$2000)。已委托订单交易包括订单信息以及对将数字交易品传送至客户委托钱包的交易的引用。

[0069] 接下来,加密适配器向加密桥发送已委托订单交易(操作410、412)。加密桥利用交易所的公钥对订单数据进行加密。为了对订单数据进行解密,需要交易所的私钥(操作414、416、418)。在一些实施例中,多个签名可以用于多个交易所。例如,订单可以被提交给交易所网络,从而使得任何交易所都可以对包括交易者的委托资产的交易进行签名。具有匹配订单的第一交易所将对引起成功执行的这两种交易都进行签名。

[0070] 接下来,加密桥利用证券经纪商的私钥对已委托订单交易进行签名,并且引用交易所的公钥以便将已委托订单交易与客户委托账户相关联,所述客户委托账户受交易所控制(操作414、416、418)。经加密订单(例如,不可译码的)被写入加密分类账(操作420、422、424)。作为共识的一部分,加密分类账指定订单的优先级。此时,公众可以看到存在三个订单,所有三个订单都具有分类账上的优先级。然而,因为订单已经被加密,所以这些订单的意向被模糊,从而使得只有交易所可以读取订单。

[0071] 一旦经加密订单被记录到加密分类账上,交易所从分类账读取订单并利用其私钥对订单进行解密(例如,利用交易所的公钥对订单进行加密)(操作426)。交易所还可以通过利用证券经纪商公钥来验证证券经纪商的私钥从而验证所述交易。交易所基于其指定的优先级来匹配订单(操作428)。在本示例中,以$100买入10份X的订单与以$100卖出10份X的订单相匹配。每一个客户委托钱包的资产或资金都被传送至交易对方的客户文件夹钱包。一旦订单被执行,则利用采用明文的执行明细(例如,订单执行可被公众查看)将订单执行写入加密分类账(例如用$100买入10份X)(操作430)。然而,在一些实现方式中,即使交易被写入分类账,在整个订单被完成之前,订单意向也未被写入分类账。因此,如果一半的订单在另一半订单完成之前被完成,则订单在ATS/交易所(例如,经由匹配组件)确定整个订单被完成(或者在一些情况下,取消或到期)之前不会被发布。每一次交易或者部分订单可以引用原始订单标识符。一旦交易所确定整个订单被完成,则以明文发布订单。在一些实施例中,稍后的已执行交易的交易标识符可以与第一交易标识符被链接在一起。然后,订单意向在链接结束时发布。

[0072] 匹配组件可以保持跟踪传入交易所的所有订单,并且利用卖出订单来匹配买入订单。匹配组件可以维护保持跟踪订单状态(例如,未完成、已结、到期、取消)的订单薄。当订单的一部分通过匹配组件被匹配时,所述匹配组件报告给交易所,从而使得所述交易可以被记录到分布式分类账。然而,在订单被完全完成之前不会发布订单的订单意向。匹配组件确定订单何时完结(也就是说,当订单被取消或者完全完成)并向交易所发送消息,所以交易所可以将订单意向记录到分布式分类账。

[0073] 在非限制性示例中，价格X的10个ABC份额的买入订单可以与价格X的5个ABC份额的卖出订单相匹配。一旦匹配组件对这两个订单(即使买入订单仅部分完成)进行了匹配，交易可以被发送至交易所，并且交易所将完成的订单记录到分布式分类账，表明已经以X的价格购入5份ABC。匹配组件可以确定整个卖出订单已经被完成并且因此通知交易所可以以明文将卖出订单的订单意向发布到所述分类账。然而，匹配组件未通知交易所所述买入订单被完成，因为买入订单占以价格X购入剩余5份ABC的订单的显著部分。因此，此时，买入订单的订单意向未被发布。一旦匹配组件将另一个卖出订单与买入订单的剩余部分相匹配并检测到整个买入订单被完成，则匹配组件可以通知交易所买入订单被完成。然后，交易所可以请求采用明文将所述订单意向发布至分布式分类账。因此，在本示例中，只有在整个订单被完成之后才发布订单意向。本示例包括利用两次交易完成的买入订单；然而，可以使用多于两次交易来完成订单。相同的概念可应用于使用多于两次交易来完成的订单。

[0074] 通常，每一个交易所具有其自身的匹配组件。在一些实施例中，不同的规则可应用于每一个匹配组件(例如，所接收的第一订单定价VS卖出订单定价VS买入订单定价)。订单可以分配至多个交易所并且由所述多个交易所完成。为了确保所述订单尚未由另一个交易所完成或者部分完成，在执行已匹配订单之前，交易所可以使订单处于临时状态，同时检查分布式分类账(例如，单个可信来源)以便确保订单尚未由另一个交易所完成或部分完成(即，以便确保待交易的数字交易品仍在预期编址账户中)。

[0075] 图5图解式地展示了用于第三方对订单意向和优先级进行验证的过程的代表性示例500。因为执行报告是以明文书写的，所以第三方可以对其进行查看(即，第三方可以看到存在以$100的10份X的买入订单和以$100卖出10份X的卖出订单)(操作502)。另外，第三方可以使用交易所公钥来取得执行交易并对其进行再加密(操作504)。如果利用交易所公钥加密的执行交易与已委托交易订单相同，则可以向第三方保证订单是相同的。因此，此验证过程在数学上证明了最终分类账交易上的明文等于订单交易上的编码值。

[0076] 图6是流程图，展示了用于对订单意向进行模糊直到订单被执行的过程600。在一些实施例中，加密集成平台的各个组件可以执行这些操作。在一些实施例中，可以执行这些操作中的一些或全部。在一些实施例中，可按不同次序或者并行地执行这些操作中的一些或全部。在接收操作602中，从证券经纪商处接收订单。在创建操作604中，创建已委托订单交易，这将订单置于待完成状态。在加密操作606中，使用交易所的公钥对已委托订单交易进行加密。在签名操作608中，使用证券经纪商的私钥对订单进行签名。在结算操作610中，在通过交易所对订单进行解密、验证并且按照其指定优先级进行匹配之后，通过以非模糊的方式将资金和资产托管置于适合的客户钱包中并将执行记录发布到分类账来对交易进行结算。

[0077] 图7是流程图，从加密集成平台的角度展示了用于对订单的意向进行模糊直到订单被执行的过程700。接收操作702接收用于通过交易系统对数字交易品进行交易以交换其他数字交易品的订单。创建操作704创建已委托订单交易，所述已委托订单交易标识与所述订单相关联的数据。加密操作706对与所述订单相关联的数据进行加密。这可以利用第一编址账户的证书来完成。第一编址账户可以是客户委托账户，并且第一编址账户证书可以由交易系统控制。

[0078] 加密签名操作708利用与第二编址账户相关联的证书对已委托订单交易进行签

名。第二编址账户可以是证券经纪商账户。验证操作710通过检查分布式分类账上的记录来验证所述订单已经被完成。所述记录可以以未经加密格式被记录并且包括已被执行来完成所述订单的一次或多次交易的交易数据(和订单数据)。取决于订单的大小和证券交易发生的频率,这种数据在订单(其可以采取许多交易)已经被完成之前不会以未经加密格式被记录到分类账。

[0079] 图8是流程图,从交易系统的角度展示了用于对订单的意向进行模糊直到订单被执行的过程800。接收操作802接收用于对数字交易品进行交易的经加密订单。解密操作804使用与第一客户委托编址账户(例如,第一客户委托编址账户的私钥)相关联的证书对订单进行解密。匹配操作806将未经加密的所述订单与用于对所述数字交易品中的至少一些进行交易的第二订单进行匹配。执行操作808通过以下方式来执行交易:将所述数字交易品的至少一部分从第一客户委托编址账户加密传送至第二客户的文件夹编址账户并且将其他数字交易品的至少一部分从第二客户的第二客户委托编址账户加密传送至第一客户的文件夹编址账户。

[0080] 判定操作810判定整个订单是否已被完成。当整个订单尚未被完成时,判定操作810分支到匹配操作812以便将所述订单与第二订单进行匹配。此后,判定操作810再次判定整个订单何时已经被完成。当整个订单已经被完成时,判定操作810分支到发送操作814,所述发送操作发送交易数据,所述交易数据包括有待以未经加密格式被记录到分布式分类账的订单数据和交易数据。使用这种方法,第三方可以验证订单和交易的内容但是不能利用信息来影响市场。

[0081] 图9至图10是简图,根据本公开的一个或多个实施例展示了对订单的意向进行模糊直到订单被执行的过程。证券经纪商接收订单(902),并且将数字交易品传送到客户文件夹账户(904)。加密适配器取得FIX订单(或者其他传统协议订单),并将所述订单转换为加密订单(906)。加密适配器查询加密分类账以确保数字交易品与客户文件夹账户相关联(908)。加密分类账获得客户文件夹账户余额并向加密适配器提供所述账户余额(910)。一旦加密适配器已确认数字交易品与客户文件夹账户相关联,则所述加密适配器就可以创建委托交易以便将数字交易品传送到由交易所控制的客户委托账户(912)。这种委托交易将数字交易品置于待完成状态(类似于代管契约),以确保当订单被执行时数字交易品将是可用的。委托交易可以包括数字交易品和客户委托账户的公钥,并且可以由加密适配器利用客户文件夹账户的私钥对所述委托交易进行签名。

[0082] 一旦数字交易品与客户委托账户相关联,加密适配器可以创建已委托订单交易(914),所述已委托订单交易引用委托交易并包括订单数据,也就是说,订单详情,比如价格、数量、订单类型(例如,市场、限制)、安全性、某方(例如,买方或卖方)、证券经纪商标识符、交易者标识符(可能匿名)、有效期(例如,天数、IOC)以及分类账标识符。已委托订单交易将会使订单与客户委托账户相关联并将引用委托交易(即,为了防止重复花费)。加密桥可以利用交易所公钥对已委托订单交易进行加密(916)。接下来,加密桥可以利用证券经纪商的私钥对已委托交易订单进行签名以便将所述订单传送至客户委托账户(918)。加密分类账可以记录经加密的已委托订单交易(920)。

[0083] 移至图10,加密分类账基于在ATS/分类账处接收到订单的时间来确定并指定订单的优先级(1002)。设置优先级确保了按照订单被接收的次序来完成订单。交易所利用证券

经纪商的公钥对已委托交易订单上证券经纪商的签名进行验证(1004)。这确保了交易实际上是由证券经纪商发起的。接下来,交易所利用交易所的私钥对订单数据进行解密(1006)。加密匹配组件基于较早指定给所述订单的订单优先级而将订单与交易对方的订单相匹配(1008)。在一些实施例中,除了或替代加密匹配组件,交易所对订单进行匹配。交易所创建执行交易(1010),从而使得客户委托钱包中的适当委托数字交易品被传送至另一方的客户文件夹钱包,并且反之亦然。因为数字交易品与客户委托账户相关联(所述客户委托账户由交易所控制),所述交易所可以利用交易所的私钥来传送数字交易品并结算所述交易(1012)。

[0084] 可以将已执行交易发布至分布式分类账(例如,买者10从卖者3处购入了100份股票XYZ)。在一些实施例中,不论订单是否被完成,都可以将已执行交易发布至分类账,因为仅发布经执行订单并不泄露订单意向。一旦加密匹配组件确定整个订单被完成(即,被执行),就可以发布所述订单的明文(1014)。第三方可以通过利用交易所的公钥对订单数据进行加密并且将结果与被发送至交易所进行匹配和执行的交易进行比较来对所述订单的有效性进行双重检查。

[0085] 本公开的各个实施例包括:

[0086] 1.一种非暂态计算机可读存储介质,包括一组指令,所述指令在由一个或多个处理器执行时使得机器:

[0087] 接收用于经由交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单,

[0088] 创建已委托订单交易,所述已委托订单交易标识与所述订单相关联的数据,

[0089] 使用与第一编址账户相关联的至少一个证书对与所述订单相关联的所述数据进行加密,其中,与所述第一编址账户相关联的所述至少一个证书受所述交易系统控制;

[0090] 使用与第二编址账户相关联的至少一个证书对所述已委托订单交易进行加密签名以便将所述已委托订单交易传送至所述第一编址账户;

[0091] 通过所述交易系统利用与所述第一编址账户相关联的另外的至少一个证书对经加密订单进行解密;

[0092] 将未经加密的所述订单与用于对所述至少一个其他数字交易品的至少一部分进行交易的第二订单进行匹配;并且

[0093] 通过从所述第一编址账户加密传送所述至少一个数字交易品的所述一部分并且将所述第二数字交易品中的所述至少一个的至少一部分加密传送至与客户相关联的第三编址账户来执行第一交易。

[0094] 2.如权利要求1所述的非暂态计算机可读存储介质,其中,所述一组指令在由所述一个或多个处理器执行时进一步使得所述机器:

[0095] 以未经加密格式生成所述第一交易的已执行交易数据;

[0096] 判定所述订单是否已经由所述第一交易完成;并且

[0097] 当所述订单已经由所述第一交易完成时,向分布式分类账发送用于以所述未经加密格式来记录所述第一交易的所述已执行交易数据的请求。

[0098] 3.如权利要求2所述的非暂态计算机可读存储介质,其中,所述一组指令在由所述一个或多个处理器执行时进一步使得所述机器:

[0099] 当所述订单尚未由所述第一交易完成时，等待直到所述订单已经由所述第一交易和随后交易完成；

[0100] 在所述订单已经由所述第一交易和所述随后交易完成之后：向所述分布式分类账发送用于以所述未经加密格式来记录所述第一交易和所述随后交易中的每一次交易的所述已执行交易数据的请求。

[0101] 4.一种计算机化方法，包括：

[0102] 接收用于经由交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单；

[0103] 创建已委托订单交易，所述已委托订单交易标识与所述订单相关联的数据；

[0104] 使用与第一编址账户相关联的至少一个证书对与所述订单相关联的所述数据进行加密，其中，与所述第一编址账户相关联的所述至少一个证书受所述交易系统控制；

[0105] 使用与第二编址账户相关联的至少一个证书对所述已委托订单交易进行加密签名；并且

[0106] 经由被记录到分布式分类账的记录来验证所述订单已经被完成，其中，所述记录包括采用未经加密格式的与所述订单相关联的至少第一已执行交易的已执行交易数据，其中，采用所述未经加密格式的所述已执行交易数据直到所述订单已经被完成才会被记录。

[0107] 5.如权利要求4所述的计算机化方法，进一步包括：

[0108] 向所述分布式分类账发送用于记录具有所述经加密数据的所述已委托订单交易的请求，其中，所述分布式分类账为所述订单指定优先级。

[0109] 6.如权利要求4所述的计算机化方法，进一步包括：

[0110] 在所述订单已经由所述交易系统验证、解密、匹配和执行之后，将所述至少一个其他数字交易品接收到第三编址账户中。

[0111] 7.如权利要求4所述的计算机化方法，进一步包括：

[0112] 在接收到用于对所述至少一个数字交易品进行交易的所述订单之后，验证所述至少一个数字交易品与第三编址账户相关联；以及

[0113] 当所述至少一个数字交易品与所述第三编址账户相关联时，创建委托交易以便将所述至少一个数字交易品加密传送至所述第一编址账户，

[0114] 其中，创建所述已委托订单交易进一步包括在所述已委托订单交易中引用所述委托交易以便防止在第二已委托订单交易中引用所述至少一个数字交易品。

[0115] 8.如权利要求4所述的计算机化方法，其中，所述至少一个数字交易品包括数字证券或资金的数字表示，其中，所述数据包括以下各项中的一项或多项：所述至少一个第一数字交易品的身份、购入或卖出所述至少一个第一数字交易品的价格以及购入或卖出所述至少一个第一数字交易品的数量。

[0116] 9.一种加密集成系统，包括：

[0117] 至少一个处理器；以及

[0118] 少一个计算机可读存储介质，其上存储有指令，所述指令在由所述至少一个处理器执行时使得所述加密集成系统：

[0119] 接收用于经由交易系统对至少一个数字交易品进行交易以交换至少一个其他数字交易品的订单；

[0120] 创建已委托订单交易，所述已委托订单交易标识与所述订单相关联的数据；

[0121] 使用与第一编址账户相关联的至少一个证书对与所述订单相关联的所述数据进行加密，其中，与所述第一编址账户相关联的所述至少一个证书受所述交易系统控制；

[0122] 使用与第二编址账户相关联的至少一个证书对所述已委托订单交易进行加密签名；并且

[0123] 经由被记录到分布式分类账的记录来验证所述订单已经被完成，其中，所述记录包括采用未经加密格式的与所述订单相关联的至少第一已执行交易的已执行交易数据，其中，采用所述未经加密格式的所述已执行交易数据直到所述订单已经被完成才会被记录。

[0124] 10.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

[0125] 向所述分布式分类账发送用于记录具有所述经加密数据的所述已委托订单交易的请求，其中，所述分布式分类账为所述订单指定优先级。

[0126] 11.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

[0127] 在所述订单已经由所述交易系统验证、解密、匹配和执行之后，将所述至少一个其他数字交易品接收到第三编址账户中。

[0128] 12.如权利要求9所述的加密集成系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述加密集成系统：

[0129] 在接收到用于对所述至少一个数字交易品进行交易的所述订单之后，验证所述至少一个数字交易品与第三编址账户相关联；并且

[0130] 当所述至少一个数字交易品与所述第三编址账户相关联时，创建委托交易以便将所述至少一个数字交易品加密传送至所述第一编址账户，

[0131] 其中，在由所述至少一个处理器执行时使得所述加密集成系统创建所述已委托订单交易的所述指令进一步使得所述加密集成系统：在所述已委托订单交易中引用所述委托交易以防止在第二已委托订单交易中引用所述至少一个数字交易品。

[0132] 13.一种计算机化方法，包括：

[0133] 将经加密订单接收到第一客户委托编址账户中以便对至少一个数字交易品进行交易以交换至少一个其他数字交易品；

[0134] 通过交易系统使用与所述第一客户委托编址账户相关联的至少一个证书对所述经加密订单进行解密；

[0135] 将未经加密的所述订单与用于对所述至少一个数字交易品的至少一部分进行交易的第二订单进行匹配；

[0136] 通过从所述第一客户委托编址账户加密传送所述至少一个数字交易品的至少一部分并且将所述至少一个其他数字交易品的至少一部分加密传送至第一客户文件夹编址账户来执行第一交易；以及

[0137] 当所述订单已经被完成时，向用于进行记录的分布式分类账发送所述第一交易的已执行交易数据以便允许对所述订单和所述交易进行第三方验证，所述已执行交易数据包括采用未经加密格式的来自所述订单的数据。

[0138] 14.如权利要求13所述的计算机化方法，其中，将所述经加密订单记录到所述分布

式分类账，所述分布式分类账基于在所述分布式分类账处的接收时间来为所述经加密订单指定优先级，并且其中，将未经加密的所述订单与所述第二订单进行匹配是基于所指定的优先级进行的。

[0139] 15.如权利要求13所述的计算机化方法，进一步包括：使用证券经纪商账户的证书来验证所述经加密订单的发送者，其中，所述证书为公钥。

[0140] 16.如权利要求13所述的计算机化方法，进一步包括：通过加密传送所述至少一个数字交易品的第二部分来执行第二交易，其中，所述已执行交易数据包括来自所述交易和所述第二交易两者的数据。

[0141] 17.一种交易系统，包括：

[0142] 至少一个处理器；以及

[0143] 至少一个计算机可读存储介质，其上存储有指令，所述指令在由所述至少一个处理器执行时使得所述加密集成系统：

[0144] 将经加密订单接收到第一客户委托编址账户中以便对至少一个数字交易品进行交易以交换至少一个其他数字交易品；

[0145] 通过交易系统使用与所述第一客户委托编址账户相关联的至少一个证书对所述经加密订单进行解密；

[0146] 将未经加密的所述订单与用于对所述至少一个数字交易品的至少一部分进行交易的第二订单进行匹配；

[0147] 通过从所述第一客户委托编址账户加密传送所述至少一个数字交易品的至少一部分并且将所述至少一个其他数字交易品的至少一部分加密传送至第一客户文件夹编址账户来执行第一交易；并且

[0148] 当所述订单已经被完成时，向用于进行记录的分布式分类账发送所述第一交易的已执行交易数据以便允许对所述订单和所述交易进行第三方验证，所述已执行交易数据包括采用未经加密格式的来自所述订单的数据。

[0149] 18.如权利要求17所述的交易系统，其中，将所述经加密订单记录到所述分布式分类账，所述分布式分类账基于接收时间为所述经加密订单指定优先级，并且其中，将未经加密的所述订单与所述第二订单进行匹配是基于所指定的优先级进行的。

[0150] 19.如权利要求17所述的交易系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述交易系统：使用证券经纪商账户的证书来验证所述经加密订单的发送者，其中，所述证书为公钥。

[0151] 20.如权利要求17所述的交易系统，其中，所述指令在由所述至少一个处理器执行时进一步使得所述交易系统：通过加密传送所述至少一个数字交易品的第二部分来执行第二交易，其中，所述已执行交易数据包括来自所述交易和所述第二交易两者的数据。

[0152] 计算机系统概览

[0153] 本公开的实施例包括以上已经描述的各步骤和操作。各个这些步骤和操作可以由硬件组件执行或者可以具体化在机器可执行指令中，所述机器可执行指令可以用于使得利用所述指令编程的通用处理器或专用处理器执行所述过程。替代性地，可以通过硬件、软件、和/或固件的组合来执行步骤。这样，图11是计算机系统1100的示例，本公开的实施例可以用于所述计算机系统。根据本示例，计算机系统1100包括互连1110、至少一个处理器

1120、至少一个通信端口1130、主存储器1140、可移除存储介质1150、只读存储器1160、和大容量存储设备1170。

[0154] 处理器1120可以是任何已知处理器。通信端口1130可以是或包括例如以下各项中的任意一项:用于基于调制解调器的拨号连接的RS-232端口、10/100以太网端口、或使用铜或光纤的千兆端口。可以取决于网络(比如局域网(LAN)、广域网(WAN)、或计算机系统1100连接至的任何网络)选择通信端口1130的本质。

[0155] 主存储器1140可以是随机存取存储器(RAM),或本领域中公知的任何其他动态存储设备。只读存储器1160可以是用于存储静态信息(比如处理器1120的指令)的任何静态存储设备(比如可编程只读存储器(PROM)芯片)。

[0156] 大容量存储设备1170可以用来存储信息和指令。例如,可以使用硬盘(Adaptec®的SCSI驱动器家族)、光盘、磁盘阵列(比如RAID(比如Adaptec的RAID驱动器家族))、或其他大容量存储设备。

[0157] 互连1110可以是或包括一个或多个总线、桥、控制器、适配器、和/或点到点连接。互连1110将处理器1120与其他存储器、存储设备、和通信块通信地耦合。取决于所使用的存储设备,互连1110可以是基于PCI/PCI-X或SCSI的系统。

[0158] 可移除存储介质1150可以是任何类型的外部硬盘驱动器、软盘驱动器、压缩盘只读存储器(CD-ROM)、压缩盘可重写(CD-RW)、数字视频磁盘只读存储器(DVD-ROM)。

[0159] 上文所描述的组件旨在例示一些类型的可能性。前述示例绝不应该限制本公开,因为它们仅仅是示例性实施例。

[0160] 术语

[0161] 下面给出了贯穿本说明书所使用的术语、缩写、和短语的简洁定义。

[0162] 术语“连接(connected)”或“耦合(coupled)”以及相关术语在操作性意义上使用并且不一定限于直接物理连接或耦合。因而,例如,两个设备可以直接、或通过一个或多个中间介质或设备耦合。作为另一示例,设备可以耦合的方式为使得可以在其之间传递信息,同时彼此之间不共享任何物理连接。基于在此所提供的公开内容,根据前述定义,本领域技术人员将理解连接或耦合存在的各种方式。

[0163] 短语“在一些实施例中(in some embodiments)”、“根据一些实施例(according to some embodiments)”、“在所示的实施例中(in the embodiments shown、)”、“在其他实施例中(in other embodiments)”、“实施例(embodiments)”等一般指紧跟着所述短语的具体特征、结构、或特性包括在本公开的至少一个实施例中,或者可以包括在本公开的不只一个实施例中。另外,此类短语不一定指相同的实施例或不同的实施例。

[0164] 如果说明书陈述组件或特征“可以(may)”、“能(can)”“可(could)”、或“可能(might)”被包括或具有特性,不需要这个具体组件或特性被包括或具有所述特性。

[0165] 术语“响应的(responsive)”包括完全或部分响应的。

[0166] 术语“模块(module)”概括地指软件、硬件、或固件(或其任意组合)组件。模块通常是可以使用(多个)指定的输入生成有用数据或其他输出的功能组件。模块可以或可以不是自含式的。应用程序(还称为“应用(application)”)可以包括一个或多个模块,或者模块可以包括一个或多个应用程序。

[0167] 术语“网络(network)”一般地指能够交换信息的一组互连的设备。网了可以少到

局域网(LAN)上的若干私人计算机或者大到互联网(全球计算机网络)。如在此所使用的，“网络”旨在涵盖能够从一个实体向另一实体传输信息的任何网络。在一些情况下，网络可以包括多个网络，甚至多个异构网络，比如一个或多个边界网络、话音网络、宽带网络、金融网络、服务提供商网络、互联网服务提供商(ISP)网络、和/或公共交换电话网络(PSTN)，所述网络通过可操作以方便各网络彼此和之间的通信的网关互连。

[0168] 同样，出于展示的目的，在此在计算机程序、物理组件、和现代计算机网络内的逻辑交互的背景下描述本公开的各实施例。重要的是，虽然这些实施例联系现代计算机网络和程序描述了本公开的各实施例，在此所描述的方法和装置同等地适用于其他系统、设备、和网络，如本领域技术人员将理解的。这样，本公开的实施例的已展示的应用部旨在是限制性的，但相反是示例。本公开的实施例适用的其他系统、设备、和网络包括例如其他类型的通信和计算机设备和系统。更确切地，实施例适用于通信系统、服务、和设备，比如电话网络和兼容设备。另外，实施例适用于所有级别的计算，从私人计算机到大型网络主机和服务器。

[0169] 总的来说，本公开提供了用于对交易意向进行模糊的新颖系统、方法、和安排。虽然上文给出了对本公开的一个或多个实施例的详细描述，在不背离本公开的精神的情况下，各种替代方案、更改、和等效物对本领域技术人员将是明显的。例如，虽然上文所描述的实施例指具体特征，本公开的范围还包括具有不同的特征组合的实施例以及不包括所描述的全部特征的实施例。因此，本公开的范围旨在涵盖落入所附权利要求书范围内的全部此类替代方案、更改、和变化，以及其等效物。因此，以上说明不应该被视为限制性的。

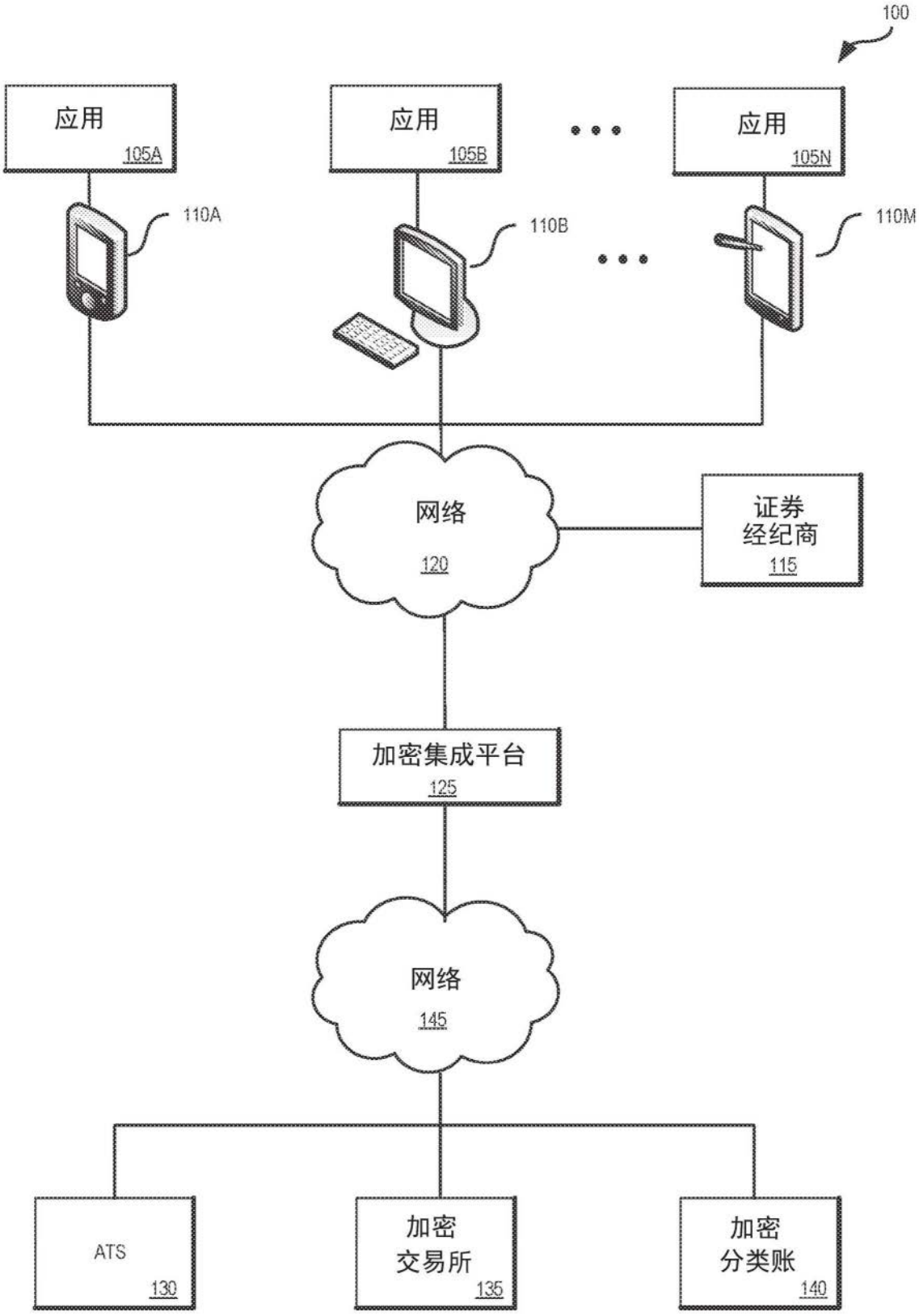

100
应用
105A
应用
105B
应用
105N
110A
110B
110M
网络
120
证券
经纪商
115
加密集成平台
125
网络
145
ATS
130
加密
交易所
135
加密
分类账
140

图1

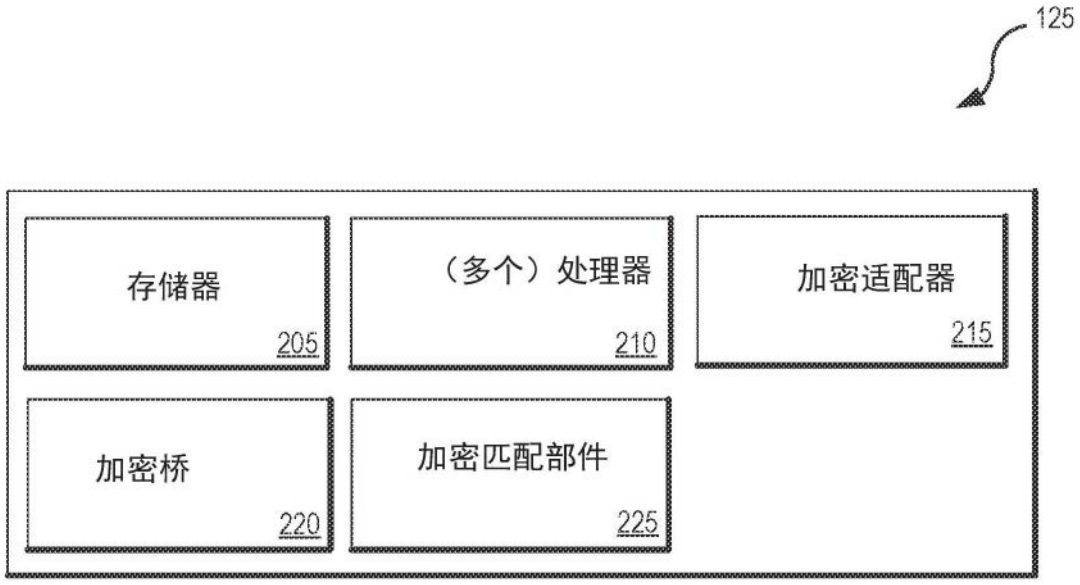


图2

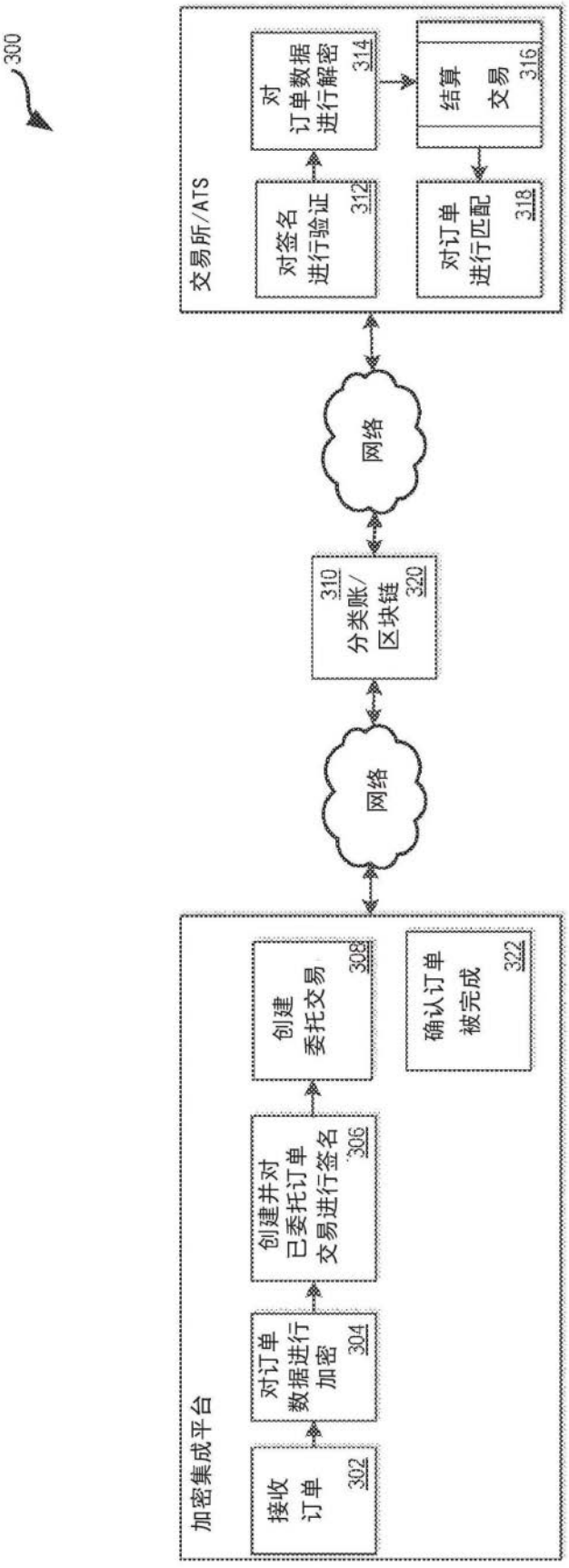

300
加密集成平台
接收订单 302
对订单数据进行加密 304
创建并对已委托订单交易进行签名 306
创建委托交易 308
确认订单被完成 322
网络
310 分类账/区块链 320
网络
交易所/ATS
对签名进行验证 312
对订单数据进行解密 314
对订单进行匹配 318
结算交易 316

图3

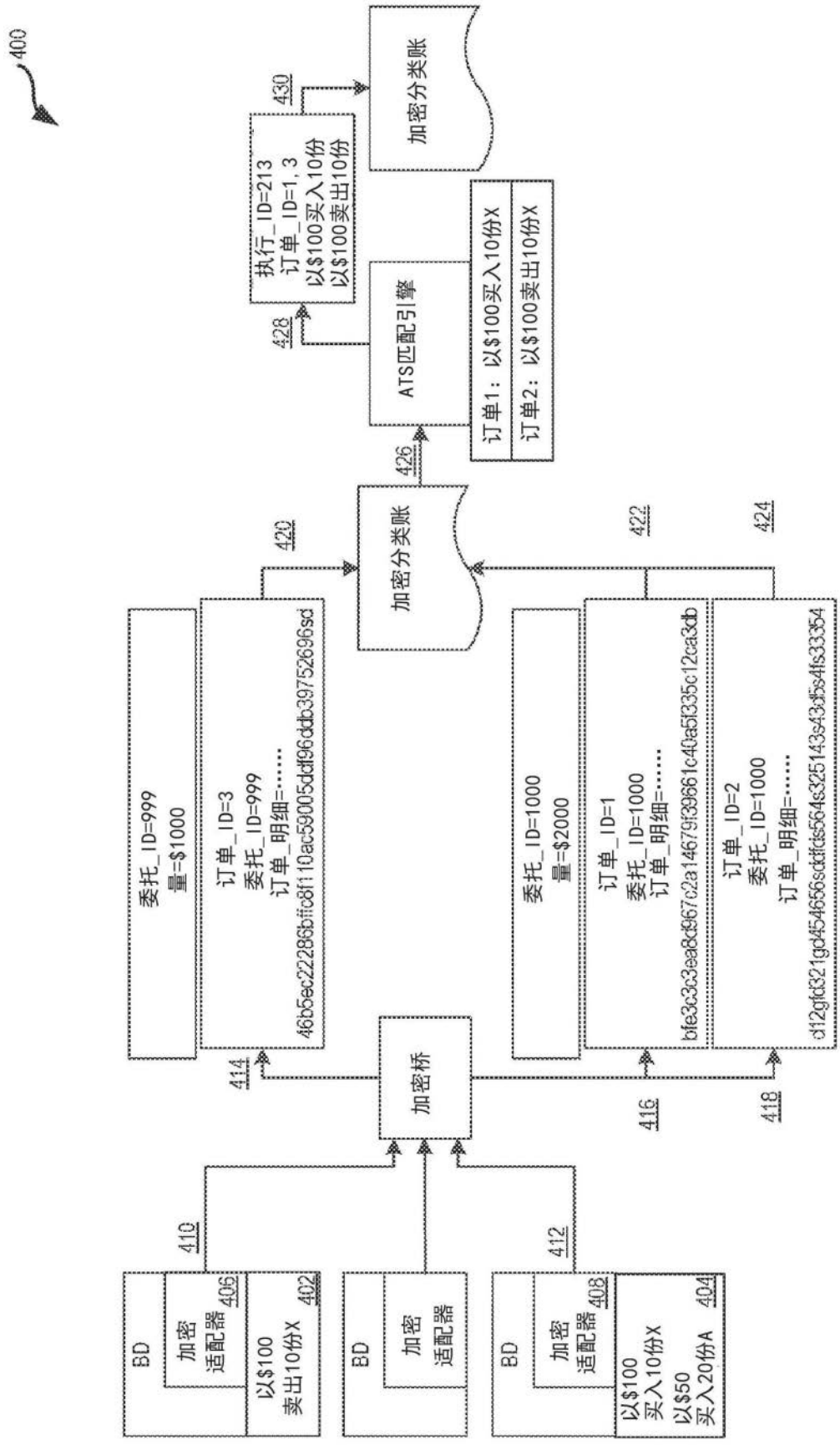

400
BD
加密
适配器 406
以$100
卖出10份X 402
410
BD
加密
适配器
BD
加密
适配器 408
以$100
买入10份X
以$50
买入20份A 404
412
加密桥
414
委托_ID=999
量=$1000
订单_ID=3
委托_ID=999
订单_明细=……
46b5ec22286bffc8f110ac59005ddf96ddb397526696sd
420
加密分类账
426
ATS匹配引擎
428
执行_ID=213
订单_ID=1, 3
以$100买入10份
以$100卖出10份
430
加密分类账
订单1：以$100买入10份X
订单2：以$100卖出10份X
416
委托_ID=1000
量=$2000
422
订单_ID=1
委托_ID=1000
订单_明细=……
bfe3c3c3eab0d967c2a14679f39661c40ab5f335c12ca3db
418
424
订单_ID=2
委托_ID=1000
订单_明细=……
d12gfd321gd45456sdffds564s3251143s43d5s4fs33354

图4

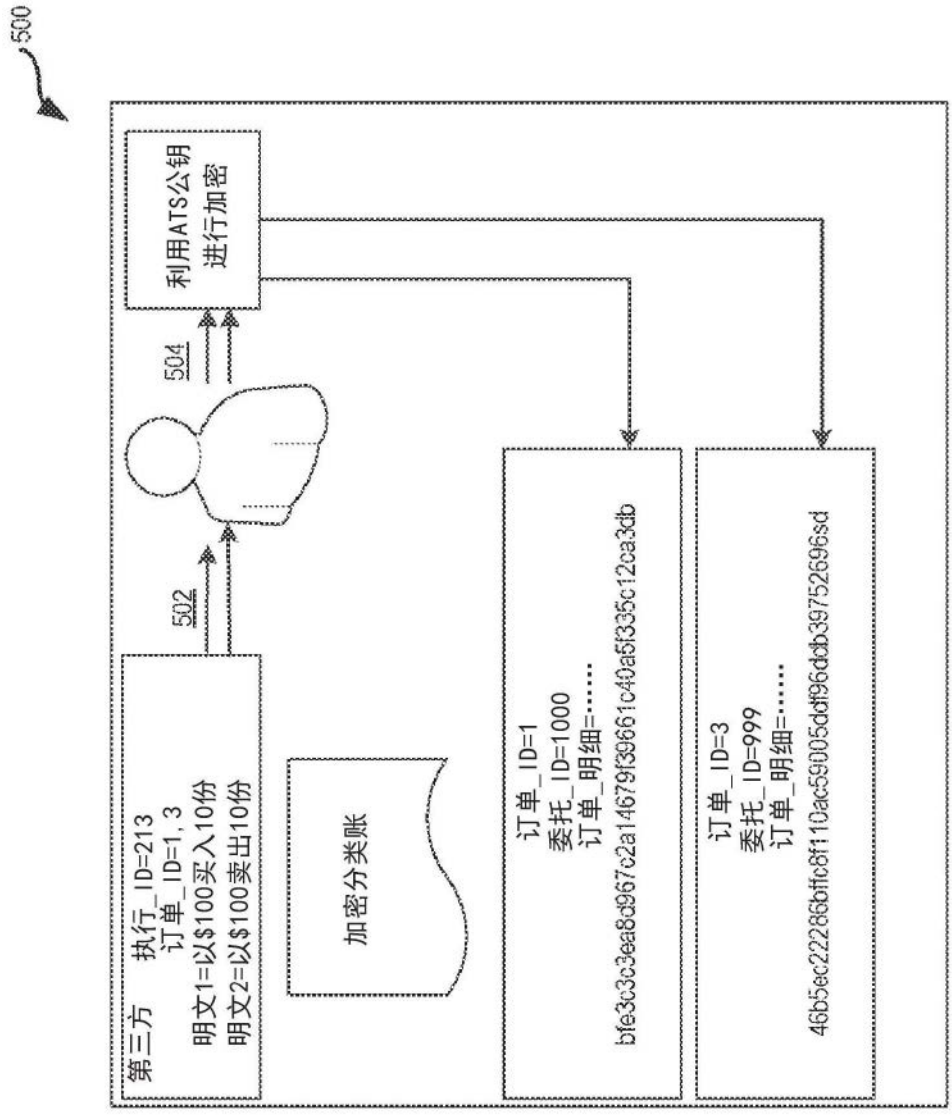

500
第三方 执行_ID=213
订单_ID=1,3
明文1=以$100买入10份
明文2=以$100卖出10份
502
504
利用ATS公钥
进行加密
加密分类账
订单_ID=1
委托_ID=1000
订单_明细=.....
bfe3c3c3ea8d967c2a14679f39661c40a5f335c12ca3db
订单_ID=3
委托_ID=999
订单_明细=.....
46b5ec22286bffc6f110ac59005ddf96ddb39752696sd

图5

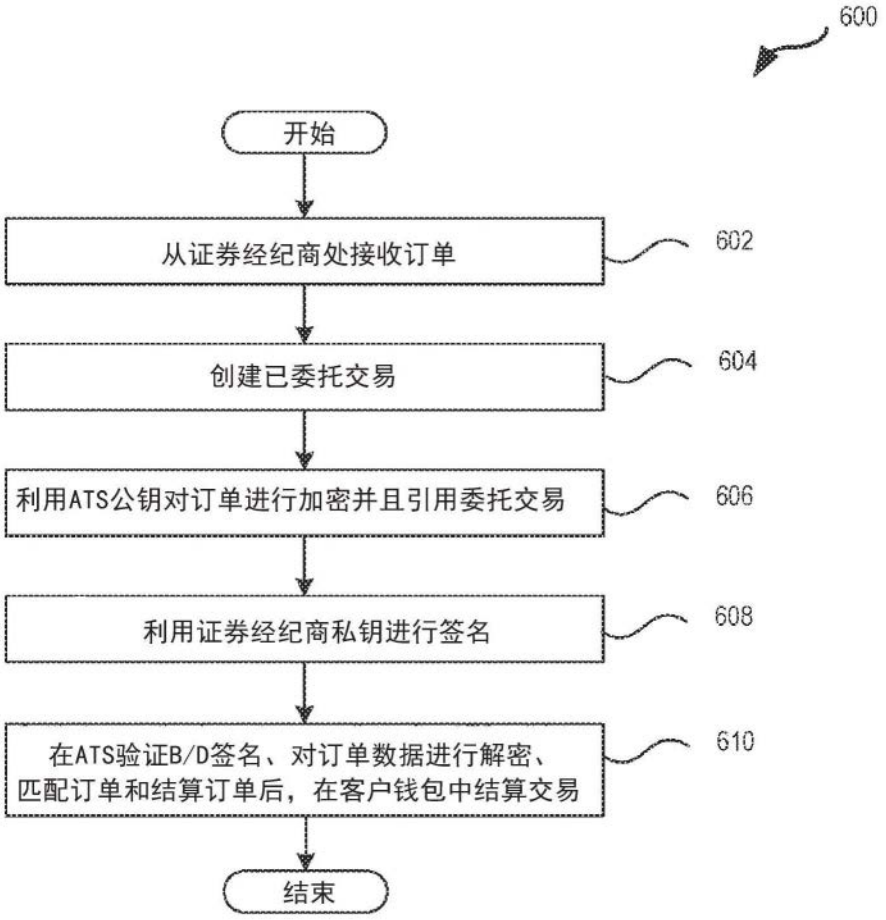

600
开始
从证券经纪商处接收订单
602
创建已委托交易
604
利用ATS公钥对订单进行加密并且引用委托交易
606
利用证券经纪商私钥进行签名
608
在ATS验证B/D签名、对订单数据进行解密、
匹配订单和结算订单后，在客户钱包中结算交易
610
结束

图6

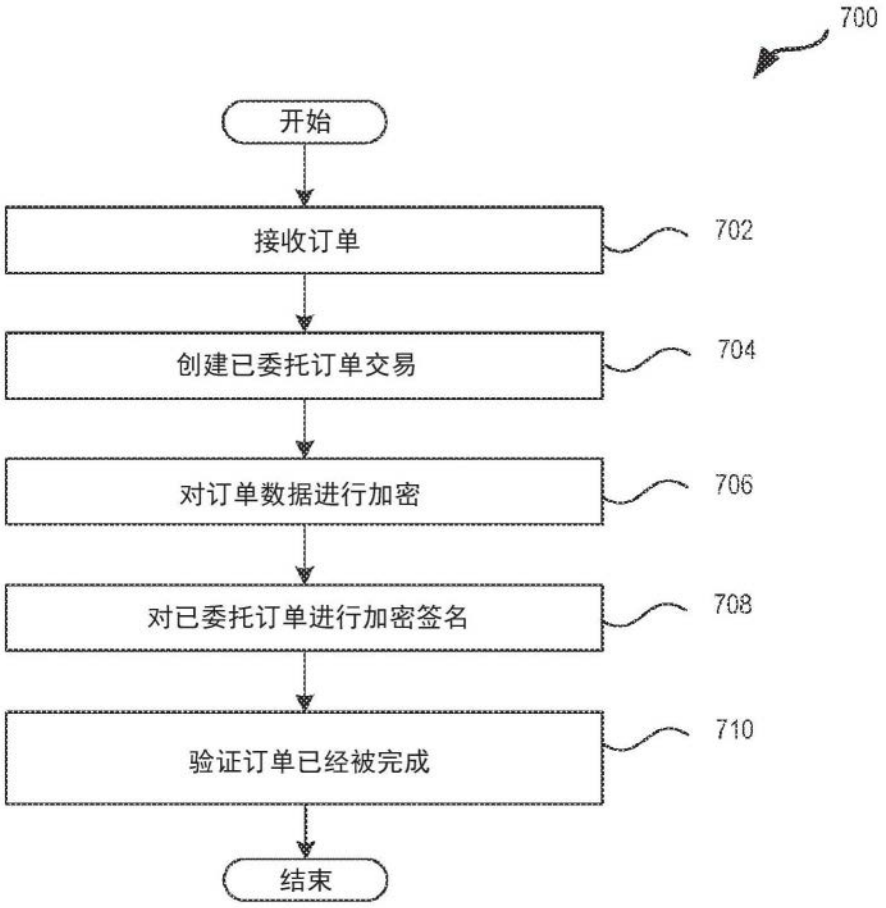

700
开始
接收订单
702
创建已委托订单交易
704
对订单数据进行加密
706
对已委托订单进行加密签名
708
验证订单已经被完成
710
结束

图7

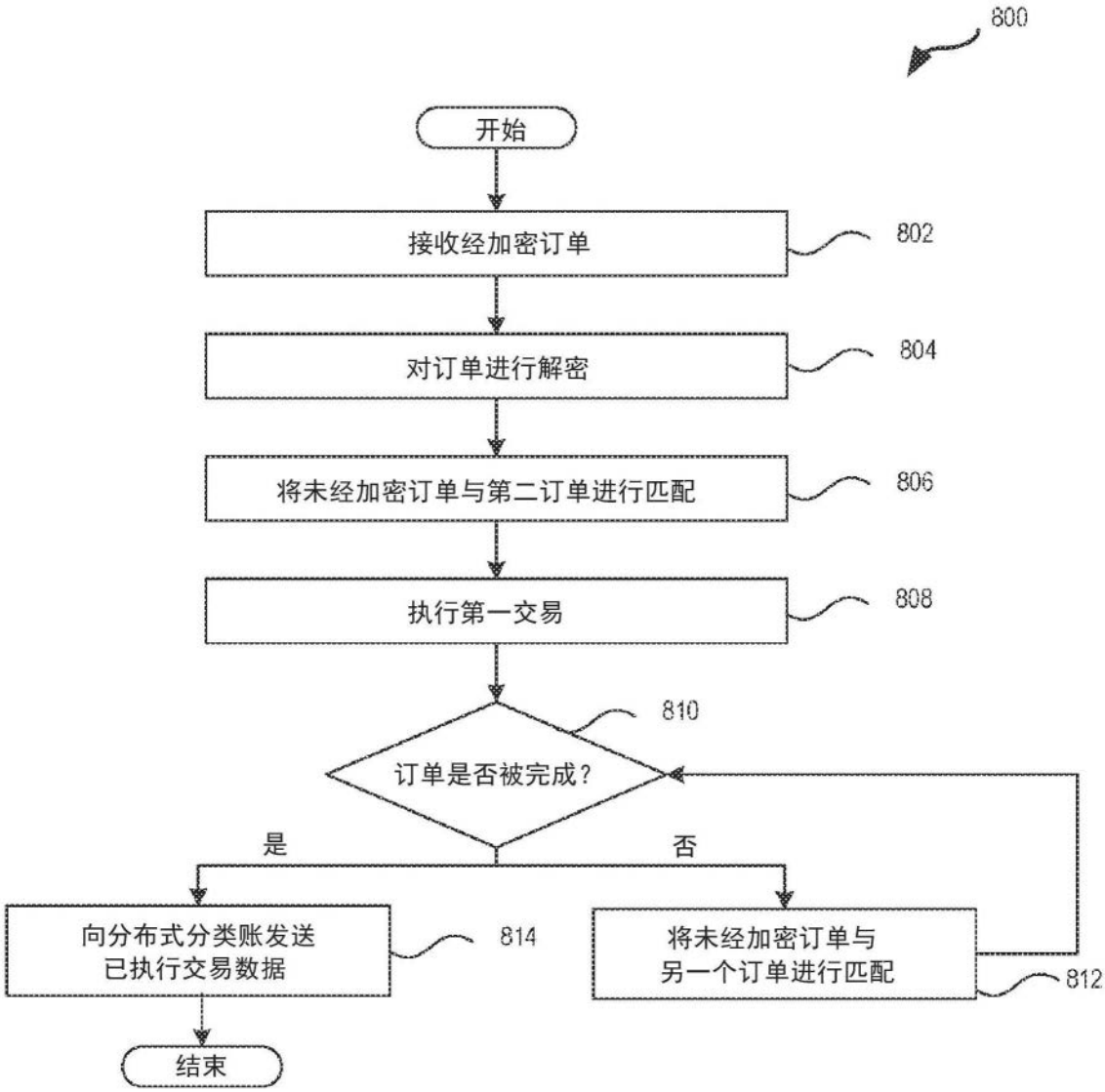

800
开始
接收经加密订单
802
对订单进行解密
804
将未经加密订单与第二订单进行匹配
806
执行第一交易
808
810
订单是否被完成?
是
否
向分布式分类账发送
已执行交易数据
814
将未经加密订单与
另一个订单进行匹配
812
结束

图8

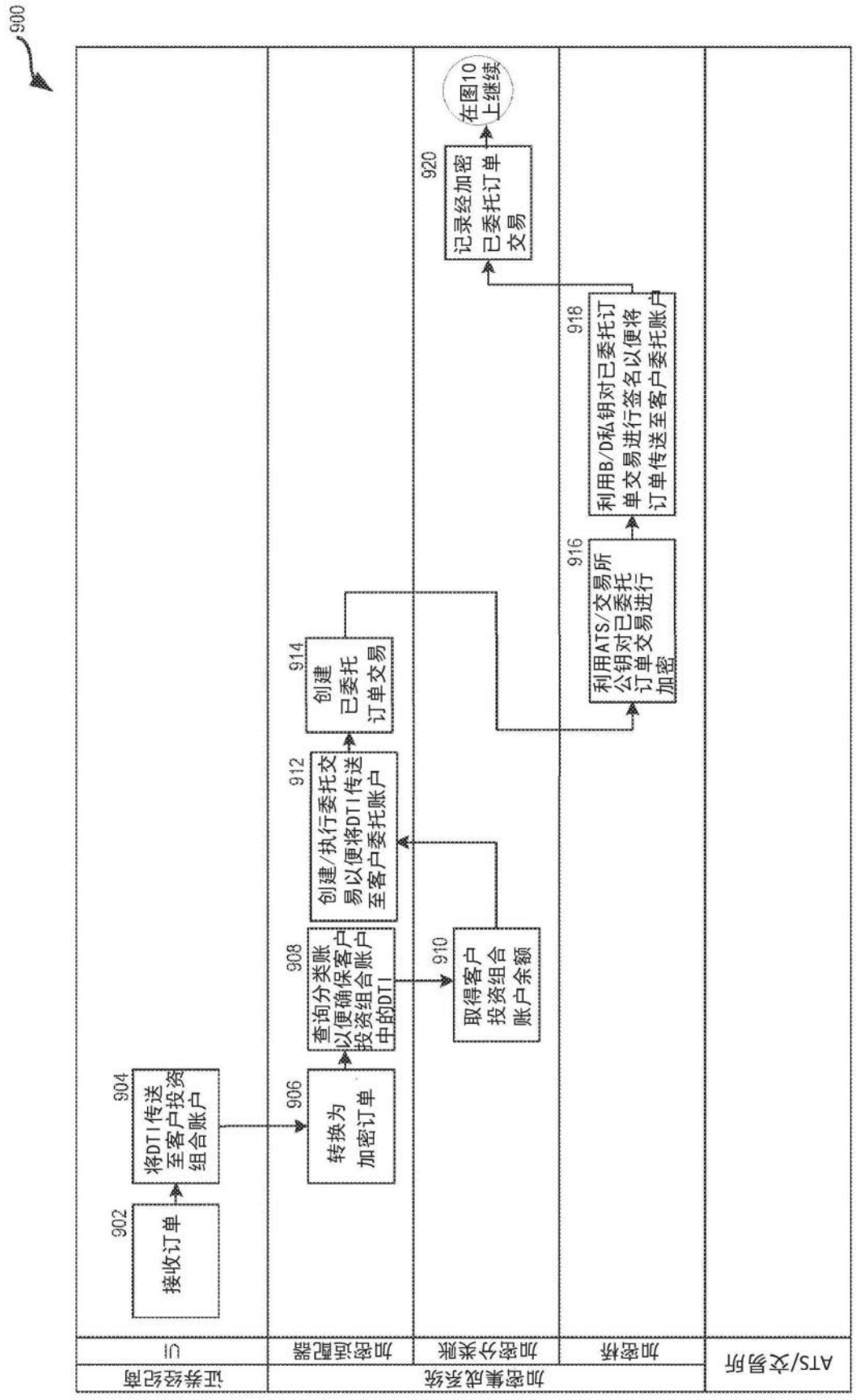

900
902
接收订单
904
将DTI传送至客户投资组合账户
906
转换为加密订单
908
查询分类账以便确保客户投资组合账户中的DTI
910
取得客户投资组合账户余额
912
创建/执行委托交易以便将DTI传送至客户委托账户
914
创建已委托订单交易
916
利用ATS/交易所公钥对已委托订单交易进行加密
918
利用B/D私钥对已委托订单交易进行签名以便将订单传送至客户委托账户
920
记录经加密已委托订单交易
在图10上继续
ATS/交易所
券商柜台
券商分类账
券商经纪商系统
C
券商经纪商
券商前置器

图9

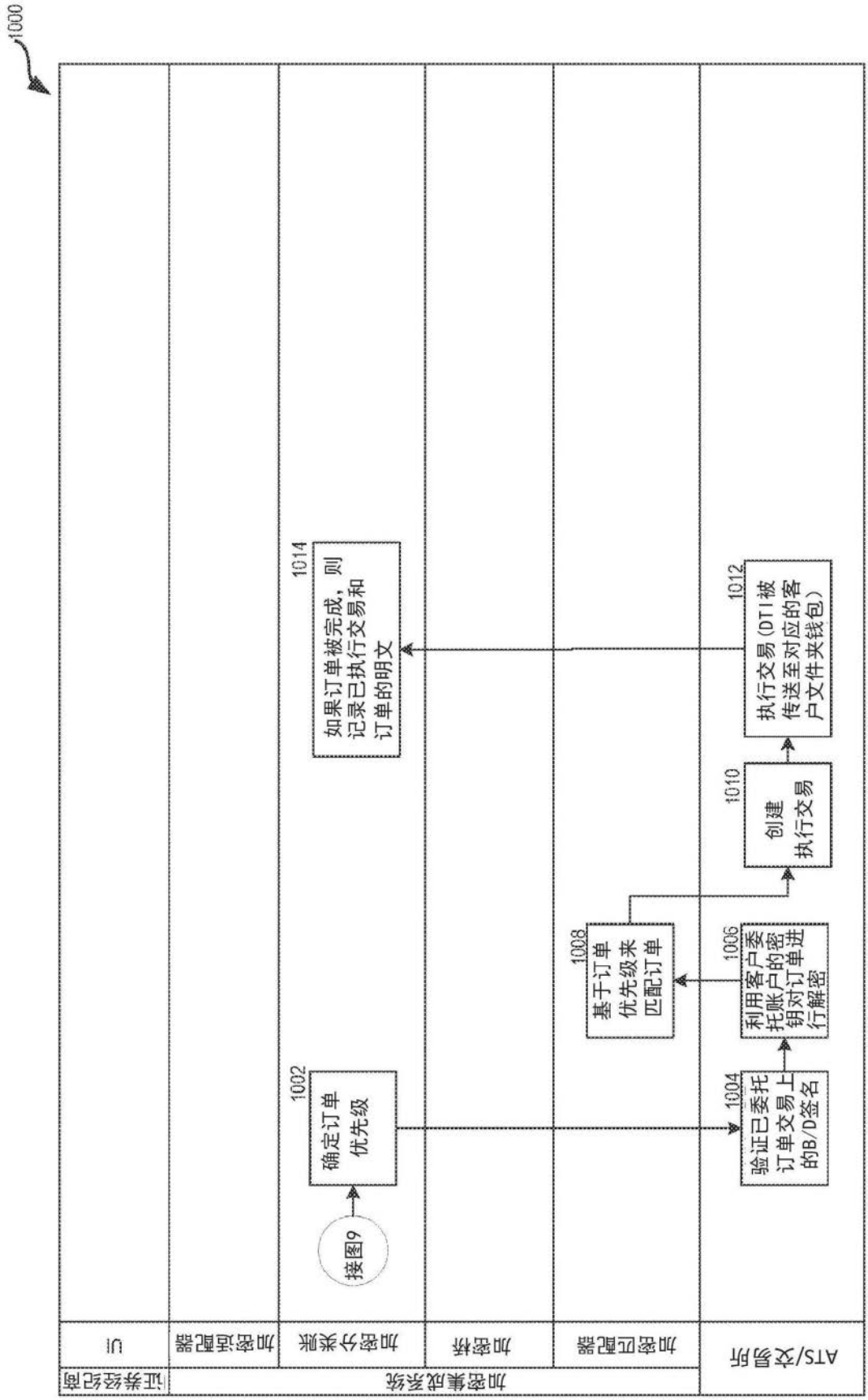

1000
证券经纪商
交易所集成系统
ATS/交易所
交易匹配器
交易桥
交易分发器
交易适配器
UI
1002
确定订单优先级
接图9
1004
验证已委托订单交易上的B/D签名
1006
利用客户委托账户的密钥对订单进行解密
1008
基于订单优先级来匹配订单
1010
创建执行交易
1012
执行交易(DTI被传送至对应的客户文件夹钱包)
1014
如果订单被完成，则记录已执行交易和订单的明文

图10

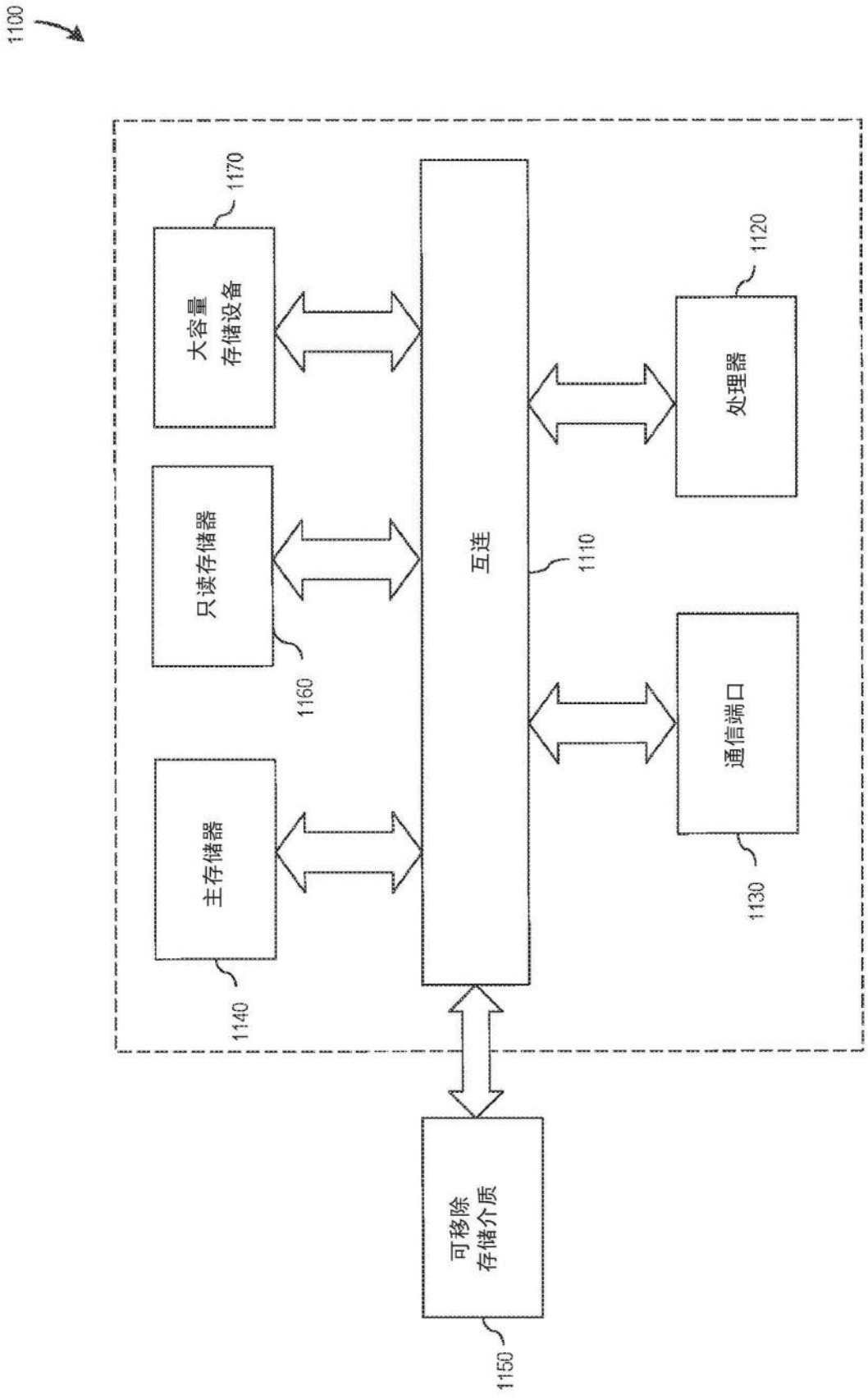

1100
大容量存储设备
1170
只读存储器
1160
主存储器
1140
互连
1110
处理器
1120
通信端口
1130
可移除存储介质
1150

图11