(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117616410 A
(43)申请公布日 2024.02.27

(21)申请号 202280046823.0

(22)申请日 2022.10.28

(30)优先权数据
17/543,143 2021.12.06 US

(85)PCT国际申请进入国家阶段日
2023.12.29

(86)PCT国际申请的申请数据
PCT/US2022/048276 2022.10.28

(87)PCT国际申请的公布数据
WO2023/107210 EN 2023.06.15

(71)申请人 贝宝公司
地址 美国加利福尼亚州

(72)发明人 休伯特·安德烈·勒范贡
吉内什·帕特尔

(74)专利代理机构 成都超凡明远知识产权代理有限公司 51258
专利代理师 张云娇

(51)Int.Cl.
G06F 16/23(2006.01)
H04L 67/60(2006.01)
H04L 41/06(2006.01)
G06F 11/14(2006.01)

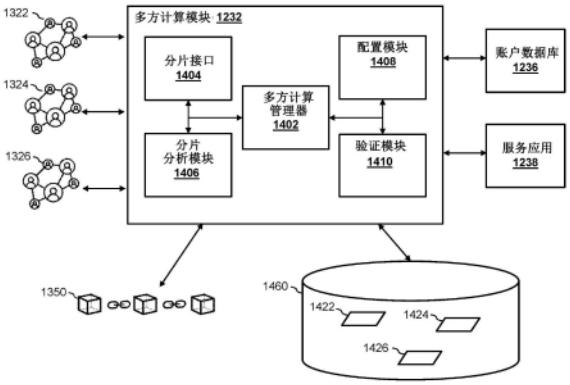
权利要求书3页 说明书37页 附图21页

(54)发明名称

计算机分片环境中的多方计算

(57)摘要

提出了提供用于促进分片环境内的多方计算的框架的方法和系统。在区块链被划分为多个分片链后,多方计算系统获得与第一分片链相关联的属性。这些属性可以表示第一分片链的特性、第一分片链中记录的交易的特性、以及被配置成管理第一分片链的计算机节点的特性。基于这些属性,多方计算系统确定多方计算方案,该方案指定参与交易验证过程所需的节点的最小阈值数量以及参与第一分片链的交易验证过程所需的至少一个所需节点。多方计算系统对被配置成管理第一分片链的计算机节点进行配置,以根据多方计算方案执行交易验证过程。



CN 117616410 A

1.一种系统,包括:

非暂态存储器;以及

一个或更多个硬件处理器,所述一个或更多个硬件处理器与所述非暂态存储器耦合并被配置成从所述非暂态存储器读取指令以使所述系统执行包括以下各项的操作:

获取与对应于区块链的多个分片链中的第一分片链相关联的属性,其中,所述属性是从被配置成管理所述第一分片链的多个计算机节点获得的;

对所述属性进行分析;

基于所述分析,确定用于对通过所述第一分片链进行的交易进行验证的多方计算方案,其中,所述多方计算方案指定(i)第一组计算机节点中的需要在对要记录在所述第一分片链中的交易进行验证时进行协作的计算机节点的最小阈值数量,以及(ii)所述第一组计算机节点中的作为必需节点的第一计算机节点,作为必需节点的所述第一计算机节点需要在对要记录在所述第一分片链中的交易进行验证时进行协作;以及

对所述第一组计算机节点进行配置以根据所述多方计算方案执行交易验证过程。

2.根据权利要求1所述的系统,其中,所述操作还包括:

基于与所述第一分片链相关联的加密密钥生成第一秘密和第二秘密,其中,使用所述第一秘密和所述第二秘密的电子数据的计算变换对使用所述加密密钥的电子数据的电子签名进行模仿;

基于所述第二秘密生成多个份额,其中,所述多个份额包括第一数量的份额,其中,需要所述多个份额中的小于第一数量的第二数量的份额来恢复所述第二秘密,并且其中,所述第二数量对应于所述多方计算方案中指定的计算机节点的所述最小阈值数量;以及

将所述第一秘密分发给所述第一计算机节点,并将所述多个份额分发给除所述第一计算机节点之外的所述第一组计算机节点。

3.根据权利要求1所述的系统,其中,所述分析包括对所述第一分片链中记录的交易进行分析。

4.根据权利要求1所述的系统,其中,所述分析包括对所述第一分片链中记录的交易的波动性进行分析。

5.根据权利要求1所述的系统,其中,所述分析包括对所述第一组节点的计算机硬件和软件配置进行分析。

6.根据权利要求1所述的系统,其中,所述多方计算方案为第一多方计算方案,并且其中,所述操作还包括:

在根据所述第一多方计算方案对所述第一组计算机节点进行配置之后,检测与所述第一组计算机节点或所述第一分片链中的至少一者相关联的条件;

响应于检测到所述条件,为所述第一分片链确定第二多方计算方案;以及

对所述第一组计算机节点进行重新配置,以根据所述第二多方计算方案执行所述交易验证过程。

7.根据权利要求6所述的系统,其中,所述第二多方计算方案指定在对要记录在所述第一分片链中的交易进行验证时进行协作的计算机节点的第二最小阈值数量。

8.根据权利要求6所述的系统,其中,所述第二多方计算方案从所述第一组计算机节点中指定作为必需节点的第二计算机节点,作为必需节点的第二计算机节点需要在对要记录

在所述第一分片中的交易进行验证时进行协作。

9.一种方法,包括:

通过一个或更多个硬件处理器与多个计算机节点交互,所述多个计算机节点被配置成对对应于区块链的多个分片链中的第一分片链进行管理;

基于所述交互并且通过所述一个或更多个硬件处理器确定与所述第一分片链相关的特性;

通过所述一个或更多个硬件处理器基于对所述特性进行分析来确定用于对通过所述第一分片链进行的交易进行验证的多方计算方案,其中,所述多方计算方案指定(i)第一组计算机节点中的需要在对要记录在所述第一分片链中的交易进行验证时进行协作的计算机节点的最小阈值数量,以及(ii)所述第一组计算机节点中作为必需节点的第一计算机节点,作为必需节点的所述第一计算机节点需要在对要记录在所述第一分片链中的交易进行验证时进行协作;以及

通过所述一个或更多个硬件处理器对所述第一组计算机节点进行配置,以根据所述多方计算方案执行交易验证过程。

10.根据权利要求9所述的方法,其中,所述多方计算方案为第一多方计算方案,并且其中,所述方法还包括:

在根据所述第一多方计算方案对所述第一组计算机节点进行配置之后,检测与所述第一组计算机节点或所述第一分片链中的至少一者相关联的条件;

响应于检测到所述条件,为所述第一分片链确定第二多方计算方案;以及

对所述第一组计算机节点进行重新配置,以根据所述第二多方计算方案执行所述交易验证过程。

11.根据权利要求10所述的方法,其中,所述条件与和所述第一分片链相关联的交易的波动性的变化相关联。

12.根据权利要求10所述的方法,其中,所述条件与交易数额的变化相关联,所述交易数额与和所述第一分片链相关的交易相关联。

13.根据权利要求10所述的方法,其中,所述条件与所述第一组计算机节点中的安全相关计算机配置的变化相关联。

14.根据权利要求10所述的方法,所述方法还包括:

对与所述多个分片链中的第二分片链相关联的第二组计算机节点进行配置,以根据第三多方计算方案执行所述交易验证过程;

响应于检测到与所述第一组计算机节点或所述第一分片链中的至少一者相关联的条件,确定用于所述第二分片链的第四多方计算方案;以及

对所述第二组计算机节点进行重新配置,以根据所述第四多方计算方案执行所述交易验证过程。

15.根据权利要求9所述的方法,其中,所述区块链与用于记录特定加密货币类型的加密货币交易的账本相关联。

16.根据权利要求9所述的方法,其中,所述区块链与用于记录智能合约交易的账本相关联。

17.一种非暂态机器可读介质,所述非暂态机器可读介质上存储有机器可读指令,所述

机器可读指令能够执行以使机器执行包括以下各项的操作：

获取与对应于区块链的多个分片链中的第一分片链相关联的属性，其中，所述属性是从被配置成管理所述第一分片链的多个计算机节点获得的；

基于对所述属性进行分析来确定用于对通过所述第一分片链进行的交易进行验证的多方计算方案，其中，所述多方计算方案指定(i)第一组计算机节点中需要在对要记录在所述第一分片链中的交易进行验证时进行协作的计算机节点的最小阈值数量，以及(ii)所述第一组计算机节点中作为必需节点的第一计算机节点，作为必需节点的所述第一计算机节点需要在对要记录在所述第一分片链中的交易进行验证时进行协作；以及

对所述第一组计算机节点进行配置以根据所述多方计算方案执行交易验证过程。

18.根据权利要求17所述的非暂态机器可读介质，其中，所述操作还包括：

基于与所述第一分片链相关联的加密密钥生成第一秘密和第二秘密，其中，使用所述第一秘密和所述第二秘密的电子数据的计算变换对使用所述加密密钥的电子数据的电子签名进行模仿；

基于所述第二秘密生成多个份额，其中，所述多个份额包括第一数量的份额，其中，需要所述多个份额中的小于所述第一数量的第二数量的份额来恢复所述第二秘密，并且其中，所述第二数量对应于所述多方计算方案中指定的计算机节点的所述最小阈值数量；以及

将所述第一秘密分发给所述第一计算机节点，并将所述多个份额分发给除所述第一计算机节点之外的所述第一组计算机节点。

19.根据权利要求17所述的非暂态机器可读介质，其中，所述多方计算方案为第一多方计算方案，并且其中，所述操作还包括：

在根据所述第一多方计算方案对所述第一组计算机节点进行配置之后，对与对应于区块链的所述多个分片链中的第二分片链相关联的条件进行检测；

响应于检测到所述条件，为所述第一分片链确定第二多方计算方案；以及

对所述第一组计算机节点进行重新配置，以根据所述第二多方计算方案执行交易验证。

20.根据权利要求19所述的非暂态机器可读介质，其中，所述条件与被配置成管理所述第二分片链的至少一个计算机节点上的计算机攻击相关联。

计算机分片环境中的多方计算

技术领域

[0001] 本说明书总体上涉及分布式计算,并且更具体地涉及根据本公开的各种实施方式提供用于计算机分片环境中的安全多方计算的框架。

背景技术

[0002] 区块链由于其固有的对等和不可变的特性,已成为一种流行的用于存储交易数据的计算机数据结构。例如,区块链已被用作去中心化分类帐来记录与各种加密货币、智能合约和其他类型的交易数据相关的交易数据。区块链的副本和/或部分可以存储在不同的计算机节点上,其中每个计算机节点可以被配置成验证交易并向区块链添加新的交易数据。当进行新交易时,一个或更多个计算机节点可以被配置成验证新交易(例如,通过工作量证明或权益证明机制等)。一旦新交易被验证,新交易的交易数据可以被一个或更多个计算机节点打包成块并附加到区块链的副本。

[0003] 随着越来越多的交易数据添加到区块链中,管理区块链的速度和效率性能可能会因区块链规模的持续增长而受到影响。提高区块链可扩展性的一种解决方案是将区块链划分为多个分片链,其中每个分片链对应于区块链的不同部分。被配置成管理区块链的计算机节点还可以分为不同的组,其中每个组可以被配置成管理对应的分片链。虽然这样的分片解决方案可以提高区块链的可扩展性,但它也使区块链(或与区块链相关的每个分片链)更容易受到攻击。例如,由于配置成存储和管理区块链的计算机节点被分为多个较小的计算机节点组来管理各个分片链,因此对分片链的51%攻击可以通过控制(例如,接管、感染病毒等)比对整个区块链完成相同攻击少得多数量的计算机节点来完成。因此,需要提供一种框架来提高分片区块链环境中电子交易的安全性。

附图说明

[0004] 图1示出了根据本公开的实施方式的用于促进一个或更多个基于区块链的交易的示例计算架构;

[0005] 图2示出了根据本公开的实施方式的示例区块链网络;

[0006] 图3示出了根据本公开的实施方式的示例区块链;

[0007] 图4是根据本公开的实施方式的示例交易消息的图;

[0008] 图5示出了根据本公开的实施方式的在区块链网络中广播的交易的示例;

[0009] 图6A是示出根据本公开的实施方式的用于执行基于区块链的交易的示例过程的流程图;

[0010] 图6B是示出根据本公开的实施方式的用于执行基于区块链的交易的另一示例过程的流程图;

[0011] 图7A示出了根据本公开的实施方式的秘密广播的区块链的示例;

[0012] 图7B示出了根据本公开的实施方式的区块链滥用的示例;

[0013] 图8示出了根据本公开的实施方式的启用区块链的店内购买系统的示例;

[0014] 图9示出了根据本公开的实施方式的支持物联网区块链的设备系统的通信的示例;

[0015] 图10示出了根据本公开的实施方式的示例系统;

[0016] 图11示出了根据本公开的实施方式的示例计算设备;

[0017] 图12是示出根据本公开的实施方式的包括电子交易系统的联网系统的框图;

[0018] 图13示出了根据本公开的实施方式的区块链的示例分片环境;

[0019] 图14是示出根据本公开的实施方式的多方计算模块的框图;

[0020] 图15示出了根据本公开的实施方式的一组计算机节点之间的秘密分布和秘密份额(share);

[0021] 图16示出了根据本公开的实施方式的用于执行验证过程的一组计算机节点间的交互;

[0022] 图17是示出根据本公开的实施方式的实现碎片链的多方计算方案的过程的流程图;

[0023] 图18是示出根据本公开的实施方式的修改碎片链的多方计算方案的过程的流程图;

[0024] 图19是示出根据本公开的实施方式的执行验证过程的过程的流程图;以及

[0025] 图20是用于实现根据本公开的实施方式的装置的系统的框图。

[0026] 通过参考下面的详细描述可以最好地理解本公开的实施方式及其优点。应当理解,相似的附图标记用于标识一幅或多幅图中所示的相似元件,其中其中的示出是为了说明本公开的实施方式的目的,而不是为了限制本公开的目的。

具体实施方式

[0027] 本公开包括用于提供用于促进分片环境内的多方计算的框架的方法和系统。如本文所讨论的,随着由多个计算机节点(在区块链网络中)管理的区块链的大小增长,将交易数据添加到区块链的速度和效率性能可能会降低。一种解决方案是将区块链分为多个部分(也称为“分片链”),使得每个计算机节点可以被配置成仅存储和管理对应的分片链(例如,区块链的对应部分)而不是整个区块链。已添加到每个分片链的交易可以随后(例如,离线等)合并到区块链。由于处理区块链的分片链的交易数据所需的处理资源大大少于处理整个区块链的交易数据所需的处理资源,因此可以提高速度和效率性能。

[0028] 然而,这样的分片解决方案也给区块链带来了新的安全风险。区块链的完整性可能取决于许多因素,包括被配置成存储和管理区块链网络内的区块链副本的计算机节点的总数。这是因为当区块链以分散的方式运行时,可以基于来自被配置成存储和管理区块链的各种副本的计算机节点的共识(例如,大多数)来确定区块链的真实版本。因此,损害区块链的完整性的一种方式(例如,向区块链添加欺诈数据和/或从区块链中删除合法数据)是控制住区块链网络内至少一半计算机节点,该至少一半计算机节点被配置成存储和管理区块链(也称为上面讨论的51%攻击)。被配置成存储和管理区块链的副本的计算机节点越多,对区块链执行此类攻击就越困难。

[0029] 通过将被配置成管理区块链的计算机节点划分为不同的节点组(例如,不同的分片网络)来存储和管理对应的分片链,被配置成管理每个分片链的节点数量大大少于分片

之前被配置成管理整个区块链的节点总数。用于存储和管理每个分片链的节点数量大大减少可能反过来会导致区块链更高的安全风险,因为在任何一个分片链上进行攻击(例如51%攻击)比在分片之前对整个区块链进行攻击更容易。

[0030] 这样,根据本公开的各个实施方式,多方计算系统可以被配置成使用多方计算技术来提高区块链的各个分片链的安全性和完整性。在一些实施方式中,多方计算系统可以访问与区块链相关联的分片链和被配置成存储和管理分片的计算机节点。多方计算系统可以确定每个分片链的一个或更多个度量。例如,多方计算系统可以为每个分片链确定表示对应于分片链的区块链部分的特性的链度量。链度量可以指示分片链的大小、分片链中的区块的年龄(例如,平均年龄等)、被添加到分片链的区块的速率或频率、以及与分片链相关联的其他信息。在一些实施方式中,链度量还可以表示整个区块链的大小、区块链的年龄、作为整体添加到区块链的区块的速率或频率、以及与区块链相关联的其他信息。

[0031] 多方计算机系统还可以确定表示记录在每个分片链中的交易的特性的交易度量。例如,交易度量可以表示分片链中记录的交易数额(例如,平均值、最小值、最大值等)、分片链中记录的交易数量、分片链中记录的交易的速率或频率、分片链中记录的交易的波动性、用于进行分片链中记录的交易的用户和/或用户设备的特性、以及与分片链中记录的交易相关联的其他信息。多方计算系统还可以确定表示被配置成存储和管理分片链的组内的计算机节点的特性的节点度量。例如,节点度量可以表示组内的每个计算机节点的安全级别、组内的每个计算机节点的硬件和/或软件配置、与组内的计算机节点之间的连接相关联的网络属性、以及与组中的计算机节点相关联的其他属性。

[0032] 基于与分片链相关联的度量,多方计算系统可以确定每个分片链的多方计算方案。多方计算方案可以指定对应于分片链的组(分片网络中)中的所有计算机节点(n个计算机节点)中用于验证要记录在分片链中的交易的参与节点的最小数量(t)。通过指定用于验证要记录在分片链中的交易的参与节点的最小数量(例如,节点组中超过一半的节点),可以提高分片的安全性。

[0033] 在一些实施方式中,为了进一步提高分片的安全性,多方计算系统还可以识别参与验证要记录在分片链中的交易所需的(也称为“必须具备的”)计算机节点。例如,多方计算系统可以针对每个特定分片链选择特定计算机节点作为参与通过特定分片验证交易所需的(“必须具备的”)计算机节点。例如,多方计算系统可以选择被配置成存储和管理特定分片链以及区块链的一个或更多个其他分片链的特定计算机节点。选择这样的计算机节点作为所需计算机节点的原因是,被配置(例如由区块链的管理员)成存储和管理多个分片链的计算机节点通常比其他节点更值得信赖并且具有更高的安全级别。因此,选择特定的计算机节点作为参与验证过程所需的节点将进一步提高分片的安全性。

[0034] 为了实现这样的多方计算过程,可以以使得需要多个秘密的组合来生成数字签名的方式来生成数字签名的多个秘密。生成的秘密的数量可以对应于一加上验证通过分片进行的交易所需的(“必须具备的”)计算机节点的数量。例如,如果验证过程仅需要一个所需的(“必须具备的”)计算机节点,则可以生成两个秘密来生成数字签名。如果验证过程需要两个所需的计算机节点,则可以生成三个秘密来生成数字签名。生成数字签名需要所有秘密的组合。多个秘密可以包括对应于一个或更多个所需计算机节点的一个或更多个非共享秘密,以及要在被配置成管理分片的组内的其他节点之间共享的共享秘密。

[0035] 多方计算系统可以在一个或更多个所需计算机节点之间分发一个或更多个非共享秘密(如果只有一个所需计算机节点,则将一个非共享秘密提供给所需计算机节点)。然后,多方计算系统可以使用本文公开的技术从剩余秘密(共享秘密)生成份额,并且将与共享秘密相关联的份额分发给组内的其他剩余计算机节点(除所需节点之外的多个计算机节点)。在一些实施方式中,多方计算系统可以根据共享秘密生成份额,并将份额分发给剩余的多个计算机节点,使得来自多个计算机节点的任意组合的份额等于t减去所需节点的数量,需要生成模拟基于共享秘密的计算的输出。在一些实施方式中,输出可以是共享秘密。在一些实施方式中,输出可以模拟基于共享秘密生成的产品。

[0036] 因此,在用于验证要记录在区块链的分片中的交易的验证过程期间,不包括所需节点的一组计算机节点可以协作使用它们对应的份额来执行一组计算以生成共享秘密或基于共享秘密的产品。如果足够数量的计算机节点(t减去所需节点的数量)参与验证过程,则该组计算机节点将使用其对应的份额成功生成与共享秘密相对应的输出(例如,共享秘密或模仿由共享秘密生成的产品)。然后,所需的节点可以使用相应的秘密对输出执行附加计算以生成数字签名。只有当生成正确的数字签名时,交易才会被记录在分片中。因此,当计算机节点的数量少于参与验证的计算机节点的最小阈值数量(t)时,或者当任何一个所需节点不参与交易的验证时,该交易不会被记录在对应的分片链中(例如,被分片网络中的计算机节点丢弃)。在一些实施方式中,当生成正确的数字签名时,所生成的数字签名也可以被记录在分片链中(例如,在与和交易相关联的交易数据相同的区块内)。

[0037] 区块链

[0038] 从最广泛的意义上来说,区块链是指支持在对等网络中以分布式方式存储、维护和更新的可信分类帐的框架。例如,在加密货币应用(诸如比特币或以太坊、Ripple、Dash、Litecoin、Dogecoin、zCash、Tether、比特币现金、Cardano、Stellar、EOS、NEO、NEM、Bitshares、Decred、Augur、Komodo、PIVX、Waves、Steem、Monero、Golem、Stratis、Bytecoin、Ardor)中,或者在数字货币兑换(诸如Coinbase、Kraken、CEX.IO、Shapeshift、Poloniex、Bitstamp、Coinmama、Bisq、LocalBitcoins、Gemini等)中,分布式分类帐代表加密货币单位在实体之间转移的每个交易。例如,使用数字货币兑换,用户可以购买任何价值的数字货币或将任何持有的数字货币兑换成全球货币或其他数字货币。每个交易都可以通过分布式分类帐进行验证,并且只有经过验证的交易才会添加到分类帐中。分类帐以及区块链的许多方面可以被称为“去中心化”,因为通常不存在中央机构。因此,分类帐的准确性和完整性不能在单一的中心位置受到攻击。为了保护账本的完整性,修改账本的全部或大部分存储位置变得困难。这在很大程度上是因为与构成对等网络的节点相关联的个人对分类帐的准确性有着既得利益。

[0039] 尽管在分布式分类帐中维护加密货币交易可能是当今区块链技术最知名的用途,但分类帐可能用于各种不同的领域。事实上,区块链技术适用于可以访问任何类型数据并保证数据准确性的任何应用。例如,供应链可以维护在区块链账本中,其中每个部件从一方到另一方以及从一个位置到另一个位置的转移可以记录在账本中以供以后检索。这样做可以更轻松地识别缺陷零件的来源以及其他此类缺陷零件的交付地点。类似地,食品可以以类似的方式从农场到杂货店再到购买者进行跟踪。

[0040] 现在将参照附图详细描述本公开的实现方式。

[0041] 应理解,本文所使用的措辞和术语是为了描述的目的,而不应当视为限制性的。相反,本文中使用的短语和术语应被赋予其最广泛的解释和含义。“包括”和“包含”及其变体的使用意味着涵盖其后列出的项目及其等同物以及附加项目及其等同物。

[0042] 计算架构

[0043] 如上所述,区块链框架中的分布式分类帐在对等网络中存储、维护和更新。在一个示例中,分布式分类帐维护许多区块链交易。图1示出了用于促进区块链交易的示例系统100。系统100包括经由网络140互连的第一客户端设备120、第二客户端设备125、第一服务器150、第二服务器152、以及物联网(IoT)设备155。第一客户端设备120、第二客户端设备125、第一服务器150和/或第二服务器152可以是参考图11更详细地描述的计算设备1105。IoT设备155可以包括多种设备中的任何设备,包括车辆、家用电器、嵌入式电子设备、软件、传感器、致动器、恒温器、灯泡、门锁、冰箱、RFID植入物、RFID标签、起搏器、可穿戴设备、智能家居设备、摄像机、跟踪器、泵、POS设备、固定和移动通信设备、以及配置成连接和交换数据的连接硬件。网络140可以是各种可用网络中的任何一种,例如互联网,并且代表支持连接到网络140的设备之间的通信的网络和网关的全球集合。系统100还可以包括一个或更多个分布式或对等(P2P)网络,例如第一、第二和第三区块链网络130a-c(通常称为区块链网络130)。如图1所示,网络140可以包括第一区块链网络130a和第二区块链网络130b。第三区块链网络130c可以与如下参考图2描述的私有区块链相关联,并且连接到一个或更多个服务器,诸如服务器152,并且因此与第一区块链网络130a和第二区块链网络103b分开示出。每个区块链网络130可以包括多个互连的设备(或节点),如参考图2更详细地描述的。如上所述,账本或区块链是一种分布式数据库,用于维护不断增长的包含任何类型信息的记录列表。如参照图3更详细地描述的,区块链可以至少存储在一个或更多个区块链网络130的多个节点(或设备)处。

[0044] 在一个示例中,基于区块链的交易通常可以涉及实体(诸如图1中的第一客户端设备120的第一用户110和第二客户端设备125的第二用户115)之间的数据或价值的传输。服务器150和152中的每一个可以包括一个或更多个应用程序,例如,被配置成通过利用与区块链网络130之一相关联的区块链来促进实体之间的交易的交易应用程序。作为示例,第一用户110可以经由在第一客户端设备120上执行的用户应用来请求或发起与第二用户115的交易。该交易可以涉及从第一用户110到第二用户115的价值或数据的转移。第一客户端设备120可以向服务器150发送交易请求。第一服务器150和/或第二服务器152可以将所请求的交易发送到区块链网络130之一以被验证和批准,如下所述。

[0045] 区块链网络

[0046] 图2示出了包括多个互连的节点或设备205a-h(通常称为节点205)的示例区块链网络200。每个节点205可以包括参考图11更详细地描述的计算设备1105。尽管图2示出了单个设备205,但是每个节点205可以包括多个设备(例如,池)。区块链网络200可以与一个或更多个区块链220a-h(通常称为区块链220)相关联。一些或所有节点205可以复制并保存区块链220的相同副本。例如,图3示出节点205b-e和205g-h存储区块链220的副本。节点205b-e和205g-h可以独立地更新它们各自的区块链220的副本,如下所述。

[0047] 区块链节点类型

[0048] 区块链节点,例如节点205,可以是全节点或轻量节点。全节点(例如节点205b-e和

205g-h)可以通过存储整个区块链220的副本并确保发布到区块链220的交易有效来充当区块链网络200中的服务器。全节点205b-e和205g-h可以在区块链220上发布新块。诸如节点205a和205f之类的轻量级节点可以具有比全节点更少的计算资源。例如,物联网设备通常充当轻量级节点。轻量级节点可以与其他节点205通信,向全节点205b-e和205g-h提供信息,并且查询由全节点205b-e和205g-h存储的区块链220的区块的状态。然而,在该示例中,如图2所示,轻量级节点205a和205f可以不存储区块链220的副本,因此,可以不在区块链220上发布新块。

[0049] 区块链网络类型

[0050] 区块链网络200及其关联的区块链220可以是公共的(无需许可的)、联合的或联盟的、或私有的。如果区块链网络200是公共的,则任何实体都可以读取和写入相关联的区块链220。然而,如果由单个实体或组织控制,则区块链网络200及其关联的区块链220可以是联合的或联盟的。此外,可以限制能够访问互联网的任何节点205参与区块链220上的交易的验证。如果对区块链网络200和区块链220的访问仅限于特定的授权实体,例如组织或个人组,则区块链网络200及其关联的区块链220可以是私有的(被许可的)。此外,区块链220的读取权限可以是公共的或受限的,而写入权限可以仅限于控制或授权实体。

[0051] 区块链

[0052] 如上所述,区块链220可以与区块链网络200相关联。图3示出了示例区块链300。区块链300可以包括多个区块305a、305b和305c(通常称为区块305)。区块链300包括第一块(未示出),有时称为创世块。每个区块305可以包括一个或更多个提交并验证的交易的记录。区块链300的区块305可以链接在一起并以密码方式保护。在某些情况下,随时间动态变化的后量子密码算法可以用于减轻量子计算破坏现有密码方案的能力。下面提供了存储在区块链块中的各种类型的数据字段的示例。区块链300的副本可以例如由节点205b-e和205g-h本地存储在云中、网格上作为文件或存储在数据库中。

[0053] 区块

[0054] 区块305中的每一者可以包括一个或更多个数据字段。区块链300内的区块305和对应的数据字段的组织可以是特定于实现方式的。作为示例,区块305可以包括相应的标头320a、320b和320c(一般称为标头320)以及区块数据375a、375b和375c(一般称为区块数据375)。标头320可以包括与其相应的区块305相关联的元数据。例如,标头320可以包括相应的区块编号325a、325b和325c。如图3所示,区块305a的区块编号325a是N-1,区块305b的区块编号325b是N,并且区块305c的区块编号325c是N+1。区块305的标头320可以包括数据字段,该数据字段包括区块大小(未示出)。

[0055] 区块305可以链接在一起并以密码方式保护。例如,区块N(区块305b)的标头320b包括数据字段(前一个区块哈希330b),该数据字段包括前一个区块N-1的标头320a的哈希表示。用于生成哈希表示的哈希算法可以是例如导致固定长度的输出的安全哈希算法256(SHA-256)。在该示例中,哈希算法是单向哈希函数,其中基于哈希函数的输出来确定哈希函数的输入在计算上是困难的。另外,区块N+1(区块305c)的标头320c包括数据字段(前一个区块哈希330c),该数据字段包括区块N(区块305b)的标头320b的哈希表示。

[0056] 区块305的标头320还可以包括数据字段,这些数据字段包括区块数据的哈希表示,诸如区块数375375据哈希370a-c。区块数据哈希370a-c可以例如通过Merkle树并通过

存储哈希或通过使用基于所有区块数据的哈希来生成。区块305的标头320可以包括相应的随机数360a、360b和360c。在一些实施方式中,随机数360a-c的值是与区块的哈希级联(或附加到区块的哈希)的任意字符串。标头320可以包括其他数据,诸如难度目标。

[0057] 区块305可以包括相应的区块数据375a、375b和375c(通常称为区块数据375)。区块数据375可以包括也已经经由共识模型(如下所述)集成到区块链200中的经验证交易的记录。如上所述,除了经验证的交易之外,区块数据375还可以包括各种不同类型的数据。区块数据375可以包括可以数字地表示和电子地存储的任何数据,诸如文本、音频、视频、图像或文件。

[0058] 区块链交易

[0059] 在一个示例中,基于区块链的交易通常可以涉及数据或价值的传输或者实体之间的交互,并且在下面更详细地描述。返回参照图1,第一服务器150和/或第二服务器152可以包括一个或更多个应用程序,例如,被配置成促进实体之间的区块链交易的交易应用程序。这些实体可以包括用户、设备等。第一用户110可以经由在第一客户端设备120上执行的用户应用来请求或发起与第二用户115的交易。该交易可以涉及从第一用户110到第二用户115的价值或数据的转移。价值或数据可以表示金钱、合同、财产、记录、权利、状态、供应、需求、警报、触发或可以以数字形式表示的任何其他资产。该交易可以表示第一用户110和第二用户115之间的交互。

[0060] 图4是由交易应用程序生成的交易465的图。交易465可以包括公钥415、与第一用户110相关联的区块链地址430、数字签名455和交易输出信息460。交易应用程序可以通过将加密哈希函数410应用到私钥405来从第一用户110的私钥405得出公钥415。加密哈希函数410可以基于SHA-2或SHA-3,但是可以利用其他加密模型。有关加密算法的更多信息,请参阅联邦信息处理标准出版物(FIPS PUB 180-3)的安全哈希标准。交易应用程序可以通过将哈希函数420应用于公钥415来得出第一用户110的地址或标识符,诸如区块链地址430。简而言之,哈希函数是可以用于将任意大小的数据映射到固定大小的数据的函数。该值也可以称为摘要、哈希值、哈希码或哈希。为了指示第一用户110是交易465的发起者,交易应用程序可以使用第一用户110的私钥405来生成交易数据435的数字签名455。交易数据435可以包括关于要转移的资产的信息以及对资产源的引用,诸如资产被转移到第一用户110的先前交易或者发起资产的事件的标识。生成数字签名455可以包括将哈希函数440应用到交易数据435,从而产生哈希交易数据445。可以使用第一用户110的私钥405对哈希交易数据445和交易数据435进行加密(经由加密函数450),从而产生数字签名455。交易输出信息460可以包括资产信息470和第二用户115的地址或标识符,诸如区块链地址475。交易465可以从第一客户端设备125发送到第一服务器150。

[0061] 所使用的加密算法的特定类型可以基于各种因素动态地变化,诸如时间长度、隐私问题等。例如,所使用的加密算法的类型可以每年、每周、每天等改变。算法类型也可能根据不同的隐私级别而变化。例如,内容的所有者可以通过利用更强的算法来实现更高级别的保护或隐私。

[0062] 区块链地址

[0063] 区块链网络可以利用区块链地址来指示使用区块链的实体或交易中的起点和终点。例如,在图4中被示为发送方430的区块链地址的第一用户110的区块链地址可以包括基

于将加密哈希函数420应用于公钥415从第一用户110的公钥415得出的字母数字字符串。用于得出地址的方法可能会有所不同,并且可能特定于区块链网络的实现方式。在一些示例中,区块链地址可以被转换成QR码表示、条形码、令牌或其他视觉表示或图形描述,以使该地址能够被移动设备、可穿戴设备、传感器、相机等光学扫描。除了地址或QR码之外,还有许多识别区块链中表示的个人、物体等QR。例如,可以通过诸如指纹、视网膜扫描、语音、面部ID、温度、心率、个人特有的手势/动作等生物识别信息以及诸如帐号、家庭住址、社会安全号码、正式姓名等等其他类型的识别信息来识别个人。

[0064] 广播交易

[0065] 第一服务器150可以从区块链网络130的用户接收交易。交易可以经由桌面应用程序、智能手机应用程序、数字钱包应用程序、网络服务或其他软件应用程序提交到第一服务器150。第一服务器150可以向区块链网络130发送或广播交易。图5示出了由服务器150广播到区块链网络130的示例交易502。交易502可以被广播到区块链网络130的多个节点205。通常,一旦交易502被广播或提交到区块链网络130,它就可以被一个或更多个节点205接收。一旦交易502被区块链网络130的一个或更多个节点205接收到,它就可以被接收节点205传播到区块链网络130的其他节点205。

[0066] 区块链网络可以根据一组规则运行。规则可以指定节点可以接受交易的条件、节点可以接受的交易类型、节点为接受和处理交易而接收的补偿类型等。例如,节点可以基于交易历史、声誉、计算资源、与服务提供商的关系等接受交易。规则可以指定向节点广播交易的条件。例如,可以基于与节点的地理位置、历史、声誉、市场条件、案卷/延迟、技术平台相关的标准,将交易广播到一个或更多个特定节点。规则可以动态修改或更新(例如,打开或关闭)以解决诸如等待时间、可扩展性和安全条件等问题。交易可以被广播到节点的子集,作为对与那些节点相关联的实体的补偿的形式(例如,通过接收将一个或更多个交易的区块添加到区块链的补偿)。

[0067] 交易验证-用户认证和交易数据完整性

[0068] 由于诸如等待时间之类的问题,并非所有全节点205都可以同时接收广播的交易502。另外,并非所有接收广播的交易502的全节点205都可以选择验证交易502。节点205可以选择例如基于与交易502相关联的交易费用来验证特定交易。交易502可以包括发送方的区块链地址505、公钥510、数字签名515和交易输出信息520。节点205可以验证交易502是否合法或者符合一组预定义的规则。节点205还可以基于建立用户真实性和交易数据完整性来验证交易502。可以通过确定交易502所指示的发送方实际上是否是交易502的实际发起者来建立用户真实性。用户真实性可以通过密码术来证明,例如,使用一对密钥(例如公钥和私钥)的非对称密钥密码术。当建立用户真实性时可以考虑附加因素,例如用户信誉、市场状况、历史、交易速度等。可以通过确定与交易502相关联的数据是否以任何方式被修改来建立交易502的数据完整性。返回参照图4,当交易应用程序创建交易465时,其可以通过包括数字签名455来指示第一用户110是交易465的发起者。

[0069] 节点205可以使用公钥510来解密数字签名515。解密的结果可以包括哈希交易数据540和交易数据530。节点205可以基于将哈希函数545应用于交易数据530来生成哈希交易数据550。节点205可以在第一哈希交易数据540和第二哈希交易数据550之间执行比较565。如果比较565的结果570指示匹配,则可以建立交易502的数据完整性并且节点205可以

指示交易502已经被成功验证。否则,交易502的数据可能已经以某种方式被修改,并且节点205可以指示交易502尚未被成功验证。

[0070] 每个全节点205可以构建其自己的区块并将经验证的交易添加到该区块。因此,不同全节点205的区块可以包括不同的经验证的交易。作为示例,全节点205a可以创建包括交易“A”、“B”和“C”的第一区块。另一个全节点205b可以创建包括交易“C”、“D”和“E”的第二区块。两个区块都可能包含有效交易。然而,只能将一个区块添加到区块链中,否则区块可能共有的交易,例如交易“C”,可能会被记录两次,从而导致交易执行两次时出现双花等问题。上述示例中可能出现的一个问题是,交易“C”、“D”和“E”在添加到区块链时可能会被过度延迟。这可以通过如下讨论的多种不同方式来解决。

[0071] 保护钥匙

[0072] 私钥、公钥和地址可以使用软件(例如数字钱包)来管理和保护。私钥也可以使用硬件来存储和保护。数字钱包还可以使用户能够进行交易并管理余额。数字钱包可以在线或离线、并且在软件或硬件或硬件和软件两者中存储或维护。如果没有公钥/私钥,用户就无法证明资产的所有权。此外,任何有权访问用户公钥/私钥的人都可以访问用户的资产。虽然资产可能记录在区块链上,但如果没有私钥,用户可能无法访问它们。

[0073] 令牌

[0074] 令牌可以指区块链中属于区块链地址的条目。该条目可以包括指示资产所有权的信息。令牌可以代表金钱、合同、财产、记录、访问权、状态、供应、需求、警报、触发、声誉、票据或可以以数字形式表示的任何其他资产。例如,令牌可以指与用于特定目的的加密货币相关的条目,或者可以代表真实世界资产(例如法定货币或房地产)的所有权。令牌合约是指代表智能合约中编码的一组规则的加密令牌。拥有该区块链地址对应私钥的人可以访问该地址处的令牌。因此,区块链地址可以代表拥有令牌的人的身份。只有区块链地址的所有者才能将令牌发送给另一个人。所有者可以通过所有者的钱包访问令牌。令牌的所有者可以通过区块链交易将令牌发送或转移给用户。例如,所有者可以用私钥签署与令牌转移相对应的交易。当用户接收到令牌时,该令牌可以被记录在区块链中用户的区块链地址处。

[0075] 建立用户身份

[0076] 虽然数字签名可以提供交易和所转移资产的所有者之间的链接,但它可能无法提供与所有者真实身份的链接。在某些情况下,可能需要建立与数字签名相对应的公钥所有者的真实身份。例如,可以基于生物统计数据、密码、个人信息等来验证公钥所有者的真实身份。生物统计数据可以包括任何物理识别信息,例如指纹、面部和眼睛图像、语音样本、DNA、人体运动、手势、步态、表情、心率特征、温度等。

[0077] 发布和验证区块

[0078] 如上所述,全节点205可以各自构建其自己的包括不同交易的区块。节点可以通过将经过验证的交易添加到区块来构建区块,直到区块达到可以由区块链规则指定的特定大小。然而,只能将其中一个区块添加到区块链中。可以基于共识模型来确定要添加到区块链的区块以及区块的排序。在工作量证明模型中,两个节点可能通过解决复杂的数学难题来竞争将各自的区块添加到区块链中。例如,这样的谜题可以包括确定随机数,如上所述,使得要添加到区块链(包括随机数)的区块的哈希(使用预定哈希算法)具有满足范围限制的值。如果两个节点同时解决了难题,则可能会创建“叉(fork)”。当全节点205解决难题时,它

可以发布其区块以由区块链网络130的验证节点205验证。

[0079] 在工作量证明共识模型中,节点验证交易,例如,通过对存储在区块链中的当前账本进行检查或搜索。该节点将为区块链创建新区块,该区块将包括一个或更多个已验证交易的数据(参见例如图3的区块375)。在比特币等区块链实现中,区块的大小受到限制。返回参考图3,在该示例中,区块将包括表示区块链中当前最后一个区块的哈希的前一个区块哈希330。该区块还可以包括其自己的交易数据的哈希370(例如,所谓的Merkle哈希)。根据特定算法,可以对来自区块的所有或选择的数据进行哈希以创建最终哈希。根据工作量证明模型的实施方式,节点将寻求修改块的数据,使得最终哈希小于预设值。这是通过添加称为随机数360的数据值来实现的。因为不能基于其输入来预测最终哈希,所以不可能估计将导致小于预设值的最终哈希的随机数360的适当值。因此,在该实施方式中,在节点处需要计算密集型操作,以通过“强力”试错法来确定合适的随机数值。一旦确定了成功的随机数值,完整的区块就会发布到区块链网络进行验证。如果得到区块链网络中大多数节点的验证,则完整的区块将被添加到每个参与节点的区块链中。当节点的区块未添加到区块链时,该区块将被丢弃,并且该节点将继续构建新区块。被丢弃的区块中的交易可以返回到队列并等待添加到下一个区块。当交易被丢弃或返回到队列时,与被丢弃交易相关的资产不会丢失,因为资产的记录将存在于区块链中。但是,当交易返回到队列时,会导致交易完成延迟。减少完成交易的时间可能很重要。一组区块链规则或处理返回交易的节点的重新枚举/补偿可以确定今后如何处理返回的交易。当交易被放入池中时,它可以具有优先级,但是规则可以指示交易优先级必须超过阈值水平。可以提高返回或丢弃的交易的优先级。减少完成交易时间的另一种方法是让系统、服务提供商、交易参与者或商家为节点处理返回的交易支付额外的奖励。作为示例,服务提供商可以基于地理位置或基于批量折扣角度来识别首选矿工的网络。可以通过将返回的交易路由到特定的优选节点来优化完成交易的时间。交易可能与地址相关联,该地址限制如果交易由于包含在丢弃的区块中而被返回,则哪些首选节点将处理该交易。值可以与交易相关联,以便它流向特定地理位置的首选矿工。此外,返回的交易可以根据预设规则进行处理。例如,规则可以指示处理特定数量的返回交易以获得额外激励或补偿的承诺。

[0080] 区块链确认

[0081] 在包含交易的区块被添加到区块链之后,可以为该交易生成区块链确认。区块链确认可以是在包含交易的区块之后添加到区块链的多个区块。例如,当交易被广播到区块链时,将不会有与该交易相关的区块链确认。如果交易未经过验证,则包含该交易的区块将不会被添加到区块链中,并且该交易将继续没有与其关联的区块链确认。但是,如果包含交易的区块经过验证,则该区块中的每个交易都将具有与该交易关联的区块链确认。因此,当区块被验证时,区块中的交易将有一个与之关联的区块链确认。当区块被添加到区块链时,区块中的每笔交易都会有两个与之关联的区块链确认。随着额外的验证块添加到区块链中,与该区块相关的区块链确认数量将会增加。因此,与交易相关的区块链确认的数量可能表明覆盖或逆转交易的难度。更高价值的交易在执行之前可能需要更多数量的区块链确认。

[0082] 共识模型

[0083] 如上所述,区块链网络可以确定哪个全节点205向区块链发布下一个区块。在未经

许可的区块链网络中,节点205可以竞争以确定哪个节点发布下一个区块。可以基于共识模型选择节点205来将其区块发布为区块链中的下一个区块。例如,所选择的或获胜的节点205可以接收奖励,例如,用于发布其区块的交易费。可以使用各种共识模型,例如工作量证明模型、权益证明模型、委托权益证明模型、循环模型、权威证明或身份证明模型、以及经过时间证明模型。

[0084] 在工作量证明模型中,节点可以通过成为第一个解决计算密集型数学问题(例如,上述数学难题)来发布下一个区块。该解决方案可以作为节点花费适当的努力来发布区块的"证明"。在区块被接受之前,解决方案可以由全节点验证。然而,工作量证明模型可能容易受到下述51%攻击。权益证明模型的计算强度通常低于工作量证明模型。与工作量证明模型向任何具有解决数学问题的计算资源的节点开放不同,权益证明模型向系统中拥有权益的任何节点开放。权益可以是区块链网络节点(用户)可能已投资到系统中的一定数量的加密货币。节点发布下一个区块的可能性可能与其权益成正比。由于该模型使用较少的资源,区块链可能会放弃奖励作为发布下一个区块的激励。循环模型通常由许可的区块链网络使用。使用这种模型,节点可以轮流发布新块。在经过时间证明模型中,每个发布节点都从其计算机系统内的安全硬件请求等待时间。发布节点可能会在等待时间内处于空闲状态,然后创建一个区块并将其发布到区块链网络。作为示例,在需要速度和/或可扩展性的情况下(例如在企业环境中),混合区块链网络可以在完全或部分许可和无许可之间切换。网络可能会根据各种因素进行切换,例如延迟、安全性、市场状况等。

[0085] 叉

[0086] 如上所述,共识模型可以用于确定区块链上事件的顺序,例如哪个节点添加下一个区块以及哪个节点的交易首先得到验证。当存在与事件顺序相关的冲突时,结果可能是区块链中的叉。叉可能会导致区块链的两个版本同时存在。共识方法通常解决与事件排序相关的冲突,从而防止叉的发生。在某些情况下,叉可能是不可避免的。例如,在工作量证明共识模型中,只有一个竞争解决难题的节点可能会通过首先解决其难题而获胜。然后获胜节点的区块将由网络进行验证。如果获胜节点的区块成功被网络验证,那么它将是添加到区块链的下一个区块。然而,有可能两个节点最终会同时解决各自的难题。在这种情况下,两个获胜节点的区块可以被广播到网络。由于不同的节点可以接收不同获胜节点的通知,因此接收作为获胜节点的第一节点的通知的节点可以将第一节点的区块添加到它们的区块链副本中。接收到第二节点作为获胜节点的通知的节点可以将第二节点的区块添加到它们的区块链副本中。这会产生两个版本的区块链或叉。这种类型的叉可以通过工作量证明共识模型的最长链规则来解决。根据最长链规则,如果存在两个版本的区块链,则区块数量较多的链可以被认为是有效的区块链。区块链的其他版本可能被视为无效并被丢弃或孤立。由于不同节点创建的区块可能包含不同的交易,因此叉可能会导致交易被包含在区块链的一个版本中,而不是另一个版本中。被丢弃的区块链的区块中的交易可以被返回到队列并等待被添加到下一个区块。

[0087] 在某些情况下,叉可能是由与区块链实现相关的更改引起的,例如,区块链协议和/或软件的更改。由于叉对大量用户的影响,叉对于无需许可的全球分布式区块链网络可能比私有区块链网络更具破坏性。对向后兼容的区块链实现的更改或更新可能会导致软叉。当出现软叉时,某些节点可能会执行更新区块链实现,而其他节点可能不会。但是,未更

新到新区块链实施的节点可能会继续与更新的节点进行交易。

[0088] 对不向后兼容的区块链实现的更改可能会导致硬叉。虽然硬叉通常是有意的,但它们也可能是由无意的软件错误/错误引起的。在这种情况下,网络中的所有发布节点可能需要更新到新的区块链实现。虽然未更新到新的区块链实现的发布节点可以继续根据先前的区块链实现来发布区块,但是这些发布节点可以拒绝基于新的区块链实现创建的区块并继续接受基于先前的区块链实现创建的区块。因此,区块链不同硬叉版本上的节点可能无法相互交互。如果所有节点都迁移到新的区块链实现,那么以前的版本可能会被丢弃或放弃。然而,将网络中的所有节点更新到新的区块链实现可能是不实际或不可行的,例如,如果更新使某些节点使用的专用硬件失效。

[0089] 基于区块链的应用:加密货币

[0090] 加密货币是可以电子方式创建并存储在区块链中的交换媒介,如图1中的区块链130a。比特币是加密货币的一个示例,但还有其他几种加密货币。可以使用各种加密技术来创建加密货币单位并验证交易。作为示例,第一用户110可以拥有10个单位的加密货币。区块链130a可以包括指示第一用户110拥有10个单位的加密货币的记录。第一用户110可以经由在第一客户端设备120上执行的钱包应用程序发起将10个单位的加密货币转移到第二用户115。钱包应用程序可以存储和管理第一用户110的私钥。钱包设备的示例包括个人计算机、膝上型计算机、智能手机、个人数据助理(PDA)等。

[0091] 图6A是示出用于在诸如图1中的第一客户端设备120的第一用户110和第二客户端设备125的第二用户115之类的实体之间执行区块链交易的示例方法600的步骤的流程图。方法600的步骤可以由图1所示的任何计算设备来执行。替代地或附加地,方法600的一些或全部步骤可以由一个或更多个其他计算设备执行。方法600的步骤可以被修改、省略和/或以其他顺序执行,和/或添加其他步骤。

[0092] 在步骤605,钱包应用程序可以生成用于将10个单位的加密货币从第一用户110转移到第二用户120的交易数据。钱包应用程序可以使用第一用户110的私钥来生成用于交易的公钥。为了表明第一用户110是交易的发起者,还可以使用第一用户110的私钥为交易生成数字签名。如参考图4所讨论的,交易数据可以包括信息,例如发送方430的区块链地址、数字签名455、交易输出信息460和发送方415的公钥。交易数据可以从第一客户端设备125发送到第一服务器150。

[0093] 第一服务器150可以从第一客户端设备125接收交易数据。在步骤610,第一服务器150可以将交易广播到区块链网络130a。该交易可以由区块链网络130a的一个或更多个节点205接收。在步骤615,在接收到交易时,节点205可以选择例如基于与交易相关联的交易费用来验证交易。如果该交易没有被任何节点205选择进行验证,则该交易可以被放置在队列中并等待被节点205选择。

[0094] 在步骤620,选择该交易的每个节点205可以验证该交易。验证交易可以包括确定交易是否合法或者是否符合该交易的预定义规则集、建立用户真实性以及建立交易数据完整性。在步骤625,如果交易被节点205成功验证,则验证的交易被添加到由该节点205构造的区块中(步骤630)。如上所述,由于不同的节点205可以选择验证不同的交易,所以不同的节点205可以构建或组装包括不同的经验证的交易的区块。因此,与第一用户110向第二用户115转移10个单位的加密货币相关联的交易可以被包括在一些区块中而不是其他区块

中。

[0095] 在步骤635,区块链网络130a可以等待区块被发布。经验证的交易可以被添加到由节点205组装的区块,直到其达到由区块链指定的最小大小。如果区块链网络130a利用工作证明共识模型,则节点205可以通过解决复杂的数学难题来竞争将其各自的区块添加到区块链的权利。首先解决其难题的节点205赢得发布其区块的权利。作为补偿,获胜节点可以被奖励与交易相关联的交易费(例如,来自第一用户110的钱包)。替代地或附加地,获胜节点可以被奖励作为从区块链网络添加到与获胜节点相关联的账户的加密货币数量的补偿(例如,“新”的加密货币单位进入流通)。后一种补偿和释放新的加密货币单位进入流通的方法有时被称为“挖矿”。在步骤640,如果区块尚未被发布,则过程600返回到步骤635并等待区块被发布。然而,在步骤640,如果已经发布了区块,则过程600进行到步骤645。

[0096] 在步骤645,将所发布的区块广播到区块链网络130a以进行验证。在步骤650,如果该区块被大多数节点205验证,则在步骤655,将经验证的区块添加到区块链220。然而,在步骤650,如果该区块没有被大多数节点205验证,则过程600前进到步骤675。在步骤675,该区块被丢弃,并且被丢弃的区块中的交易被返回到队列。队列中的交易可以由一个或更多个节点205选择用于下一个区块。构建被丢弃的区块的节点205可以构建新的下一个区块。

[0097] 在步骤660,如果交易被添加到区块链220,则服务器150可以等待接收该交易的最小数量的区块链确认。在步骤665,如果尚未接收到交易的最小数量的确认,则过程可返回到步骤660。然而,如果在步骤665,已经接收到最小数量的确认,则过程进行到步骤670。在步骤670,可以执行交易并且可以将来自第一用户110的资产转移到第二用户115。例如,在交易接收到至少三个确认之后,第一用户110拥有的10个单位的加密货币可以从第一用户110的金融账户转移到第二用户115的金融账户。

[0098] 智能合约

[0099] 智能合约是存储在区块链中的协议,当协议的预定条款和条件得到满足时自动执行。该协议的条款和条件可能对区块链的其他用户可见。当满足预先定义的规则时,就会自动执行相关代码。该协议可以使用Java、C++、JavaScript、VBScript、PHP、Perl、Python、Ruby、ASP、Tcl等编程语言编写为脚本。该脚本可以作为区块链上的交易上传到区块链。

[0100] 作为示例,第一用户110(也称为租户110)可以从第二用户115(也称为房东115)租用公寓。租户110和房东115之间可以利用智能合约来支付租金。智能合约可以表明租户110同意在当月28日之前支付下个月的租金1000美元。该协议还可以指示,如果租户110支付租金,则房东115向租户110提供电子收据和公寓的数字进入钥匙。协议还可以表明,如果租户110在当月28日之前支付租金,则在当月的最后一天,将进入密钥和租金分别释放给租户110和房东115。

[0101] 图6B是示出用于在诸如租户110和房东115的实体之间执行智能合约交易的示例方法601的步骤的流程图。方法601的步骤可以由图1所示的任何计算设备来执行。替代地或附加地,方法601的一些或全部步骤可以由一个或更多个其他计算设备执行。方法601的步骤可以被修改、省略和/或以其他顺序执行,和/或添加其他步骤。

[0102] 在步骤676,可以创建租户110和房东115之间的协议或智能合约,然后将其作为交易提交给区块链网络130a。交易可以被添加到由区块链网络130a的节点205开采的区块,包括交易的区块可以由区块链网络130a验证并且然后被记录在区块链220中(如在图6A中的

步骤610-655中所示)。与交易相关的协议可以被赋予唯一的地址以供识别。

[0103] 在步骤678,过程601等待接收关于与协议相关的条件的信息。例如,过程601可以等待接收$1000从与租户110相关联的区块链地址发送并且在当月28日在与房东115相关联的区块链地址接收的通知。在步骤680,如果没有接收到这样的通知,则过程601返回到步骤678。然而,如果在步骤680接收到通知,则过程601进行到步骤682。

[0104] 在步骤682,基于确定接收到的通知满足触发智能合约的各个条款的执行所需的条件,过程601进行到步骤684。然而,在步骤682,如果确定接收到的通知不满足触发智能合约的执行所需的条件,则过程601返回到步骤678。在步骤684,过程601创建并记录与智能合约的执行相关联的交易。例如,交易可以包括接收到的付款的信息、接收到付款的日期、租户110的标识和房东115的标识。交易可以被广播到区块链网络130a并且被记录在区块链220中(如图6A的过程600的步骤610-655所示)。如果交易被成功记录在区块链220中,则可以执行交易。例如,如果在28日收到付款,则可以生成电子收据并将其发送给租户110。然而,在当月的最后一天,数字输入密钥和租金均被分别释放给租户110和房东115。

[0105] 智能合约可以基于从不在区块链或链下资源上的实体接收的数据来执行。例如,智能合约可以被编程为在智能传感器或物联网传感器的温度读数低于10度时执行。智能合约无法从链下资源中提取数据。替代地,这些数据需要推送到智能合约。此外,由于智能合约是在网络的多个节点上复制的,因此即使数据的微小变化也可能会出现问题。例如,第一节点可以接收9.8度的温度读数,第二节点可以接收10度的温度读数。由于交易的验证基于节点之间的共识,因此即使接收到的数据发生微小变化也可能导致智能合约的条件被评估为不满足。可以利用第三方服务来检索链下资源信息并将其推送到区块链。这些第三方服务可能被称为预言机。预言机可以是软件应用程序,例如大数据应用程序,也可以是硬件,例如物联网或智能设备。例如,预言机服务可以预先评估接收到的温度读数,以确定读数是否低于10度,然后将此信息推送到智能合约。然而,使用预言机可能会在整个过程中引入另一个可能的故障点。预言机可能会遇到错误,推送不正确的信息,甚至可能会倒闭。

[0106] 由于区块链是不可变的,修改或更新驻留在区块链中的智能合约可能具有挑战性,因此比基于文本的合约更昂贵和/或更受限制。

[0107] 物联网(IOT)

[0108] 物联网网络可能包括收集数据并通过网关相互转发数据的设备和传感器。网关可以在设备和传感器的不同协议之间进行转换,并管理和处理数据。例如,物联网设备可以从其环境中收集信息,例如运动、手势、声音、语音、生物识别数据、温度、空气质量、湿度和光线。收集到的信息通过互联网发送以供进一步处理。通常,物联网设备使用低功耗网络、蓝牙、Wi-Fi或卫星连接到互联网或“云”。区块链可能能够检测到的一些物联网相关问题包括物联网设备制造阶段缺乏合规性。例如,区块链可以跟踪物联网设备是否经过充分测试。

[0109] 如上所述,来自链下资源(包括物联网设备)的信息可以通过称为预言机的第三方实体推送到智能合约。作为示例,智能冰箱可以监控冰箱中存储的物品(例如牛奶)的使用情况。冰箱内的各种传感器可以用于定期确定冰箱中储存的牛奶量。存储在区块链中的智能合约可能会表明,如果存储的牛奶重量低于10盎司,则会自动购买并交付一箱新牛奶。冰箱传感器可以定期将其读数发送给第三方服务或预言机。预言机可以评估传感器读数以确定是否满足购买新盒牛奶的条件。当确定存储的牛奶重量低于10盎司时,预言机可以向智

能合约推送信息,表明智能合约的执行条件已经满足。智能合约可以被执行,并且可以自动购买一盒新牛奶。智能合约的执行和新纸箱的购买都可以记录在区块链中。在一些情况下,条件可以是事件的发生,例如需要或预期的需要,或者便利因素,例如交付日、成本、促销或激励。

[0110] 与区块链集成到物联网相关的一些问题包括交易速度和计算复杂性。当具有数百或数千个连接设备的物联网网络同时运行和交易时,在区块链上执行交易的速度可能很重要。物联网设备通常是为连接而不是计算而设计的,因此可能不具备支持区块链共识算法(例如工作量证明)的处理能力。物联网设备也往往容易受到互联网黑客攻击和/或物理篡改。例如,物联网设备可能更容易受到DDoS和恶意软件攻击。黑客可能会瞄准特定网络并在短时间内开始向网络发送垃圾邮件。由于流量激增,带宽可能会很快过载,整个系统可能崩溃。

[0111] 供应链监控和物流

[0112] 产品的供应链可能包括参与产品创建及其最终销售给客户的实体和活动网络。例如,可以利用基于区块链的产品供应链记录来追踪零件和材料的来源并防止假冒零件进入供应链。将区块链集成到产品供应链中可以利用物联网设备和数据、预言机和智能合约。例如,RFID标签可以附着在产品上,以便物理跟踪产品并记录其在供应链中的位置。此外,智能合约可以用于记录产品供应链中涉及的实体之间的各种活动和交互。如上面参考图6A和6B所讨论的,可以数字地表示和电子地存储的任何数据或信息可以通过提交数据作为区块链交易的一部分来记录在区块链中。当交易包含在添加到区块链的经过验证的区块中时,交易及其关联数据将记录在区块链中。

[0113] 例如,许可的区块链可以用于记录和监控食品分配中涉及的实体和活动,例如水果或蔬菜。区块链可以供种子和农药供应商、农民、分销商、杂货店、客户和监管机构等实体访问。区块链可以记录诸如向农民销售农药和/或种子、水果的收获和包装、将其运送到分销商的仓库、到达各个商店以及消费者最终购买等活动。传感器和RFID设备可以用于通过供应链跟踪水果。例如,水果可以包装在贴有独特RFID设备标签的板条箱中。当贴有标签的板条箱被装载到卡车上从农场运送到经销商时,板条箱可能会被扫描,并且其运输记录可能会上传到区块链。当板条箱到达仓库时,它可能会被再次扫描,并且其到达仓库的记录可能会上传到区块链。此外,智能合约可以在整个供应链中执行。例如,当板条箱在仓库被扫描时,可以执行农民和仓库之间的智能合约,指示板条箱已成功从农民运送到仓库并被仓库接收。

[0114] 作为另一个示例,汽车的许可区块链可以存储与汽车制造中使用的组件相关的实体和活动的记录。区块链可供各种实体访问,例如汽车原始设备制造商、材料和部件的分销商和供应商、经销商、机械师、保险提供商等。在评估涉及保单持有人的汽车的事故时,第一用户110(在该示例中为保险提供者110)可以确定该事故可能是由汽车车轮中使用的有缺陷的部件引起的。保险提供商110可能希望基于记录在许可的区块链中的信息来追踪部件的出处。保险提供商110可以经由例如在第一客户端设备120上执行的区块链查询应用程序来查询区块链数据以获取与部件相关的信息。该查询可以包括与该部件相关联的识别信息。例如,部件可以用该部件或一组部件唯一的标识来标记。查询结果可能包括区块链中参与部件创建及其最终销售给汽车制造商的实体和活动的记录。

[0115] 区块链支持店内购买

[0116] 参考图8中所示的系统800、图6A中所示的过程600和图6B中所示的过程601来描述支持区块链的店内购买的示例。图8示出了支持区块链的店内购买系统800的示例。系统800包括经由网络840连接的移动设备805、商家系统810和服务器850。商家系统810可以经由本地无线网络连接到商店内的各种IoT设备,例如店内智能货架815和店内智能结账检测器830。

[0117] 商店可以包括一个或更多个智能货架,例如店内智能货架815。智能货架815可以包括RFID标签、RFID读取器和天线。一种或更多种产品可以存储在店内智能货架815上。每个产品可以包括RFID标签,例如附接到第一产品816a的第一产品标签820a和附接到第二产品816b的第二产品标签820b。店内智能货架815可以基于读取产品标签820a和820b,全天向商家系统810发送关于产品816a和816b的信息。商家系统810又可以更新当前在商店内的产品的库存。

[0118] 购物者可以使用移动设备805穿过商店。移动设备805上的数字购物清单可以包括购物者可能需要购买的物品的列表。例如,购物清单可以包括与第一产品816a匹配的项目。当购物者靠近店内智能货架815时,移动设备805可以通知购物者第一产品816a当前在店内智能货架815上可用。购物者可以从店内智能货架815移除第一产品816a并将其放入智能购物车835中。智能购物车835可以读取第一产品标签820a以及附加到可能已经放置在智能购物车835中的其他产品的产品标签。当购物者准备结账时,购物者可以推着购物车835走出商店。当购物者走出商店时,店内智能结账检测器830可以检测智能购物车835。智能购物车835可以与店内智能结账检测器830通信并传输关于智能购物车中的产品的信息。店内智能结账检测器830可以将关于产品(例如第一产品816a)的信息和支付信息从移动设备805发送到商家系统810。商家系统810可以从店内智能结账检测器830接收信息和支付信息,并且继续发起第一产品816a的购买。

[0119] 参考图6A所示的过程600的步骤605,移动设备805上的钱包应用程序可以生成用于将与第一产品816a的销售价格匹配的加密货币数量从购物者转移到商家的交易数据。钱包应用程序可以使用购物者的私钥生成用于交易的公钥。为了表明购物者是交易的发起者,还可以使用购物者的私钥为交易生成数字签名。交易数据可以从移动设备805发送到服务器850。

[0120] 服务器850可以从移动设备805接收交易数据。在步骤610,服务器850可以将交易广播到区块链网络130a。该交易可以由区块链网络130a的一个或更多个节点205接收。在步骤615,在接收到交易时,节点205可以选择例如基于与交易相关联的交易费用来验证交易。如果该交易没有被任何节点205选择进行验证,则该交易可以被放置在队列中并等待被节点205选择。

[0121] 在步骤620,选择该交易的每个节点205可以验证该交易。在步骤625,如果交易被节点205成功验证,则在步骤630,验证的交易被添加到由该节点205构造的区块。在步骤635,区块链网络130a可以等待区块被发布。在步骤640,如果区块尚未被发布,则过程600返回到步骤635并等待区块被发布。然而,在步骤640,如果已经发布了区块,则过程600进行到步骤645。

[0122] 在步骤645,将所发布的区块广播到区块链网络130a以进行验证。在步骤650,如果

该区块被大多数节点205验证,则在步骤655,将经验证的区块添加到区块链220。在步骤660,如果交易被添加到区块链220,则服务器850可以等待接收该交易的最小数量的区块链确认。在步骤665,如果尚未接收到交易的最小数量的确认,则过程可返回到步骤660。然而,如果在步骤665,已经接收到最小数量的确认,则过程进行到步骤670。在步骤670,可以执行交易并且可以将第一产品816a的销售价格从购物者转移到商家。

[0123] 当店内智能结账检测器830将关于产品的信息(例如第一产品816a)和支付信息从移动设备805发送到商家系统810时,可以根据图6B所示的流程601在购物者和商家之间创建并执行智能合约。例如,在步骤676,可以创建购物者和商家之间的智能合约,然后将其作为交易提交给区块链网络130a。例如,在步骤678,过程601可以等待接收等于第一产品816a的销售价格的加密货币数量从与购物者相关联的区块链地址发送并且在第一产品816a从智能购物车835中移除时在与商家相关联的区块链地址处接收到的通知。如果当购物者从智能购物车835取出第一产品816a时,第一产品816a的支付成功地从购物者转移到商家,则可以生成电子收据并将其发送给购物者。否则,可以警告商家系统815购物者正试图在不支付第一产品816a的情况下离开场所。

[0124] 区块链支持车内购物

[0125] 参考图9中所示的系统900、图6A中所示的过程600和图6B中所示的过程601来描述支持区块链的车内购买的示例。图9示出了用于支持区块链的车内购买的示例系统900。系统900包括支持IoT的智能车辆908。车辆908可以包括实现车辆系统910、车辆导航系统930、支付系统960和燃料管理系统935的一个或更多个计算设备。车辆908可以包括RFID标签,例如车辆识别标签912。系统900还可以包括各种商家系统,例如燃料商家系统915和收费站系统916。系统900还可以包括属于车辆908的驾驶员的移动设备905。

[0126] 当驾驶员进入车辆908时,支付信息可以从驾驶员的移动设备905加载到车辆支付系统910中,因此可以用于对其他设备的安全支付,以便完成车内购买,例如车内购买燃油、车内支付通行费等。智能车辆的驾驶员可以使用支持物联网的智能车辆908来支付停车费、快餐费。另外,支持IoT的智能车辆908还可以促进智能手机应用程序、音乐、有声读物以及其他商品和服务的车内购买。

[0127] 燃料管理系统935可以执行与燃料使用相关的各种功能并且与车辆系统916通信。例如,燃料管理系统935可以监测燃料使用情况,并且基于检测到燃料低于阈值,通知车辆系统910。车辆系统910可以与车辆导航系统930通信以确定附近的加油站。加油站的选择可以基于各种因素,例如附近加油站处的燃料的可用性、车辆的当前路线和位置、附近加油站可以提供的激励等。车辆系统910可以通知向驾驶员告知关于燃料站的选择,并且车辆908可以被重新安排路线到所选择的燃料站。到达选定的加油站后,驾驶员可以将车停在燃料泵处。燃料泵可以包括燃料泵系统965,其被配置成检测车辆的RFID标签,例如车辆识别标签912,以便获得车辆的标识。燃料泵系统965和支付系统960可以被配置成彼此通信。燃料支付系统960可以将支付信息发送到燃料泵系统965。当驾驶员完成加油后,驾驶员可以简单地开车离开。燃料泵系统965可以向燃料商家系统915发送关于车辆908的标识、购买的燃料量以及支付信息的信息。燃料商家系统915可以使用该信息来完成与驾驶员的购买燃料的交易。例如,燃料商家系统915可以与服务器950通信以根据图6A所示的过程600向驾驶员收取燃料费用。另外,燃料商家系统915可以与服务器950通信,以便在驾驶员和燃料商家之

间创建智能合同。可以根据图6B所示的流程601来创建和执行智能合约。

[0128] 增强现实(AR)、混合现实和基于区块链的电子商务

[0129] AR或混合现实设备,例如可穿戴智能眼镜、头戴式设备、全息设备或智能手机应用程序,将数字内容叠加在真实世界视图之上,从而增强用户对真实世界的体验。覆盖内容可以是基于3D扫描真实世界对象生成的3D模型。AR使用户能够在虚拟环境中体验网上购物。例如,使用AR浏览虚拟商店并查看虚拟商店中待售商品的3D模型。就像在真实世界中一样,客户可以处理和检查产品的各种物理细节。区块链智能合约可以用于提供电子商务平台,客户可以使用加密货币和数字钱包从在线商家购买商品。有关产品的信息,例如原产国、材料、成分、价格、描述、测量、条款和条件、实物产品的3D模型等,可以被哈希并记录在区块链中。这提供了虚拟商品和产品的所有权证明,并能够准确跟踪对此信息所做的任何更改。人工智能(AI)可以用于基于产品的2D图像生成产品的3D模型。智能合约可以用于在商家和客户之间进行交易。

[0130] 举例来说,顾客可以通过可穿戴AR设备(例如智能眼镜)浏览虚拟购物中心中的不同商店来购买服装。客户可以像在真实世界中一样检查衬衫的3D模型。此外,顾客可以使用顾客身体的3D模型虚拟试穿衬衫。如果顾客决定购买衬衫,则顾客可以与商店的商家发起交易。交易可以通过客户的数字钱包提交到区块链,以将钱(加密货币)从客户转移到商家。可以利用各种智能合约来实现电子商务过程的各个方面。例如,基于检测到衬衫的销售价格已从顾客成功转移到商家,可以执行智能合约以启动将衬衫从商家的仓库运送到顾客。如上文参考供应链监控和跟踪所描述的,RFID标签和其他物联网设备可以用于跟踪衬衫从商家仓库的运输到衬衫运送到顾客住所的过程。

[0131] 量子计算

[0132] 量子计算的担忧之一是它可能会增加破解密码算法的可能性,从而削弱区块链的整体安全性。这可以通过要求某些加密算法使用更大的密钥大小或切换到量子证明算法来解决。在某些情况下,如果担心块将来可能被解密,则可以使用动态变化的加密哈希。可以基于各种因素为特定区块或整个区块链动态选择不同的加密哈希,例如是否担心该区块将来会被解密,增加哈希的强度,使用更适合保护隐私的哈希。在某些情况下,可以为不同的区块选择不同的加密哈希。

[0133] 匿名和隐私

[0134] 如上所述,在验证区块链交易期间使用私钥/公钥对来建立用户真实性可以提供一定程度的隐私性,因为它不会泄露用户身份。然而,存储在区块链上的交易可能对公众可见。已经表明,用户身份可以从公开的交易信息中获得。

[0135] 区块链大小

[0136] 根据区块链中记录事件的频率,区块链的大小可能会快速增长。可能需要计算/存储容量(即更快的处理器、更大的存储组件)来支持区块链的扩展。在某些情况下,块可以在添加到链之前被压缩。在某些情况下,区块可能会被消除,例如,在区块链的开头,当它们变得陈旧或不相关时。例如,用有效模仿1000笔交易哈希的新区块“替换”前1000笔交易的方法对于管理区块链大小可能很有用。

[0137] 区块链不变性

[0138] 在某些情况下,可能需要删除区块链中的内容。例如,如果存在安全漏洞或内容不

再相关,则可能需要删除内容。区块链的不变性级别可能取决于区块链的类型。例如,在公共区块链中更改内容可能很困难,因为它可能会影响大量用户。根据一些技术,存储在私有区块链或由几个实体控制的公共区块链中的数据可以通过记录进行更改的标志(当前块)并将当前块(由标志引用)添加到区块链来更改。然后,添加的区块可以指示对前一个区块做出的改变。

[0139] 作为另一个示例,可能需要更改区块链才能解决断开的链接。例如,更改后的区块的哈希可能不再与存储在块+1中的哈希匹配。在某些情况下,可能需要更改区块链才能扭转非法交易的结果。在某些情况下,可能需要更改区块链以解决软件错误、错误交易或删除机密或法律要求删除的信息。如果区块链是不可变的,这些错误和信息可能会永久嵌入区块链中。此外,区块链可能需要进行更改以符合监管问题,例如欧盟即将出台的《通用数据保护条例》(GDPR)或有关消费者数据隐私和所有权的《加州消费者隐私法案》(CCPA)、要求记录的用户可识别个人财务数据是可编辑的《美国公平信用报告法》和美国证券交易委员会的“SP条例”。

[0140] 某些技术可能允许对区块链进行修改,以解决软件错误、法律和监管要求等,方法是允许指定机构在不破坏区块链的情况下编辑、重写或删除以前的区块。此类技术可以通过使用“变色龙”哈希函数的变体和安全私钥来实现区块链编辑。此编辑可能允许更新有问题的智能合约,以便将更改延续到区块链中的后续智能合约。使用这些技术,已更改的区块可能会使用即使受信任方也无法删除的“疤痕”或标记。

[0141] 根据一些技术,当对区块进行哈希时,任何机密信息(例如个人身份信息和IP地址)不包括在该区块中,因为它不是被哈希的数据值的一部分。但由于机密信息没有哈希,因此可能会被更改。根据某些技术,机密信息可能不会被放置或记录到区块链中。更确切的说,信息可能驻留在区块链外部的文件中。然而,该文件的哈希可能会记录在区块链中。例如,用户的机密信息可以在本地删除,而不影响区块链。

[0142] 作为另一个示例,假设在将区块添加到区块链之后不能改变区块链中的区块中包括的所有内容,则可以在将数据添加到区块链之前确定是否需要稍后删除该数据中的一些或全部。例如,机密信息(即,稍后要删除的数据)可以存储为区块和区块链外部的文件。为了创建区块的目的,可以将到包含机密信息的文件的链接和包含机密信息文件的文件的哈希添加到区块。HTTP链接就是链接的示例。在确认要添加到区块链的区块期间,网络节点能够访问机密信息并基于区块中文件的哈希来验证机密信息。由于文件的哈希是区块的一部分,因此包含机密信息的文件可能不容易被更改。然而,可以通过改变其中的数据并添加随机数来改变机密信息文件。这可能会寻求更改随机数,直到生成的哈希等于存储在区块链中的哈希。然而,这将很困难(可能几乎不可能),并且对修改后的机密信息文件的检查将揭示添加的随机数,这可能会让人怀疑信息自首次添加到区块链以来已被更改。

[0143] 包含机密信息的文件可以在哈希操作之前被加密(例如,通过非对称密钥加密功能)。当“删除”机密信息时,包含机密信息的文件可能会被删除或移除,导致存储在区块链中的链接无法检索该文件。文件的哈希和链接保留在区块链中,因此通过哈希函数进行的区块链接不会受到影响。然而,由于这一变化,作为该区块的一部分或不同特殊块的一部分的交易可以被添加到区块链中,以表明该链接不再有效并且机密信息文件不再是区块链的一部分。这可以有效地将机密信息排除在区块链之外,同时向区块链的用户提供机密信息,

并在机密信息从区块链中删除之前证明其真实性。这可能会带来缺点,因为对数据的访问意味着可以存储此类数据。因此,那些有权访问机密信息文件的人,虽然它是区块链的一部分,但可能已将该信息存储在在上述“删除”操作期间可能不再可达的另一个位置。

[0144] 51%攻击

[0145] “51%攻击”是指单个挖矿节点或一组挖矿节点控制了区块链网络50%以上的挖矿算力,也称为哈希率或哈希算力。哈希率是区块链网络上计算哈希的速率的度量。如上所述,哈希可以包括获取给定长度的输入字符串,并通过密码哈希函数运行它以便产生固定长度的输出。区块链网络的哈希率可以用1KH/s(千哈希每秒)(其是每秒1,000个哈希)、1MH/s(兆哈希每秒)(其是每秒1,000,000个哈希)、1TH/s(太哈希每秒)(其是每秒1,000,000,000,000个哈希)、或1PH/s(拍哈希每秒)(其是每秒1,000,000,000,000,000个哈希)表示。举个示例,区块链中利用工作量证明共识模型(PoW)的挖掘节点可以执行哈希,以便找到困难数学问题的解决方案。挖掘节点的哈希率可能取决于该节点可用的计算资源。成功解决数学问题的挖掘节点可能能够向区块链添加一个区块。因此,通过确保无效交易不会被包含在区块中,挖掘节点可以提高网络的可靠性。如果交易试图花费比当前拥有的更多的钱或进行双重支出,则交易可能会被视为无效。如果挖掘节点有意或无意地在区块中包含无效交易,则该区块将不会被网络验证。此外,接受无效块为有效块并继续在无效块之上添加块的节点最终也会浪费计算资源。因此,挖矿节点不会通过故意将无效交易添加到区块并接受无效区块作为有效区块来进行作弊。

[0146] 某个实体可能能够通过控制50%的网络哈希率来破坏网络。在51%攻击中,区块链节点可能会故意逆转或覆盖交易并进行双重支出。当节点生成有效的交易块时,它将该区块广播到网络以进行验证。在某些情况下,控制超过50%网络哈希率的节点可能会私下开采区块,而不会将其广播到网络。在这种情况下,网络的其余部分可能遵循区块链的公共版本,而控制节点可能遵循其私有版本的区块链。图7A示出了区块链700的欺诈版本和有效版本。顶部的有效区块链包括有效区块705、710a、715a和720。底部的欺诈区块链不会广播到网络,并且包括区块705、710b、715b和无效区块720。

[0147] 图7B示出了区块链的另一个欺诈版本和有效版本。区块链的有效版本包括节点740、745a、750a和755a。区块链的欺诈版本包括节点740、745b、750b、755b和775。然而,遵循最长链规则,网络可以选择并利用包括节点740、745b、750b、755b和775的私有或欺诈区块链。由于它是最长的链,之前的交易可能会根据这条链进行更新。作弊节点可能在区块链的公共或欺诈版本上包含花钱的交易,例如包含150BTC交易的区块750b,而不将这些交易包含在私有版本的区块链中。因此,在区块链的私有版本中,作弊节点可能会继续拥有所花费的150BTC。当作弊节点控制超过50%的网络哈希资源时,它可能能够广播其私有版本的区块链,并继续比网络其他节点更快地在私有区块链上创建区块,从而导致更长的区块链。由于区块链有两个版本,网络可能会选择最长的或欺诈性的私有区块链作为有效区块链。因此,网络的其余部分可能被迫使用更长的区块链。然后,区块链的公共或有效版本可以被丢弃或放弃,并且该区块链中不在私有或欺诈版本的区块链中的所有交易都可以被逆转。控制或作弊节点可能会继续拥有所花费的钱,因为支出交易不包含在区块链的欺诈版本中,因此作弊节点可能会在未来的交易中花费该钱。

[0148] 由于获得比整个网络其他部分加起来还要多的哈希算力所需的财务资源,成功的

51％攻击通常可能难以实现。然而,在哈希率较低的网络上实现51％攻击比在哈希率较高的网络上实现51％攻击的成本要低。此外,随着使用多个节点可以组合其计算资源的矿池,成功51％攻击的概率会增加,例如,当从同一个矿池执行挖掘时。

[0149] 计算设备

[0150] 图10示出了系统1000。系统1000可以包括经由网络1040通信的至少一个客户端设备1010(也称为“控制处理设备”)、至少一个数据库系统1020和/或至少一个服务器系统1030。应当理解,所示的网络连接是说明性的,并且可以使用在计算机之间建立通信链路的任何手段。假定诸如TCP/IP、以太网、FTP、HTTP等的各种网络协议以及诸如GSM、CDMA、WiFi和LTE的各种无线通信技术中的任一种的存在,并且本文描述的各种计算设备可以被配置成使用任何这些网络协议或技术进行通信。本文描述的任何设备和系统可以全部或部分地使用关于图10描述的一个或更多个计算系统来实现。

[0151] 客户端设备1010可以使用如本文所描述的一个或更多个客户端应用程序(未示出)来访问服务器应用程序和/或资源。客户端设备1010可以是移动设备,例如膝上型计算机、智能电话、移动电话或平板电脑,或者计算设备,例如台式计算机或服务器、可穿戴设备、嵌入式设备。替代性,客户端设备1010可以包括其他类型的设备,例如游戏控制台、相机/录像机、视频播放器(例如,结合DVD、蓝光、红色激光、光学和/或流技术)、智能电视、以及其他网络连接设备(如果适用)。

[0152] 数据库系统1020可以被配置成维护、存储、检索和更新服务器系统1030的信息。此外,数据库系统1020可以周期性地或根据请求向服务器系统1030提供信息。在这点上,数据库系统1020可以是能够跨节点集群存储、维护和更新大量数据的分布式数据库。数据库系统1020可以提供各种数据库,包括但不限于关系数据库、分层数据库、分布式数据库、内存数据库、平面文件数据库、XML数据库、NoSQL数据库、图形数据库和/或其组合。

[0153] 服务器系统1030可以配置有能够与如这里所描述的客户端应用程序和数据库系统1020接口的服务器应用程序(未示出)。在这点上,服务器系统1030可以是独立服务器、企业服务器、或者位于服务器场或云计算机环境中的服务器。根据一些示例,服务器系统1030可以是托管在能够支持多个虚拟服务器的硬件上的虚拟服务器。

[0154] 网络1040可以包括任何类型的网络。例如,网络1040可以包括局域网(LAN)、广域网(WAN)、无线电信网络和/或任何其他通信网络或其组合。应当理解,所示的网络连接是说明性的,并且可以使用在计算机之间建立通信链路的任何手段。假定诸如TCP/IP、以太网、FTP、HTTP等的各种网络协议以及诸如GSM、CDMA、WiFi和LTE的各种无线通信技术中的任一种的存在,并且本文描述的各种计算设备可以被配置成使用任何这些网络协议或技术进行通信。

[0155] 传输至系统1000中的各种计算设备以及从系统1000中的各种计算设备传输的数据可以包括安全且敏感的数据,例如机密文档、客户个人身份信息和账户数据。因此,可能期望使用安全网络协议和加密来保护此类数据的传输,和/或当存储在各种计算设备上时保护数据的完整性。例如,基于文件的集成方案或基于服务的集成方案可以用于在各种计算设备之间传输数据。可以使用各种网络通信协议来传输数据。安全数据传输协议和/或加密可以用在文件传输中以保护数据的完整性,例如文件传输协议(FTP)、安全文件传输协议(SFTP)和/或良好隐私(PGP)加密。在许多实施方式中,一个或更多个网络服务可以在各种

计算设备内实现。Web服务可以由授权的外部设备和用户访问以支持系统1000中的各种计算设备之间的数据的输入、提取和操纵。为支持个性化显示系统而构建的Web服务可以是跨域和/或跨平台的,并且可以为企业使用而构建。可以使用安全套接字层(SSL)或传输层安全(TLS)协议来传输数据以提供计算设备之间的安全连接。Web服务可以使用WS-Security标准来实现,从而使用XML加密提供安全的SOAP消息。专用硬件可以用于提供安全的网络服务。例如,安全网络设备可以包括内置功能,例如硬件加速的SSL和HTTPS、WS-Security和/或防火墙。这样的专用硬件可以被安装和配置在系统1000中的一个或更多个计算设备前面,使得任何外部设备可以直接与专用硬件通信。

[0156] 现在转向图11,描述了可以与一个或更多个计算系统一起使用的计算设备1105。计算设备1105可以包括用于控制计算设备1105的整体操作的处理器1103及其相关联的部件,包括RAM 1105、ROM 1107、输入/输出设备11011、通信接口1111和/或存储器1115。数据总线可以互连处理器1103、RAM 1106、ROM 1107、存储器1115、I/O设备1109和/或通信接口1111。在一些实施方式中,计算设备1105可以表示、并入和/或包括各种设备,例如台式计算机、计算机服务器、移动设备(例如膝上型计算机、平板计算机、智能电话)、任何其他类型的移动计算设备等、和/或任何其他类型的数据处理设备。

[0157] 输入/输出(I/O)设备1109可以包括计算设备1105的用户可以通过其提供输入麦克风、小键盘、触摸屏和/或触笔运动、手势,并且还可以包括用于提供音频输出的扬声器和用于提供文本、视听和/或图形输出的视频显示设备中的一个或更多个。软件可以存储在存储器1115内以向处理器1103提供指令,从而允许计算设备1105执行各种动作。例如,存储器1115可以存储计算设备1105使用的软件,例如操作系统1117、应用程序1119和/或相关联的内部数据库1121。存储器1115中的各种硬件存储器单元可以包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据之类的信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。存储器1115可以包括一个或更多个物理持久性存储器设备和/或一个或更多个非持久性存储器设备。存储器1115可以包括但不限于随机存取存储器(RAM)1106、只读存储器(ROM)1107、电可擦除可编程只读存储器(EEPROM)、闪存或其他存储器技术、光盘存储器、磁带盒、磁带、磁盘存储或其他磁存储设备、或可以用于存储期望信息并且可以由处理器1103访问的任何其他介质。

[0158] 通信接口1111可以包括用于使用本文描述的任何协议经由任何有线或无线网络进行通信的一个或更多个收发器、数字信号处理器和/或附加电路和软件。

[0159] 处理器1103可以包括可以是单核或多核处理器的单个中央处理单元(CPU)或者可以包括多个CPU。处理器1103和相关联的部件可以允许计算设备1100执行一系列计算机可读指令以执行本文描述的过程中的一些或全部。尽管图11中未示出,但是计算设备1105中的存储器1115或其他部件内的各种元件可以包括一个或更多个高速缓存,例如,由处理器1103使用的CPU高速缓存、由操作系统1117使用的页高速缓存、硬盘驱动器和/或用于缓存来自数据库1121的内容的数据库缓存。对于包括CPU高速缓存的实施方式,CPU高速缓存可以由一个或更多个处理器1103使用以减少存储器等待时间和访问时间。处理器1103可以从CPU高速缓存检索数据或向CPU高速缓存写入数据,而不是读取/写入存储器1115,这可以提高这些操作的速度。在一些示例中,可以创建数据库高速缓存,其中来自数据库1121的某些数据被高速缓存在与数据库分离的存储器中的单独的较小数据库中,例如RAM 1106中或单

独的计算设备上。例如,在多层应用程序中,应用程序服务器上的数据库缓存可以通过不需要通过网络与后端数据库服务器进行通信来减少数据检索和数据操作时间。这些类型的高速缓存和其他类型的高速缓存可以被包括在各种实施方式中,并且可以在本文描述的设备、系统和方法的某些实现中提供潜在的优点,例如在发送和接收数据时更快的响应时间以及对网络状况的更少依赖。

[0160] 尽管单独地描述了计算设备1105的各个部件,但是各个部件的功能可以由单个部件和/或通信的多个计算设备来组合和/或执行,而不脱离本发明。

[0161] 发明描述

[0162] 图12示出了联网系统1200,在该联网系统内可以实现根据本公开的一个实施方式的多方计算系统。注意,然而,本技术可以应用于许多不同的计算和技术环境,并且不限于图中所示的那些。联网系统1200包括可以经由网络1260彼此通信地耦合的服务提供商服务器1230、商家服务器1220、用户设备1210、以及计算机节点1270、1280和1290的网络。在一个实施方式中,网络1260可以被实现为单个网络或多个网络的组合。例如,在各种实施方式中,网络1260可以包括互联网和/或一个或更多个内联网、陆线网络、无线网络和/或其他适当类型的通信网络。在另一示例中,网络1260可以包括适于与诸如互联网之类的其他通信网络进行通信的无线电信网络(例如,蜂窝电话网络)。

[0163] 在一个实施方式中,用户1240可以利用用户设备1210通过网络1260与商家服务器1220和/或服务提供商服务器1230交互。用户1240可以是自然人或实体(例如,公司、合伙企业、组织等)。例如,用户1240可以使用用户设备110经由由商家服务器1220托管的网站或与商家服务器1220相关联的移动应用来与商家服务器120进行在线交易。用户1240还可以登录用户账户以访问账户服务或与服务提供商服务器1230进行电子交易(例如,账户转账或支付、加密货币交易等)。在各种实施方式中,用户设备1210可以使用被配置用于通过网络1260进行有线和/或无线通信的硬件和/或软件的任何适当的组合来实现。在各种实现方式中,用户设备1210可以包括无线蜂窝电话、可穿戴计算设备、PC、膝上型电脑等中的至少一种。

[0164] 在一个实施方式中,用户设备1210包括用户接口(UI)应用1212(例如,网络浏览器、移动支付应用等),用户1240可以利用用户接口应用112来通过网络1260与商家服务器1220和/或服务提供商服务器1230交互。在一个实现方式中,用户接口应用程序1212包括软件程序(例如,移动应用程序),软件程序为用户1240提供图形用户接口(GUI)以经由网络1260与服务提供商服务器1230和/或商家服务器1220进行接口连接和通信。在另一实现方式中,用户接口应用程序1212包括浏览器模块,浏览器模块提供网络接口以通过网络1260浏览可用的信息。例如,用户接口应用程序1212可以部分地实现为网络浏览器以通过网络1260查看可用的信息。

[0165] 用户设备1210可以包括用于促进与商家服务器1220和/或服务提供商服务器1230的支付交易的数字钱包应用1216。在一些实施方式中,数字钱包应用1216可以包括与一个或更多个资金来源(例如,信用卡、借记卡、银行账户等)相关联的数据,其可以用于与商家服务器1220和/或服务提供商服务器1230进行的一个或更多个支付交易中的支付。在一些实施方式中,数字钱包应用1216可以包括与加密货币账户(例如,与加密货币账户相关联的私钥等)相关联的数据,其可以用于与商家服务器1220、服务提供商服务器1230或任何其他

加密货币数字钱包执行加密货币交易。

[0166] 在一个实施方式中,用户设备1210可以包括至少一个标识符1214,至少一个标识符可以被实现为例如操作系统注册表项、与用户接口应用1212和/或认证应用1216相关联的cookie、与用户设备1210的硬件相关联的标识符(例如,媒体控制访问(MAC)地址)、或各种其他适当的标识符。在各种实施方式中,标识符1214可以与用户登录请求一起经由网络1260传递到服务提供商服务器1230,并且标识符1214可以由服务提供商服务器1230使用来将用户1240与由服务提供商服务器1230维护的特定用户账户(例如,和特定的简档)相关联。

[0167] 在各种实现方式中,用户1240能够将数据和信息输入到用户设备1210的输入部件(例如,键盘)中。例如,用户1240可以使用输入部件来与UI应用1212交互(例如,以从第三方服务器诸如商家服务器1220检索内容,以向服务提供商服务器1230提供与目标相关的输入等)。

[0168] 虽然图12中仅示出了一个用户设备1210,但是已经设想各自与服务提供商服务器1230的不同用户账户相关联的多个用户设备可以经由网络1260连接到用户设备1210、商家服务器1220和服务提供商服务器1230。

[0169] 在各种实施方式中,商家服务器1220可以由商业实体(或者在一些情况下,由商业实体的代表商业实体处理交易的合作伙伴)维护。商业实体的示例包括商家、资源信息提供商、公用事业提供商、房地产管理提供商、社交网络平台等,其提供用于查看、访问和/或购买的各种物品,并处理购买的支付。如所示出的,商家服务器1220可以包括用于识别可用项目的商家数据库1224,可用项目可以是能由用户设备1210获得以供用户查看和购买。

[0170] 在一个实施方式中,商家服务器1220可以包括市场应用程序或服务器1222,市场应用程序或服务器122可以被配置成通过网络1260向用户设备1210的用户接口应用程序1212提供信息(例如,可显示内容)。在一个实施方式中,市场应用程序1222可以包括托管商家的商家网站的网络服务器。例如,用户设备1210的用户1240可以借助网络1260通过用户接口应用程序1212与市场应用程序1222进行交互,以搜索和查看商家数据库1224中可以用于访问和/或购买的各种项目。在一个实施方式中,商家服务器1220可以包括至少一个商家标识符1226,至少一个商家标识符可以被包括作为可供购买的一个或更多个物品的一部分,使得例如特定物品与特定商家相关联。在一个实现方式中,商家标识符1226可以包括与商家相关的一个或更多个属性和/或参数,例如商业和银行信息。商家标识符1226可以包括与商家服务器1220相关的属性,例如标识信息(例如,序列号、位置地址、GPS坐标、网络标识号等)。

[0171] 虽然图12中仅示出了一个商家服务器1220,但是已经设想,各自与不同商家相关联的多个商家服务器可以经由网络1260连接到用户设备1210和服务提供商服务器1230。

[0172] 计算机节点1270、1280和1290的网络(例如,分片网络)中的每一个可以对应于区块链的分片链。区块链可以与特定的交易平台相关联,例如特定的加密货币、用于记录和管理智能合约的特定平台等。在区块链与特定的加密货币(例如,比特币、以太坊等)相关联的示例中,区块链可以与特定的交易平台相关联,区块链可以记录使用特定加密货币进行的所有交易。当使用特定加密货币的新交易被发起时,在与区块链关联的计算机节点验证新交易时(例如,使用工作量证明或权益证明机制等),新交易可以记录在区块链内。在另一个

示例中,区块链可以与用于执行智能合约的特定交易平台相关联。区块链可以记录通过特定交易平台进行的所有智能合约。当执行新的智能合约时,在与区块链关联的计算机节点验证智能合约之后,智能合约可以被记录在区块链中。这些记录可以包括代表相应区块(以及相应交易)的合法性的数字签名。一旦区块被插入到区块链中,该区块就不再可变。因此,随着更多交易被记录,区块链的规模将继续增长。

[0173] 如本文所讨论的,随着区块链大小的增长,将附加交易记录到区块链中的速度和效率性能可能会受到影响。提高与区块链相关的性能的一种解决方案是将区块链划分为单独的分片链,其中每个分片链对应于区块链的不同部分。在一些实施方式中,被配置成存储和管理区块链的计算机节点被分为各种组(例如,各种分片网络),以及用于单独存储和管理区块链的分片链。这样,每组计算机节点(例如,每个分片网络)可以负责存储和管理对应的分片链。由于每条分片链仅包含整个区块链的一小部分,因此操作分片链所需的处理资源大大少于操作整个区块链所需的处理资源,从而使操作区块链的整体速度和效率表现得到大幅提升。

[0174] 在一个示例中,区块链可能已分为三个独立的分片链。然而,在另一个示例中,分片链可以单独创建并一起形成新的区块链。在任一情况下,每个分片链可以由不同的计算机节点网络(例如,分片网络1270、分片网络1280和分片网络1290)管理。这样,每个分片网络中的计算机节点可以存储对应分片链的副本并且可以被配置成管理对应分片(例如,生成区块并将区块附加到对应分片中等)。例如,分片网络1270内的计算机节点可以存储区块链的第一分片链的各种副本,并且可以被配置成将交易记录到第一分片链。分片网络1280内的计算机节点可以存储区块链的第二分片链的各种副本,并且可以被配置成将交易记录到第二分片链。分片网络1290内的计算机节点可以存储区块链的第三分片链的各种副本,并且可以被配置成将交易记录到第三分片链。在一些实施方式中,每组计算机节点可以被配置成在将交易添加到对应的分片链之前使用验证机制(如本文所讨论的)来验证交易。在一些实施方式中,涉及在单独的分片中处理的钱包的交易(即,分片间交易)可以经由每个分片中的指定节点的协作来单独管理。

[0175] 在一个实施方式中,服务提供商服务器1230可以由交易处理实体或在线服务提供商维护,交易处理实体或在线服务提供商可以为用户设备1210的用户与一个或更多个商家或其他类型的收款人之间的电子交易提供处理。这样,服务提供商服务器1230可以包括服务应用程序1238,服务应用程序138可以适于通过网络1260与用户设备1210和/或商家服务器1220交互以促进对项目的搜索、选择、购买、支付、交易认证和/或由服务提供商服务器1230提供的其他服务。在一个示例中,服务提供商服务器1230可以由美国加利福尼亚州圣何塞的PayPal®,nc.和/或可以在不同位置提供多个销售点设备以促进商家与例如服务实体之间的交易路由的一个或更多个服务实体或相应中介提供。

[0176] 在一些实施方式中,服务应用1238可以包括支付处理应用(未示出),用于处理用户和商家之间或任何两个实体之间(例如,两个用户之间等)的电子交易的购买和/或支付。在一个实现方式中,支付处理应用通过验证、交付和结算来协助解决电子交易。这样,支付处理应用程序解决用户和商家之间的债务,其中账户可以直接和/或自动地借记和/或贷记货币资金。在一些实施方式中,为了处理法定支付交易,服务应用1238可以经由支付网络与与发行银行和/或收单银行相关联的各种服务器通信(例如,通过一系列命令)。在一些实施

方式中,为了处理加密货币支付交易,服务应用1238可以与与区块链相关联的各种计算机节点(例如,分片网络1270、1280或1290中的计算机节点)通信。

[0177] 服务提供商服务器1230还可以包括被配置成向用户提供内容(例如,网页内容)并与用户交互的接口服务器1234。例如,接口服务器1234可以包括被配置成响应于HTTP请求而提供网页内容的网页服务器。在另一示例中,接口服务器1234可以包括应用程序服务器,应用程序服务器被配置成经由一个或更多个协议(例如,REST API、SOAP等)与安装在用户设备1210上的对应应用程序(例如,服务提供商移动应用程序)交互。这样,接口服务器1234可以包括准备好提供给用户的预先生成的电子内容。例如,接口服务器1234可以存储登录页面,并被配置成向用户提供登录页面,用于登录用户的用户账户以访问服务提供商服务器1230提供的各种服务。接口服务器1234还可以包括与服务提供商服务器1230提供的不同服务(例如,电子交易服务等)相关联的其他电子页面。结果,用户(例如,用户1240)或与商家服务器1220相关联的商家等)可以通过生成指向服务提供商服务器1230的HTTP请求来访问与该用户相关联的用户账户并且访问由服务提供商服务器1230提供的各种服务(例如,通过用户的用户账户进行支付交易、数据访问交易等各种交易)。

[0178] 在一个实施方式中,服务提供商服务器1230可以被配置成在账户数据库1236中维护一个或更多个用户账户和商家账户(例如,数字钱包账户等),其中每个用户账户和商家账户可以与简档相关联并且可以包括与一个或更多个个人用户(例如,与用户设备1210等相关联的用户1240)和商家(例如,链接到数字钱包应用1216的资金源、与加密货币钱包账户相关联的钥匙等)相关联的账户信息。在一种实现方式中,用户可以具有凭证以向服务提供商服务器1230认证或验证身份。因此,服务提供商服务器可以将用户的凭证存储在与用户账户相关联的账户数据库1236的对应记录中。

[0179] 在各种实施方式中,服务提供商服务器1230包括实现如本文所讨论的多方计算系统的至少一部分的多方计算(MPC)模块1232。MPC模块1232可以配置各种分片网络中的计算机节点以使用本文公开的多方计算技术来执行验证过程,以验证通过一个或更多个分片链进行的电子交易。这样,MPC模块1232可以访问区块链的每个分片链以及分片网络1270、1280和1290。MPC模块1232可以确定表征分片链和/或分片网络内的计算机节点的各种度量。各种度量可以包括表示整个区块链的特征的链度量、表示分片链的特征的分片度量、表示分片链中记录的交易的特征的交易度量、以及表示分片网络内的计算机节点的特征的节点度量。基于各种度量,MPC模块1232可以为每个分片链确定多方计算方案。多方计算方案可以指定参与验证过程所需的计算机节点的阈值数量,以便验证相应分片链的交易。在一些实施方式中,多方计算方案还可以指定一个或更多个所需的(“必须具有的”)计算机节点用于参与验证过程,以便验证对应分片链的交易。MPC模块1232还可以在相应分片网络的计算机节点中实现多方计算方案,使得计算机节点可以使用多方计算方案来验证要记录在相应分片链中的交易。

[0180] 图13示出了与区块链1310相关联的分片环境1300。在该示例中,区块链1310可以与特定加密货币或特定交易平台相关联。区块链1310由计算机节点网络(区块链网络)1320管理。这样,区块链网络1320中的每个计算机节点可以存储区块链1310的副本,并且可以被配置成管理区块链1310(例如,执行交易的验证并在区块链中记录交易等)。如本文所讨论的,随着区块链1310的大小增长(例如,交易继续被记录到区块链1310),计算机节点1320的

区块链网络中的每个计算机节点执行交易的验证和记录所需的计算资源也增加。结果,操作区块链1310的速度和效率性能可能受到影响。

[0181] 在一些实施方式中,为了提高操作区块链1310的性能,区块链可以经历分片过程,其中区块链可以被划分为多个分片链1312、1314和1316。分片链1312、1314和1316中的每一个可以对应于区块链1310的不同部分,并且分片链1312、1314和116的组合构成区块链1310。可以以不同的方式执行区块链1310的划分。例如,区块链1310可以基于用户账户(例如,加密货币钱包账户)进行划分,使得与第一一个或更多个用户账户相关联的交易被记录在分片链1312中,与第二一个或更多个用户账户相关联的交易被记录在分片链1314中,并且与第三一个或更多个用户账户相关联的交易被记录在分片链1316中。在另一示例中,区块链1310可以基于进行交易的地理区域来划分,使得在第一一个或更多个区域中进行的交易被记录在分片链1312中,在第二一个或更多个区域中进行的交易被记录在分片链1314中,并且在第三一个或更多个区域中进行的交易被记录在分片链1316中。

[0182] 如本文所讨论的,在一些实施方式中,代替将现有区块链划分为多个分片链,可以单独地创建分片链1312、1314和1316,并且这些分片链1312、1314和1316一起形成新的区块链。因此,分片过程可以涉及新区块链的分片链1312、1314和1316的初始创建。

[0183] 在一些实施方式中,分片过程还可以将计算机节点1320的区块链网络划分为多个分片网络,其中每个分片网络负责存储和管理对应的分片链。在该示例中,区块链网络1320可以被划分为分片网络1322、分片网络1324和分片网络1326。替代地,当分片链1312、1314和1316被单独创建时,分片网络1322、1324和1326可以被独立地分配给各个分片链。分片网络1322可以被配置成存储和管理分片链1312,分片网络1324可以被配置成存储和管理分片链1314,并且分片网络1326可以被配置成存储和管理分片链1316。虽然分片链1310和区块链网络1320分别被划分为三个分片链和三个分片网络,但是应当注意的是,区块链1310和区块链网络1320可以根据需要被划分为任意数量的分片链和分片网络(例如,5、10、100等)。替代地,可以创建任意数量的分片链来形成新的区块链。在一些实施方式中,为了促进添加到分片链1312、1314和1316的交易的同步,可以生成中央链(也称为“信标链”)1350。中央链1350被配置成跟踪分片链1312、1314和1316发生的所有改变,使得可以经由中央链1350容易地访问整个区块链1310的可信版本。此外,中央链1350可以在验证要添加到分片链1312、1314和1316中的任何一个的新交易期间使用。例如,在验证分片链的新交易时,相应分片网络内的计算机节点可以基于中央链1350中记录的先前交易来验证新交易(例如,以确保新交易中使用的资金不是花费在另一个分片链的先前交易中,等等)。

[0184] 在一种实现方式中,中央链1350中的每个区块可以包括将中央链1350的区块链接到分片链1312、1314和1316中的对应区块的交联。由于在该示例中存在三个分片链,因此中央链1350中的每个区块可以包括三个交联,每个交联将中央链1350的区块链接到对应分片链的区块。这些交联使得分片链1312、1314和1316中的每一个与中央链1350之间能够同步,并且还能够在分片链1312、1314和1316之间进行通信(例如,对于涉及与不同分片链相关联的数字钱包的交易等)。关于中央链和分片链操作的更多细节可以在文章中找到:The Beacon Chain Ethereum 2.0(https://ethos.dev/beacon-chain/)。

[0185] 由于每个分片网络被配置成仅存储和管理大小小得多的分片链(在该示例中,每个分片链可以大约是区块链1310的大小的三分之一),因此在分片链1312、1314和1316中的

每一个中验证和记录新交易所需的计算机资源可能大大少于在区块链1310中验证和记录新交易所需的计算机资源。然而,虽然分片环境1300提高了操作区块链1310的速度和效率性能,但它也引入(或增加)了分片链1312、1314和1316的安全风险。例如,为了在分片之前对区块链1310发起51％攻击,恶意用户将需要在分片过程之前控制(例如,接管)区块链网络1320中一半以上的计算机节点。因此,如果区块链网络1320包括90个计算机节点,则恶意用户可能需要控制超过45个计算机节点。当区块链1310被划分为分片链1312、1314和1316后,由于区块链网络1320也被划分为三个分片网络,其中每个分片网络可以包括30个计算机节点,因此恶意用户可能只需要控制15个计算机节点来破坏每个分片链的完整性,这比控制超过45个计算机节点要容易得多。因此,根据本公开的各种实施方式,MPC模块1232可以被配置成在分片网络1322、1324和1316中的每一个中实现多方计算过程,以验证要记录在每个分片链1312、1314和1316中的交易,以提高分片链1312、1314和1316的安全性。

[0186] 图14示出了根据本公开的实施方式的MPC模块1232的框图。MPC模块1232包括MPC管理器1402、分片接口1404、分片分析模块1406、配置模块1408和验证模块1410。在一些实施方式中,MPC模块1232可以通信地耦合到中央链1350以及被配置成分别管理分片1312、1314和1316的分片网络1322、1324和1326。MPC模块1232可以与分片网络1322、1324和1326中的计算机节点协作,以分别配置和实现分片链1312、1314和1316的多方计算方案。在一些实施方式中,MPC模块1232可以被配置成通过管理中央链1350来促进区块链1310的同步。例如,MPC模块1232可以被配置成将被验证以添加到分片链1312、1314和1316中的任何一个的任何新交易添加到中央链1350。

[0187] 在一些实施方式中,分片分析模块1406可以经由分片接口1404访问分片网络1322、1324和1326中的每一个以分析计算机节点和存储在计算机节点中的分片链的副本。例如,分片分析模块1406可以访问存储在分片网络1322、1324和1306中的分片链1312、1314和1316的副本。分片分析模块1406可以分析分片链1312、1314和1316的副本以确定链度量。由于分片链1312、1314和1316的组合对应于整个区块链1310,因此分片分析模块1406可以基于对分片链1312、1314和1316的分析来确定表示区块链1310的各种特性的链度量。。链度量可以表示区块链1310的各种特性,例如区块链1310的大小(例如,记录在区块链1310中的交易或块的数量、交易的合计值或平均值、区块链1310的存储器大小)等等)、区块链1310的年龄(例如,记录在区块链1310中的交易的平均年龄等)、被添加到区块链1310(例如,添加到分片链1312、1314和1316中的任何一个)的速率或频率、以及与区块链1310相关联的其他信息。

[0188] 分片分析模块1406还可以为每个单独的分片链(例如,分片链1312)确定分片度量。分片度量可以表示分片链的各种特性,例如分片链的大小(例如,分片链1312中记录的交易或区块的数量)、分片链中区块的年龄(例如,平均年龄等)、区块被添加到分片链的速率或频率、以及与分片链相关的其他信息。

[0189] 分片分析模块1406还可以针对每个分片链(例如,分片链1312)确定表示在每个分片链中记录的交易的特性的交易度量。例如,交易度量可以表示分片链1312中记录的交易的数额或值(例如,平均值、最小值、最大值等)、分片链1312中记录的交易的数量、分片链1312中记录的交易的速率或频率、分片链1312中记录的交易的波动性、用于进行分片链1312中记录的交易的用户和/或用户设备的特性、进行分片链1312中记录的交易的地理区

域、以及与分片链1312中记录的交易相关联的其他信息。

[0190] 分片分析模块1406还可以为每个分片链(例如,分片链1312)确定表示被配置成存储和管理分片链1312的分片网络(例如,分片网络1322)内的计算机节点的特性的节点度量。例如,节点度量可以表示分片网络1322内的每个计算机节点的安全级别、分片网络1322内的每个计算机节点的硬件和/或软件配置、与分片网络1322内的计算机节点之间的连接相关联的网络属性、以及与分片网络1322内的计算机节点相关联的其他属性。

[0191] 分片分析模块1406可以确定分片链1312、1314和1316中的每一个的各种度量。基于为区块链1310和分片链1312、1314和1316确定的各种度量,配置模块1408可以为分片链1312、1314和1316中的每一个确定多方计算方案。针对特定分片链的多方计算方案可以指定该特定分片链对应的分片网络中的所有计算机节点(n个计算机节点)中参与节点的最小数量(t),用于验证要记录在分片链中的交易。通过指定最小数量的参与节点(例如分片网络中超过一半的节点)来验证分片链中记录的交易,可以提高分片链的安全性。

[0192] 在一些实施方式中,为了进一步提高分片的安全性同时减少所需节点的数量,配置模块1408还可以确定多方计算方案以指定用于参与验证要记录在分片链中的交易所需的("必须具备的")计算机节点。例如,配置模块1408可以针对每个特定分片链选择特定计算机节点作为用于参与通过特定分片链验证交易所需的("必须具备的")计算机节点。在一些实施方式中,配置模块1408可以选择被配置成存储和管理特定分片以及区块链的一个或更多个其他分片链的特定计算机节点。例如,对于分片链1312,配置模块可以选择作为分片网络1322的一部分以及分片网络1324和1326中的至少之一的计算机节点。选择被配置成管理多个分片链的计算机节点作为所需计算机节点的原因是,(例如由区块链的管理员)配置用于存储和管理多个分片链的计算机节点通常是经过强化,比其他节点更值得信赖且安全级别更高。此外,被配置成管理多个分片链的特定计算机节点可能具有其他计算机节点可能不具有的洞察力,这将提高交易验证过程的安全性。例如,特定计算机节点可以确定该交易是由已经链接到与一个或更多个其他分片链相关联的一个或更多个欺诈交易的用户帐户进行的。与分片链相关联的其他计算机节点不具有的该信息可以允许特定计算机节点确定不验证要记录在分片链中的交易。因此,选择特定的计算机节点作为参与验证过程所需的节点将进一步提高分片链的安全性。

[0193] 在一些实施方式中,配置模块1408可以基于各种度量来调整参与节点的最小数量(t)和所需计算机节点的数量。执行验证过程所需的计算机节点数量(t)与计算机节点集合中的计算机节点总数(n)之间的比率决定了分片链验证过程的安全性和弹性。对于给定的一组计算机节点(n),较大的t将提高验证过程的安全性,但会降低其弹性。相反,较小的t会提高验证过程的弹性,但会降低安全性。在一些实施方式中,配置模块1408可以确定超过组中一半的计算机节点的最小数量(t),使得分片网络中超过一半的计算机节点需要协作验证交易。因此,在采用这种多方计算方案实现的分片网络上,典型的51%攻击不会成功。

[0194] 在一些实施方式中,基于各种度量,配置模块308可以进一步增加(或减少)执行验证过程所需的最小数量(t)和/或增加(或减少)执行验证过程所需的节点数量。例如,当各种指标表明交易数额普遍较高(例如超过阈值)、分片网络中的计算机节点没有最新版本的软件或计算机节点上没有安装任何安全软件、分片网络中节点之间的连接缺乏安全性、交易频率高于阈值和/或其他因素时,配置模块1408可以增加分片链的多方计算方案中的最

小数量(t)和/或增加用于验证交易所需的计算机节点的数量。

[0195] 一旦已经为分片链确定了多方计算方案,MPC管理器1402就可以经由分片接口1404在与分片链相关联的计算机节点之间实现多方计算方案。例如,MPC管理器1402可以为分片链1312、1314和1316中的每一个生成(或以其他方式获得)一对对应的公钥和私钥。在一些实施方式中,MPC管理器1402可以使用非对称加密算法为分片链1312、1314和1316中的每一个生成一对对应的密钥,例如公钥和私钥。公钥和私钥对彼此对应,使用私钥加密的数据只能使用公钥解密,反之亦然。私钥可以由管理员或与区块链1310相关联的计算机服务器保密,并且不与任何人共享。由一组内的一个或更多个计算机节点参与的验证过程产生的数字签名的真实性(例如,使用与对应分片链相关联的私钥加密的数据)可以通过使用对应的公钥解密数字签名来验证,以恢复未加密形式的数据。

[0196] 在该示例中,MPC管理器1402可以生成分片链1312的私钥1422、分片链1314的私钥1424以及分片链1316的私钥1426。MPC管理器1402可以将私钥1422、1424和1426临时存储在数据存储器1460中。每个分片链的数字签名可以使用对应的私钥来生成(例如,通过使用对应的私钥加密一条数据)。因此,可以使用私钥1422来生成分片链1312的数字签名。类似地,可以使用私钥1424生成分片链1314的数字签名,并且可以使用私钥1426生成分片链1316的数字签名。然而,使用多方计算方案,而不是使用实际的私钥,可以使用不同的可共享值来生成模仿分片链的数字签名的输出,如下面将更详细地解释的。

[0197] 在一些实施方式中,验证过程的法定数和所需(必须具备的)节点的组合要求可以根据多方计算方案在算法级别中实现,使得与相关联的计算机节点组的任何子集分片链可以协作生成正确的数据片段(例如,使用分片链的私钥模拟加密的数据),只要该子集包括所需的计算机节点并且至少包括最小阈值数量(t)的计算机节点。换句话说,算法可以被设计和实现为要求在计算机节点的子集之间执行一组计算,使得任何人(例如,任何设备,并且不限于一个集中式权威设备)都可以确定法定数和基于计算集的输出,满足所需节点要求(等于或超过节点的最小阈值数量(t)的节点数量,包括已参与验证过程的所需节点)。这样,如果满足法定数要求的多个计算机节点(包括所需的节点)通过执行对应的计算(例如,对应的验证例程)参与验证过程,则可以生成正确的输出。另一方面,如果不满足法定数要求或者不包括所有需要的节点的节点数量通过执行对应的计算(例如,对应的认证例程)参与认证过程,则可能会生成不正确的输出(或无输出)。在一些实施方式中,正确的输出可以对应于与分片链相关联的数字签名(例如,使用分片链的私钥加密的数据片段)。虽然在计算(例如,验证过程)中可能不使用实际的私钥,但在验证过程期间由一组计算生成的输出可以模仿通过使用分片链的私钥加密一段数据而生成的数字签名。

[0198] 为了实现该算法,可以基于所需节点的数量生成多个秘密。例如,如果认证过程只需要一个所需的计算机节点,则可以生成两个秘密来生成数字签名。如果认证过程需要两个所需的计算机节点,则可以生成三个秘密来生成数字签名。秘密之一(例如,共享秘密)可以被分成多个部分以生成与该秘密相关联的份额。份额可以分布在用于验证过程的计算机节点之间,不包括所需的节点。剩余的秘密(未共享的秘密)可以分发到所需的节点。因此,每个所需节点可以拥有相应的非共享秘密,而每个剩余计算机节点可以拥有与共享秘密相关联的份额。秘密的一个份额可以包括可以与其他份额使用以生成共享秘密的一个或更多个值。

[0199] 在一些实施方式中,可以生成秘密,使得需要基于所有生成的秘密执行的计算(例如,一组顺序计算)以便产生正确的输出(例如,分片链的数字签名)。例如,如果生成两个秘密(由于需要一个节点要求),则包括基于两个秘密中的第一个的第一计算和基于两个秘密中的第二个的第二计算(其中第二计算可以进一步基于第一计算的输出)的顺序计算可能需要生成分片链的数字签名。在该示例中,第一秘密可以在除了所需节点之外的计算机节点之间划分和共享,并且第二秘密可以被提供给所需节点。此外,生成份额(包括秘密的部分)并在其余计算机节点之间分发,使得重新生成共享秘密(例如,第一个秘密)不需要所有份额,而是至少需要所需的最小阈值数量t的份额。

[0200] 图15示出了根据本公开的一些实施方式的秘密和与秘密相关联的份额可以如何在与分片链相关联的计算机节点的分片网络之间生成和分布。在该示例中,配置模块1408可以确定用于验证通过由分片网络1322管理的分片链1312进行的交易的多方计算方案,分片网络1322包括计算机节点1512、1514、1516、1518和1520。配置模块1408可以基于与分片链1312和分片网络1322中的计算机节点相关联的各种度量来确定需要计算机节点1322的分片网络中的五个计算机节点中的至少三个计算机节点执行验证过程以便验证要记录在分片链1312中的交易。此外,在该示例中,配置模块1408可以将计算机节点1512指定为分片链1312的验证过程所需的(必须具备的)节点,使得除了具有法定数(例如,验证过程中的三个参与节点)之外,计算机节点1512还必须是验证过程的一部分以验证要记录在分片链1312中的交易。在一些实施方式中,配置模块1408至少部分地基于计算机节点1512是分片网络1322以及其他分片网络1324和1326中的一个或更多个的一部分来将计算机节点1512指定为所需节点。

[0201] 如图所示,由于根据为分片链1312确定的多方计算方案为分片链1312指定了一个所需节点,因此MPC管理器1402可以基于与分片链1312(或分片网络1322)相关联的私钥1422生成两个秘密1504和1506。秘密1504和1506中的每一个可以包括字符串,该字符串可以是加密密钥或可以由分片网络1322的计算机节点使用以执行与验证过程相关联的计算的数据,这将在下面更详细地解释。在一些实施方式中,基于私钥1422生成的两个秘密1504和1506是不可逆的,这意味着私钥1422不能从秘密1504和1506重新生成。然而,秘密1504和1506可以用在由计算机节点组协作执行的一组计算(验证过程)中,以模仿使用私钥1422签署(例如,加密)一段数据的功能。该组计算可以包括基于秘密1506的第一计算(例如,使用秘密1506对数据块执行第一操作以生成第一输出)和基于秘密1504的第二计算(例如,基于秘密1504对第一输出执行第二操作以生成第二输出)。第二输出可以对应于分片网络的数字签名(第二输出与使用私钥1422加密该数据段相同)。一旦生成秘密1504和1506,MPC管理器1402就可以丢弃私钥1422(例如,永久地去除私钥1422)。

[0202] MPC管理器1402然后可以将秘密1504分发到所需的节点(例如,计算机节点1512)。响应于从MPC管理器1402接收秘密1504,计算机节点1512可以将秘密1504安全地存储在计算机节点1512上(例如,诸如硬盘驱动器、闪存驱动器等的持久数据存储装置)。

[0203] 在一些实施方式中,MPC管理器1402可以生成与秘密1506相关联的份额。每个份额可以包括秘密1506的一个或更多个部分,或者可以与其他份额一起使用以重新生成秘密1506的信息。这些份额可以分布在其余计算机节点1514、1516、1518和1520之间。例如,MPC管理器1402可以为计算机节点1514、1516、1518和1520生成份额1522、1524、1526和1528。

MPC管理器1402可以将份额1522、1524、1526和1528分别分发到计算机节点1514、1516、1518和1520。在一些实施方式中,MPC管理器1402通过将秘密1506划分为多个部分来生成份额,其中每一份额包括秘密1506的一个或更多个部分。例如,MPC管理器1402可以生成份额1522、1524、1526和1528,其中每个份额包括秘密1506的多个部分(但不是所有部分),使得每个计算机节点不拥有秘密1506的全部。此外,不同的份额可以包括多个部分的不同集合,使得计算机节点1514、1516、1518和1520的一部分(但不是所有计算机节点)需要具有秘密1506的所有部分。在一些实施方式中,可以基于Shamir的秘密共享技术来生成份额,其中秘密1506可以被变换成多项式并且每个份额包括多项式的不同数据点(具有一组坐标)。在秘密1506被变换成多项式的一些实施方式中,秘密1504可以被实现为多项式的偏移。

[0204] 当接收到对应的份额1522、1524、1526和1528时,计算机节点1514、1516、1518和1520可以存储对应的份额1522、1524、1526和1528。在分发秘密1504和秘密1506的份额1522、1524、1526和1528之后,计算机节点1322的分片网络准备好执行验证过程以根据多方计算方案来验证交易。在一些实施方式中,在分发秘密1504和份额1522、1524、1526和1528之后,MPC管理器1402还可以从其存储器中丢弃(删除或以其他方式销毁)秘密1504和份额1522、1524、1526和1528的副本。

[0205] 图16示出了根据本公开的一些实施方式的由计算机节点1322的分片网络执行以验证要记录在分片链1312中的交易的示例验证过程。在一些实施方式中,用户1240可以使用用户设备110来发起与服务提供商服务器1230的交易。交易可以是加密货币交易(例如,将一定量的加密货币从一个钱包转移到另一钱包等)、智能合约交易或任何类型的交易。在一些实施方式中,用户1240可以将交易请求发送到服务提供商服务器1230。交易请求可以包括与用户账户相关联的凭证(例如,用户名、密码等)。在验证凭证后,服务提供商服务器1230可以确定用于记录交易的特定分片链。例如,服务提供商服务器1230可以基于用于进行交易的用户账户的身份、进行交易的位置和/或其他因素来确定特定分片链。在该示例中,服务提供商服务器1230可以确定分片链1312适合于记录交易。因此,服务提供商服务器1230可以将与交易相关联的交易数据1602传输到计算机节点1322的网络中的一个或更多个计算机节点,包括计算机节点1512、1514、1516、1518和1520。交易数据1602可以由服务提供商服务器1230直接发送到计算机节点1512、1514、1516、1518和1520中的每一个。替代地,一旦分片网络1322内的任何一个计算机节点接收到交易数据1602,该计算机节点就可以被配置成自动将交易数据1602广播到分片网络1322中的其他计算机节点。

[0206] 在一些实施方式中,验证过程包括有序的连续计算集,其中该计算集必须基于秘密和/或秘密的部分按顺序执行。因此,可以对分发到计算机节点的秘密和/或秘密的部分进行标记(例如,基于顺序)。当计算机节点1512、1514、1516、1518和1520接收交易(或与交易相关联的交易数据)时,计算机节点1512、1514、1516、1518和1520中的每一个可以验证交易。例如,每个计算机节点可以遍历其分片链1312的副本,以基于分片链1312中记录的其他交易来确定该交易是否合法。当确定交易被验证时,每个计算机节点可以基于存储在计算机节点上的秘密1506的第一部分来确定该计算机节点是否可以执行初始计算(例如,作为验证过程的一部分的初始验证例程)。如果计算机节点确定其可以基于其拥有的秘密1506的第一部分(第一部分包括在计算机节点上存储的对应份额中)来执行初始计算,则计算机节点可以基于交易数据和其相应份额内的秘密1506的第一部分(标记为第一部分)来执行

初始计算。初始计算的执行可以基于秘密1506的第一部分操纵交易数据1602并且生成第一输出。计算机节点可以将第一输出广播到其他计算机节点。每个计算机节点可以基于秘密1506的第二部分来确定其是否能够执行第二计算(例如,作为验证过程的一部分的第二验证例程)。如果计算机节点确定其可以基于其所拥有的秘密1560的第二部分(包括在计算机节点上存储的对应份额中的第二部分)来执行第二计算,则其可以执行第二计算。第二计算可以涉及使用秘密1506的第二部分来操纵第一输出。计算机节点1514、1516、1518和1520可以使用它们拥有的秘密1506的部分继续执行计算作为验证过程的一部分,直到涉及秘密1506的所有计算完成。最后的计算可以生成输出1604。当涉及秘密1506的所有计算完成时,执行最后计算的计算机节点可以将输出1604传输到所需的计算机节点1512。

[0207] 当接收到输出1604时,计算机节点1512可以基于存储在计算机节点1512上的秘密1504来执行与验证过程相对应的计算。在一些实施方式中,由计算机节点1512执行的计算进一步基于秘密1504操纵输出1604以生成输出1606,其是验证过程的最终输出。在一些实施方式中,最终输出1606可以对应于与分片链1312相关联的数字签名。计算机节点1512可以将输出1606广播到分片网络1312中的其他计算机节点,使得分片网络1312中的每个计算机节点可以将交易连同输出1606(例如,分片链1312的数字签名)一起记录到它们的分片链1312的副本。由于数字签名也被包括在分片链1312中,因此任何设备(例如,分片网络1322中的任何计算机节点或其他计算机节点)可以通过使用与分片链相关联的公钥解密输出1606来验证数字签名1312并验证解密的签名对应于存储在分片链1312中的交易数据。如果来自分片网络1322的计算机节点的最小阈值数量(例如,三个)多于所需的计算机节点1512参与验证过程,则输出1606应对应于分片链1312的数字签名(例如,使用分片链1312的公钥解密输出1606应该产生与交易数据1602匹配的值)。另一方面,如果参与验证过程的计算机节点的最小阈值数量(例如,两个)或者所需的计算机节点1512未能参与验证过程,则输出1606将不对应于分片链1312(例如,使用分片链1312的公钥解密输出1606将产生与交易数据1602不匹配的值)。

[0208] 分片网络1322中的每个计算机节点可以相应地验证输出1606,并且仅当输出1606被验证时,才可以将交易数据1602和输出1606添加到其分片链1312的副本(将交易数据1602和输出1606添加到区块并将该区块附加到分片链1312)。如果输出1606未被验证,则计算机节点应当丢弃该交易。

[0209] 在一些实施方式中,在分片网络(例如,分片网络1322、1324、1326等)内实现多方计算方案之后,MPC管理器1402可以继续监视分片网络(例如,分片网络1322、1324、1326等)和对应的分片链(例如,分片链1312、1314、1316等)的不同特性。例如,分片分析模块1406可以继续监视(例如,周期性地等)被添加到每个分片链的交易的不同属性、被添加到每个分片链的新交易的波动性,每个分片网络中的计算机节点的状况(例如,安全状况等)、每个分片网络中的计算机节点之间的网络状况以及其他属性。基于分片网络的更新的特性,配置模块1408可以确定是否修改一个或更多个分片链的一种或更多种多方计算方案。

[0210] 例如,如果确定与添加到分片链的新交易(例如,在阈值时间之后添加的交易)相关联的量显著大于(例如,超过阈值)与分片链中旧交易(例如在阈值时间之前添加的交易)相关联的量,或者最近一段时间内添加到分片链上的交易数量明显大于过去相同时间段内添加到分片链上的交易数量,则配置模块1408可以确定针对分片链增加参与验证交易所需

的计算机节点的最小阈值数量、增加验证交易所需的计算机节点的数量、或两者。

[0211] 又例如,如果确定现有的分片链多方计算方案中被指定为所需计算机节点的计算机节点存在安全问题(例如软件不是最新的、最近对计算机节点的攻击等),配置模块1408可以针对分片链增加验证交易所需的节点的数量和/或指定另一计算机节点作为所需的节点。

[0212] 在又一示例中,如果确定分片链中新交易的波动性显著大于旧交易,则配置模块1408还可以针对分片链增加参与验证交易所需的计算机节点的最小阈值数量、增加验证交易所需的计算机节点数量、或两者。

[0213] 在一些实施方式中,基于分片链(例如,分片链1312)的更新的特性,配置模块1408还可以修改一个或更多个其他分片链(例如,分片链1314、1316等)的一个或更多个多方计算方案。因为如果一条分片链的安全风险增加,可能也会影响其他分片链的安全风险。例如,如果在一个分片网络(例如,分片网络1322)上检测到数量增加的攻击,则配置模块1408可以预见类似的攻击趋势也可能发生在其他分片网络中。因此,配置模块1408可以通过基于在一个分片链上检测到的事件来修改多个分片链(例如,分片链1312、1314和1316)的多方计算方案来增加安全性。

[0214] 一旦多方计算方案被修改,MPC管理器1402就可以在分片网络内实现修改后的多方计算方案。在一些实施方式中,为了实现修改的多方计算方案,MPC管理器1402可以生成新的秘密和新的秘密份额,并且可以使用此处描述的技术在分片网络内的计算机节点之间分发新的秘密和新的秘密份额。

[0215] 图17示出了根据本公开的各种实施方式的用于确定和实现多方计算方案的过程1700。在一些实施方式中,过程1700的至少一部分可以由MPC模块1232执行。注意,虽然在一些实施方式中,MPC模块1232可以被实现为用于实现跨多个分片的多方计算方案的集中式模块,但在其他实施方式中,可以实现单独的MPC模块1232,用于单独地为每个分片实现多方计算方案。过程1700可以通过访问(在步骤1705)对应于区块链的多个分片链和分片网络来开始。例如,分片分析模块1406可以经由分片接口访问分片网络1322、1324和1326内的计算机节点。分片分析模块1406可以获得存储在计算机节点内的分片链的副本。例如,分片分析模块1406可以从分片网络1322中的计算机节点访问分片链1312的副本。类似地,分片分析模块1406可以从分片网络1324中的计算机节点访问分片链1314的副本,并且从分片网络1326中的计算机节点访问分片链1316的副本。

[0216] 过程1700然后分析(在步骤1710)每个分片链中记录的交易的交易特性。例如,分片分析模块1406可以分析记录在分片链1312、1314和1316中的交易。在一些实施方式中,分片分析模块1406可以确定与分片链中记录的交易相关联的数额、交易的平均数额、交易的波动性、交易的总数以及其他交易属性。

[0217] 过程1700然后分析(在步骤1715)每个分片链中的节点的节点特性。例如,分片分析模块1406可以分析分片网络1322、1324和1326中的每一个内的计算机节点。分片分析模块1406可以确定每个计算机节点的硬件和/或软件配置(例如,计算机节点上是否安装了任何安全硬件或软件等)、每个计算机节点的网络属性、以及分片网络中每个计算机节点的其他计算机属性。

[0218] 过程1700然后分析(在步骤1720)与每个分片链相关联的链特性。例如,分片分析

模块1406可以分析存储在分片网络的计算机节点中的分片链的副本。分片分析模块1406可以确定分片链的大小、分片链中的区块的年龄、区块被添加到分片链的速率或频率、以及分片链所属的区块链的特性。

[0219] 过程1700基于分片链的特性为每个分片链确定(在步骤1725)多方计算方案。例如,配置模块1408可以确定分片链1312、1314和1316中的每一个的多方计算方案。每个多方计算方案可以指定参与计算机节点的最小阈值数量以及用于验证要记录在相应分片链中的交易所需的一个或更多个计算机节点。

[0220] 过程1700然后在每个分片网络内实现(在步骤1730)对应的多方计算方案。例如,MPC管理器1402可以与分片网络1322、1324和1326中的每一个中的计算机节点交互,以根据对应的多方计算方案来配置计算机节点。在一些实施方式中,MPC管理器1402可以基于每个分片链的私钥生成秘密和秘密的份额,并且可以在分片网络中的计算机节点之间分发秘密和秘密的份额。一旦多方计算方案被实现,分片网络1322、1324和1326就可以开始在对应的多方计算方案下验证交易。

[0221] 图18示出了根据本公开的各种实施方式的用于修改多方计算方案的过程1800。在一些实施方式中,过程1800的至少一部分可以由MPC模块1232执行。过程1800可以通过监视(在步骤1805)每个分片链和分片网络的特性开始。例如,分片分析模块1406可以监视被添加到分片链1312、1314和1316的交易的交易特性、分片网络1322、1324和1326中的每一个中的计算机节点的节点特性、以及分片链1312、1314和1316的链特性。

[0222] 过程1800然后确定(在步骤1810)条件是否存在。例如,MPC管理器1402可以确定交易特性、节点特性和链特性是否存在变化。当变化大于阈值时,MPC管理器1402可以确定条件存在。如果该条件不存在,则过程1800返回到步骤1805并继续监视分片链和分片网络中的每一个的特性。然而,如果存在这样的条件,则过程1800分析(在步骤1815)该条件并基于该条件修改(在步骤1820)一个或更多个分片链的多方计算方案。例如,配置模块1408可以分析分片链的特性(以及特性的变化),并且可以确定用于分片链的修改的多方计算方案。修改可以包括调整(例如,增加或减少)参与验证过程所需的计算机节点的最小阈值数量、改变参与验证过程所需的计算机节点的数量、和/或分配不同的所需计算机节点来参与验证过程。在一些实施方式中,基于分片链中检测到的条件,MPC模块1232可以仅修改该分片链的多方计算方案。在一些实施方式中,MPC模块1232还可以基于检测到的分片链的条件来修改用于一个或更多个其他分片链的多方计算方案。

[0223] 过程1800然后在一个或更多个分片链中实现(在步骤1825)修改后的多方计算方案。在一些实施方式中,为了实现修改的多方计算方案,MPC管理器1402可以生成新的秘密和新的秘密份额并将新的秘密和新的秘密份额分发到分片网络中的计算机节点。

[0224] 图19示出了根据本公开的各种实施方式的用于执行验证过程的过程1900。在一些实施方式中,过程1900的至少一部分可以由与分片网络相关联的计算机节点执行。过程1900可以通过接收(在步骤1905)与分片链相关联的交易开始。例如,当服务提供商服务器1230接收到交易请求时,服务提供商服务器1230可以生成与交易请求相关联的交易数据,并且可以将交易数据发送到与分片链相关联的计算机节点。当接收到交易数据时,与分片链相关联的计算机节点可以将交易数据广播到与分片链相关联的分片网络中的其他计算机节点,使得分片网络中的每个计算机节点接收交易数据。

[0225] 然后,过程1900通过与一个或更多个其他计算机节点协作来生成数字签名来执行(在步骤1910)该交易的验证过程。例如,分片网络中的计算机节点可以相互协作,使用其拥有的秘密份额来执行一系列计算。如果使用其秘密份额参与验证过程的计算机节点满足多方计算方案中指定的标准(例如,满足最小阈值数量要求并且包括所需的计算机节点的计算机节点),将产生基于交易数据的正确数字签名。另一方面,如果参与验证过程的计算机节点不满足多方计算方案中指定的标准,则会产生不正确的数字签名(或无数字签名)。

[0226] 接下来,过程1900确定(在步骤1915)签名是否有效,并且如果签名有效则在分片链中记录(在步骤1920)该交易。另一方面,如果签名无效,则过程1900丢弃(在步骤1925)该交易。例如,分片网络中的每个计算机节点可以确定来自验证过程的输出签名是否是有效签名。计算机节点可以通过使用与分片链相关联的公钥解密签名并确定解密的签名是否对应于交易数据来验证签名。如果签名有效,计算机节点可以将交易添加到区块中,并将该区块附加到分片链上。另一方面,如果签名无效,则计算机节点可以丢弃该交易。

[0227] 图20是适合于实现本公开的一个或更多个实施方式的计算机系统2000的框图,包括服务提供商服务器1230、商家服务器1220、用户设备1210、以及计算机节点1512、1514、1516、1518和1520。在各种实现方式中,用户设备1210和其他用户设备可以包括适于无线通信的移动蜂窝电话、个人计算机(PC)、膝上型计算机、可穿戴计算设备等,并且服务提供商服务器1230、商家服务器1220以及计算机节点1512、1514、1516、1518和1520中的每一个可以包括网络计算设备,诸如服务器。因此,应当理解,设备/服务器1210、1220、1230、1512、1514、1516、1518和1520可以以如下方式实现为计算机系统2000。

[0228] 计算机系统2000包括总线2012或用于在计算机系统2000的各个部件之间传送信息数据、信号和信息的其他通信机制。这些部件包括输入/输出(I/O)部件2004,输入/输出部件处理用户(即,发送方、接收方、服务提供商)动作,诸如从小键盘/键盘选择按键、选择一个或更多个按钮或链接等,并向总线2012发送对应的信号。I/O部件2004还可以包括输出部件,诸如显示器2002和光标控件2008(诸如键盘、小键盘、鼠标等)。显示器2002可以被配置成呈现用于登录用户账户的登录页面或用于从商家购买物品的结账页面。还可以包括可选的音频输入/输出部件2006以允许用户通过转换音频信号来使用语音来输入信息。音频I/O部件2006可以允许用户听到音频。收发器或网络接口2020经由网络2022诸如图12的网络1260在计算机系统2000和其他设备诸如另一用户设备、商家服务器或服务提供商服务器之间传输和接收信号。在一个实施方式中,传输是无线的,但其他传输介质和方法也可以是合适的。处理器2014可以是微控制器、数字信号处理器(DSP)或其他处理部件,处理这些各种信号,诸如用于在计算机系统2000上显示或经由通信链路2024传输到其他设备。处理器2014还可以控制信息诸如cookie或IP地址到其他设备的传输。

[0229] 计算机系统2000的部件还包括系统存储器部件2010(例如RAM)、静态存储装置部件2016(例如ROM)和/或磁盘驱动器2018(例如固态驱动器、硬盘驱动器)。计算机系统2000通过处理器2014和其他部件通过执行系统存储器部件2010中包含的一个或更多个指令序列来执行特定操作。例如,处理器2014可以根据过程1700、1800和1900执行本文描述的交易验证功能。

[0230] 逻辑可以被编码在计算机可读介质中,计算机可读介质可以指参与向处理器2014提供指令以供执行的任何介质。这样的介质可以采取多种形式,包括但不限于非易失性介

质、易失性介质和传输介质。在各种实现方式中,非易失性介质包括光盘或磁盘,易失性介质包括动态存储器诸如系统存储器部件2010,并且传输介质包括同轴电缆、铜线和光纤,包括构成总线2012的线。在一个实施方式中,逻辑被编码在非暂态计算机可读介质中。在一个示例中,传输介质可以采用声波或光波的形式,诸如在无线电波、光和红外数据通信期间生成的那些。

[0231] 计算机可读介质的一些常见形式包括例如软盘、柔性盘、硬盘、磁带、任何其他磁性介质、CD-ROM、任何其他光学介质、打孔卡、纸带、具有孔图案的任何其他物理介质、RAM、PROM、EPROM、FLASH-EPROM、任何其他存储器芯片或盒、或计算机适于读取的任何其他介质。

[0232] 在本公开的各种实施方式中,用于实践本公开的指令序列的执行可以由计算机系统2000来执行。在本公开的各种其他实施方式中,通过通信链路2024耦合到网络(诸如,LAN、WLAN、PTSN和/或各种其他有线或无线网络,包括电信、移动、以及蜂窝电话网络)的多个计算机系统2000可以执行指令序列以彼此协调地实践本公开。

[0233] 在适用的情况下,本公开提供的各种实施方式可以使用硬件、软件或者硬件和软件的组合来实现。此外,在适用的情况下,在不脱离本公开的精神的情况下,本文阐述的各种硬件部件和/或软件部件可以组合成包括软件、硬件和/或两者的复合部件。在适用的情况下,在不脱离本公开的精神的情况下,本文阐述的各种硬件部件和/或软件部件可以被分成包括软件、硬件或两者的子部件。另外,在适用的情况下,设想软件部件可以被实现为硬件部件,并且反之亦然。

[0234] 根据本公开的软件诸如程序代码和/或数据可以存储在一个或更多个计算机可读介质上。还设想本文所标识的软件可以使用联网的一个或更多个通用或专用计算机和/或计算机系统和/或以其他方式实现。在适用的情况下,本文描述的各个步骤的顺序可以改变、组合成复合步骤和/或分成子步骤以提供本文描述的特征。

[0235] 本文描述的各种特征和步骤可以被实现为系统,该系统包括存储本文描述的各种信息的一个或更多个存储器以及耦合到该一个或更多个存储器和网络的一个或更多个处理器,其中一个或更多个处理器可操作以执行本文描述的、作为包括多个机器可读指令的非瞬态机器可读介质的步骤,非瞬态机器可读介质在由一个或更多个处理器执行时,适于使一个或更多个处理器执行包括本文描述的步骤的方法,以及由一个或更多个设备诸如硬件处理器、用户设备、服务器和本文描述的其他设备执行的方法。

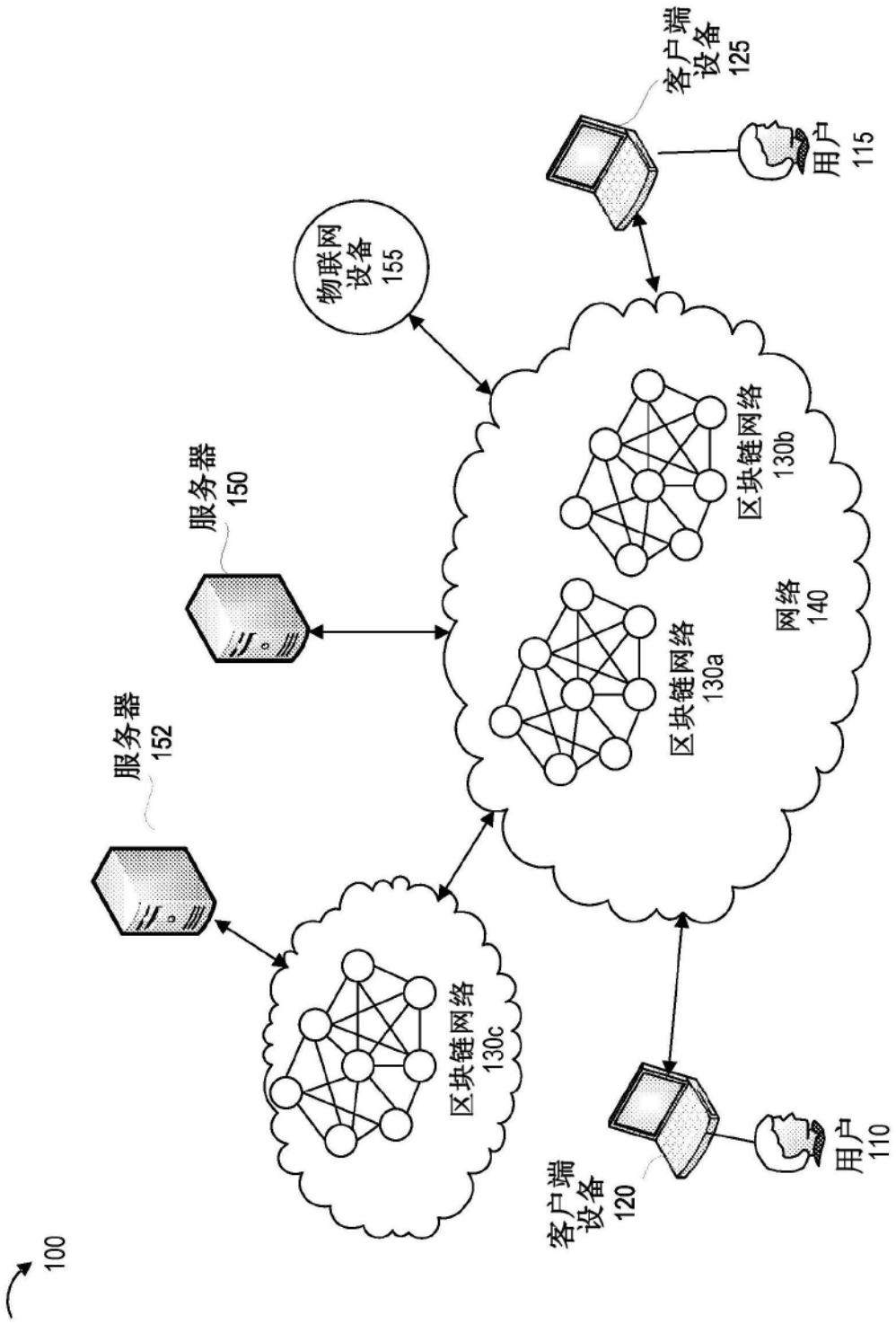

100
客户端设备 125
用户 115
物联网设备 155
服务器 150
服务器 152
区块链网络 130b
区块链网络 130a
网络 140
区块链网络 130c
客户端设备 120
用户 110

图1

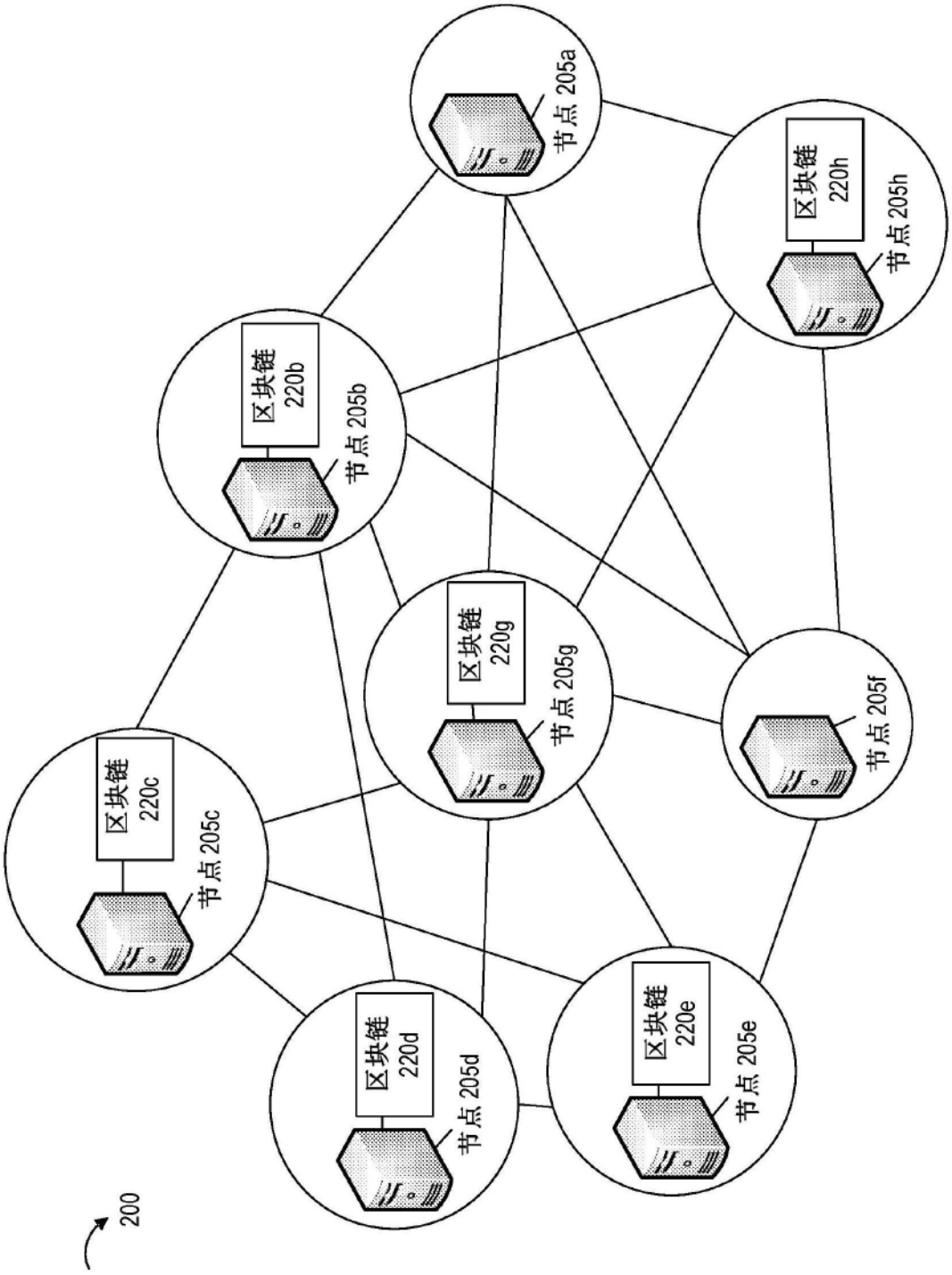

节点 205a
区块链 220h
节点 205h
区块链 220b
节点 205b
区块链 220g
节点 205g
节点 205f
区块链 220c
节点 205c
区块链 220d
节点 205d
区块链 220e
节点 205e
200

图2

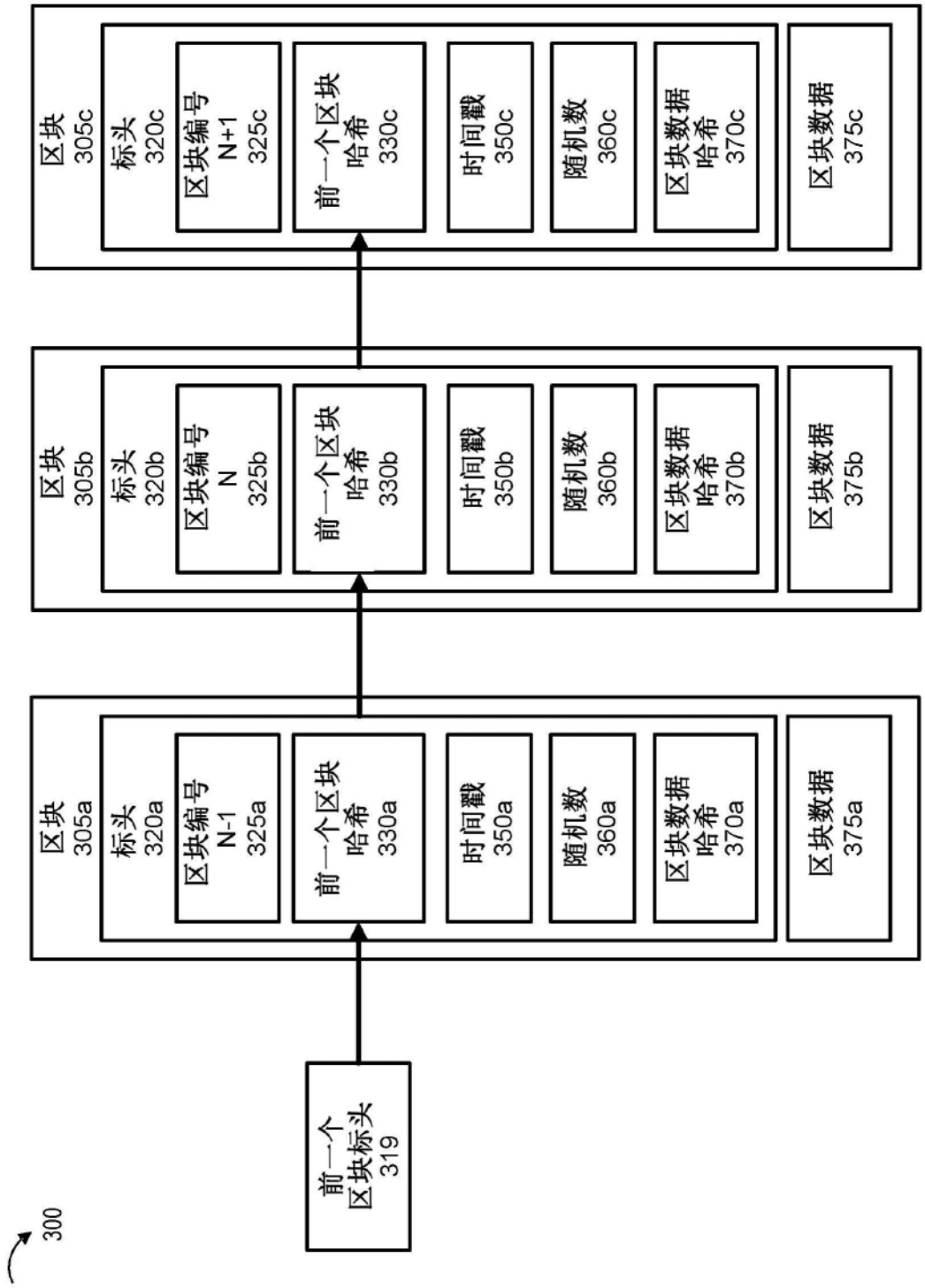

300
前一个区块标头319
区块305a
标头320a
区块编号N-1 325a
前一个区块哈希330a
时间戳350a
随机数360a
区块数据哈希370a
区块数据375a
区块305b
标头320b
区块编号N 325b
前一个区块哈希330b
时间戳350b
随机数360b
区块数据哈希370b
区块数据375b
区块305c
标头320c
区块编号N+1 325c
前一个区块哈希330c
时间戳350c
随机数360c
区块数据哈希370c
区块数据375c

图3

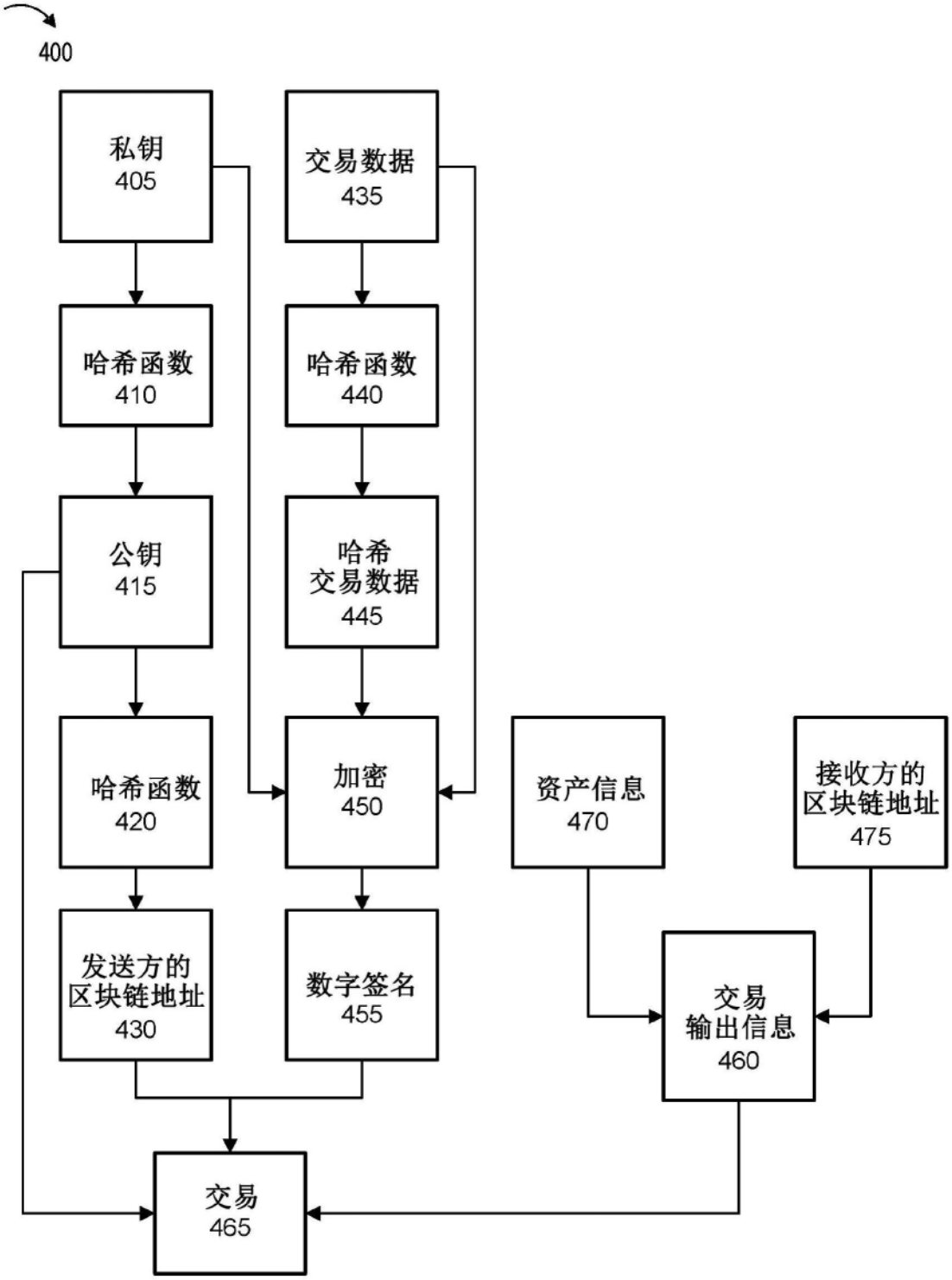

400
私钥
405
交易数据
435
哈希函数
410
哈希函数
440
公钥
415
哈希
交易数据
445
哈希函数
420
加密
450
资产信息
470
接收方的
区块链地址
475
发送方的
区块链地址
430
数字签名
455
交易
输出信息
460
交易
465

图4

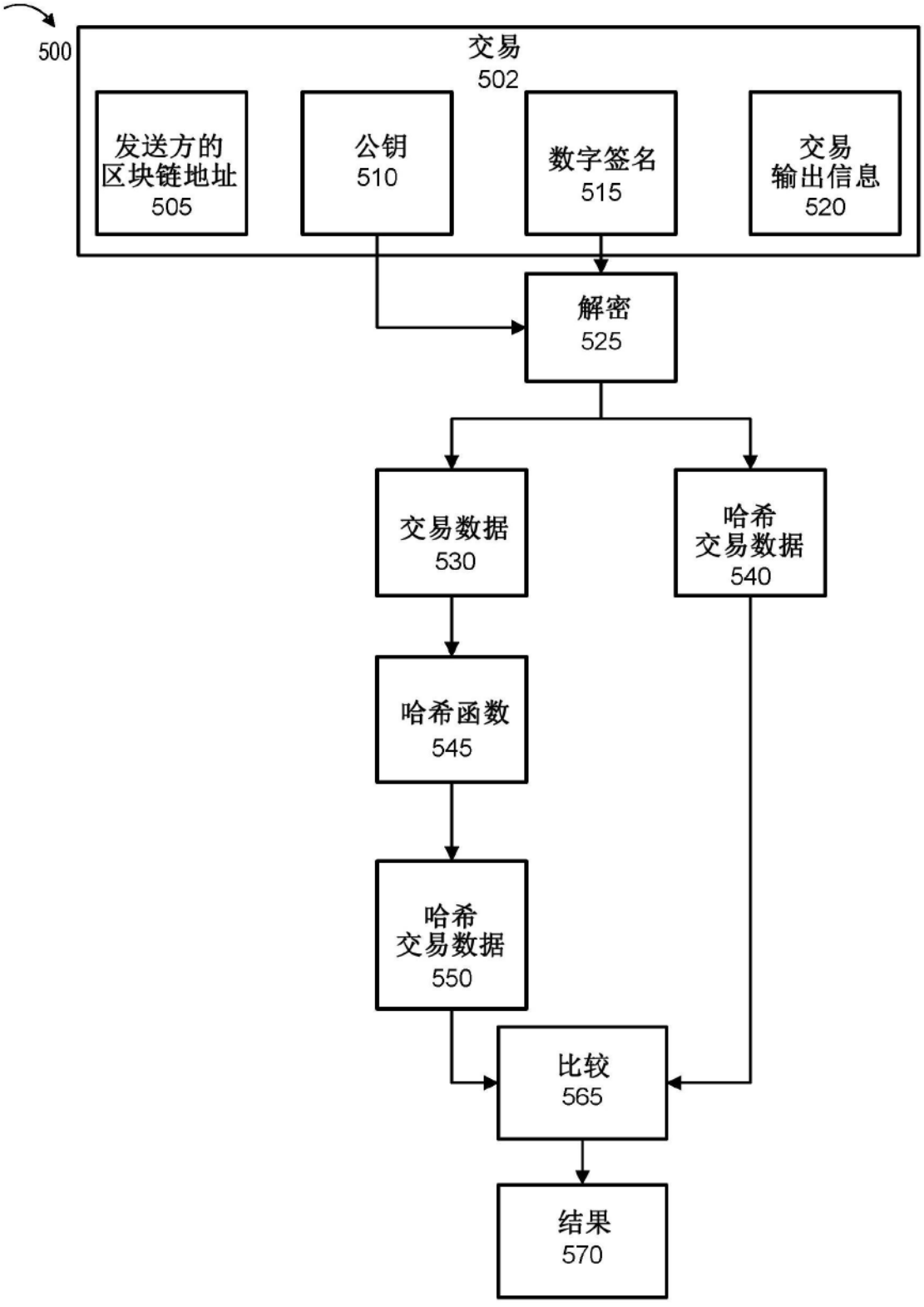

500
交易
502
发送方的
区块链地址
505
公钥
510
数字签名
515
交易
输出信息
520
解密
525
交易数据
530
哈希
交易数据
540
哈希函数
545
哈希
交易数据
550
比较
565
结果
570

图5

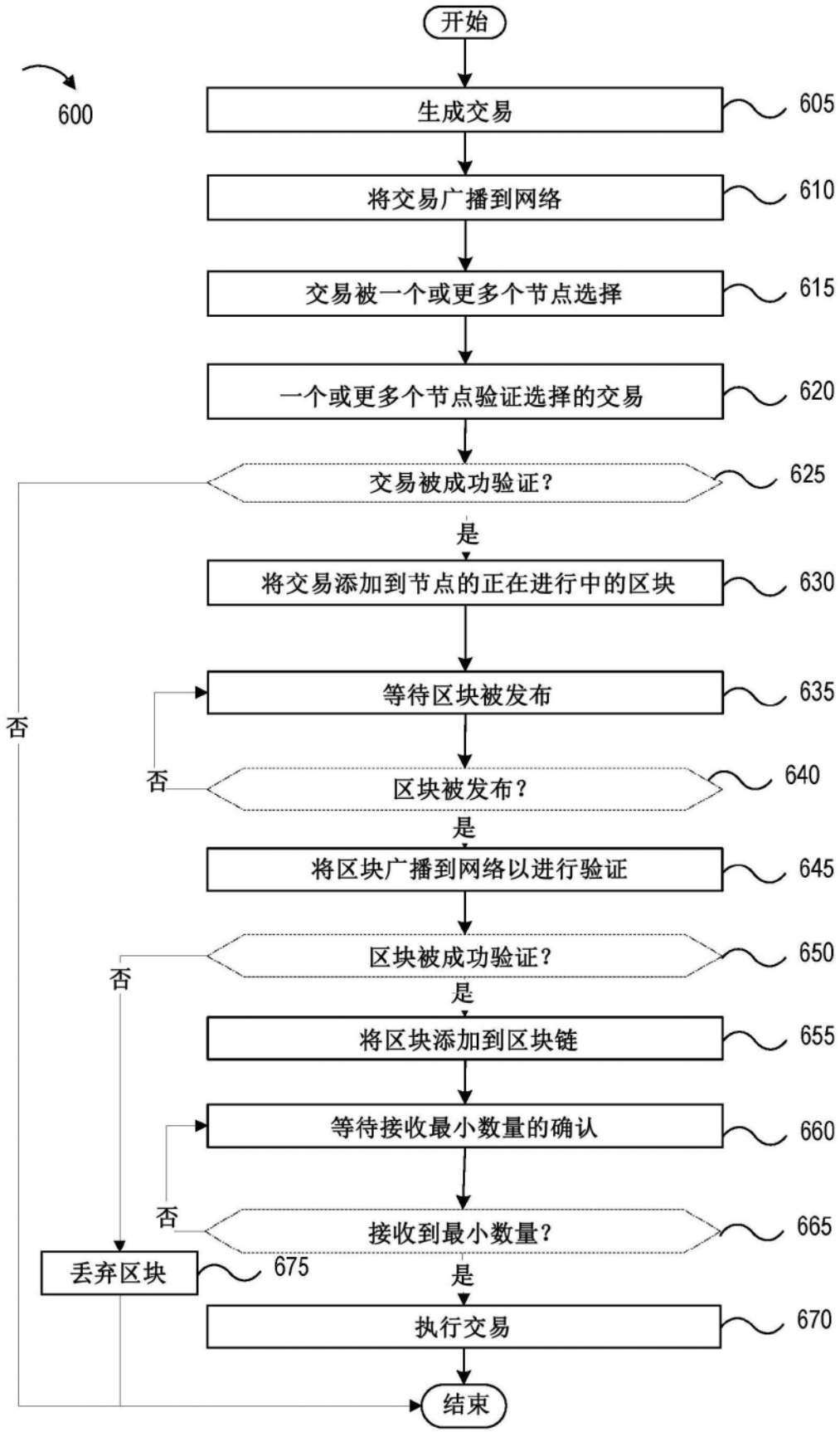

开始
600
生成交易
605
将交易广播到网络
610
交易被一个或更多个节点选择
615
一个或更多个节点验证选择的交易
620
交易被成功验证？
625
是
将交易添加到节点的正在进行中的区块
630
等待区块被发布
635
否
否
区块被发布？
640
是
将区块广播到网络以进行验证
645
区块被成功验证？
650
否
是
将区块添加到区块链
655
等待接收最小数量的确认
660
否
接收到最小数量？
665
丢弃区块
675
是
执行交易
670
结束

图6A

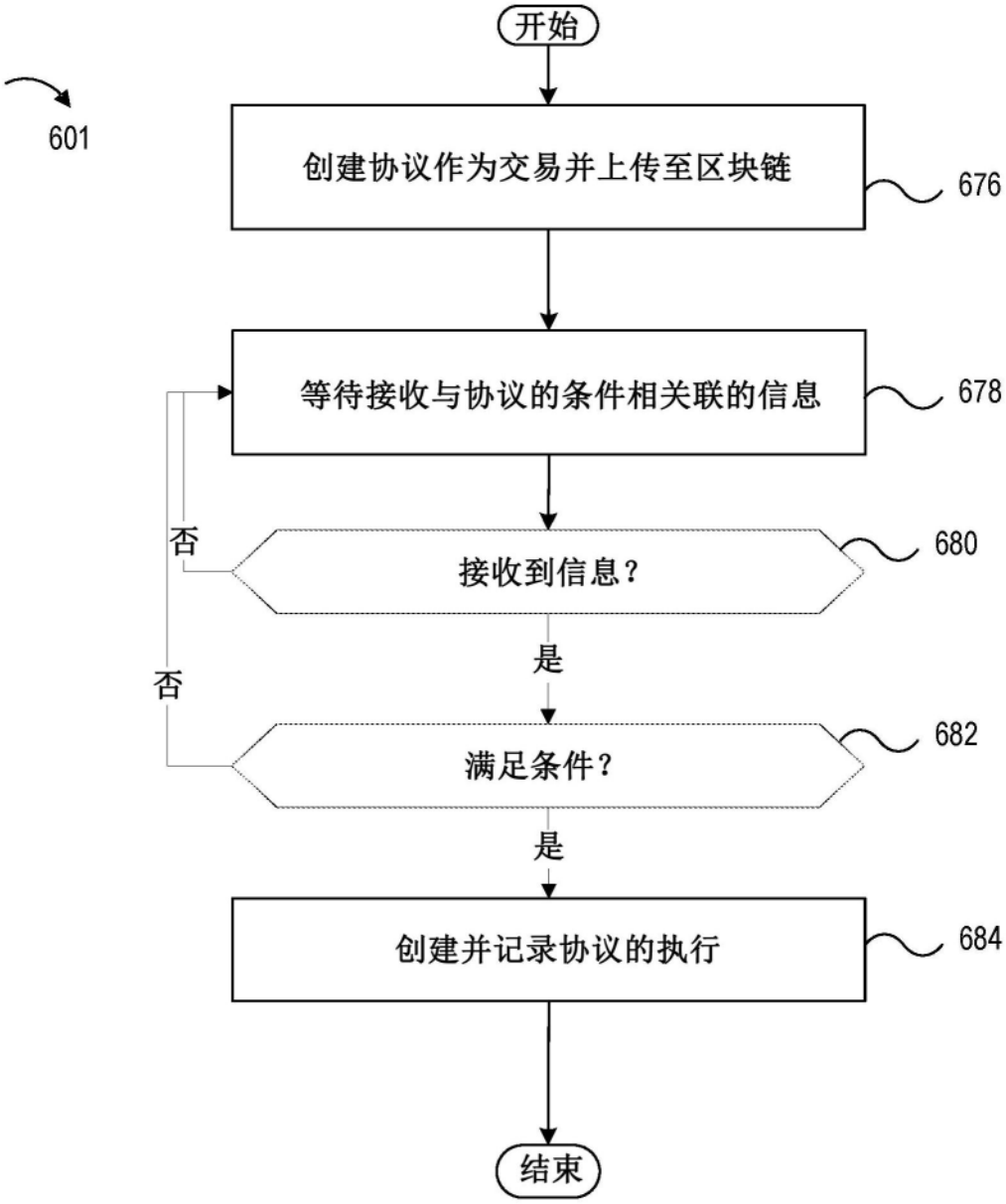

开始
601
创建协议作为交易并上传至区块链
676
等待接收与协议的条件相关联的信息
678
否
接收到信息？
680
是
否
满足条件？
682
是
创建并记录协议的执行
684
结束

图6B

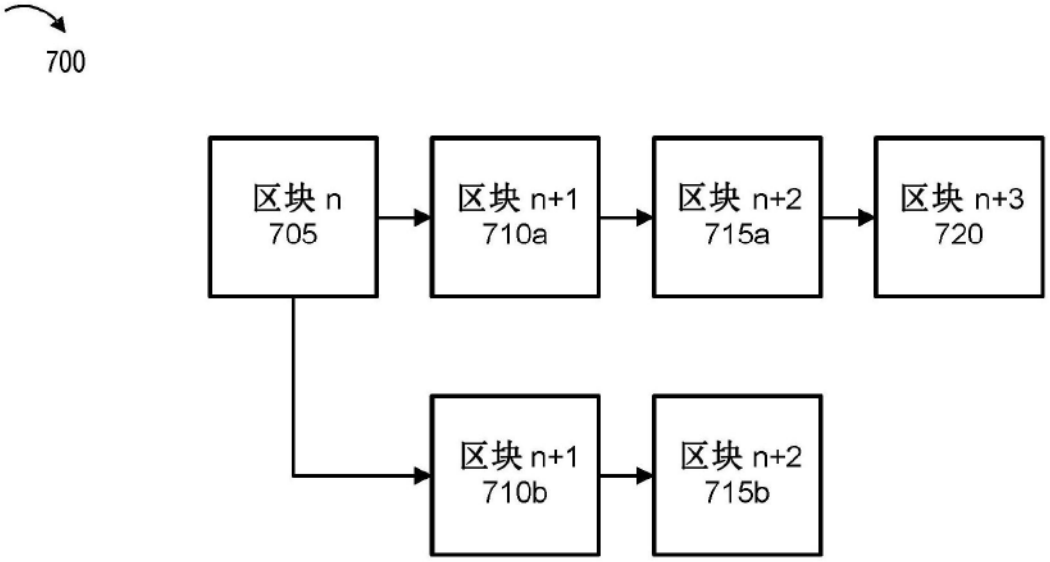

700
区块 n
705
区块 n+1
710a
区块 n+2
715a
区块 n+3
720
区块 n+1
710b
区块 n+2
715b

图7A

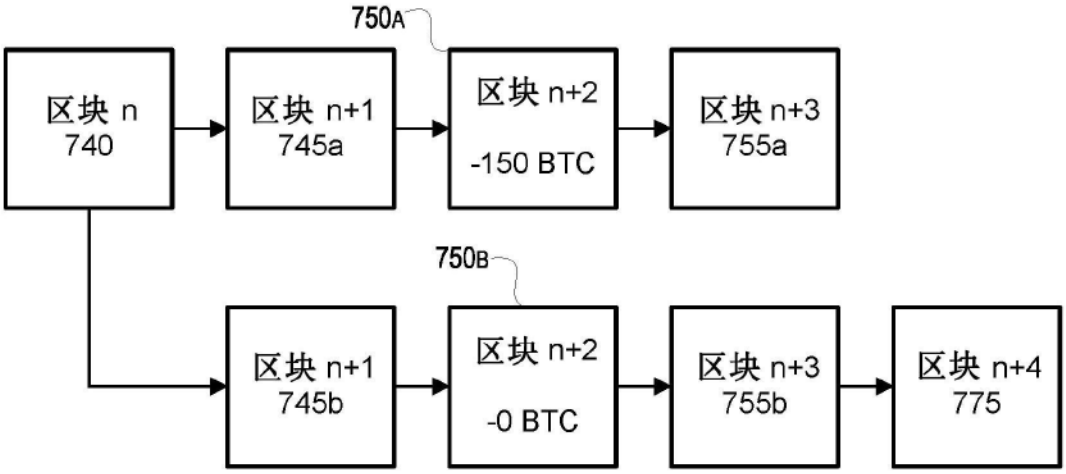

750A
区块 n
740
区块 n+1
745a
区块 n+2
-150 BTC
区块 n+3
755a
750B
区块 n+1
745b
区块 n+2
-0 BTC
区块 n+3
755b
区块 n+4
775

图7B

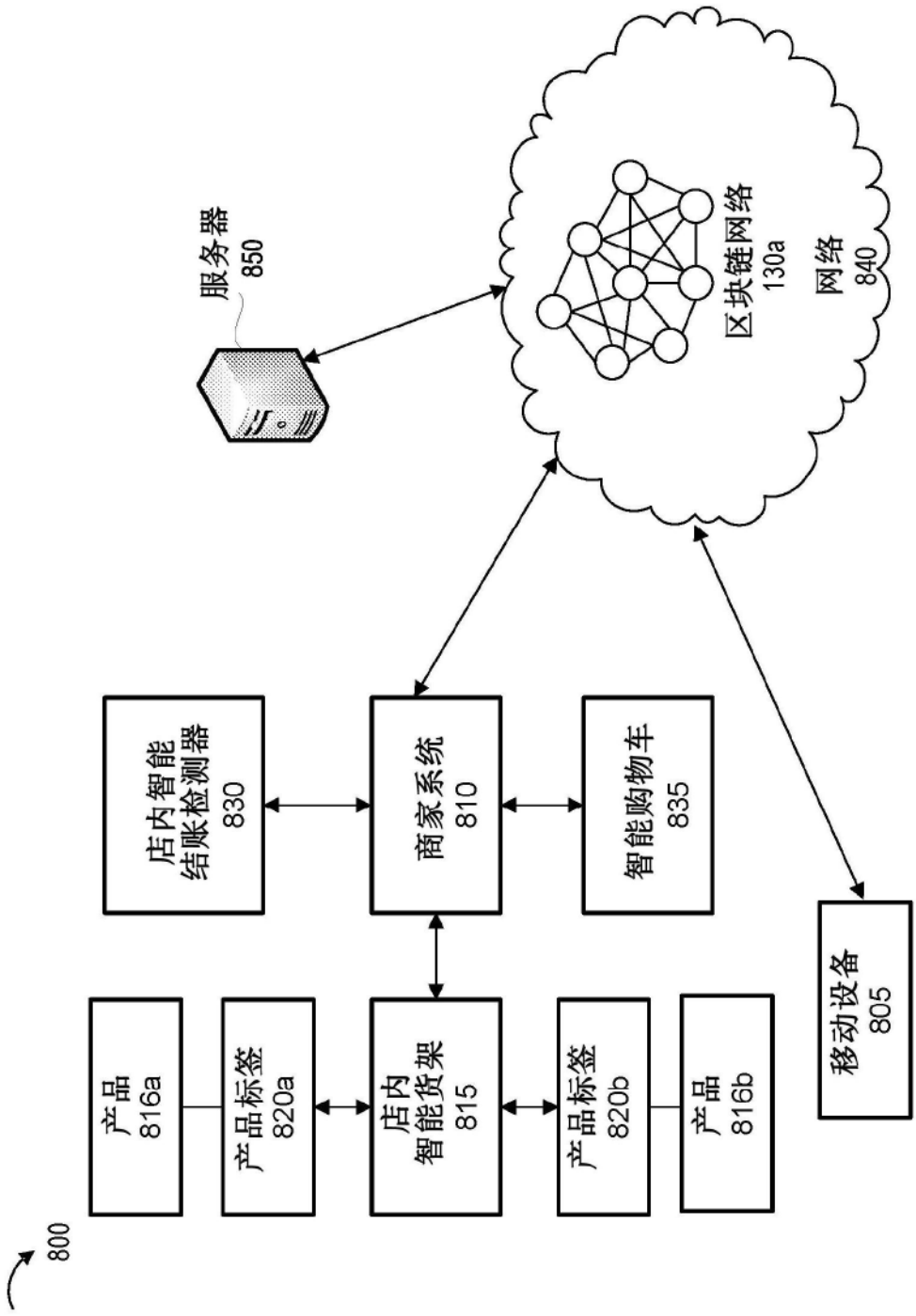

服务器
850
区块链网络
130a
网络
840
店内智能
结账检测器
830
商家系统
810
智能购物车
835
移动设备
805
产品
816a
产品标签
820a
店内
智能货架
815
产品标签
820b
产品
816b
800

图8

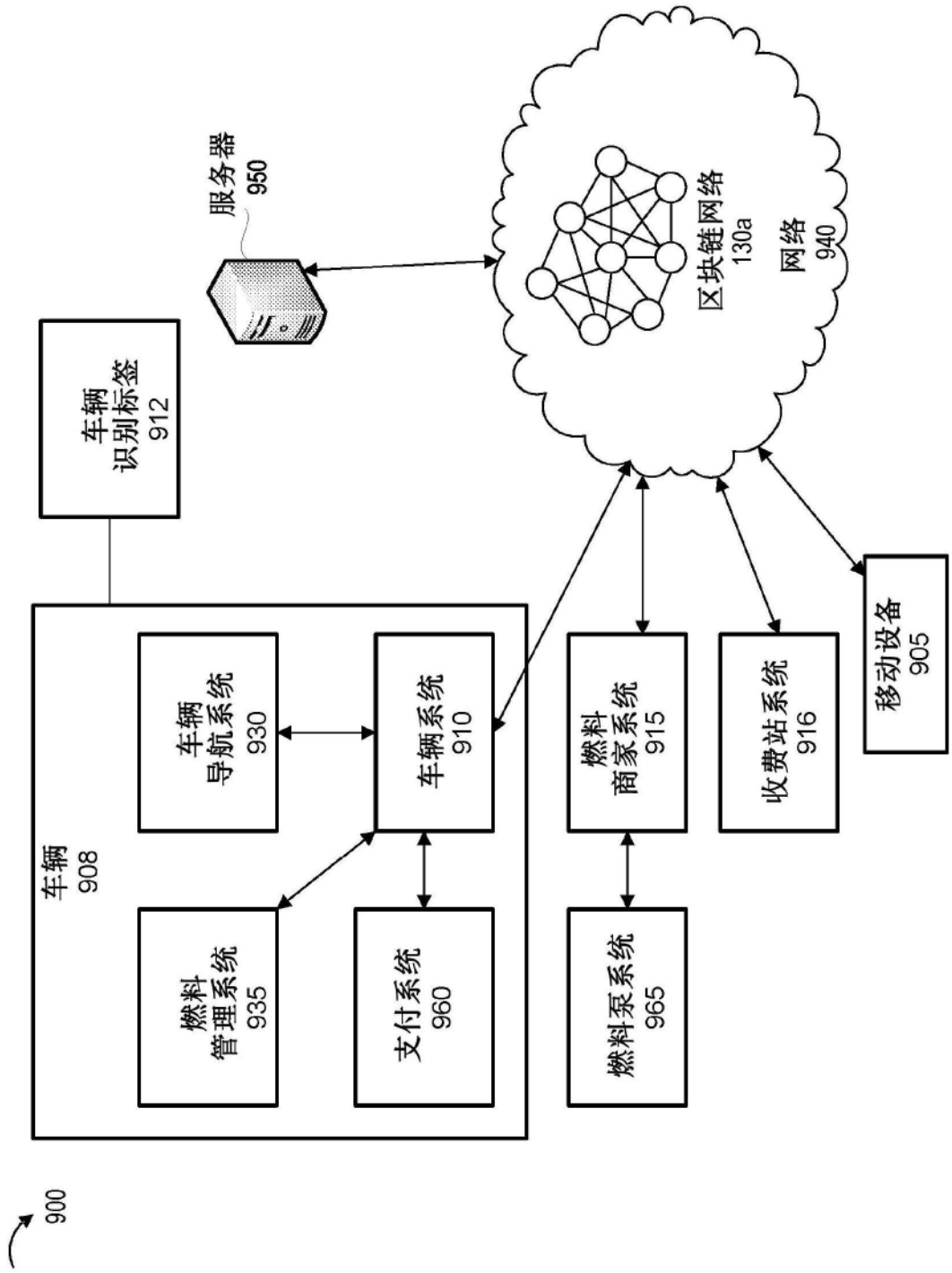

服务器
950
区块链网络
130a
网络
940
车辆
识别标签
912
车辆
908
车辆
导航系统
930
车辆系统
910
燃料
管理系统
935
支付系统
960
燃料
商家系统
915
燃料泵系统
965
收费站系统
916
移动设备
905
900

图9

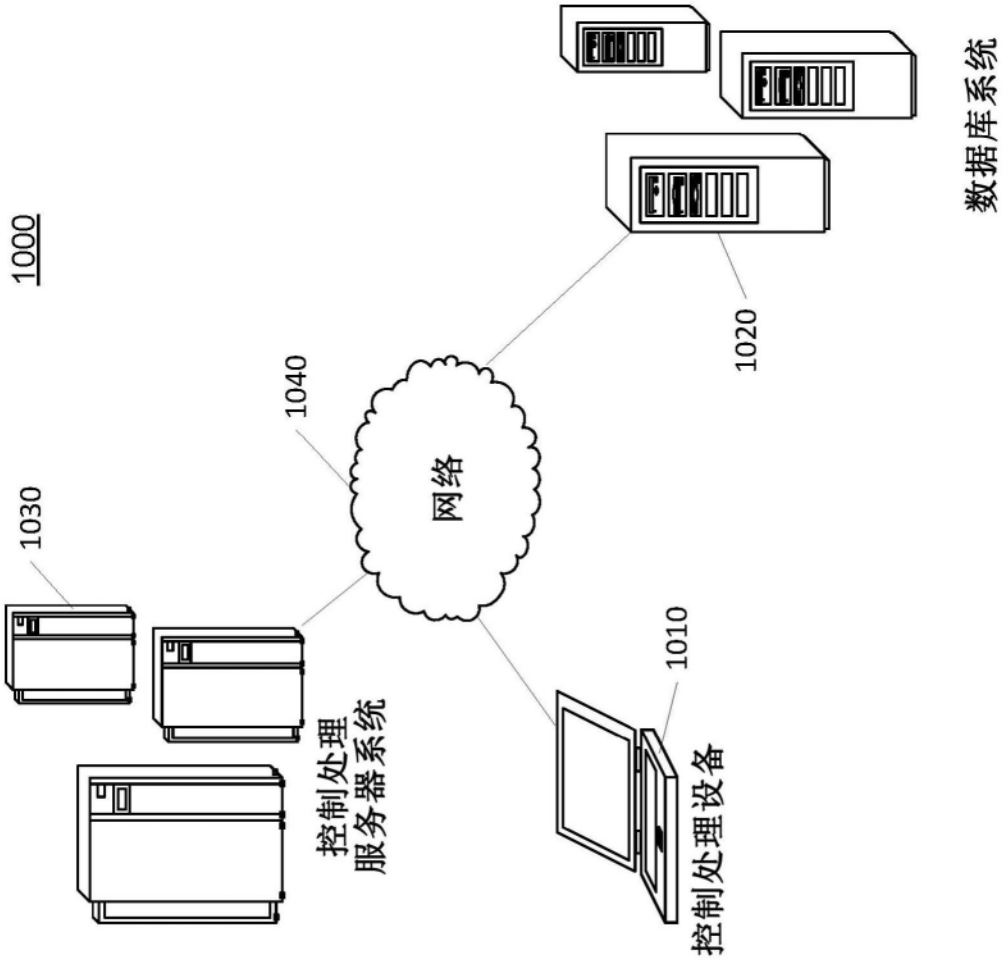


图10

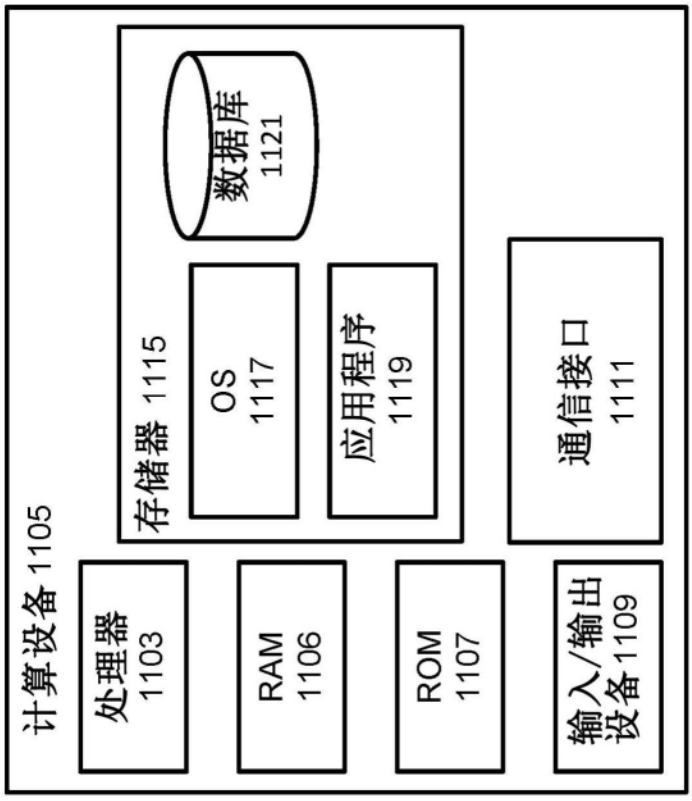

计算设备 1105
处理器 1103
RAM 1106
ROM 1107
输入/输出设备 1109
存储器 1115
OS 1117
应用程序 1119
数据库 1121
通信接口 1111

图11

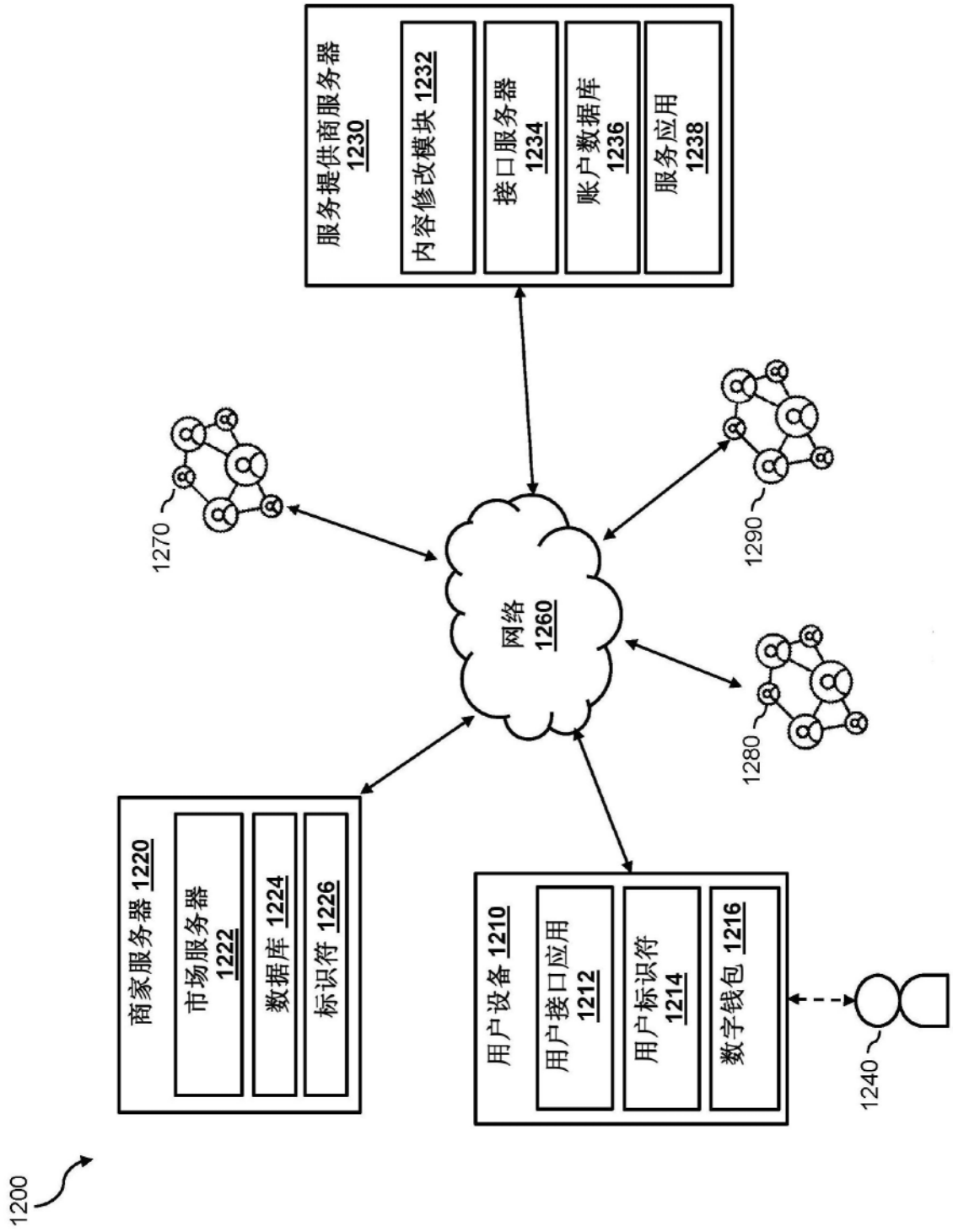

服务提供商服务器 1230
内容修改模块 1232
接口服务器 1234
账户数据库 1236
服务应用 1238
网络 1260
1270
1290
1280
商家服务器 1220
市场服务器 1222
数据库 1224
标识符 1226
用户设备 1210
用户接口应用 1212
用户标识符 1214
数字钱包 1216
1240
1200

图12

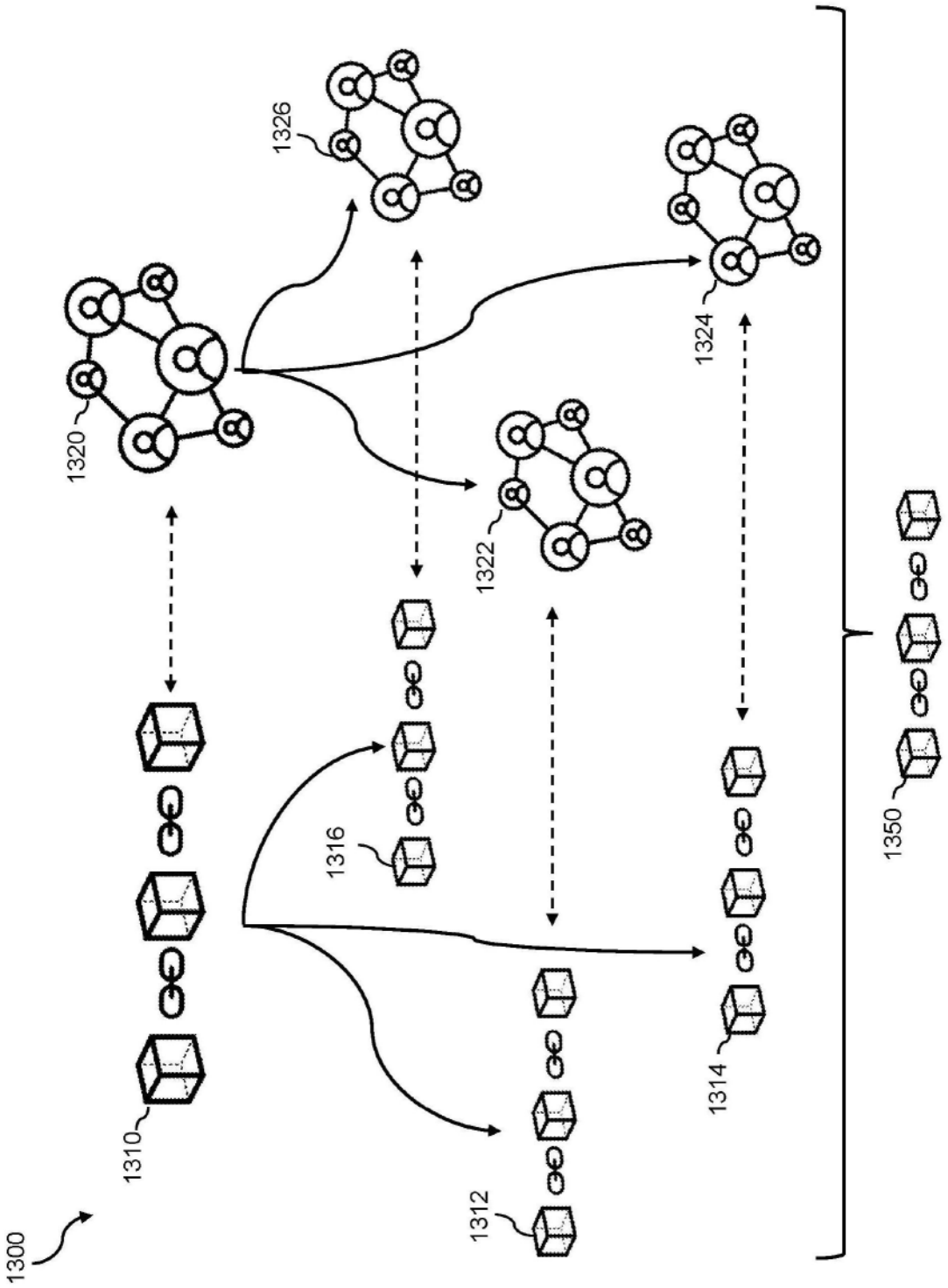


图13

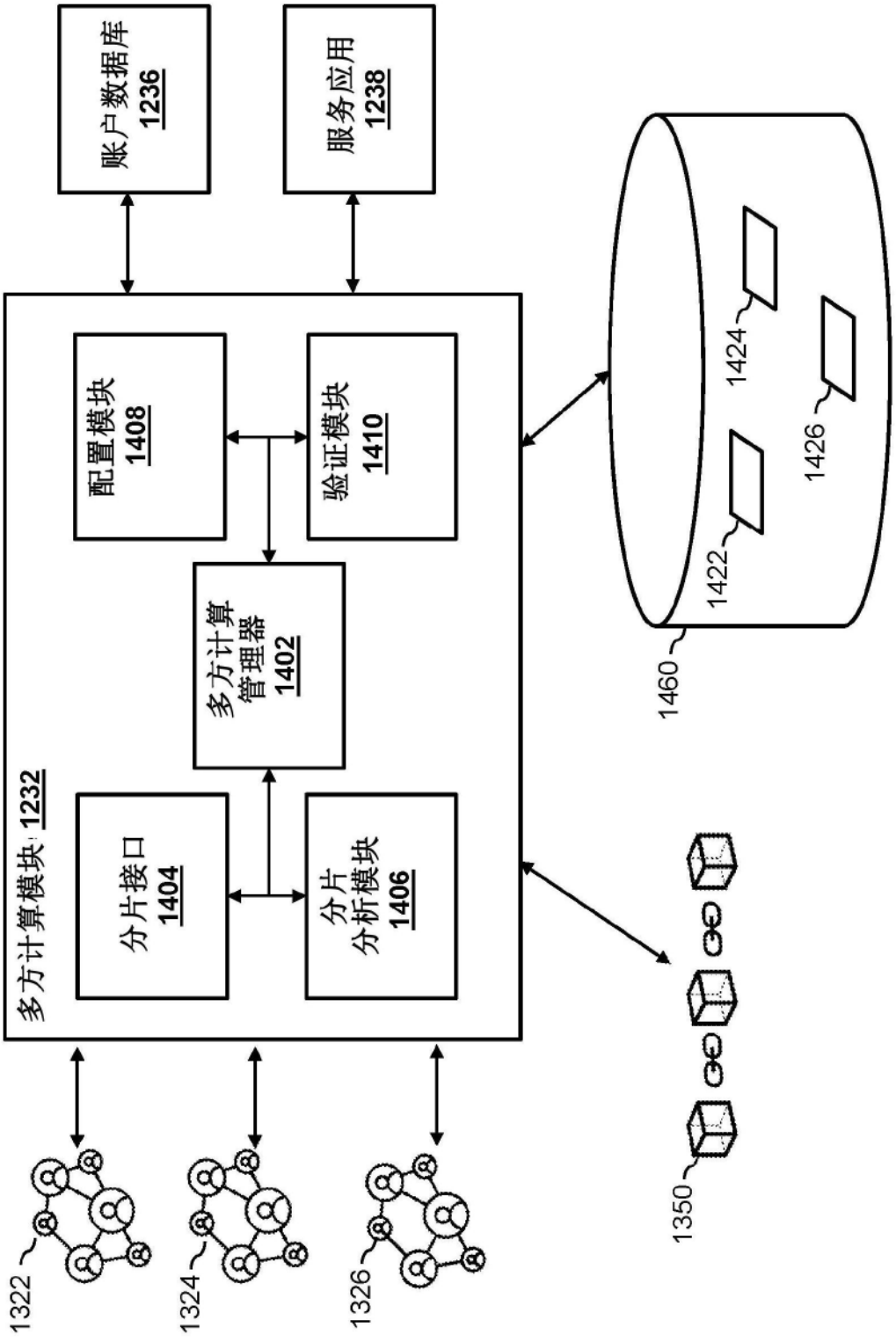

账户数据库
1236
服务应用
1238
配置模块
1408
验证模块
1410
多方计算
管理器
1402
分片接口
1404
分片
分析模块
1406
多方计算模块 1232
1424
1426
1422
1460
1350
1322
1324
1326

图14

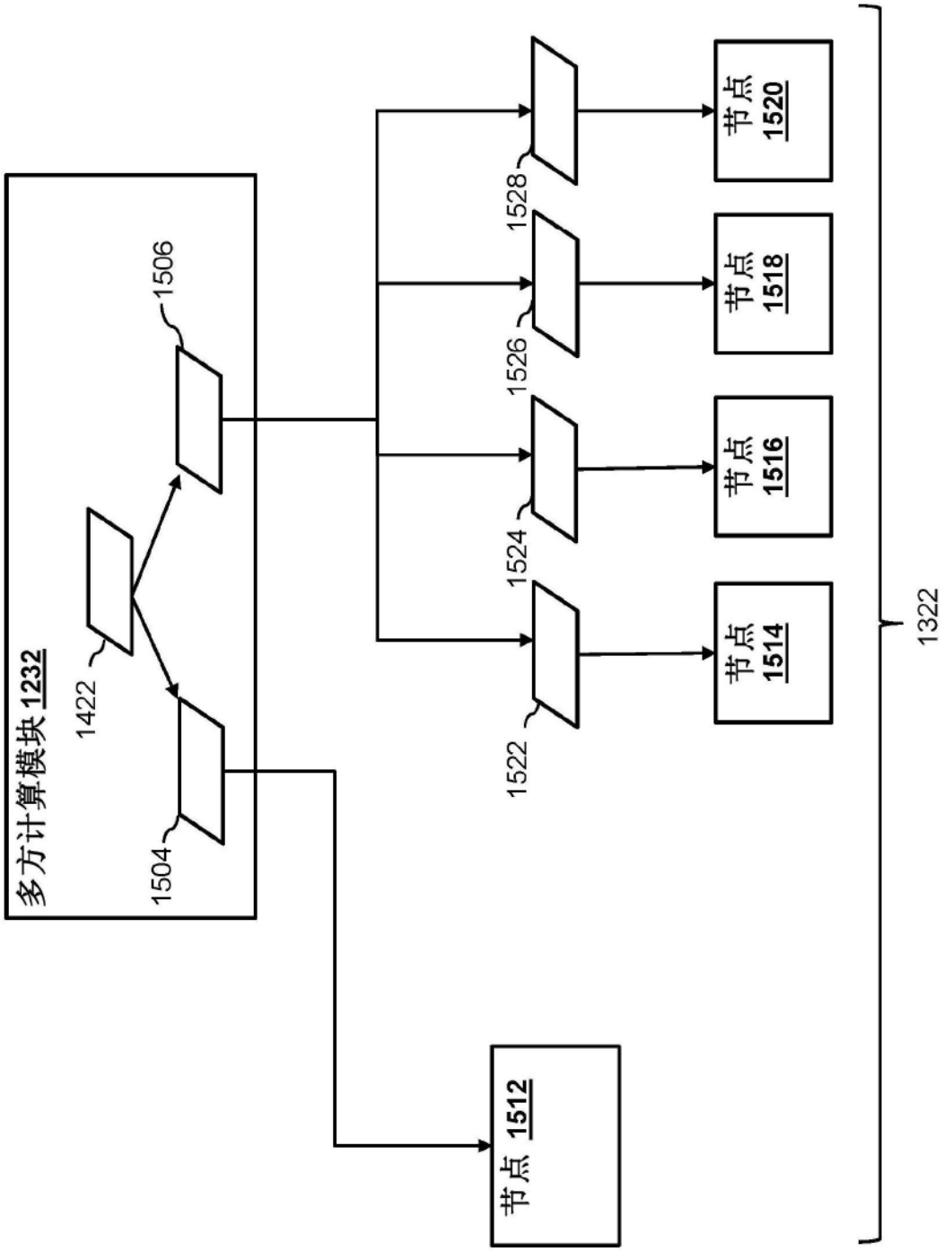

多方计算模块 1232
1422
1504
1506
1512
1514
1516
1518
1520
1522
1524
1526
1528
1322

图15

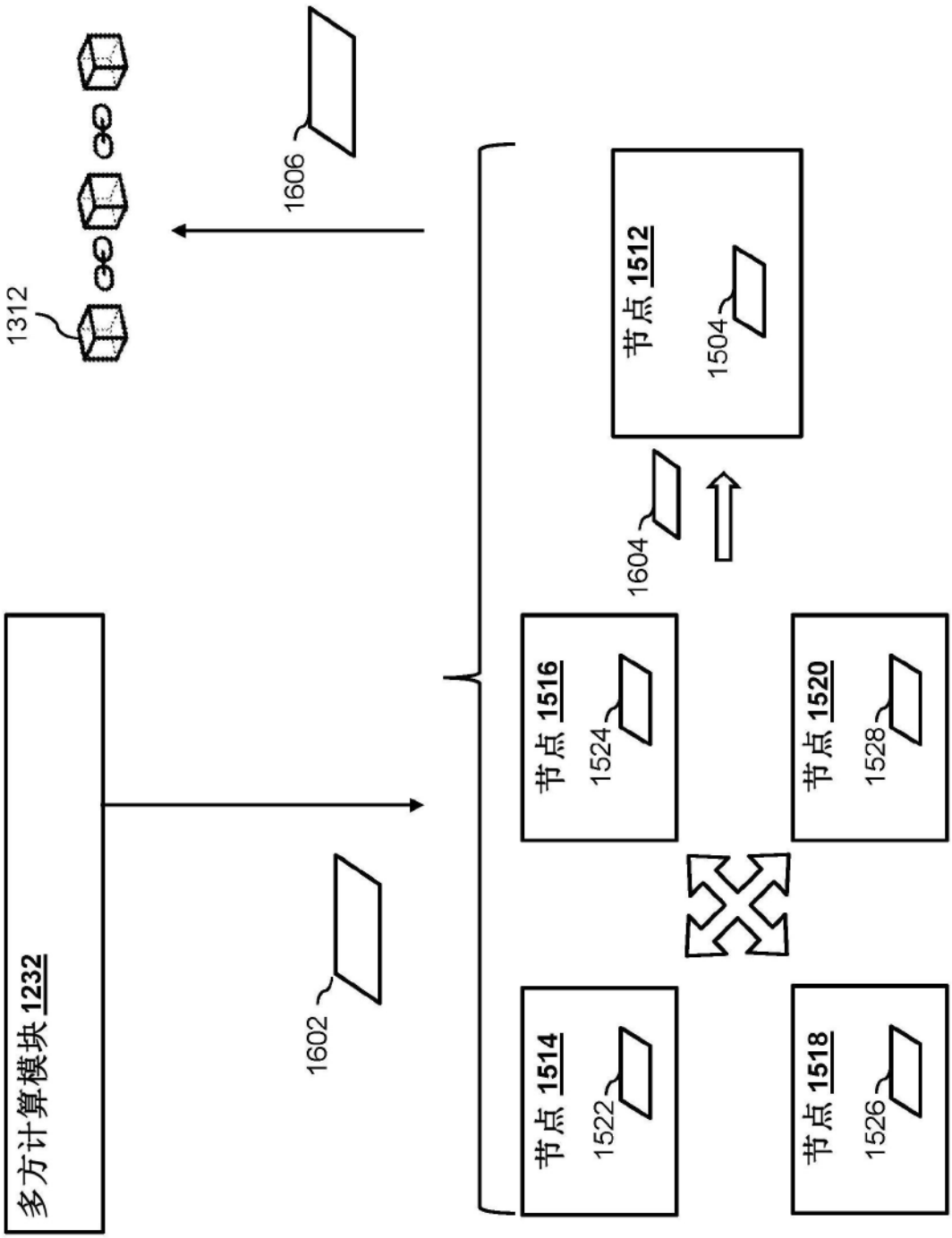

多方计算模块1232
1602
1606
1312
节点1514
1522
节点1516
1524
节点1518
1526
节点1520
1528
节点1512
1504
1604

图16

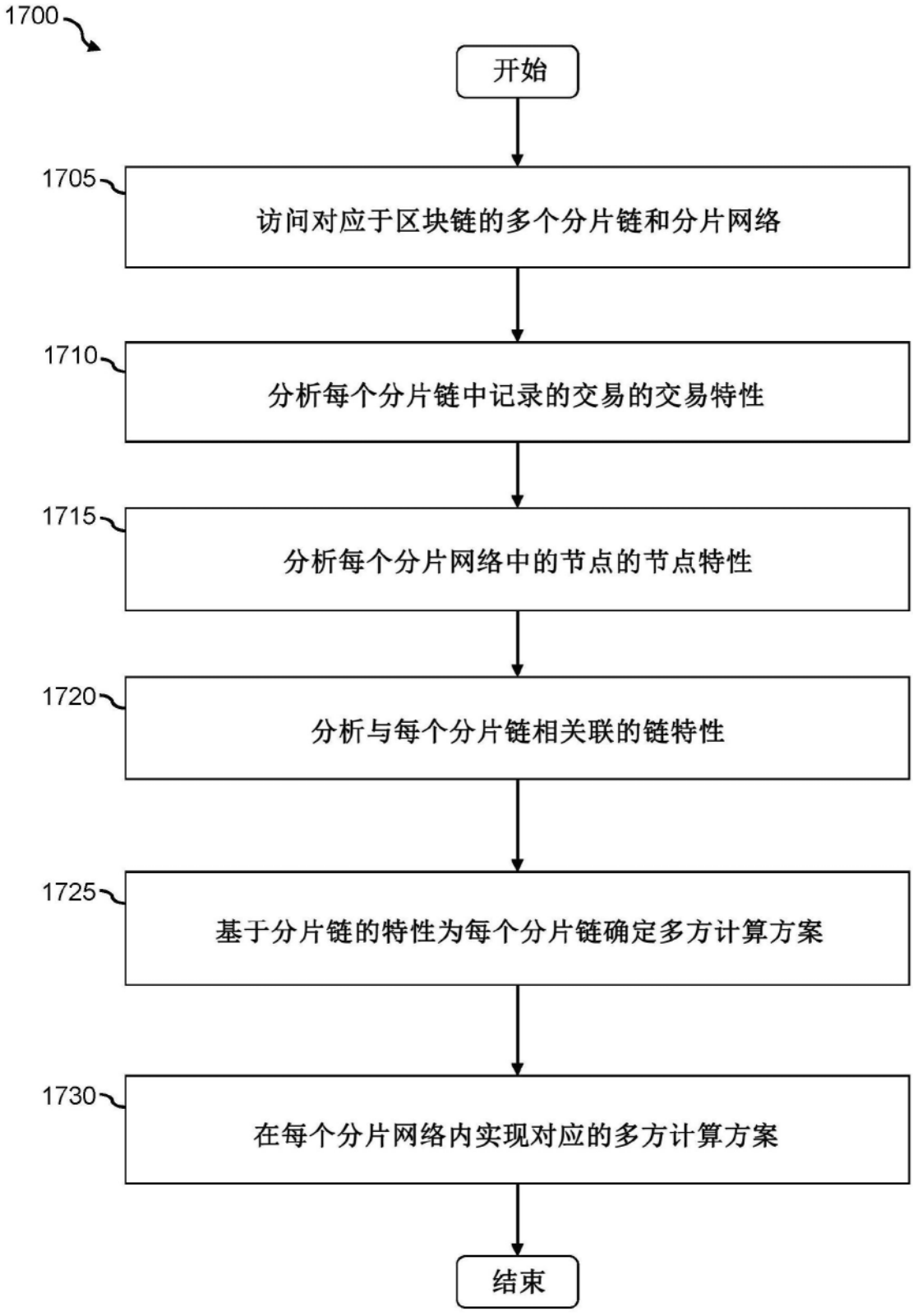

1700
开始
1705
访问对应于区块链的多个分片链和分片网络
1710
分析每个分片链中记录的交易的交易特性
1715
分析每个分片网络中的节点的节点特性
1720
分析与每个分片链相关联的链特性
1725
基于分片链的特性为每个分片链确定多方计算方案
1730
在每个分片网络内实现对应的多方计算方案
结束

图17

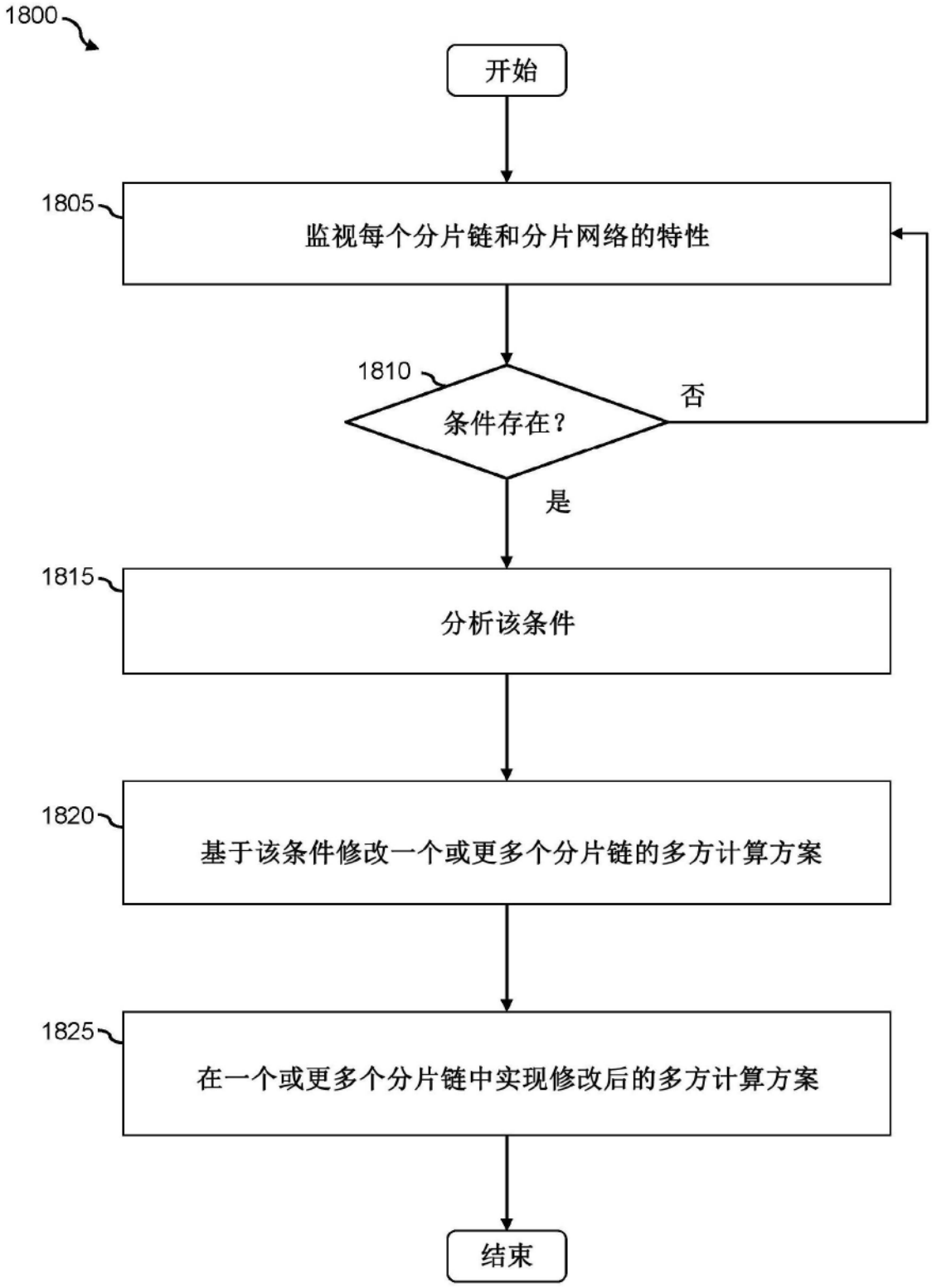

1800
开始
1805
监视每个分片链和分片网络的特性
1810
条件存在？
否
是
1815
分析该条件
1820
基于该条件修改一个或更多个分片链的多方计算方案
1825
在一个或更多个分片链中实现修改后的多方计算方案
结束

图18

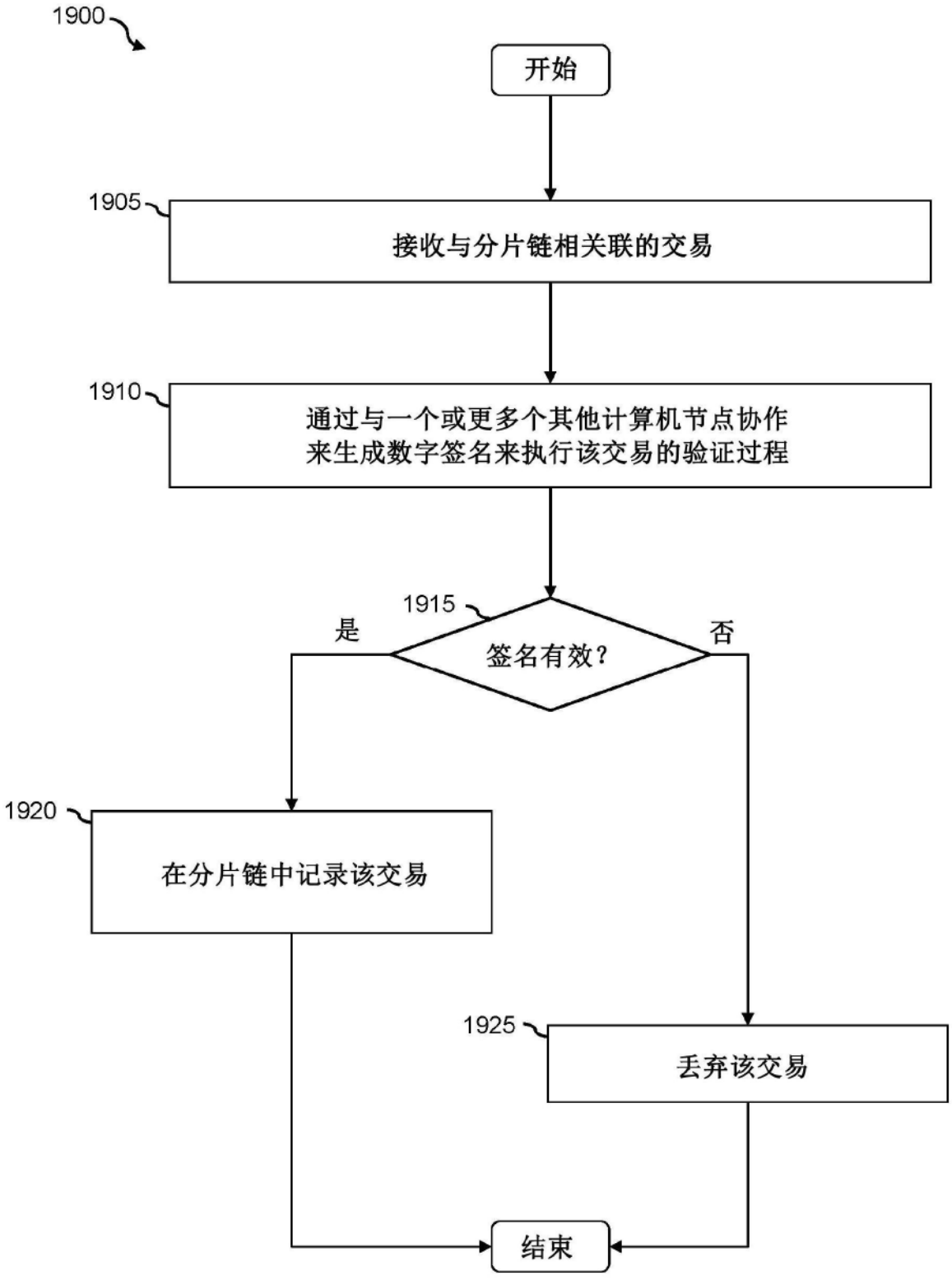

1900
开始
1905
接收与分片链相关联的交易
1910
通过与一个或更多个其他计算机节点协作
来生成数字签名来执行该交易的验证过程
1915
是
签名有效?
否
1920
在分片链中记录该交易
1925
丢弃该交易
结束

图19

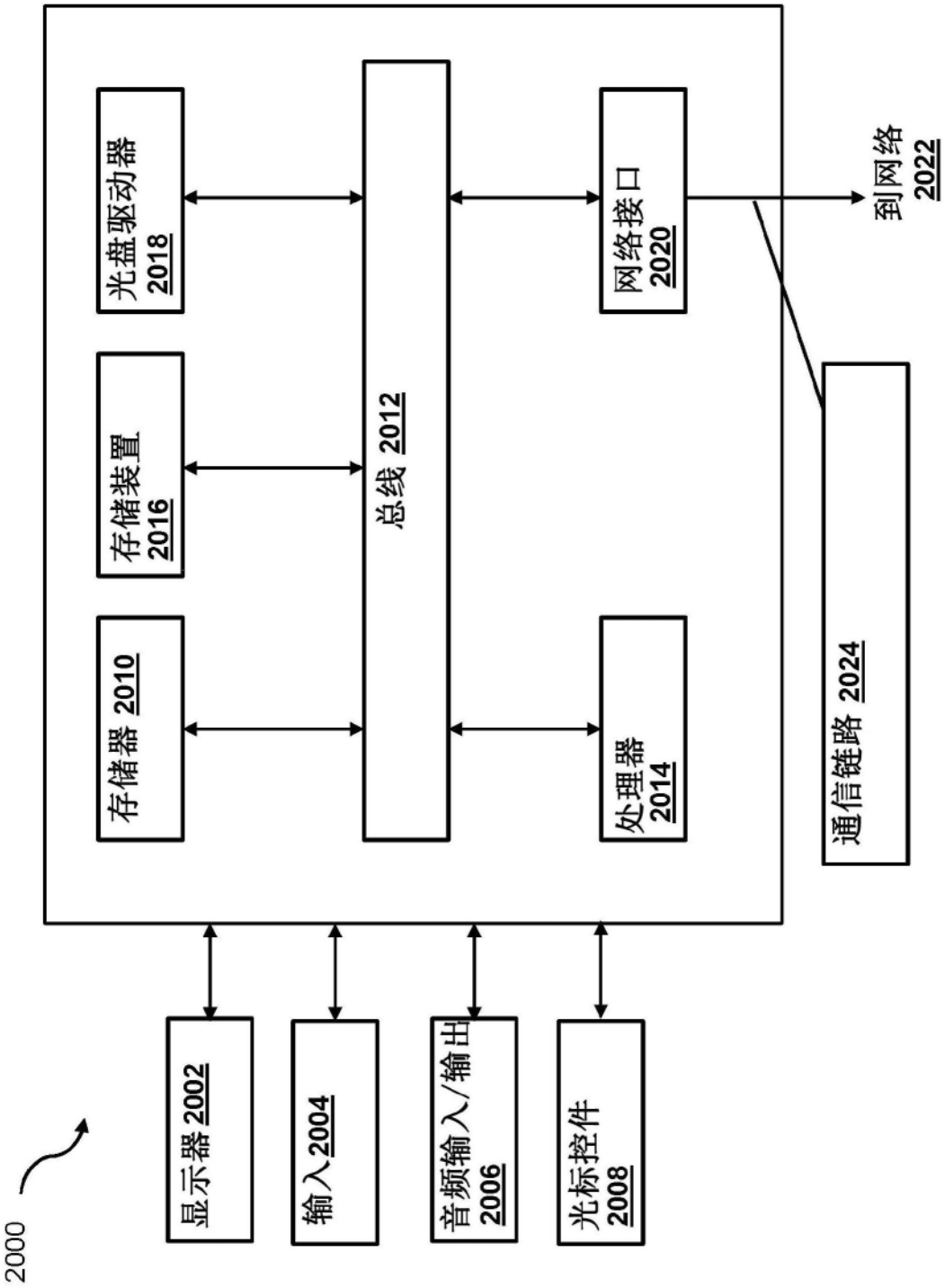

2000
显示器 2002
输入 2004
音频输入/输出 2006
光标控件 2008
光盘驱动器 2018
存储装置 2016
存储器 2010
总线 2012
处理器 2014
网络接口 2020
到网络 2022
通信链路 2024

图20