(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109242453 A
(43)申请公布日 2019.01.18

(21)申请号 201810891689.X

(22)申请日 2018.08.07

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 杨新颖

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

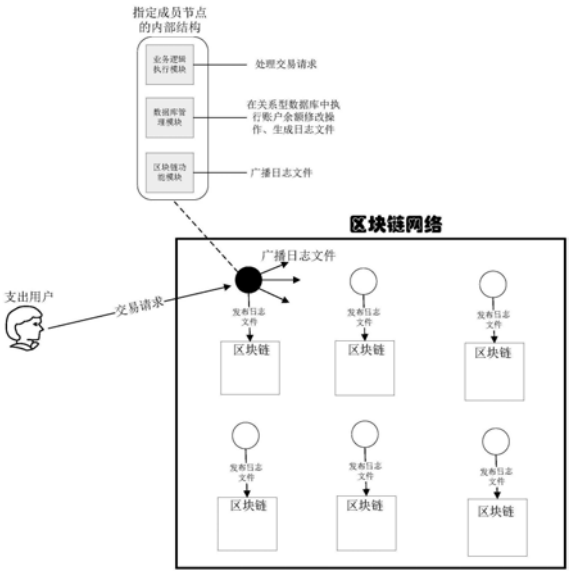
权利要求书2页 说明书12页 附图9页

(54)发明名称

一种基于中心化结算与区块链存证的交易方法及系统

(57)摘要

公开了一种基于中心化结算与区块链存证的交易方法及系统。区块链网络包括若干成员节点，用户在指定成员节点上注册有虚拟资源账户，所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块。由业务逻辑执行模块针对交易请求进行交易可行性验证，并于验证通过后，指令数据管理模块执行账户余额修改操作，即从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额。并且，所述数据库管理模块还会生成用于记录所述账户余额修改操作的日志文件，将所述日志文件发送给区块链功能模块，由区块链功能模块将所述日志文件广播至所述区块链网络。



CN 109242453 A

1.一种基于中心化结算与区块链存证的交易方法,区块链网络包括若干成员节点,用户在指定成员节点上注册有虚拟资源账户,所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块,所述方法包括:

所述业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求;所述支出用户是支出所述指定资源数额的用户,所述收入用户是收入所述指定资源数额的用户;

所述业务逻辑执行模块根据所述交易请求,进行交易可行性验证,并在验证通过后,向所述数据库管理模块发送账户余额修改指令;

所述数据库管理模块根据所述账户余额修改指令,执行账户余额修改操作,并生成用于记录所述账户余额修改操作的日志文件;所述账户余额修改操作为,从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额,并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额;

所述数据库管理模块将所述日志文件发送给所述区块链功能模块;

所述区块链功能模块向所述区块链网络广播所述日志文件,以使各成员节点基于共识机制将所述日志文件发布至区块链。

2.如权利要求1所述的方法,所述区块链功能模块向所述区块链网络广播所述日志文件,具体包括:

所述区块链功能模块根据所述日志文件,采用哈希算法,生成所述日志文件对应的日志文件摘要;

所述区块链功能模块向所述区块链网络广播所述日志文件和所述日志文件摘要,以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链;

所述方法还包括:

所述区块链功能模块将所述日志文件摘要发送给所述数据库管理模块;

所述数据库管理模块将所述日志文件摘要发送给所述业务逻辑执行模块;

所述业务逻辑执行模块将所述日志文件摘要发送给所述支出用户和/或所述收入用户,以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

3.如权利要求2所述的方法,所述区块链功能模块将所述日志文件摘要发送给所述数据库管理模块,具体包括:

所述区块链功能模块若确定所述日志文件被发布至区块链,则将所述日志文件摘要发送给所述数据库管理模块。

4.如权利要求2所述的方法,所述数据库管理模块将所述日志文件摘要发送给所述业务逻辑执行模块,具体包括:

所述数据库管理模块将所述日志文件摘要和修改成功通知发送给所述业务逻辑执行模块。

5.一种基于中心化结算与区块链存证的交易设备,区块链网络包含若干成员节点,所述设备为任一成员节点,用户在所述设备上注册有虚拟资源账户,所述设备包括业务逻辑执行模块、数据库管理模块和区块链功能模块;

所述业务逻辑执行模块,接收包含支出用户的支出用户标识、指定资源数额和收入用

户的收入用户标识的交易请求;所述支出用户是支出所述指定资源数额的用户,所述收入用户是收入所述指定资源数额的用户;根据所述交易请求,进行交易可行性验证,并在验证通过后,向所述数据库管理模块发送账户余额修改指令;

所述数据库管理模块,根据所述账户余额修改指令,执行账户余额修改操作,并生成用于记录所述账户余额修改操作的日志文件,所述账户余额修改操作为,从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额,并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额;将所述日志文件发送给所述区块链功能模块;

所述区块链功能模块,向所述区块链网络广播所述日志文件,以使各成员节点基于共识机制将所述日志文件发布至区块链。

6.如权利要求5所述的设备,所述区块链功能模块,根据所述日志文件,采用哈希算法,生成所述日志文件对应的日志文件摘要;向所述区块链网络广播所述日志文件和所述日志文件摘要,以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链;将所述日志文件摘要发送给所述数据库管理模块;

所述数据库管理模块,将所述日志文件摘要发送给所述业务逻辑执行模块;

所述业务逻辑执行模块,将所述日志文件摘要发送给所述支出用户和/或所述收入用户,以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

7.如权利要求6所述的设备,所述区块链功能模块,若确定所述日志文件被发布至区块链,则将所述日志文件摘要发送给所述数据库管理模块。

8.如权利要求6所述的设备,所述数据库管理模块,将所述日志文件摘要和修改成功通知发送给所述业务逻辑执行模块。

9.一种基于中心化结算与区块链存证的交易系统,包括由若干成员节点组成的区块链网络,其中,各成员节点中包含权利要求5～8任一项所述的设备。

10.一种基于中心化计算与区块链存证的交易方法,区块链网络包括若干成员节点,用户在指定成员节点上注册有虚拟资源账户,所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块,所述方法包括:

所述指定成员节点通过所述业务逻辑执行模块,接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求;所述支出用户是支出所述指定资源数额的用户,所述收入用户是收入所述指定资源数额的用户;

通过所述业务逻辑执行模块,根据所述交易请求,进行交易可行性验证,并在验证通过后,通过所述数据库管理模块,执行账户余额修改操作,生成用于记录所述账户余额修改操作的日志文件;所述账户余额修改操作为,从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额,并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额;

通过所述区块链功能模块,向所述区块链网络广播所述日志文件,以使各成员节点基于共识机制将所述日志文件发布至区块链。

一种基于中心化结算与区块链存证的交易方法及系统

技术领域

[0001] 本说明书实施例涉及信息技术领域，尤其涉及一种基于中心化结算与区块链存证的交易方法及系统。

背景技术

[0002] 目前，在线电子交易的主要模式为，由中心化的结算平台(如银行、支付宝等)负责管理用户的账户，用户之间的交易由结算平台执行并进行记录，用户可以自行向结算平台查询自己账户的收支记录以便进行核对。

[0003] 然而，结算平台存储的用户账户的收支记录存在被篡改的可能性，从而不能作为可信的对账凭证。

发明内容

[0004] 为了解决中心化的结算平台存储的用户账户的收支记录不可信的问题，本说明书实施例提供一种基于中心化结算与区块链存证的交易方法及系统，技术方案如下：

[0005] 根据本说明书实施例的第1方面，提供一种基于中心化结算与区块链存证的交易方法，区块链网络包括若干成员节点，用户在指定成员节点上注册有虚拟资源账户，所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块，所述方法包括：

[0006] 所述业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求；所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；

[0007] 所述业务逻辑执行模块根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令；

[0008] 所述数据库管理模块根据所述账户余额修改指令，执行账户余额修改操作，并生成用于记录所述账户余额修改操作的日志文件；所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；

[0009] 所述数据库管理模块将所述日志文件发送给所述区块链功能模块；

[0010] 所述区块链功能模块向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0011] 根据本说明书实施例的第2方面，提供一种基于中心化结算与区块链存证的交易设备，区块链网络包含若干成员节点，所述设备为任一成员节点，用户在所述设备上注册有虚拟资源账户，所述设备包括业务逻辑执行模块、数据库管理模块和区块链功能模块；

[0012] 所述业务逻辑执行模块，接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求；所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令；

[0013] 所述数据库管理模块，根据所述账户余额修改指令，执行账户余额修改操作，并生成用于记录所述账户余额修改操作的日志文件，所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；将所述日志文件发送给所述区块链功能模块；

[0014] 所述区块链功能模块，向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0015] 本说明书实施例所提供的技术方案，区块链网络包括若干成员节点，用户在指定成员节点上注册有虚拟资源账户，所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块。所述指定成员节点当接收到交易请求时，由业务逻辑执行模块针对交易请求进行交易可行性验证，并于验证通过后，指令数据管理模块执行账户余额修改操作，即从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额。并且，所述数据库管理模块还会生成用于记录所述账户余额修改操作的日志文件，将所述日志文件发送给区块链功能模块，由区块链功能模块将所述日志文件广播至所述区块链网络，使得各成员节点基于共识机制将所述日志文件发布至区块链。也就是说，针对一笔交易，所述指定成员节点执行交易结算时产生的日志文件会被发布至区块链进行存证，相当于中心化结算平台存储的用户账户的会被发布至区块链进行存证。因此，用户账户的收支记录难以被篡改，可以作为可信的对账凭证。

[0016] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[0017] 此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[0018] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[0019] 图1是本说明书实施例提供的一种基于中心化结算与区块链存证的交易方法的流程示意图；

[0020] 图2a是本说明书实施例提供的一种基于中心化结算与区块链存证的交易方法的流程示例图；

[0021] 图2b是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的流程示例图；

[0022] 图2c是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的流程示例图；

[0023] 图3是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的流程示意图；

[0024] 图4是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的流程示意图；

[0025] 图5是本说明书实施例提供的一种基于中心化结算与区块链存证的交易装置的结构示意图；

[0026] 图6是本说明书实施例提供的一种基于中心化结算与区块链存证的交易设备的结构示意图；

[0027] 图7是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易设备的结构示意图；

[0028] 图8是本说明书实施例提供的一种基于中心化结算与区块链存证的交易系统的结构示意图；

[0029] 图9是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易系统的结构示意图；

[0030] 图10是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易系统的结构示意图；

[0031] 图11是用于配置图1所示方法的一种计算机设备的结构示意图。

具体实施方式

[0032] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[0033] 以下结合附图，详细说明本说明书各实施例提供的技术方案。

[0034] 图1是本说明书实施例提供的一种基于中心化结算与区块链存证的交易方法的流程示意图，包括以下步骤：

[0035] S100：指定成员节点接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求。

[0036] 在本说明书实施例中，区块链网络包括若干成员节点。需要说明的是，在本文中，“节点”可以是由管理方(人或机构)管理的一个设备或多个设备，各成员节点分别对应的管理方通常不同。

[0037] 在本说明书实施例中，用户在指定成员节点上注册有虚拟资源账户。其中，所述指定成员节点可以根据实际业务需要指定。例如，假设所述区块链网络是由10个金融机构(包括银行、电子支付平台等)组成的联盟链网络，可以将电子支付平台管理的成员节点指定为指定成员节点，用户在电子支付平台注册有虚拟资源账户。

[0038] 需要说明的是，用户在所述指定成员节点上注册的虚拟资源账户实际上是在所述指定成员节点的关系型数据库中进行维护的。

[0039] 还需要说明的是，本文中所述的虚拟资源不限于电子货币，还可以是积分、游戏币、虚拟物品等。总之，根据实际业务规则，用户之间可以以任何虚拟资源为交易媒介进行交易。

[0040] 在步骤S100中，指定成员节点，可以接收支出用户发送的交易请求，也可以接收收入用户发出的交易请求。其中，所述交易请求通常包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识，所述支出用户是支出所述指定资源数额的用户，所述收

入用户是收入所述指定资源数额的用户。

[0041] S102:根据所述交易请求,进行交易可行性验证,并在验证通过后,执行账户余额修改操作。

[0042] 在本文中,交易可行性验证是指,对交易是否合理可执行进行验证,主要包括对支出用户的账户余额是否充足进行验证。此外,在实践中,根据实际业务规则,也可以对交易的其他事项也可以是可行性验证的内容,例如,支出用户是否有权限。若通过验证,则说明交易是合理可执行的。

[0043] 若指定成员节点针对交易请求进行可行性验证通过,则进行执行账户余额修改操作,也就是从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额,并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额。

[0044] S104:生成用于记录所述账户余额修改操作的日志文件,并向所述区块链网络广播所述日志文件。

[0045] 在本步骤S104中,指定成员节点可以生成用于记录上述账户余额修改操作的日志文件。此处需要说明的是,日志文件是用于记录软件系统(如windows系统、业务逻辑处理系统、数据库管理系统等)的操作事件的记录文件或文件集合,日志文件一般是是后缀名为.log的文件。

[0046] 所述指定成员节点生成所述日志文件后,可以向所述区块链网络广播所述日志文件,使得各成员节点基于共识机制将所述日志文件发布至区块链。

[0047] 此处需要说明的是,所述区块链网络并不需要根据所述日志文件,对所述交易请求的可行性进行验证。各成员节点基于共识机制,将所述日志文件发布至区块链即可。

[0048] 还需要说明的是,在本说明书实施例中,不对步骤S102和步骤S104的执行顺序进行限制。可以在执行步骤S102后,再执行步骤S104,也可以在执行步骤S104后,再执行步骤S102,还可以同时执行步骤S102和S104。

[0049] 通过图1所示的基于中心化结算与区块链存证的交易方法,针对一笔交易,所述指定成员节点执行交易结算时产生的日志文件会被发布至区块链进行存证,相当于中心化结算平台存储的用户账户的收支记录会被发布至区块链进行存证。因此,用户账户的收支记录难以被篡改,可以作为可信的对账凭证。

[0050] 图2a是本说明书实施例提供的一种基于中心化结算与区块链存证的交易方法的流程示例图。如图2a所示,区块链网络由多个(图中示出6个)成员节点组成,其中,实心点为指定成员节点,空心点为除指定成员节点外的其他成员节点。支出用户可以发起一笔交易,向指定成员节点发送交易请求,指定成员节点先在本地进行账户余额修改操作,并生成记录所述账户余额修改操作的日志文件,然后,将所述日志文件广播至全网,使得各成员节点将所述日志文件发布至自身的区块链。值得强调的是,指定成员节点需要对交易进行可行性验证,而所述区块链网络并不需要对交易进行可行性验证。

[0051] 此外,在本说明书实施例中,所述指定成员节点可以根据所述日志文件,采用哈希算法生成所述日志文件对应的日志文件摘要,然后向所述区块链网络广播所述日志文件和所述日志文件摘要,使得各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链。

[0052] 另外,所述指定成员节点可以将所述日志文件摘要发送给所述支出用户和/或所

述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0053] 众所周知，针对一段信息，执行哈希运算可以得到这段信息的摘要(一段字符串)，可以唯一标识这段信息。因此，所述日志文件摘要可以作为所述日志文件的标识，将所述日志文件摘要提供给所述支出用户和/或所述收入用户后，所述支出用户或所述收入用户就能够以所述日志文件摘要为线索，向区块链查询所述日志文件，以确定所述指定成员节点已经执行过所述账户余额修改操作。

[0054] 实践中，所述日志文件被广播给各成员节点之后，会被各成员节点分别存入自己的缓存中(或称交易池)中，当满足指定的共识触发条件时(如经过指定周期)，各成员节点会基于共识机制，选举一个成员节点从交易池中捞取若干日志文件和相应的日志文件摘要打包成区块，并将该区块向全网广播，使得各成员节点将该区块分别发布至区块链，至此，上述的日志文件和日志文件摘要才会被存证。

[0055] 因此，进一步地，在本说明书实施例中，所述指定成员节点可以在确定所述日志文件被发布至区块链之后，再将所述日志文件摘要发送给所述支出用户和/或所述收入用户。

[0056] 这种情况下，支出用户和/或收入用户当接收到指定成员节点发送的日志文件摘要时，意味着交易成功。若支出用户和/或收入用户未接收到所述日志文件摘要，则哪怕所述指定成员节点已经执行了账户余额修改操作，也并不意味着交易成功(因为日志文件还未被发布至区块链)。

[0057] 此外，所述指定成员节点也可以在确定所述日志文件被打包进区块之后，将所述日志文件摘要发送给所述支出用户和/或所述收入用户。

[0058] 另外，所述指定成员节点可以包括业务逻辑执行模块、数据库管理模块和区块链功能模块。

[0059] 其中，所述业务逻辑执行模块负责向外对接用户，根据用户的业务请求处理业务，所述业务逻辑执行模块通常是安装于所述指定成员节点上的软件，也可以是所述指定成员节点的硬件组成部分。

[0060] 所述数据库管理模块负责对所述指定成员节点的本地数据库进行管理，如修改数据库中的数据。所述数据库管理模块通常是安装于所述指定成员节点上的软件，也可以是所述指定成员节点的硬件组成部分。

[0061] 所述区块链功能模块是所述执行成员节点接入所述区块链网络的接口，其通常是安装于所述指定成员节点上的软件，也可以是所述指定成员节点的硬件组成部分。

[0062] 如此，在步骤S100中，所述指定成员节点可以通过所述业务逻辑执行模块接收所述交易请求。在步骤S102中，所述指定成员节点通过所述业务逻辑执行模块，根据所述交易请求，进行交易可行性验证。若验证通过，则通过所述数据库管理模块，执行账户余额修改操作。

[0063] 在步骤S104中，所述指定成员节点可以通过业务逻辑执行模块生成所述日志文件(参见图2b)，也可以通过所述数据库管理模块生成所述日志文件(参见图2c)。接着，所述指定成员节点可以通过所述区块链功能模块，向所述区块链网络广播所述日志文件，并随后通过所述区块链功能模块，将所述日志文件发布至自身的区块链。

[0064] 图3是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的

流程示意图，包括以下步骤：

[0065] S300：所述业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求。

[0066] 在图3所示的方法中，区块链网络包括若干成员节点，用户在指定成员节点上注册有虚拟资源账户，所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块。

[0067] S302：所述业务逻辑执行模块根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令。

[0068] S304：所述数据库管理模块根据所述账户余额修改指令，在数据库中执行账户余额修改操作。

[0069] 在图3所示的方法中，由所述业务逻辑执行模块负责受理交易请求以及执行模块负责进行交易可行性验证。验证通过后，业务逻辑执行模块可以指令数据库管理模块执行账户余额修改操作，即从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额。

[0070] S306：所述业务逻辑执行模块生成用于记录所述账户余额修改操作的日志文件，以及将所述日志文件发送给所述区块链功能模块。

[0071] 在图3所示的方法中，所述业务逻辑执行模块负责生成所述日志文件，并将生成的日志文件发送给所述区块链功能模块。

[0072] 具体地，可以预先在业务逻辑执行模块中写入日志文件生成逻辑，交由所述业务逻辑执行模块执行。所述日志文件生成逻辑可以不仅包含记录所述账户余额修改操作的逻辑，也可以包含记录其他交易相关信息(如交易时间、交易地点、交易附言等信息)的逻辑。

[0073] 在图3所示的方法中，所述数据库管理模块执行所述账户余额修改操作后，可以向所述业务逻辑执行模块返回修改成功通知。所述业务逻辑执行模块在接收到所述修改成功通知后，方可生成用于记录所述账户余额修改操作的日志文件。

[0074] S308：所述区块链功能模块向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0075] 在步骤S308中，由区块链功能模块负责向区块链网络广播所述日志文件。

[0076] 此外，在步骤S308中，所述区块链功能模块具体可以根据所述日志文件，采用哈希算法，生成所述日志文件对应的日志文件摘要，然后向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链。

[0077] 所述区块链功能模块可以将所述日志文件摘要发送给将所述日志文件摘要发送给所述业务逻辑执行模块，然后，所述业务逻辑执行模块将所述日志文件摘要所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0078] 进一步地，所述区块链功能模块若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述业务逻辑执行模块。

[0079] 针对图3所示的方法，需要说明的是，由所述业务逻辑执行模块负责生成所述日志文件，无须对业务逻辑执行模块进行复杂的改造，仅需要在业务逻辑执行模块中写入日志

文件生成逻辑即可。此外，由所述业务逻辑执行模块负责生成所述日志文件，还可以实现对日志文件的内容的定制化，如此，所述日志文件不仅用于记录所述账户余额修改操作，还可以用于记录其他交易相关信息。

[0080] 图4是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易方法的流程示意图，包括以下步骤：

[0081] S400：所述业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求。

[0082] 在图4所示的方法中，区块链网络包括若干成员节点，用户在指定成员节点上注册有虚拟资源账户，所述指定成员节点包括业务逻辑执行模块、数据库管理模块和区块链功能模块。

[0083] S402：所述业务逻辑执行模块根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令。

[0084] S404：所述数据库管理模块根据所述账户余额修改指令，执行账户余额修改操作，并生成用于记录所述账户余额修改操作的日志文件。

[0085] 在图4所示的方法中，由所述业务逻辑执行模块负责受理交易请求以及执行模块负责进行交易可行性验证。验证通过后，业务逻辑执行模块可以指令数据库管理模块执行账户余额修改操作，即从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额。

[0086] 在图4所示的方法中，所述数据库管理模块负责生成所述日志文件，并将生成的日志文件发送给所述区块链功能模块。

[0087] 为本领域技术人员所熟知的是，所述数据库管理模块在针对数据库进行数据修改时，为了保证事务的原子性，一般首先生成记录有数据修改操作的数据库日志，再根据该数据库日志执行数据修改操作。

[0088] 由此可见，在图4所示的方法中，所述日志文件即是所述数据库日志。并且，所述数据库管理模块可以在执行所述账户余额修改操作之前，生成所述日志文件。

[0089] S406：所述数据库管理模块将所述日志文件发送给所述区块链功能模块。

[0090] S408：所述区块链功能模块向所述区块链网络广播所述日志文件。

[0091] 在步骤S408中，所述区块链功能模块根据所述日志文件，采用哈希算法，生成所述日志文件对应的日志文件摘要，然后向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链。

[0092] 所述区块链功能模块可以将所述日志文件摘要发送给所述数据库管理模块，然后所述数据库管理模块将所述日志文件摘要发送给所述业务逻辑执行模块，所述业务逻辑执行模块将所述日志文件摘要发送给所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0093] 进一步地，所述区块链功能模块若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述数据库管理模块。此外，所述指定成员节点也可以在确定所述日志文件被打包进区块之后，将所述日志文件摘要发送给所述支出用户和/或所述收入用户。

[0094] 此外需要说明的是，所述数据库管理模块可以在执行账户余额修改操作后，立即向所述业务逻辑执行模块返回修改成功通知，也可以在执行账户余额修改操作后，暂时不

返回修改成功通知，而是待到接收到所述区块链功能模块返回的日志文件摘要后，将所述修改成功通知与所述日志文件摘要一并返回给业务逻辑执行模块。

[0095] 基于图1所示的基于中心化结算与区块链存证的交易方法，本说明书实施例还对应提供了一种基于中心化结算与区块链存证的交易设备，如图5所示，区块链网络包括若干成员节点，所述设备为任一成员节点，用户在所述设备上注册有虚拟资源账户，所述设备包括：

[0096] 接收模块501，接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求；所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；

[0097] 结算模块502，根据所述交易请求，进行交易可行性验证，并在验证通过后，执行账户余额修改操作；所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；

[0098] 存证模块503，生成用于记录所述账户余额修改操作的日志文件，并向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0099] 所述存证模块503，根据所述日志文件，采用哈希算法生成所述日志文件对应的日志文件摘要；向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链；

[0100] 所述设备还包括：发送模块504，将所述日志文件摘要发送给所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0101] 所述发送模块504，若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述支出用户和/或所述收入用户。

[0102] 基于图3所示的基于中心化结算与区块链存证的交易方法，本说明书实施例还对应提供了一种基于中心化结算与区块链存证的交易设备，如图6所示，区块链网络包含若干成员节点，所述设备为任一成员节点，用户在所述设备上注册有虚拟资源账户，所述设备包括业务逻辑执行模块601、数据库管理模块602和区块链功能模块603；

[0103] 所述业务逻辑执行模块601，接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求，所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令；生成用于记录账户余额修改操作的日志文件，并将所述日志文件发送给所述区块链功能模块；所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；

[0104] 所述数据库管理模块602，根据所述账户余额修改指令，执行账户余额修改操作；

[0105] 所述区块链功能模块603，向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0106] 所述业务逻辑执行模块601，生成用于记录所述账户余额修改操作和记录其他交易相关信息的日志文件。

[0107] 所述数据库管理模块602，执行所述账户余额修改操作后，向所述业务逻辑执行模块返回修改成功通知；

[0108] 所述业务逻辑执行模块601，在接收到所述修改成功通知后，生成用于记录所述账户余额修改操作的日志文件。

[0109] 所述区块链功能模块603，根据所述日志文件，采用哈希算法，生成所述日志文件对应的日志文件摘要；向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链；将所述日志文件摘要发送给所述业务逻辑执行模块；

[0110] 所述业务逻辑执行模块601，将所述日志文件摘要发送给所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0111] 所述区块链功能模块603，若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述业务逻辑执行模块。

[0112] 基于图4所示的基于中心化结算与区块链存证的交易方法，本说明书实施例还对应提供了一种基于中心化结算与区块链存证的交易设备，如图7所示，区块链网络包含若干成员节点，所述设备为任一成员节点，用户在所述设备上注册有虚拟资源账户，所述设备包括业务逻辑执行模块701、数据库管理模块702和区块链功能模块703；

[0113] 所述业务逻辑执行模块701，接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求；所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令；

[0114] 所述数据库管理模块702，根据所述账户余额修改指令，执行账户余额修改操作，并生成用于记录所述账户余额修改操作的日志文件，所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；将所述日志文件发送给所述区块链功能模块；

[0115] 所述区块链功能模块703，向所述区块链网络广播所述日志文件，以使各成员节点基于共识机制将所述日志文件发布至区块链。

[0116] 所述区块链功能模块703，根据所述日志文件，采用哈希算法，生成所述日志文件对应的日志文件摘要；向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链；将所述日志文件摘要发送给所述数据库管理模块；

[0117] 所述数据库管理模块702，将所述日志文件摘要发送给所述业务逻辑执行模块；

[0118] 所述业务逻辑执行模块701，将所述日志文件摘要发送给所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0119] 所述区块链功能模块703，若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述数据库管理模块。

[0120] 所述数据库管理模块702，将所述日志文件摘要和修改成功通知一并发送给所述业务逻辑执行模块。

[0121] 图8是本说明书实施例提供的一种基于中心化结算与区块链存证的交易系统的结构示意图，包括由若干成员节点组成的区块链网络，用户可在指定成员节点上注册虚拟资源账户；

[0122] 所述指定成员节点，接收的包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求，所述支出用户是支出所述指定资源数额的用户，所述收入用户是收入所述指定资源数额的用户；根据所述交易请求，进行交易可行性验证，并在验证通过后，执行账户余额修改操作，所述账户余额修改操作为，从所述支出用户标识对应的虚拟资源账户中扣除所述指定资源数额，并向所述收入用户标识对应的虚拟资源账户中增加所述指定资源数额；生成用于记录所述账户余额修改操作的日志文件，并向所述区块链网络广播所述日志文件；

[0123] 其他成员节点，与所述指定成员节点基于共识机制，将所述日志文件发布至区块链。

[0124] 所述指定成员节点，根据所述日志文件，采用哈希算法生成所述日志文件对应的日志文件摘要；向所述区块链网络广播所述日志文件和所述日志文件摘要，以使各成员节点基于共识机制将所述日志文件和所述日志文件摘要发布至区块链；将所述日志文件摘要发送给所述支出用户和/或所述收入用户，以便所述支出用户和/或所述收入用户使用所述日志文件摘要向区块链查询所述日志文件。

[0125] 所述指定成员节点，若确定所述日志文件被发布至区块链，则将所述日志文件摘要发送给所述支出用户和/或所述收入用户。

[0126] 图9是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易系统的结构示意图，包括由若干成员节点组成的区块链网络，其中，各成员节点中包含图6所示的设备，用户在所述设备上注册有虚拟资源账户。

[0127] 图10是本说明书实施例提供的另一种基于中心化结算与区块链存证的交易系统的结构示意图，包括由若干成员节点组成的区块链网络，其中，各成员节点中包含图7所示的设备，用户在所述设备上注册有虚拟资源账户。

[0128] 本说明书实施例还提供一种计算机设备，区块链网络包括若干成员节点，所述设备为任一成员节点，用户在所述设备上注册有虚拟资源账户；

[0129] 所述设备至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现图1所述方法的功能。

[0130] 图11示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器1110、存储器1120、输入/输出接口1130、通信接口1140和总线1150。其中处理器1110、存储器1120、输入/输出接口1130和通信接口1140通过总线1150实现彼此之间在设备内部的通信连接。

[0131] 处理器1110可以采用通用的CPU(Central Processing Unit，中央处理器)、微处理器、应用专用集成电路(Application Specific Integrated Circuit，ASIC)、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[0132] 存储器1120可以采用ROM(Read Only Memory，只读存储器)、RAM(Random Access Memory，随机存取存储器)、静态存储设备，动态存储设备等形式实现。存储器1120可以存储

操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器1120中，并由处理器1110来调用执行。

[0133] 输入/输出接口1130用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中(图中未示出)，也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[0134] 通信接口1140用于连接通信模块(图中未示出)，以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如USB、网线等)实现通信，也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

[0135] 总线1150包括一通路，在设备的各个组件(例如处理器1110、存储器1120、输入/输出接口1130和通信接口1140)之间传输信息。

[0136] 需要说明的是，尽管上述设备仅示出了处理器1110、存储器1120、输入/输出接口1130、通信接口1140以及总线1150，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[0137] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现图1所述方法的功能。

[0138] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0139] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[0140] 上述实施例阐明的系统、方法、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0141] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于设备和设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法

实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0142] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。

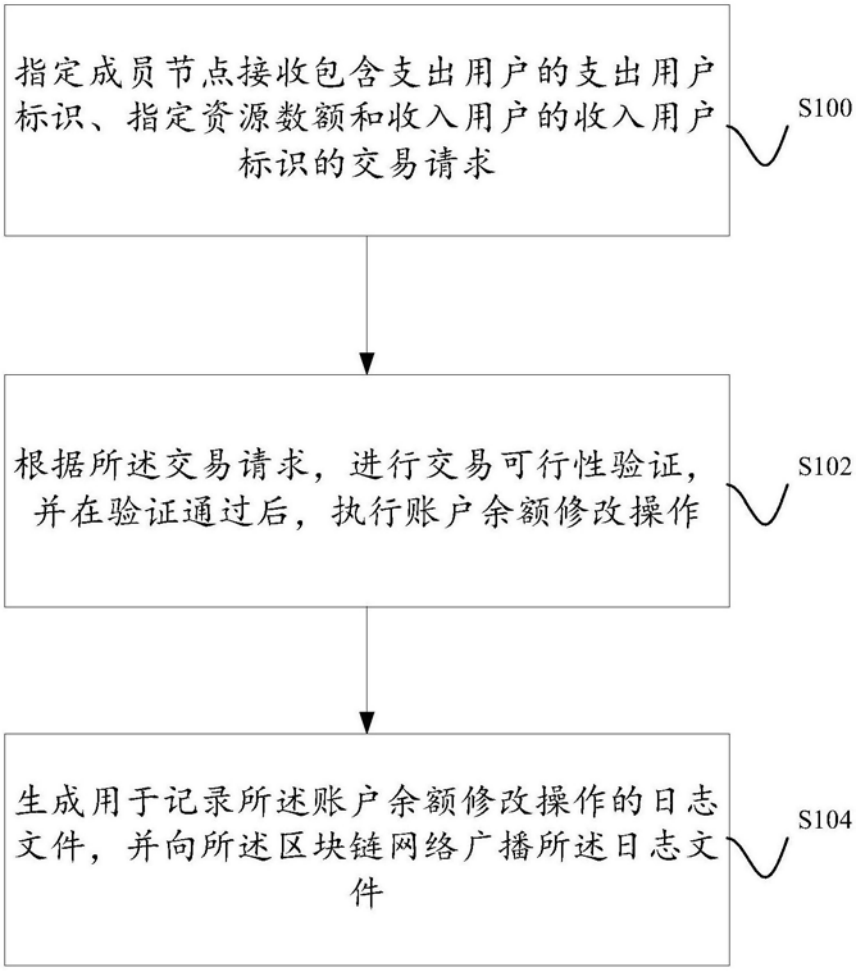

指定成员节点接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求
S100
根据所述交易请求，进行交易可行性验证，并在验证通过后，执行账户余额修改操作
S102
生成用于记录所述账户余额修改操作的日志文件，并向所述区块链网络广播所述日志文件
S104

图1

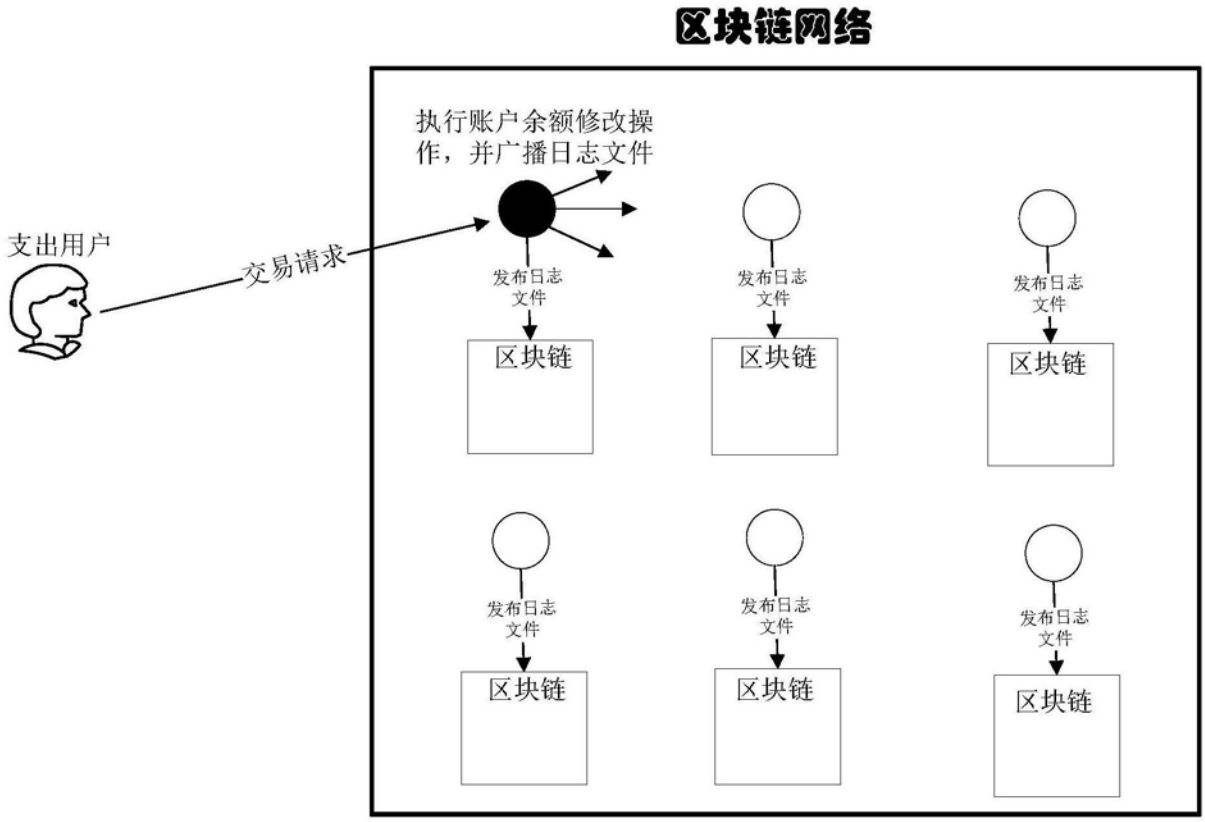

区块链网络
执行账户余额修改操作，并广播日志文件
支出用户
交易请求
发布日志文件
区块链
发布日志文件
区块链
发布日志文件
区块链
发布日志文件
区块链
发布日志文件
区块链
发布日志文件
区块链

图2a

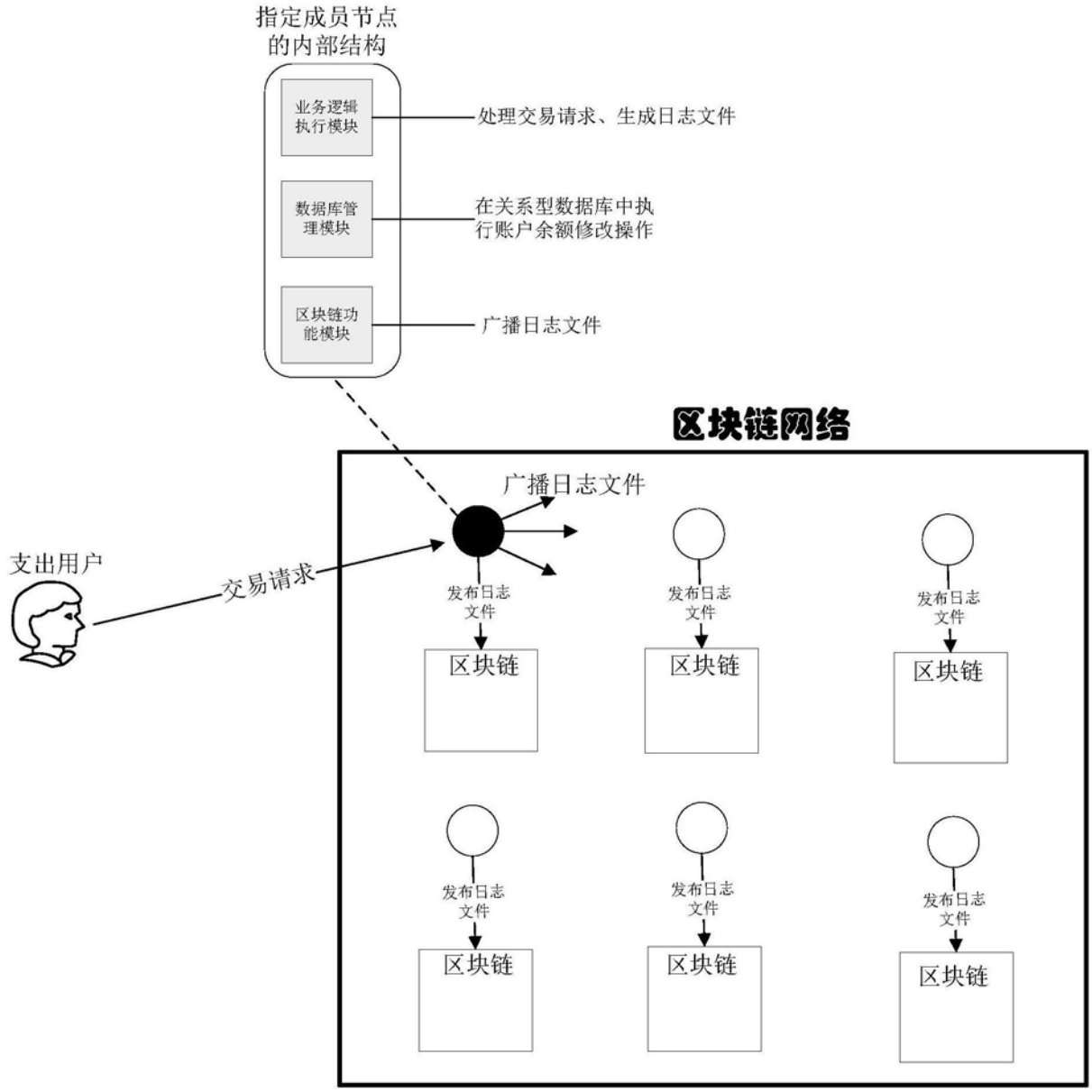

指定成员节点
的内部结构
业务逻辑
执行模块
处理交易请求、生成日志文件
数据库管
理模块
在关系型数据库中执
行账户余额修改操作
区块链功
能模块
广播日志文件
区块链网络
广播日志文件
支出用户
交易请求
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链

图2b

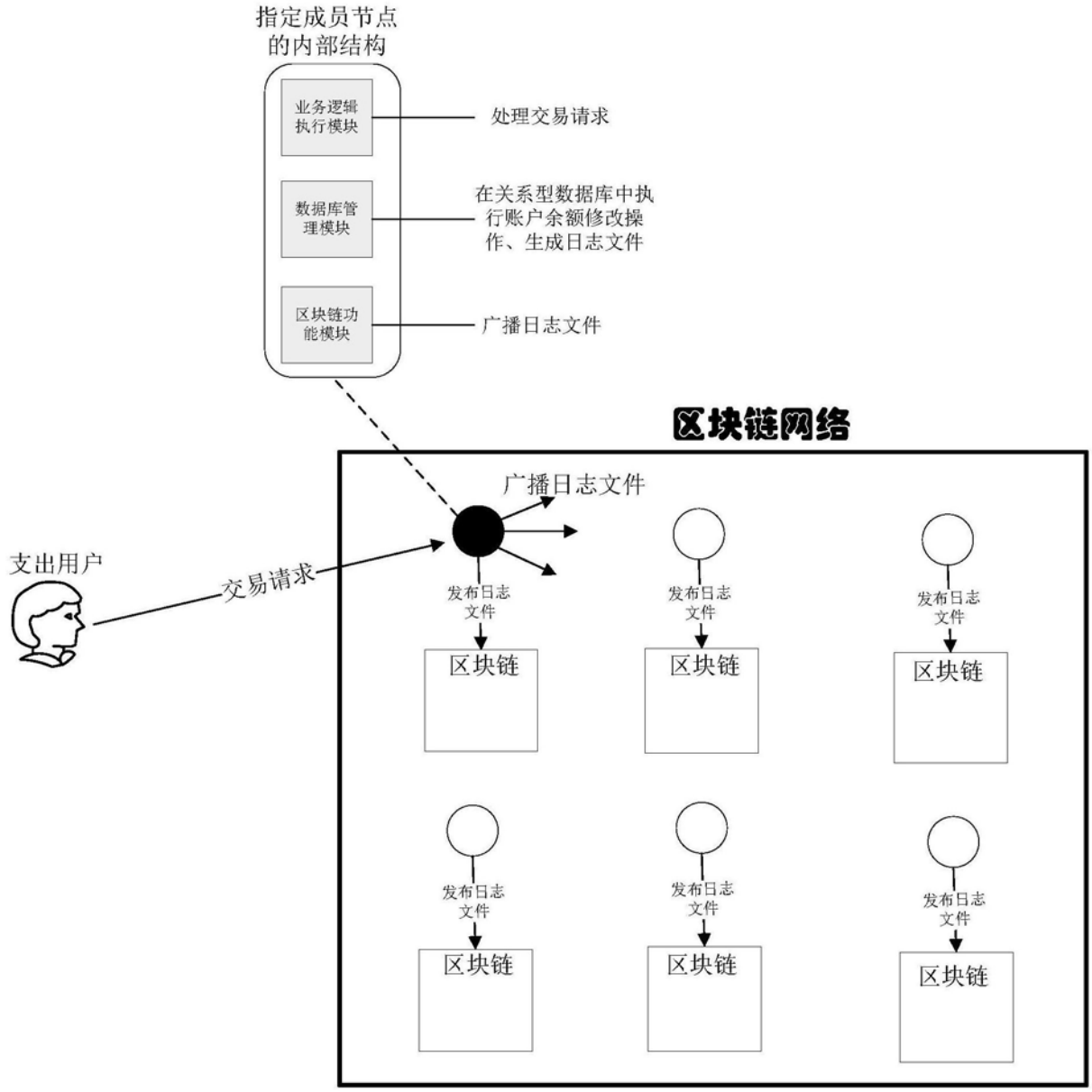

指定成员节点
的内部结构
业务逻辑
执行模块
处理交易请求
数据库管
理模块
在关系型数据库中执
行账户余额修改操
作、生成日志文件
区块链功
能模块
广播日志文件
区块链网络
广播日志文件
支出用户
交易请求
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链
发布日志
文件
区块链

图2c

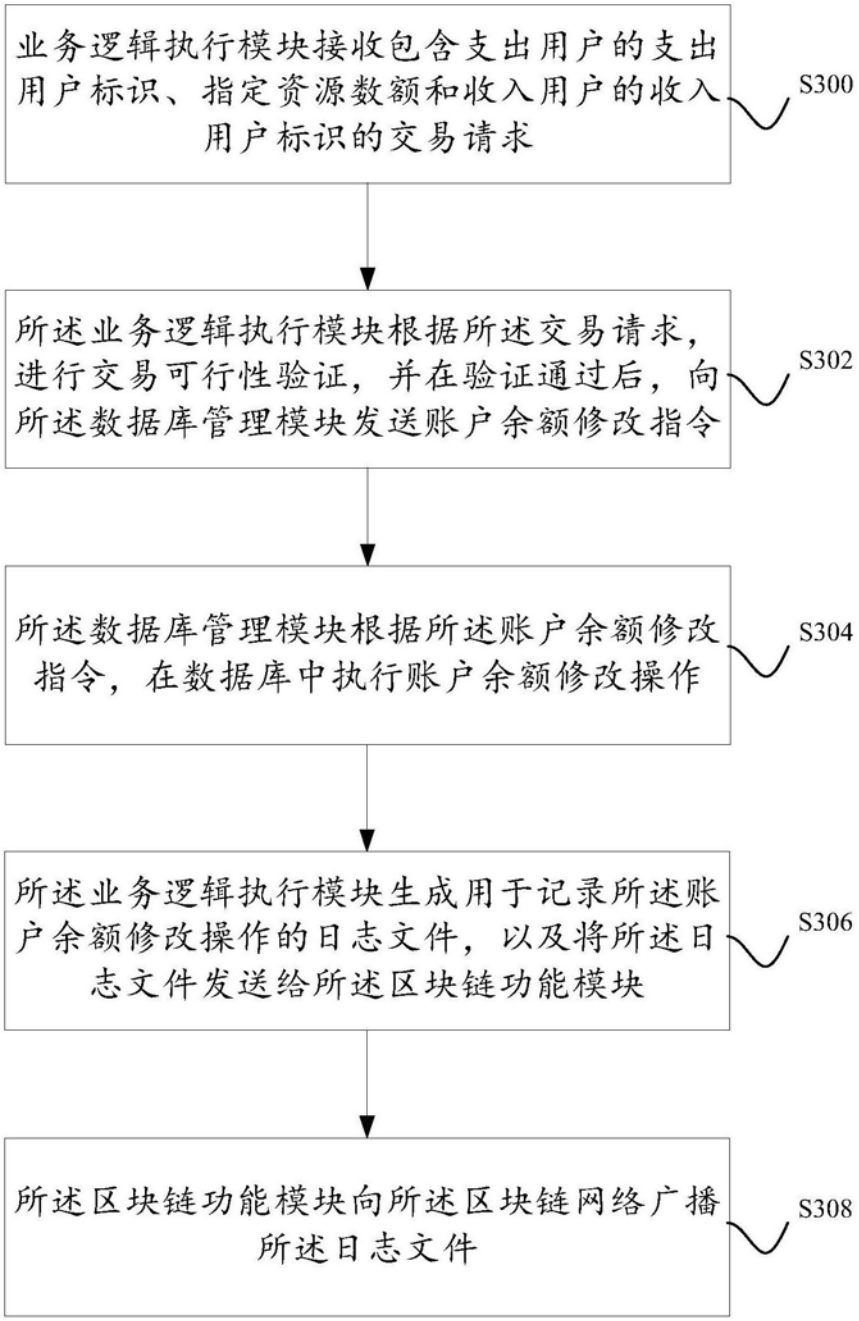

业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求
S300
所述业务逻辑执行模块根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令
S302
所述数据库管理模块根据所述账户余额修改指令，在数据库中执行账户余额修改操作
S304
所述业务逻辑执行模块生成用于记录所述账户余额修改操作的日志文件，以及将所述日志文件发送给所述区块链功能模块
S306
所述区块链功能模块向所述区块链网络广播所述日志文件
S308

图3

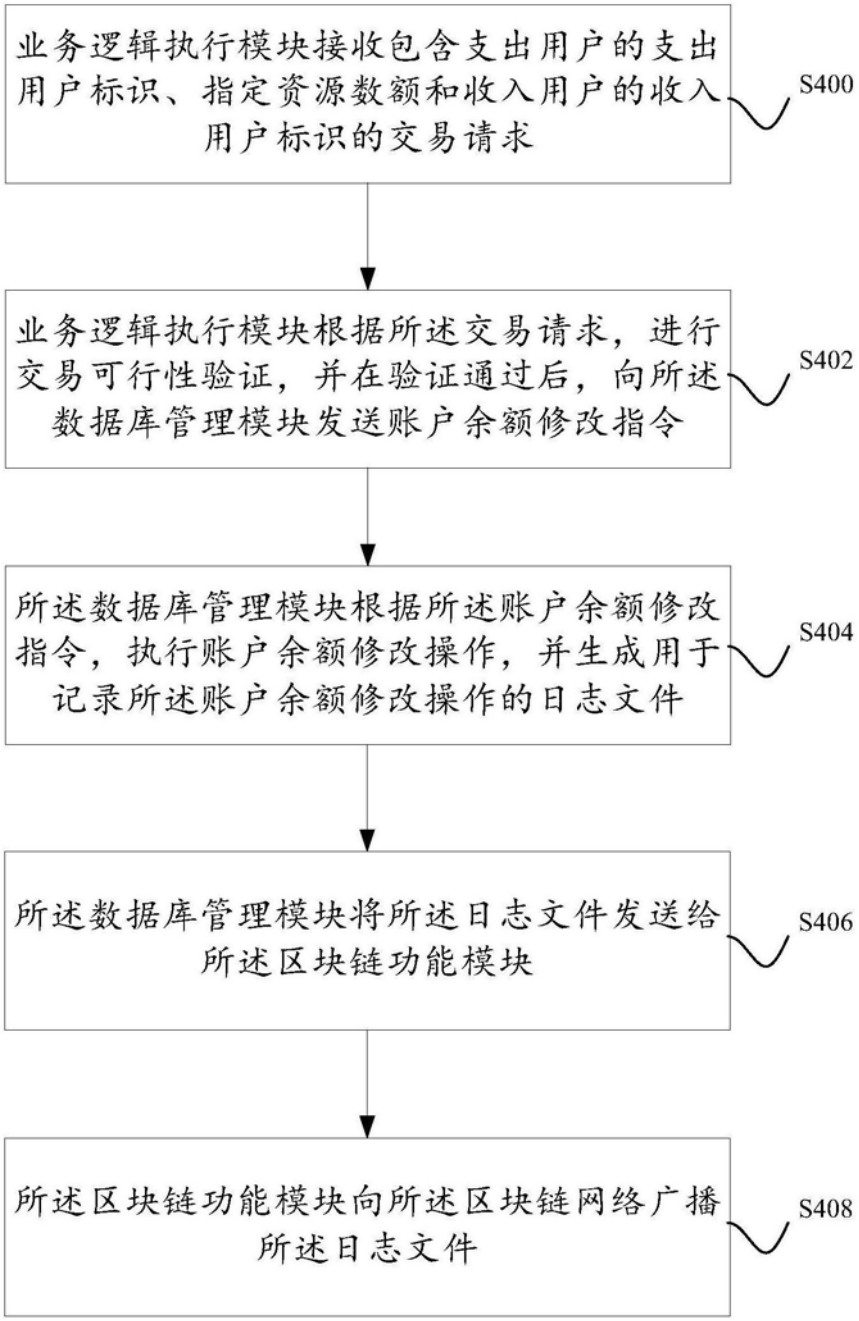

业务逻辑执行模块接收包含支出用户的支出用户标识、指定资源数额和收入用户的收入用户标识的交易请求
S400
业务逻辑执行模块根据所述交易请求，进行交易可行性验证，并在验证通过后，向所述数据库管理模块发送账户余额修改指令
S402
所述数据库管理模块根据所述账户余额修改指令，执行账户余额修改操作，并生成用于记录所述账户余额修改操作的日志文件
S404
所述数据库管理模块将所述日志文件发送给所述区块链功能模块
S406
所述区块链功能模块向所述区块链网络广播所述日志文件
S408

图4

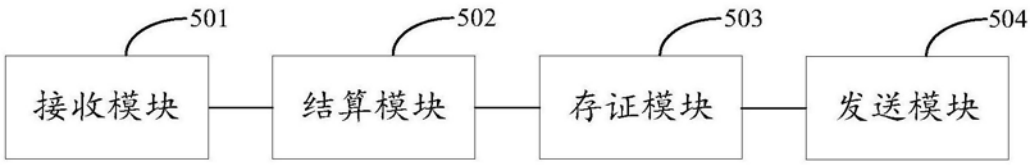

501
接收模块
502
结算模块
503
存证模块
504
发送模块

图5

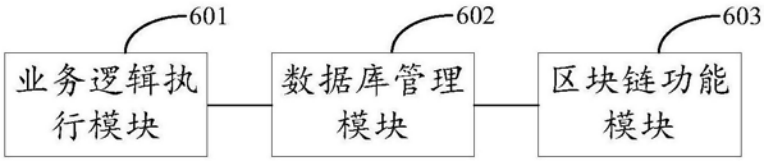

601
602
603
业务逻辑执行模块
数据库管理模块
区块链功能模块

图6

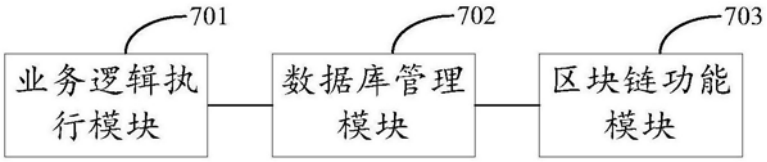

701
702
703
业务逻辑执行模块
数据库管理模块
区块链功能模块

图7

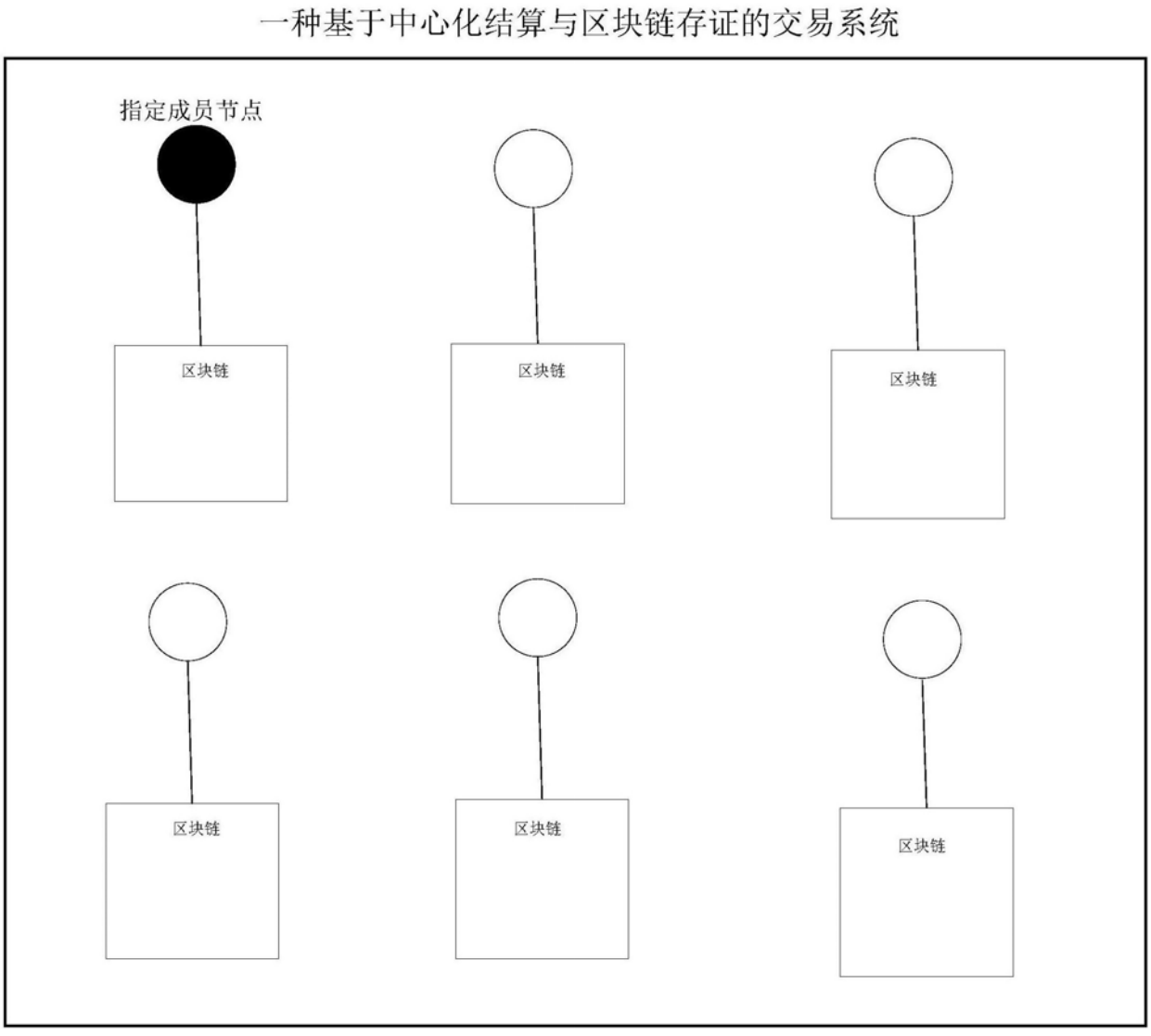

一种基于中心化结算与区块链存证的交易系统
指定成员节点
区块链
区块链
区块链
区块链
区块链
区块链

图8

一种基于中心化结算与区块链存证的交易系统

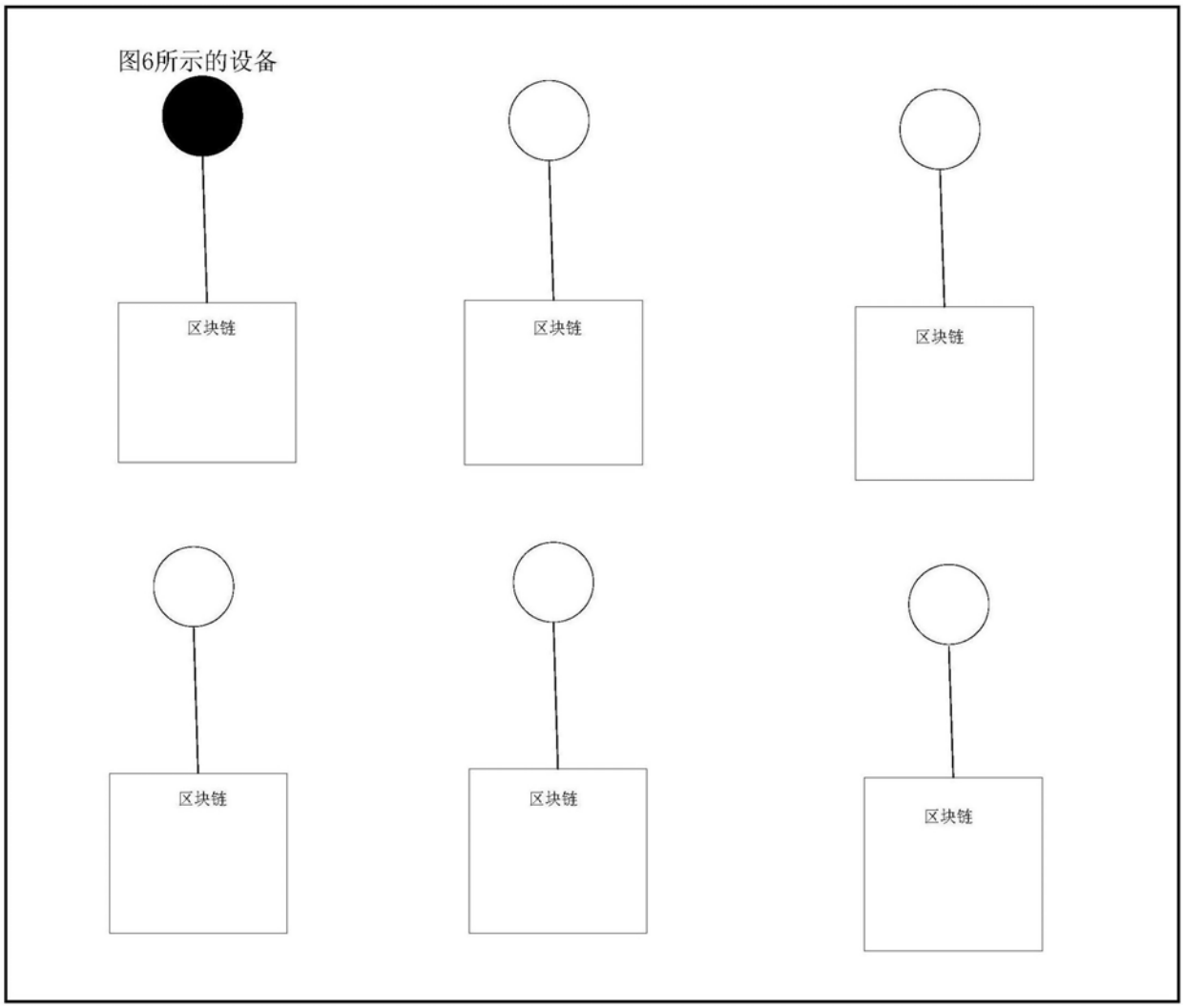


图9

一种基于中心化结算与区块链存证的交易系统

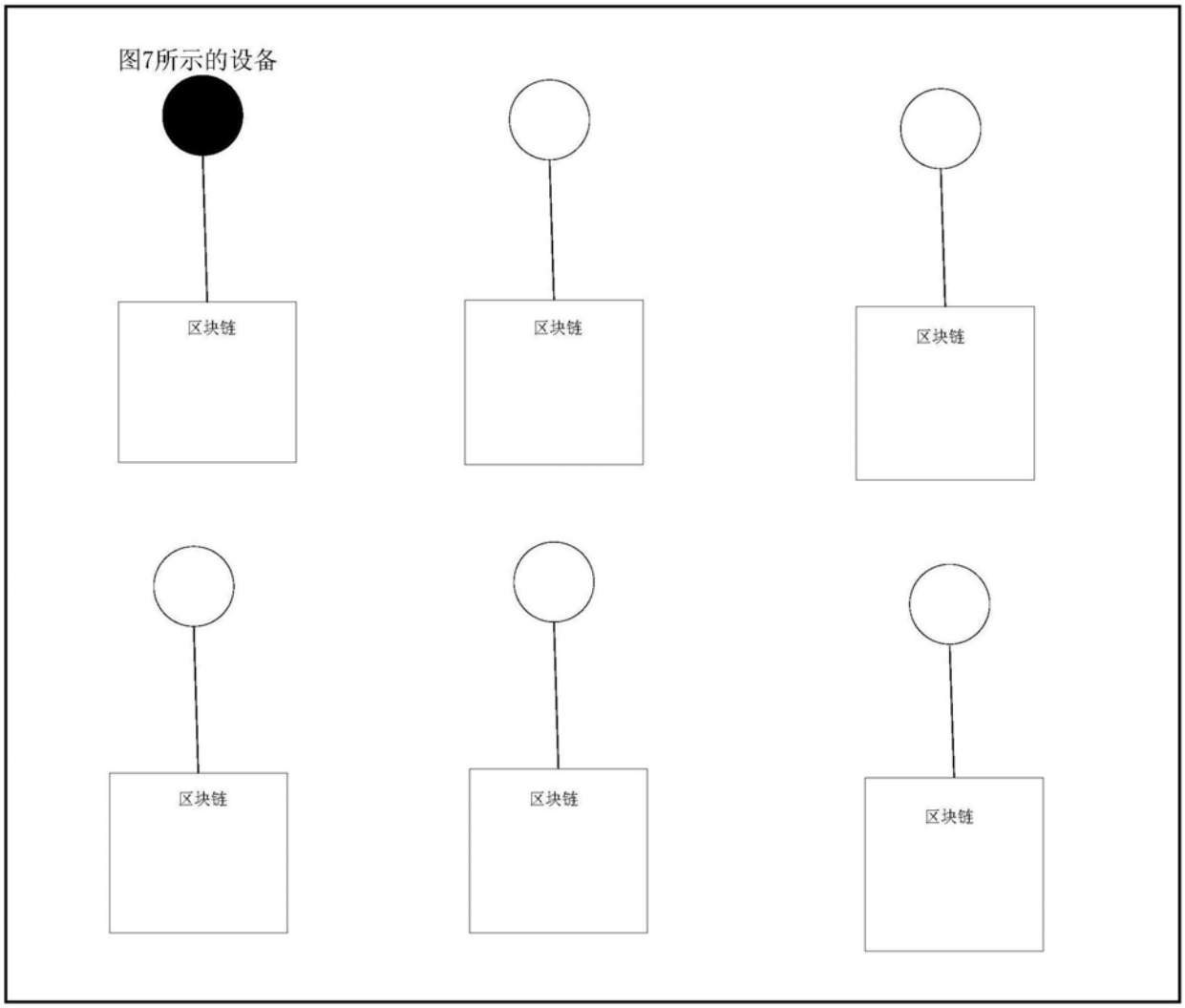


图10

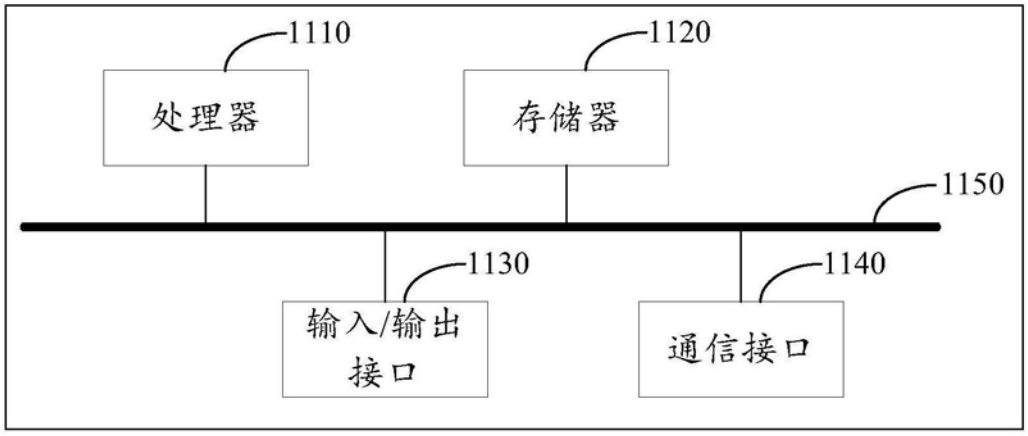


图11