(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109756582 B
(45)授权公告日 2022.08.12

(21)申请号 201910197771.7

(22)申请日 2019.03.15

(65)同一申请的已公布的文献号
申请公布号 CN 109756582 A

(43)申请公布日 2019.05.14

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 李茂材 王宗友 蓝虎 杨常青 周开班 时一防 刘区城 张劲松 陈秋平 朱耿良 孔利

(74)专利代理机构 深圳市联鼎知识产权代理有限公司 44232
专利代理师 刘抗美

(51)Int.Cl.
H04L 67/1097(2022.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
G06Q 40/04(2012.01)

(56)对比文件
CN 108764874 A,2018.11.06
CN 108764874 A,2018.11.06
CN 109447648 A,2019.03.08
CN 107911216 A,2018.04.13
US 2017243177 A1,2017.08.24

审查员 王田

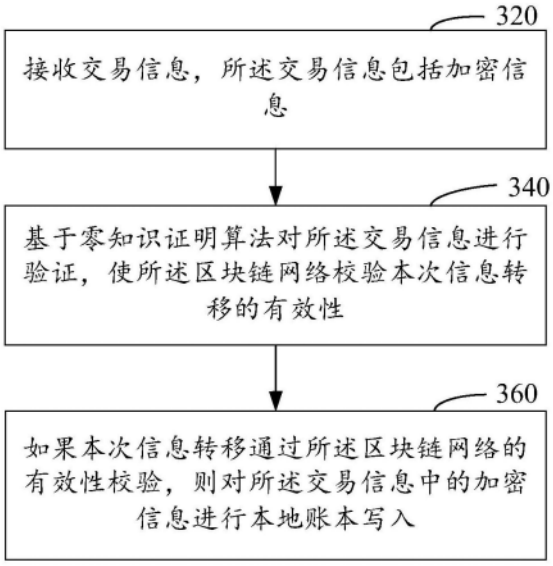
权利要求书3页 说明书15页 附图11页

(54)发明名称

区块链网络中的信息记录方法、装置、节点及存储介质

(57)摘要

本发明公开了一种区块链网络中的信息记录方法、装置、节点及存储介质，所述区块链网络中的信息记录方法包括：接收交易信息，所述交易信息包括加密信息，所述加密信息是利用加密密钥对发送方转移至接收方的信息进行加密生成的；基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性；如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入。采用本发明所提供的区块链网络中的信息记录方法、装置、节点及存储介质解决了现有技术中信息转移的私密性不足的问题。



CN 109756582 B

1.一种区块链网络中的信息记录方法，其特征在于，所述方法应用于区块链网络和业务网络共同组成的通信网络，所述区块链网络包括区块链节点，所述业务网络包括业务节点，所述方法由所述区块链节点和所述业务节点相互配合执行，所述方法包括：

所述业务节点获取发送方的私钥和公钥，以及获取接收方的私钥和公钥，并基于共享密钥交换算法，根据所述发送方的私钥和所述接收方的公钥生成加密密钥，以及根据所述接收方的私钥和所述发送方的公钥生成解密密钥；根据所述加密密钥对所述发送方待转移至所述接收方的信息进行加密，得到加密信息；对所述加密信息进行零知识证明处理，生成交易信息；在所述区块链网络中广播所述交易信息，使所述区块链网络中的所述区块链节点获取到所述交易信息；其中，根据所述加密密钥对所述发送方待转移至所述接收方的信息进行加密，得到加密信息，包括：从所述发送方待转移至所述接收方的信息中提取得到待隐藏信息，所述待隐藏信息包括发送方标识、接收方标识、资源转移份额；利用所述加密密钥加密所述待隐藏信息，得到隐藏信息；以所述隐藏信息替代所述待隐藏信息，存储至待转移至所述接收方的信息，形成所述加密信息；

所述区块链节点接收所述交易信息，并基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性；如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入；

在所述区块链节点记录所述加密信息之后，所述业务节点基于所述解密密钥的解密操作，由所述加密信息得到所述发送方待转移至所述接收方的信息，并将得到的信息反馈至所述接收方。

2.如权利要求1所述的方法，其特征在于，所述业务节点获取发送方的私钥和公钥，以及获取接收方的私钥和公钥，包括：

基于所述发送方的私钥，确定所述发送方的公钥；

进行所述发送方的公钥与所述接收方的公钥之间的交换，得到所述接收方的公钥。

3.如权利要求2所述的方法，其特征在于，所述基于所述发送方的私钥，确定所述发送方的公钥之前，所述方法还包括：

根据非对称加密算法生成非对称密钥对，所述非对称密钥对包括所述发送方的公钥和所述发送方的私钥。

4.如权利要求1所述的方法，其特征在于，所述对所述加密信息进行零知识证明处理，生成所述交易信息，包括：

对所述加密信息相关的发送方信息进行加密，得到发送方数据；

对所述加密信息相关的接收方信息进行加密，得到接收方数据；

基于所述零知识证明算法，由所述发送方数据和所述接收方数据计算得到证明数据；

将所述发送方数据、所述接收方数据和所述证明数据封装，得到所述交易信息。

5.如权利要求1所述的方法，其特征在于，所述基于零知识证明算法对所述交易信息进行验证之后，所述方法还包括：

如果所述交易信息通过验证，则生成确认消息；

根据所述确认消息，请求所述区块链网络针对本次信息转移的有效性进行共识；

当共识成功后，本次信息转移通过所述区块链网络的有效性校验。

6.如权利要求5所述的方法，其特征在于，所述根据所述确认消息，请求所述区块链网

络针对本次信息转移的有效性进行共识之后，所述方法还包括：

接收所述区块链网络中所述节点反馈的确认消息；

如果接收到的确认消息的数量超过设定阈值，则判定共识成功。

7.如权利要求1至6任一项所述的方法，其特征在于，所述方法还包括：从所述区块链网络中选取进行所述交易信息接收的区块链节点；

所述从所述区块链网络中选取进行所述交易信息接收的区块链节点，包括：

基于所述区块链网络中各区块链节点的运行状况，获取所述区块链网络中各区块链节点的运行数据；

确定所述区块链网络中各区块链节点与所述发送方之间的物理距离；

根据所述运行数据和所述物理距离，对所述区块链网络中各区块链节点进行筛选，得到进行所述交易信息接收的区块链节点。

8.如权利要求7所述的方法，其特征在于，所述根据所述运行数据和所述物理距离，对所述区块链网络中各区块链节点进行筛选，得到进行所述交易信息接收的区块链节点，包括：

基于所述区块链网络中各区块链节点的运行数据，确定每一个区块链节点的第一分数；

基于所述区块链网络中各区块链节点与所述发送方之间的物理距离，确定每一个区块链节点的第二分数；

对每一个区块链节点的第一分数和第二分数进行加权求和，得到每一个区块链节点的总分数；

选取总分数最大的区块链节点作为进行所述交易信息接收的区块链节点。

9.一种区块链网络中的信息记录装置，其特征在于，所述装置部署于区块链网络和业务网络共同组成的通信网络，所述区块链网络包括区块链节点，所述业务网络包括业务节点，所述装置部署于所述区块链节点和所述业务节点；

所述装置包括：

交易信息生成模块，用于所述业务节点获取发送方的私钥和公钥，以及获取接收方的私钥和公钥，并基于共享密钥交换算法，根据所述发送方的私钥和所述接收方的公钥生成加密密钥，以及根据所述接收方的私钥和所述发送方的公钥生成解密密钥；根据所述加密密钥对所述发送方待转移至所述接收方的信息进行加密，得到加密信息；对所述加密信息进行零知识证明处理，生成交易信息；在所述区块链网络中广播所述交易信息，使所述区块链网络中的所述区块链节点获取到所述交易信息；其中，根据所述加密密钥对所述发送方待转移至所述接收方的信息进行加密，得到加密信息，包括：从所述发送方待转移至所述接收方的信息中提取得到待隐藏信息，所述待隐藏信息包括发送方标识、接收方标识、资源转移份额；利用所述加密密钥加密所述待隐藏信息，得到隐藏信息；以所述隐藏信息替代所述待隐藏信息，存储至待转移至所述接收方的信息，形成所述加密信息；

交易信息处理模块，用于所述区块链节点接收交易信息，并基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性；如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入；

信息反馈模块，用于在所述区块链节点记录所述加密信息之后，所述业务节点基于所

述解密密钥的解密操作，由所述加密信息得到所述发送方待转移至所述接收方的信息，并将得到的信息反馈至所述接收方。

10.一种节点，其特征在于，包括：

处理器；及

存储器，所述存储器上存储有计算机可读指令，所述计算机可读指令被所述处理器执行时实现如权利要求1至8中任一项所述的区块链网络中的信息记录方法。

11.一种存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至8中任一项所述的区块链网络中的信息记录方法。

区块链网络中的信息记录方法、装置、节点及存储介质

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种区块链网络中的信息记录方法、装置、节点及存储介质。

背景技术

[0002] 随着区块链技术的发展，商户可以借由区块链网络实现信息转移，例如，商户A向商户B发起报销请求，商户B响应于报销请求开具电子发票，并借由区块链网络转移至商户A，同时通过该区块链网络中的节点记录本次电子发票转移事件。

[0003] 对于区块链网络而言，由于每一个节点对信息转移进行了记录，也即是说，无论是否属于信息转移的直接参与方，例如商户A或者商户B，区块链网络中的任何一个节点都能够查看到所有的历史信息转移记录，而导致信息转移的私密性不足。

发明内容

[0004] 为了解决相关技术中存在的信息转移的私密性不足的问题，本发明各实施例提供一种区块链网络中的信息记录方法、装置、节点及存储介质。

[0005] 其中，本发明所采用的技术方案为：

[0006] 根据本发明实施例的一方面，一种区块链网络中的信息记录方法，所述区块链网络包括节点，所述方法由所述节点执行，所述方法包括：接收交易信息，所述交易信息包括加密信息，所述加密信息是利用加密密钥对发送方转移至接收方的信息进行加密生成的；基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性；如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入。

[0007] 根据本发明实施例的一方面，一种区块链网络中的信息记录装置，所述区块链网络包括节点，所述装置部署于所述节点，所述装置包括：信息接收模块，用于接收交易信息，所述交易信息包括加密信息，所述加密信息是利用加密密钥对发送方转移至接收方的信息进行加密生成的；信息验证模块，用于基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性；信息记录模块，用于如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入。

[0008] 根据本发明实施例的一方面，一种节点，包括处理器及存储器，所述存储器上存储有计算机可读指令，所述计算机可读指令被所述处理器执行时实现如上所述的区块链网络中的信息记录方法。

[0009] 根据本发明实施例的一方面，一种存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如上所述的区块链网络中的信息记录方法。

[0010] 在上述技术方案中，对于区块链网络包括的节点而言，接收包括加密信息的交易信息，以基于零知识证明算法对交易信息进行验证，以使区块链网络校验本次信息转移的有效性，并在本次信息转移通过区块链网络的有效性校验时，进行交易信息中加密信息的

本地账本写入，由此，在整个信息转移过程中，由发送方转移至接收方的信息始终以密文形式存在，即加密信息，仅作为直接参与方的发送方和接收方才知道该信息中的具体内容，而对于其他非直接参与方，例如节点，无法查看到该信息中的具体内容，从而解决了现有技术中存在的信息转移的私密性不足的问题。

[0011] 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，并不能限制本发明。

附图说明

[0012] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并于说明书一起用于解释本发明的原理。

[0013] 图1是根据本发明所涉及的实施环境的示意图。

[0014] 图2是根据一示例性实施例示出的一种服务器的硬件结构框图。

[0015] 图3是根据一示例性实施例示出的一种区块链网络中的信息记录方法的流程图。

[0016] 图4是根据一示例性实施例示出的另一种区块链网络中的信息记录方法的流程图。

[0017] 图5是图4对应实施例中步骤310在一个实施例的流程图。

[0018] 图6是图5对应实施例中步骤311在一个实施例的流程图。

[0019] 图7是图4对应实施例中步骤330在一个实施例的流程图。

[0020] 图8是图7对应实施例示出的电子发票中待隐藏信息基于加密密钥进行加密前后的示意图。

[0021] 图9是图4对应实施例中步骤350在一个实施例的流程图。

[0022] 图10是根据一示例性实施例示出的另一种区块链网络中的信息记录方法的流程图。

[0023] 图11是根据一示例性实施例示出的另一种区块链网络中的信息记录方法的流程图。

[0024] 图12是根据一示例性实施例示出的另一种区块链网络中的信息记录方法的流程图。

[0025] 图13是图12对应实施例中步骤410在一个实施例的流程图。

[0026] 图14是一应用场景中一种区块链网络中的信息记录方法的时序图。

[0027] 图15是根据一示例性实施例示出的一种区块链网络中的信息记录装置的框图。

[0028] 图16是根据一示例性实施例示出的一种节点的框图。

[0029] 通过上述附图，已示出本发明明确的实施例，后文中将有更详细的描述，这些附图和文字描述并不是为了通过任何方式限制本发明构思的范围，而是通过参考特定实施例为本领域技术人员说明本发明的概念。

具体实施方式

[0030] 这里将详细地对示例性实施例执行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明相一致的所有实施方式。相反，它们仅是与如所附

权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

[0031] 图1为一种区块链网络中的信息记录方法所涉及的实施环境的示意图。

[0032] 如图1(a)所示，该实施环境包括信息转移系统100，该信息转移系统100包括用户所持终端110、用户所持终端130、以及区块链网络中的节点。

[0033] 其中，用户所持终端110、用户所持终端130可供客户端运行，可以是台式电脑、笔记本电脑、平板电脑、智能手机、掌上电脑、个人数字助理等等，在此不进行限定。

[0034] 在此说明的是，客户端，是指提供信息转移功能的客户端，例如，信息可以是电子发票，相应地，客户端可以是具备开具电子发票功能的购物客户端、打车客户端等等，该客户端可以是应用程序形式的，还可以是网页形式的，相应地，客户端向用户展示的用户界面可以是程序窗口形式的，也可以是网页页面形式的，在此也并未加以限定。

[0035] 进一步地，用户所持终端110是指发送方，用户所持终端130则是指接收方，信息转移即是在发送方与接收方之间进行。

[0036] 区块链网络，本实施环境中，实质由多台提供后台服务的服务器构成，该服务器即是为信息转移系统100配置的节点，该后台服务即是指信息转移服务，也可以理解为，用于执行信息转移服务的节点部署于服务器。

[0037] 当然，根据实际运营的需要，对于区块链网络中用于执行信息转移服务的各节点而言，并不局限于独立部署于多台服务器，也可以全部部署于同一台服务器，本发明实施例并未对此进行具体限定。

[0038] 区块链网络中节点与用户所持终端110、用户所持终端130之间通过无线或者有线等方式预先构建通信网络150，以便于通过构建的通信网络150实现二者之间的数据传输。例如，待传输的数据包括发送方转移至接收方的信息等。

[0039] 具体而言，当客户端在作为发送方的用户所持终端110上运行，发送方便可向区块链网络发起针对接收方的信息转移请求，以通过该信息转移请求将信息转移至接收方。

[0040] 在区块链网络中，节点151与用户所持终端110交互，便可接收到信息转移请求，进而从中得到待转移至接收方的信息，以对该信息进行加密和零知识证明处理，从而得到本次信息转移需要的交易信息。

[0041] 当基于该交易信息验证本次信息转移通过区块链网络的有效性校验后，区块链网络中的各节点，例如，节点151、节点153、节点155、节点157，便可将交易信息中的加密信息写入本地账本。

[0042] 此时，对于节点153而言，通过与用户所持终端130交互，便能够将经过解密的信息反馈至用户所持终端130，即接收方，从而完成信息转移。

[0043] 根据实际运营的需要，整个信息转移过程，并不局限于由区块链网络独立完成，如图1(b)所示，该实施环境中，通信网络150包括区块链网络和业务网络，其中，区块链网络包括节点155和节点157，业务网络包括节点151和节点153。

[0044] 也就是说，区块链网络中的节点155和节点157承担的角色仅包括：验证、共识、记账等，而业务网络中的节点151和节点153承担的角色则包括：加密、零知识证明处理、解密等，以基于区块链网络和业务网络的相互配合实现整个信息转移过程。

[0045] 其中，区块链网络和业务网络均部署于通信网络150，故而，二者之间便可经由该通信网络150实现彼此之间的数据传输。例如，待传输的数据包括交易信息、加密信息等。

[0046] 下面各实施例将基于区块链网络和业务网络相互配合来实现整个信息转移过程进行详细地说明。

[0047] 图2是根据一示例性实施例示出的一种服务器的硬件结构框图。该种服务器适用于图1所示出实施环境中区块链网络中的节点、或者业务网络中的节点。

[0048] 需要说明的是，该种服务器只是一个适配于本发明的示例，不能认为是提供了对本发明的使用范围的任何限制。该种服务器也不能解释为需要依赖于或者必须具有图2中示出的示例性的服务器200中的一个或者多个组件。

[0049] 服务器200的硬件结构可因配置或者性能的不同而产生较大的差异，如图2所示，服务器200包括：电源210、接口230、至少一存储器250、以及至少一中央处理器(CPU，Central Processing Units)270。

[0050] 具体地，电源210用于为服务器200上的各硬件设备提供工作电压。

[0051] 接口230包括至少一有线或无线网络接口，用于与外部设备交互。例如，进行图1所示出实施环境中各节点之间的交互。

[0052] 当然，在其他本发明适配的示例中，接口230还可以进一步包括至少一串并转换接口233、至少一输入输出接口235以及至少一USB接口237等，如图2所示，在此并非对此构成具体限定。

[0053] 存储器250作为资源存储的载体，可以是只读存储器、随机存储器、磁盘或者光盘等，其上所存储的资源包括操作系统251、应用程序253及数据255等，存储方式可以是短暂存储或者永久存储。

[0054] 其中，操作系统251用于管理与控制服务器200上的各硬件设备以及应用程序253，以实现中央处理器270对存储器250中海量数据255的运算与处理，其可以是Windows ServerTM、Mac OS XTM、UnixTM、LinuxTM、FreeBSDTM等。

[0055] 应用程序253是基于操作系统251之上完成至少一项特定工作的计算机程序，其可以包括至少一模块(图2中未示出)，每个模块都可以分别包含有对服务器200的一系列计算机可读指令。例如，信息记录装置可视为部署于节点的应用程序253。

[0056] 数据255可以是存储于磁盘中的照片、图片等，还可以是待转移至接收方的信息等，存储于存储器250中。

[0057] 中央处理器270可以包括一个或多个以上的处理器，并设置为通过至少一通信总线与存储器250通信，以读取存储器250中存储的计算机可读指令，进而实现对存储器250中海量数据255的运算与处理。例如，通过中央处理器270读取存储器250中存储的一系列计算机可读指令的形式来完成区块链网络中的信息记录方法。

[0058] 此外，通过硬件电路或者硬件电路结合软件也能同样实现本发明，因此，实现本发明各实施例并不限于任何特定硬件电路、软件以及两者的组合。

[0059] 请参阅图3，在一示例性实施例中，一种区块链网络中的信息记录方法适用于图1所示实施环境区块链网络中的节点，该节点的结构可以如图2所示。

[0060] 该种区块链网络中的信息记录方法可以由区块链网络中的节点执行，可以包括以下步骤：

[0061] 步骤320，接收交易信息。

[0062] 其中，所述交易信息包括加密信息，所述加密信息是利用加密密钥对发送方转移

至接收方的信息进行加密生成的。

[0063] 在业务网络中的节点生成交易信息之后，便会在区块链网络中进行该交易信息的广播，那么，对于区块链网络中的节点而言，便会接收到该交易信息。

[0064] 下面对业务网络中节点如何生成交易信息的过程加以说明。

[0065] 如图4所示，在一实施例的实现中，交易信息的生成过程可以由业务网络中的节点执行，可以包括以下步骤：

[0066] 步骤310，生成加密密钥。

[0067] 如前所述，信息转移，是在发送方与接收方之间进行，无论是发送方还是接收方，实质是可供客户端运行的用户所持终端，如果用户期望借助所持终端将信息由发送方转移至接收方，便会向区块链网络发起信息转移请求，该信息转移请求中携带了待转移至接收方的信息。

[0068] 待转移至接收方的信息，可以是商品交易信息，例如，商品订单，还可以是票据信息，例如，电子发票，又或者是货币信息，本实施例并不对该信息的类型作具体限定。相应地，由于该信息的不同类型可对应不同的应用场景，例如，商品交易信息可对应商品贸易场景，票据信息可对应发票报销场景，货币信息可对应银行支付场景，因此，本实施例所提供的信息转移可应用于区块链相关的多种应用场景，包括但不限于上述应用场景，还可以是供应链金融场景、股票交易场景、房地产交易场景等等。

[0069] 其次，对于区块链网络而言，为了保证信息转移的私密性，首先需要生成加密密钥，以便于后续基于该加密密钥对待转移至接收方的信息进行加密。

[0070] 本实施例中，加密密钥的生成，基于加密算法实现。

[0071] 加密密钥，可以是对称密钥，也即是用于加密信息的加密密钥和用于解密信息的解密密钥是一致的；还可以是非对称密钥，也即是用于加密信息的加密密钥和用于解密信息的解密密钥有所区别。

[0072] 为此，关于生成加密密钥的加密算法，可以是对称加密算法，例如，对称加密算法包括但不限于：DES算法，3DES算法，TDEA算法，Blowfish算法，RC5算法，IDEA算法等等；还可以是非对称加密算法，例如，非对称加密算法包括但不限于：RSA算法、Elgamal算法、背包算法、Rabin算法、ECC(椭圆曲线加密)算法等等。

[0073] 步骤330，根据所述加密密钥对待转移至接收方的信息进行加密，得到加密信息。

[0074] 在生成加密密钥之后，便能够利用该加密密钥加密待转移至接收方的信息。

[0075] 由此，对于区块链网络而言，在后续的信息转移过程中，待转移至接收方的信息不再以明文的形式存在，而是以密文的形式存在，即加密信息，也可以理解为，在未进行加密信息解密之前，只有发送方才知道待转移至接收方的信息中的具体内容，从而保证了信息转移的私密性。

[0076] 步骤350，对所述加密信息进行零知识证明处理，生成所述交易信息。

[0077] 在进行信息记录之前，为了保证信息转移的完备性和正确性，区块链网络需要校验本次信息转移的有效性。

[0078] 为此，零知识证明处理，则是期望后续区块链网络中节点在验证交易信息时，无法获知任何额外的知识，例如，待转移至接收方的信息。

[0079] 换而言之，基于零知识证明，对于区块链网络而言，便能够在完全不知道待转移至

接收方的信息中的具体内容的情况下，完成本次信息转移的有效性校验，以此保障信息转移的私密性。

[0080] 步骤340，基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性。

[0081] 由于交易信息是经过零知识证明处理的，为此，本实施例中，交易信息的验证是基于零知识证明算法实现的，以使区块链网络完成本次信息转移的有效性校验。

[0082] 如果本次信息转移通过区块链网络的有效性校验，表示本次信息转移有效，则跳转执行步骤360。

[0083] 反之，如果本次信息转移未通过区块链网络的有效性校验，表示本次信息转移无效，则终止本次信息转移，也即是，不将信息转移至接收方。

[0084] 步骤360，如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入。

[0085] 在本次信息转移通过区块链网络的有效性校验之后，对于区块链网络而言，便会在交易信息验证成功的节点中完成加密信息的本地账本写入，以使交易信息验证成功的节点对本次信息转移进行记录。随着本地账本完成加密信息的写入，也即是，该本地账本记录了本次信息转移，从而保证本次信息转移不可篡改，由此实现了去中心化的不可篡改的分布式账本技术。

[0086] 然而，即使在交易信息验证成功的节点上对本次信息转移进行记录，由于待转移至接收方的信息是经过加密的，因此该些节点都无法查看到待转移至接收方的信息中的具体内容。

[0087] 此时，为了向接收方反馈信息，对于业务网络中的节点而言，此时，便会利用解密密钥解密完成本地账本写入的加密信息。

[0088] 其中，解密密钥和加密密钥可以属于对称密钥，即由对称加密算法生成，也可以属于非对称密钥，即由非对称加密算法生成，故而，在区块链网络中节点记录加密信息之后，业务网络中的节点便可基于解密密钥的解密操作，由加密信息得到信息，并反馈至接收方。对称加密算法和非对称加密算法如前所述，此处不再一一赘述，本实施例并未对此作出具体限定。

[0089] 那么，对于接收方而言，便能够得到区块链网络反馈的经过解密的信息，从而完成发送方至接收方的信息转移。

[0090] 通过如上所述的过程，在区块链网络中的节点完成本地账本写入，待转移至接收方的信息即进行了加密，进行加密信息解密之前，待转移至接收方的信息始终以密文形式存在，即加密信息，只在需要将信息反馈至接收方时，方才对该加密信息进行解密，由此，整个信息转移过程中，只有发送方和接收方才知道信息中的具体内容，而对于区块链网络而言，并不清楚且无法查看该信息中的具体内容，从而有效保障了信息转移的私密性。

[0091] 此外，整个信息转移过程基于区块链网络实现，无需协调，充分确保了区块链去中心化的优势。

[0092] 请参阅图5，在一示例性实施例中，步骤310可以由业务网络中的节点执行，可以包括以下步骤：

[0093] 步骤311，获取所述发送方的私钥和所述接收方的公钥。

[0094] 发送方的私钥,来自于发送方生成的非对称密钥对。

[0095] 接收方的公钥,来自于接收方生成的非对称密钥对。

[0096] 补充说明的是,无论是发送方的非对称密钥对,还是接收方的非对称密钥对,均包含有公钥和私钥,是由非对称加密算法生成的。非对称加密算法如前所述,此处不再一一赘述,本实施例并未对此作出具体限定。

[0097] 对于发送方而言,关于接收方的公钥的获取,如图6所示,在一实施例的实现中,步骤311可以由业务网络中的节点执行,可以包括以下步骤:

[0098] 步骤3111,基于所述发送方的私钥,确定所述发送方的公钥。

[0099] 步骤3113,进行所述发送方的公钥与所述接收方的公钥之间的交换,得到所述接收方的公钥。

[0100] 由此,对于发送方而言,便得到了发送方的私钥和接收方的公钥,进而使得后续进行信息加密的加密密钥的生成得以实现。

[0101] 对于接收方而言,便得到了发送方的公钥和接收方的私钥,进而使得后续进行加密信息解密的解密密钥的生成得以实现。

[0102] 步骤313,基于共享密钥交换算法,根据所述发送方的私钥和所述接收方的公钥,生成所述加密密钥。

[0103] 共享密钥交换(Diffie-Hellman,DH)算法,实质是基于发送方的非对称密钥对和接收方的非对称密钥对,生成密钥,以实现发送方和接收方对该密钥的共享。

[0104] 举例来说,假设发送方S的非对称密钥对包括:私钥Spri和公钥Spub,接收方R的非对称密钥对包括:私钥Rpri和公钥为Rpub。

[0105] 基于共享密钥交换算法,密钥key＝DH(Spri,Rpub)＝DH(Spub,Rpri)。

[0106] 那么,对于发送方S而言,将DH(Spri,Rpub)作为加密密钥key1,对于接收方R而言,将DH(Spub,Rpri)作为解密密钥key2,由此即实现了发送方S和接收方R对密钥key的共享,也即是,密钥key＝加密密钥key1＝解密密钥key2。

[0107] 由此,发送方S便能够利用加密密钥key1对待转移至接收方的信息进行加密,而接收方R则能够利用解密密钥key2将由发送方S加密得到的加密信息解密。

[0108] 上述过程中,基于共享密钥交换算法,使得发送方和接收方计算出一个仅有他们才知道的相同的共享密钥,不仅使得整个信息转移过程中待转移至接收方的信息能够以密文的形式存在,而且充分保障了对该信息的加密解密操作无法被第三方知道,以此保护了信息转移的私密性。

[0109] 请参阅图7,在一示例性实施例中,步骤330可以由业务网络中的节点执行,可以包括以下步骤:

[0110] 步骤331,从待转移至所述接收方的信息中提取得到待隐藏信息。

[0111] 其中,所述待隐藏信息包括用于唯一识别发送方的发送方标识、用于唯一识别接收方的接收方标识、资源转移份额。

[0112] 以待转移至接收方的信息为电子发票举例说明如下。

[0113] 例如,如图8(a)所示,电子发票中,包括发票抬头“用户A”、发票金额“100.00”、开票单位“商户B”、开票时间“2018-12-09”、发票代码“14403180911”、发票号码“000000001”。

[0114] 其中,待隐藏信息包括作为发送方标识的开票单位“商户B”、作为接收方标识的发

票抬头“用户A”、作为资源转移份额的发票金额“100.00”。

[0115] 当然，根据应用场景的实际需要，待隐藏信息还可以包括信息标识，例如上述例子中的发票代码和发票号码，此处并非对此构成具体限定。

[0116] 步骤333，利用所述加密密钥加密所述待隐藏信息，得到隐藏信息。

[0117] 仍以上述例子加以说明，用F表示基于加密密钥的加密操作，那么，隐藏信息包括F(商户B)、F(用户A)、F(100.00)、F(14403180911)、F(000000001)。

[0118] 步骤335，以所述隐藏信息替代所述待隐藏信息，存储至待转移至所述接收方的信息，形成所述加密信息。

[0119] 仍以上述例子加以说明，加密信息，即经过待隐藏信息加密的电子发票，如图8(b)所示，“?”表示信息被隐藏。当然，在其他实施例中，也可以通过“#”、“*”等其他字符串来表示信息被隐藏，此处并非对此构成具体限定。

[0120] 那么，对于非直接参与方而言，将无法获知该电子发票中的部分具体内容，以此实现对该电子发票的私密性的保护。

[0121] 在上述实施例的作用下，实现了对非直接参与方隐藏信息中的具体内容，满足了直接参与方希望对信息中的具体内容进行保密的合理需求，保证了信息转移的私密性，还有利于提升用户体验。

[0122] 请参阅图9，在一示例性实施例中，步骤350可以由业务网络中的节点执行，可以包括以下步骤：

[0123] 步骤351，对所述加密信息相关的发送方信息进行加密，得到发送方数据。

[0124] 步骤353，对所述加密信息相关的接收方信息进行加密，得到接收方数据。

[0125] 基于加密信息，相关的发送方信息包括但不限于：发送方标识、资源转移份额、发送方的私钥和公钥、发送方的加密密钥等。

[0126] 相关的接收方信息包括但不限于：接收方标识、接收方的公钥、接收方的解密密钥等。

[0127] 举例来说，假设H表示加密操作，input表示加密信息相关的发送方信息，output表示加密信息相关的接收方信息。

[0128] 那么，发送方数据inputkey＝H(input)，接收方数据outputkey＝H(output)。

[0129] 其中，H涉及的加密算法可以是如前所述的对称加密算法，也可以是如前所述的非对称加密算法，在此不再一一赘述，此处并未加以限定。

[0130] 步骤355，基于所述零知识证明算法，由所述发送方数据和所述接收方数据计算得到证明数据。

[0131] 仍以前述例子进行说明，则证明数据的计算方法为：

[0132] Proof＝Prove(inputkey,outputkey)。

[0133] 其中，Prove表示零知识证明算法，该零知识证明算法的输入为发送方数据inputkey和接收方数据outputkey，输出即为证明数据Proof。

[0134] 该零知识证明算法包括但不限于：zkSNARK(zero-knowledge succinct non-interactive argument of knowledge)算法、椭圆曲线加密算法、RSA算法等，在此并未加以限定。

[0135] 步骤357，将所述发送方数据、所述接收方数据和所述证明数据封装，得到所述交

易信息。

[0136] 仍以前述例子继续说明，则交易信息包括：发送方数据inputkey、接收方数据outputkey和证明数据Proof。

[0137] 由上可知，由于交易信息是由经过加密的若干数据封装得到的，那么，对于区块链网络中节点而言，即使得到了交易信息，仍无法知道待转移至接收方的信息中的具体内容，即无法知道任何额外的知识。

[0138] 结合上述零知识证明处理过程，下面对区块链网络中节点对交易信息进行验证进行说明。

[0139] 如前所述，交易信息包括发送方数据、接收方数据和证明数据，该些数据都是经过加密得到的。

[0140] 因此，针对区块链网络中节点而言，在不对交易信息中的发送方数据、接收方数据和证明数据进行解密操作的前提下，本实施例中，基于零知识证明算法对交易信息进行验证。

[0141] 基于零知识证明算法进行的验证，实质是指采用的验证算法对应于零知识证明算法。例如，如果零知识证明算法为zkSNARK算法，对应地，验证采用zkVerify验证算法。

[0142] 以交易信息包括发送方数据inputkey、接收方数据outputkey和证明数据Proof为例，对交易信息的验证过程说明如下：

[0143] zkVerifier＝zkVerify(inputkey,outputkey,Proof)。

[0144] 其中，zkVerify表示对应于零知识证明算法——zkSNARK算法的验证算法，该验证算法的输入为发送方数据inputkey、接收方数据outputkey和证明数据Proof，输出即为验证结果zkVerifier，用于指示交易信息是否验证成功。

[0145] 通过上述过程，在区块链网络中节点完全不知道待转移至接收方的信息的具体内容的前提下，通过验证结果的指示，便可确认本次信息转移是否确实发生在发送方与接收方之间，即本次信息转移是否有效，以此保障了基于区块链网络的信息转移的私密性得以实现。

[0146] 请参阅图10，在一示例性实施例中，如上所述的方法还可以由区块链网络中的节点执行，可以包括以下步骤：

[0147] 步骤510，如果所述交易信息通过验证，则生成确认消息。

[0148] 对于区块链网络中节点而言，如果验证结果指示所述交易信息验证成功，则生成确认消息，以便于后续区块链网络对本次信息转移进行有效性校验。

[0149] 反之，如果验证结果指示交易信息验证失败，则本次信息转移将被交易信息验证失败的节点拒绝。

[0150] 步骤530，根据所述确认消息，请求所述区块链网络针对本次信息转移的有效性进行共识。

[0151] 本实施例中，共识，是指区块链网络中超过设定阈值的节点上交易信息通过基于零知识证明算法的验证。

[0152] 那么，当共识成功，本次信息转移通过区块链网络的有效性校验。

[0153] 其中，共识，可以由专门的共识节点执行，也可以由区块链网络中区别于进行交易信息验证的节点的其他任意一个节点执行，本实施例并未对此加以限定。

[0154] 下面以专门的共识节点负责共识,对区块链网络中的共识过程加以说明。

[0155] 如图11所示,在一示例性实施例中,步骤530之后,如上所述的方法还可以由区块链网络中的共识节点执行,可以包括以下步骤:

[0156] 步骤550,接收所述区块链网络中所述节点反馈的确认消息。

[0157] 步骤570,如果接收到的确认消息的数量超过设定阈值,则判定共识成功。

[0158] 对于共识节点而言,如果接收到的确认消息的数量超过设定阈值,表示交易信息已在超过设定阈值的节点上通过基于零知识证明算法的验证,此时,便能够触发区块链网络针对本次信息转移的有效性达成共识,即本次信息转移通过区块链网络的有效性校验。

[0159] 其中,设定阈值是指已配置的达成共识所要求的节点的数量,可根据应用场景的实际需要灵活地调整,本实施例并未对此进行具体限定。

[0160] 在一示例性实施例中,如上所述的方法还可以包括以下步骤:

[0161] 从所述区块链网络中选取进行所述交易信息接收的节点。

[0162] 可以理解,为了保证区块链网络的可靠性,可以在区块链网络中部署多个节点,以从中选取进行所述交易信息接收的节点。

[0163] 关于节点的选取,可以从部署的多个节点中随机选取,还可以根据节点的运行状况从部署的多个节点中选取,或者,根据节点与发送方之间的物理距离进行选取。

[0164] 为此,本实施例中,在区块链网络中,部署一个代理节点,以实现节点的选取和配置。

[0165] 具体地,在一实施例的实现中,如图12所示,上述步骤可以由区块链网络中的代理节点执行,可以包括以下步骤:

[0166] 步骤410,基于所述区块链网络中各节点的运行状况,获取所述区块链网络中各节点的运行数据。

[0167] 其中,节点的运行数据,包括负载数、内存占用率、CPU占用率、网络速率、丢包率等等,是通过代理节点监控区块链网络中各节点的运行状况获得的。

[0168] 步骤430,确定所述区块链网络中各节点与所述发送方之间的物理距离。

[0169] 步骤450,根据所述运行数据和所述物理距离,对所述区块链网络中各节点进行筛选,得到进行所述交易信息接收的节点。

[0170] 那么,在代理节点选取得到进行交易信息接收的节点之后,对于区块链网络而言,便会将业务网络中节点生成的交易信息发送至选取到的节点。

[0171] 在上述实施例的作用下,通过在区块链网络中部署多个节点,即使其中一个节点运行异常,仍可以由运行正常的节点执行信息转移服务,避免信息转移服务的中断,由此充分保证了区块链网络的可靠性。

[0172] 请参阅图13,在一示例性实施例中,步骤410可以由区块链网络中的代理节点执行,可以包括以下步骤:

[0173] 步骤411,基于所述区块链网络中各节点的运行数据,确定每一个节点的第一分数。

[0174] 步骤413,基于所述区块链网络中各节点与所述发送方之间的物理距离,确定每一个节点的第二分数。

[0175] 步骤415,对每一个节点的第一分数和第二分数进行加权求和,得到每一个节点的

总分数。

[0176] 步骤417,选取总分数最大的节点作为进行所述交易信息接收的节点。

[0177] 举例来说,对于区块链网络中的每一个节点来说,根据该节点的运行数据确定该节点第一分数a,以及根据该节点与发送方之间的物理距离确定该节点的第二分数b。

[0178] 然后,基于上述运行数据和物理距离分别对应的权重系数m、n,对上述第一分数a和第二分数b进行加权求和,便得到了该节点的总分数=a×m+b×n。

[0179] 那么,基于区块链网络中所有节点的总分数,便可将总分数最大的节点作为进行所述交易信息接收的节点。

[0180] 通过上述过程,实现了基于运行数据和物理距离的节点筛选,充分保障了选取的节点的最大优势,例如,与发送方之间的物理距离最近,或者,运行状况最佳,那么,基于选取的节点执行信息转移服务时,出现异常中断的可能性最小,以此有利于提高信息转移的可靠性。

[0181] 在一示例性实施例中,如上所述的方法还可以由区块链网络中的代理节点执行,可以包括以下步骤:

[0182] 通过代理节点监控区块链网络中各节点的运行状况,对区块链网络中的节点进行更新处理。

[0183] 应当理解,在执行信息转移服务的过程中,各个节点可能随时发生异常,例如,节点死机、故障等等,如果不及时排除异常的节点,则可能导致信息转移服务异常中断。

[0184] 因此,在区块链网络中,需要保证各个节点是可用的。

[0185] 如前所述,节点的运行数据包括负载数、内存占用率、CPU占用率、网络速率、丢包率等等,可通过代理节点对区块链网络中各个节点的运行状况进行监控获得,进而实时地获知区块链网络中各个节点是否发生异常。例如,如果监控到节点的丢包率居高不下,则表明该节点可能存在异常,或者,如果监控到节点的网络速率过低,也可能是该节点存在异常。

[0186] 当节点的运行状况发生变化,便需要进行相应的更新处理,该更新处理包括节点剔除、节点恢复等等。

[0187] 例如,当监控到节点异常,则将异常的节点从区块链网络中剔除,或者,当监控到异常的节点由异常恢复正常,则将恢复正常的节点重新部署至区块链网络中。

[0188] 通过上述过程,有效地提高了区块链网络的可靠性,进而避免了信息转移服务的异常中断。

[0189] 在一示例性实施例中,如上所述的方法还可以由区块链网络中的代理节点执行,可以包括以下步骤:

[0190] 通过代理节点监控区块链网络中节点的运行状况,进行节点的主备切换处理。

[0191] 可以理解,节点的异常包括但不限于:负载数过大、内存占用率过高、CPU占用率过高、网络速率过低、丢包率过高、甚至于节点死机、故障等等。

[0192] 基于此,针对每一个节点,区块链网络中都分别部署了主节点和备节点。

[0193] 由此,在节点执行信息转移服务过程中,当代理节点根据主节点的运行数据监控到主节点出现异常时,则运行备节点,以控制备节点替代主节点执行信息转移服务。

[0194] 通过上述过程,实现了基于区块链网络的容灾方案,即备节点在主节点正常时不

运行，仅当主节点异常时，运行备节点执行信息转移服务，进一步地保证了区块链网络的可靠性，避免信息转移服务的异常中断。

[0195] 图14是一应用场景中一种区块链网络中的信息记录方法的时序图。该应用场景中，待转移至接收方的信息为电子发票。

[0196] 该应用场景包括开票方、接收方、业务网络和区块链网络，由此便可以利用区块链技术的优势，实现去中心化的不可篡改的电子发票报销系统，各部分交互时序如图14所示。

[0197] 假设开票方为淘宝卖家，接收方为淘宝买家，如果淘宝买家在淘宝卖家处购买了一定金额的商品，则淘宝买家就可以请求淘宝卖家开具购买商品相应金额的电子发票。基于此，在淘宝买家与淘宝卖家之间便触发了电子发票报销流程，而在该电子发票报销流程中，淘宝买家与淘宝卖家之间将需要基于区块链网络进行待报销电子发票的转移。

[0198] 应当理解，电子发票报销流程包括电子发票发行环节、开票环节、报销环节。

[0199] 在电子发票发行环节，开票方将向电子发票发行方申领若干电子发票，以便于后续向接收方提供开票服务。

[0200] 随着接收方向开票方发起开票请求，电子发票报销流程由电子发票发行环节流转至开票环节，此时，开票方在开具了一定金额的电子发票之后，便会向区块链网络发起发票转移请求，以使该电子发票转移至接收方。

[0201] 业务网络中节点对发票转移请求中的电子发票进行加密之后，区块链网络中节点则基于加密的电子发票进行本次发票转移的有效性校验，并在共识成功之后基于加密的电子发票进行本地账本写入，直至向接收方反馈电子发票时，该加密的电子发票才由业务网络中的节点进行解密。

[0202] 由上可知，在整个电子发票转移过程中，电子发票均是以密文的形式存在的，对于区块链网络中各节点而言，都无法获知电子发票中的具体内容，例如开票方、接收方、金额等等，从而保证了电子发票在由开票方转移至接收方的过程中的私密性。

[0203] 随着接收方获得电子发票，电子发票报销流程即可由开票环节流转至报销环节，使得接收方可凭据该电子发票申请报销。

[0204] 由此，即完成了电子发票报销流程。

[0205] 下述为本发明装置实施例，可以用于执行本发明所涉及的区块链网络中的信息记录方法。对于本发明装置实施例中未披露的细节，请参照本发明所涉及的区块链网络中的信息记录方法的方法实施例。

[0206] 请参阅图15，在一示例性实施例中，一种区块链网络中的信息记录装置900，所述区块链网络包括节点，所述信息记录装置900部署于所述节点。

[0207] 相应地，所述信息记录装置900包括但不限于：信息接收模块910、信息验证模块930和信息记录模块950。

[0208] 其中，信息接收模块910，用于接收交易信息，所述交易信息包括加密信息，所述加密信息是利用加密密钥对发送方转移至接收方的信息进行加密生成的。

[0209] 信息验证模块930，用于基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性。

[0210] 信息记录模块950，用于如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入。

[0211] 在一示例性实施例中，如上所述的信息记录装置900还包括但不限于：消息生成模块和请求共识模块。

[0212] 其中，消息生成模块，用于如果所述交易信息通过验证，则生成确认消息。

[0213] 请求共识模块，用于根据所述确认消息，请求所述区块链网络针对本次信息转移的有效性进行共识。

[0214] 当共识成功后，本次信息转移通过所述区块链网络的有效性校验。

[0215] 在一示例性实施例中，如上所述的信息记录装置900还包括但不限于：消息接收模块和共识模块。

[0216] 其中，消息接收模块，用于接收所述区块链网络中所述节点反馈的确认消息。

[0217] 共识模块，用于如果接收到的确认消息的数量超过设定阈值，则判定共识成功。

[0218] 在一示例性实施例中，如上所述的信息记录装置900还包括但不限于：节点选取模块。

[0219] 其中，节点选取模块，用于从所述区块链网络中选取进行所述交易信息接收的节点。

[0220] 相应地，所述节点选取模块包括但不限于：运行数据获取单元、物理距离确定单元和节点筛选单元。

[0221] 其中，运行数据获取单元，用于基于所述区块链网络中各节点的运行状况，获取所述区块链网络中各节点的运行数据。

[0222] 物理距离确定单元，用于确定所述区块链网络中各节点与所述发送方之间的物理距离。

[0223] 节点筛选单元，用于根据所述运行数据和所述物理距离，对所述区块链网络中节点进行筛选，得到进行所述交易信息接收的节点。

[0224] 在一示例性实施例中，所述节点筛选单元包括但不限于：第一分数确定子单元、第二分数确定子单元、分数加权子单元和节点选取子单元。

[0225] 其中，第一分数确定子单元，用于基于所述区块链网络中各节点的运行数据，确定每一个节点的第一分数。

[0226] 第二分数确定子单元，用于基于所述区块链网络中各节点与所述发送方之间的物理距离，确定每一个节点的第二分数。

[0227] 分数加权子单元，用于对每一个节点的第一分数和第二分数进行加权求和，得到每一个节点的总分数。

[0228] 节点选取子单元，用于选取总分数最大的节点作为进行所述交易信息接收的节点。

[0229] 在一示例性实施例中，另一种区块链网络中的信息记录装置，还将部署于业务网络中的节点。

[0230] 相应地，所述信息记录装置包括但不限于：加密密钥生成模块、信息加密模块、信息处理模块和信息广播模块。

[0231] 其中，加密密钥生成模块，用于生成所述加密密钥。

[0232] 信息加密模块，用于根据所述加密密钥对待转移至所述接收方的信息进行加密，得到所述加密信息。

[0233] 信息处理模块，用于对所述加密信息进行零知识证明处理，生成所述交易信息。

[0234] 信息广播模块，用于在所述区块链网络中广播所述交易信息，使所述区块链网络中的所述节点获取到所述交易信息。

[0235] 在一示例性实施例中，所述加密密钥生成模块包括但不限于：密钥获取单元和密钥计算单元。

[0236] 其中，密钥获取单元，用于获取所述发送方的私钥和所述接收方的公钥。

[0237] 密钥计算单元，用于基于共享密钥交换算法，根据所述发送方的私钥和所述接收方的公钥，生成所述加密密钥。

[0238] 在一示例性实施例中，所述密钥获取单元包括但不限于：公钥确定子单元和公钥交换子单元。

[0239] 其中，公钥确定子单元，用于基于所述发送方的私钥，确定所述发送方的公钥。

[0240] 公钥交换子单元，用于进行所述发送方的公钥与所述接收方的公钥之间的交换，得到所述接收方的公钥。

[0241] 在一示例性实施例中，如上所述的信息记录装置还包括但不限于：密钥对生成模块。

[0242] 其中，密钥对生成模块，用于根据非对称加密算法生成非对称密钥对，所述非对称密钥对包括所述发送方的公钥和所述发送方的私钥。

[0243] 在一示例性实施例中，所述信息加密模块包括但不限于：信息提取单元、信息加密单元和信息存储单元。

[0244] 其中，信息提取单元，用于从待转移至所述接收方的信息中提取得到待隐藏信息，所述待隐藏信息包括发送方标识、接收方标识、资源转移份额。

[0245] 信息加密单元，用于利用所述加密密钥加密所述待隐藏信息，得到隐藏信息。

[0246] 信息存储单元，用于以所述隐藏信息替代所述待隐藏信息，存储至待转移至所述接收方的信息，形成所述加密信息。

[0247] 在一示例性实施例中，所述信息处理模块包括但不限于：第一加密单元、第二加密单元、计算单元和封装单元。

[0248] 其中，第一加密单元，用于对所述加密信息相关的发送方信息进行加密，得到发送方数据。

[0249] 第二加密单元，用于对所述加密信息相关的接收方信息进行加密，得到接收方数据。

[0250] 计算单元，用于基于所述零知识证明算法，由所述发送方数据和所述接收方数据计算得到证明数据。

[0251] 封装单元，用于将所述发送方数据、所述接收方数据和所述证明数据封装，得到所述交易信息。

[0252] 需要说明的是，上述实施例所提供的区块链网络中的信息记录装置在执行基于区块链网络的信息转移服务时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即区块链网络中的信息记录装置的内部结构将划分为不同的功能模块，以完成以上描述的全部或者部分功能。

[0253] 另外，上述实施例所提供的区块链网络中的信息记录装置与区块链网络中的信息

记录方法的实施例属于同一构思，其中各个模块执行操作的具体方式已经在方法实施例中进行了详细描述，此处不再赘述。

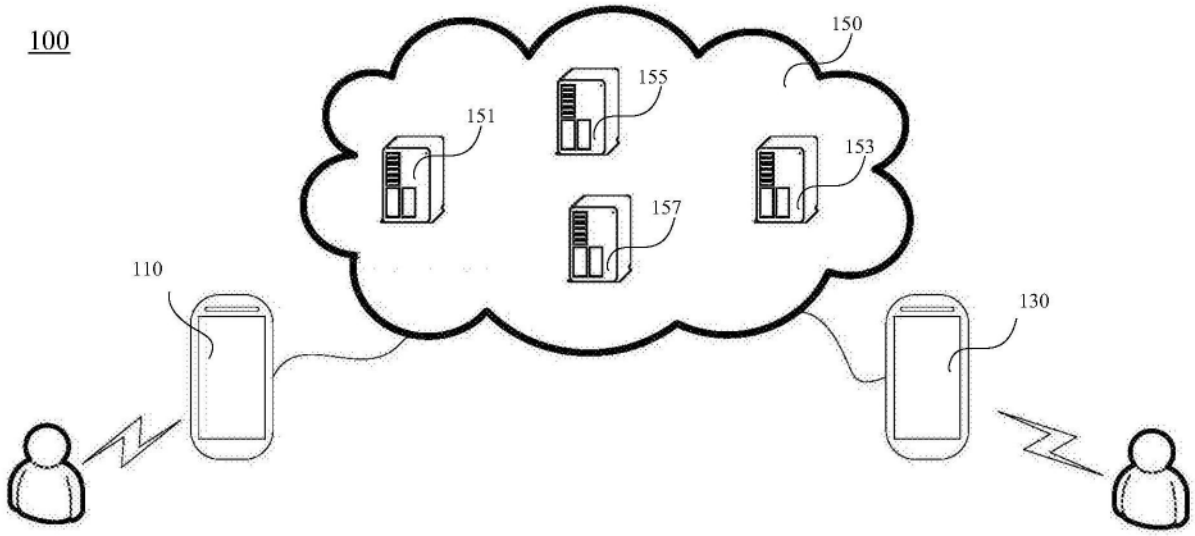
[0254] 请参阅图16，在一示例性实施例中，一种节点1000，包括至少一处理器1001、至少一存储器1002、以及至少一通信总线1003。

[0255] 其中，存储器1002上存储有计算机可读指令，处理器1001通过通信总线1003读取存储器1002中存储的计算机可读指令。

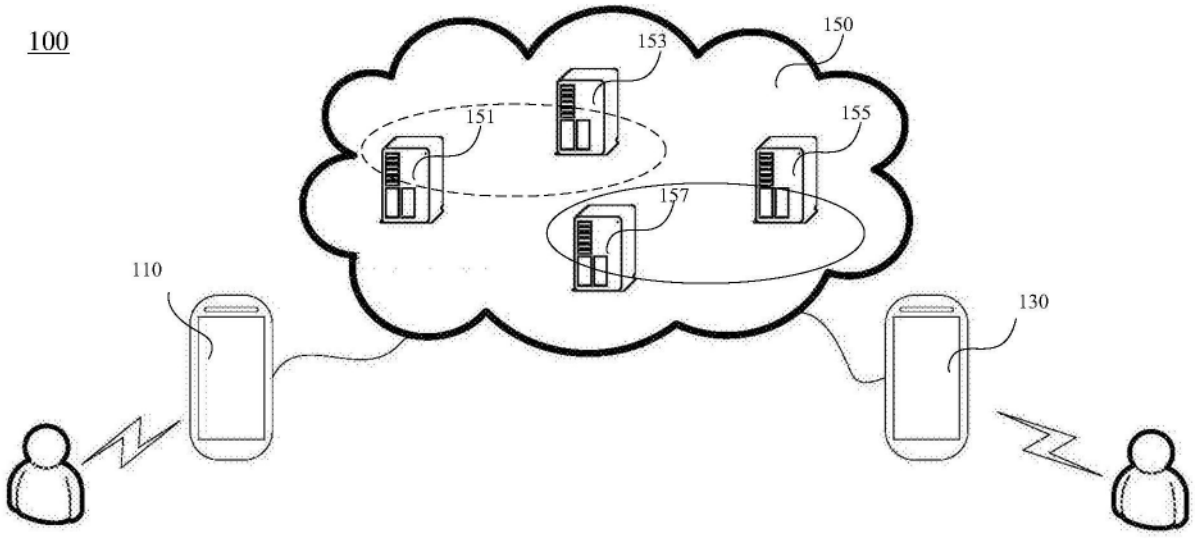
[0256] 该计算机可读指令被处理器1001执行时实现上述各实施例中的区块链网络中的信息记录方法。

[0257] 在一示例性实施例中，一种存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述各实施例中的区块链网络中的信息记录方法。

[0258] 上述内容，仅为本发明的较佳示例性实施例，并非用于限制本发明的实施方案，本领域普通技术人员根据本发明的主要构思和精神，可以十分方便地进行相应的变通或修改，故本发明的保护范围应以权利要求书所要求的保护范围为准。



(a)



(b)

图1

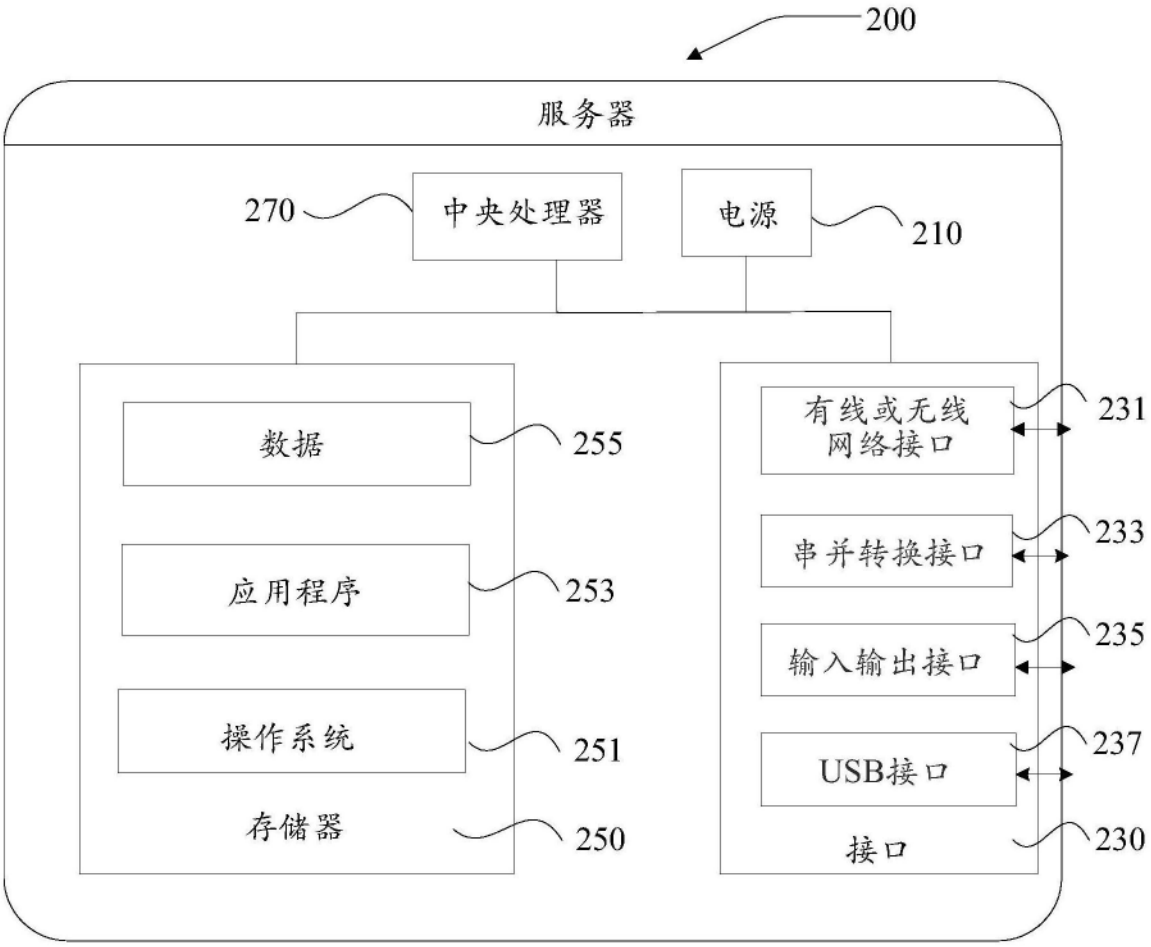

200
服务器
270
中央处理器
电源
210
数据
255
应用程序
253
操作系统
251
存储器
250
有线或无线
网络接口
231
串并转换接口
233
输入输出接口
235
USB接口
237
接口
230

图2

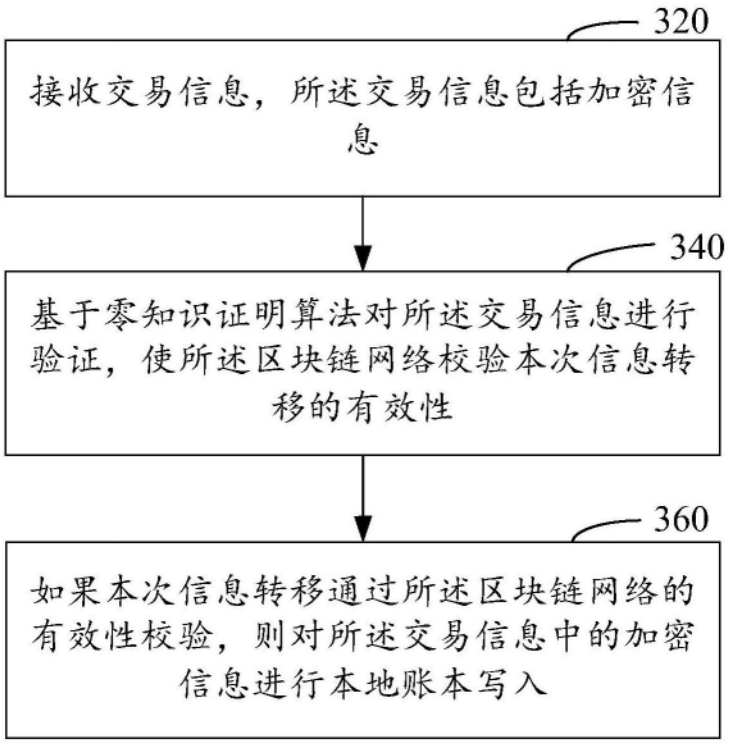

320
接收交易信息，所述交易信息包括加密信息
340
基于零知识证明算法对所述交易信息进行验证，使所述区块链网络校验本次信息转移的有效性
360
如果本次信息转移通过所述区块链网络的有效性校验，则对所述交易信息中的加密信息进行本地账本写入

图3

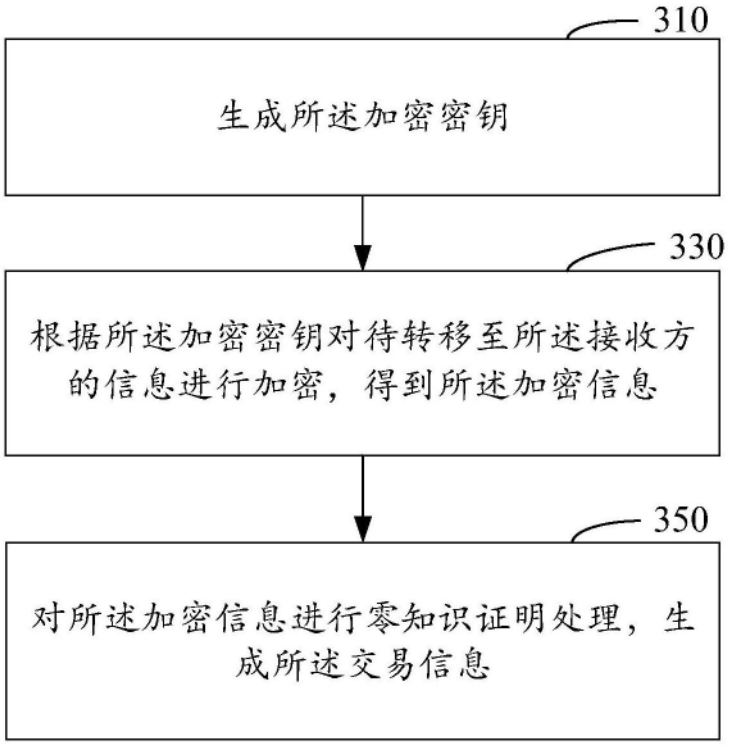

310
生成所述加密密钥
330
根据所述加密密钥对待转移至所述接收方的信息进行加密，得到所述加密信息
350
对所述加密信息进行零知识证明处理，生成所述交易信息

图4

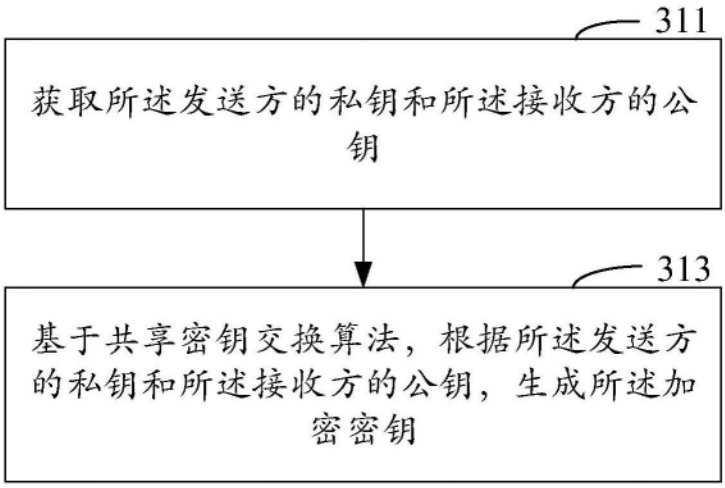

311
获取所述发送方的私钥和所述接收方的公钥
313
基于共享密钥交换算法，根据所述发送方的私钥和所述接收方的公钥，生成所述加密密钥

图5

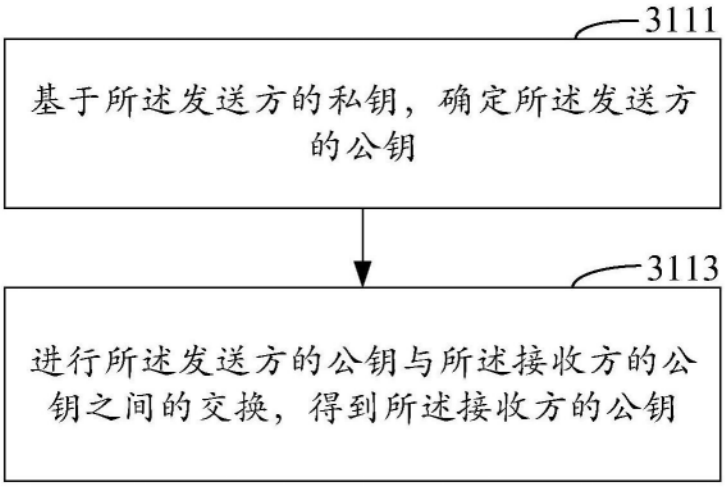

3111
基于所述发送方的私钥，确定所述发送方的公钥
3113
进行所述发送方的公钥与所述接收方的公钥之间的交换，得到所述接收方的公钥

图6

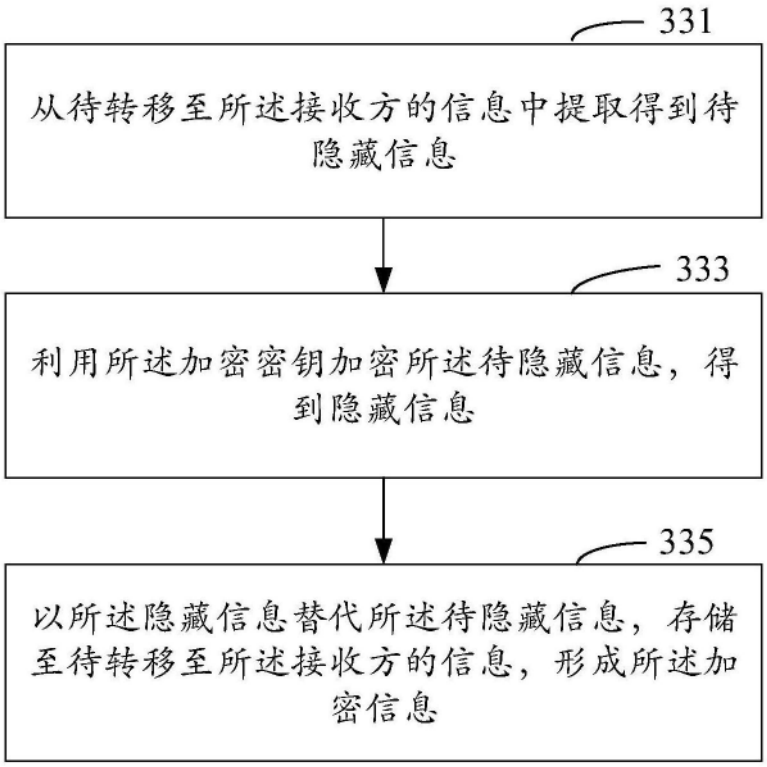

331
从待转移至所述接收方的信息中提取得到待隐藏信息
333
利用所述加密密钥加密所述待隐藏信息，得到隐藏信息
335
以所述隐藏信息替代所述待隐藏信息，存储至待转移至所述接收方的信息，形成所述加密信息

图7


增值税电子普通发票
发票抬头 用户A
发票金额 100.00
开票单位 商户B
开票时间 2018-12-09
发票代码 14403180911
发票号码 000000001

(a)

(b)

图8

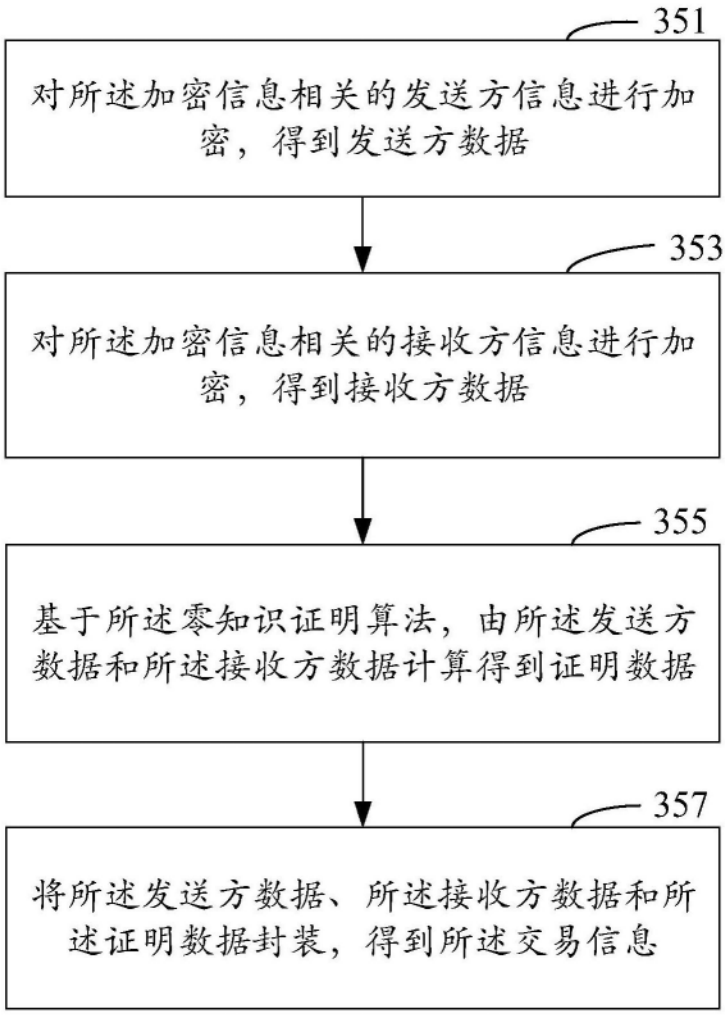

351
对所述加密信息相关的发送方信息进行加密，得到发送方数据
353
对所述加密信息相关的接收方信息进行加密，得到接收方数据
355
基于所述零知识证明算法，由所述发送方数据和所述接收方数据计算得到证明数据
357
将所述发送方数据、所述接收方数据和所述证明数据封装，得到所述交易信息

图9

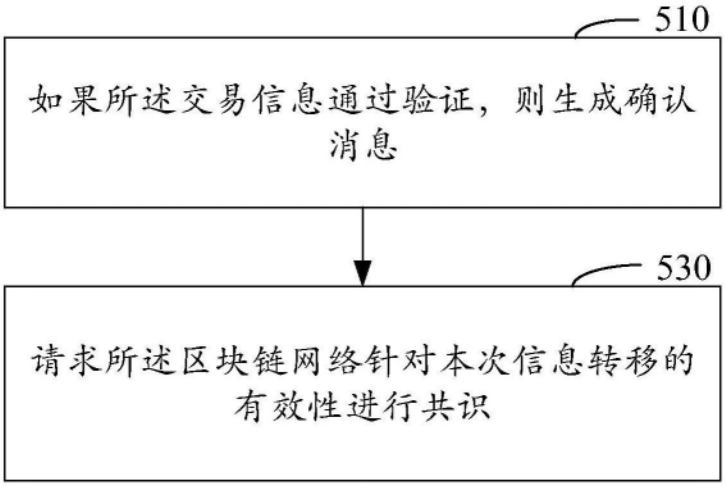

510
如果所述交易信息通过验证，则生成确认消息
530
请求所述区块链网络针对本次信息转移的有效性进行共识

图10

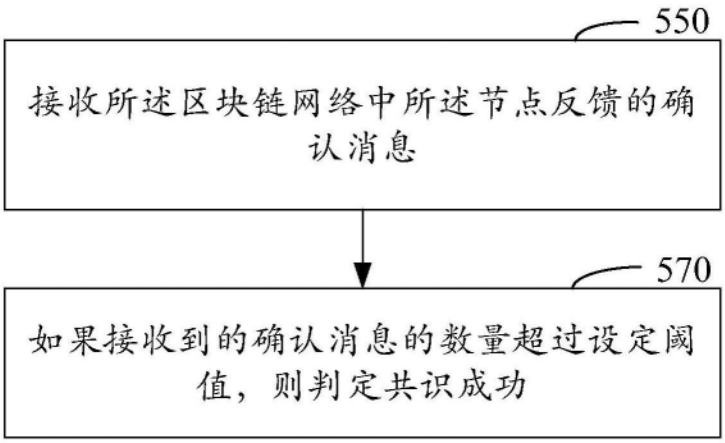

550
接收所述区块链网络中所述节点反馈的确认消息
570
如果接收到的确认消息的数量超过设定阈值，则判定共识成功

图11

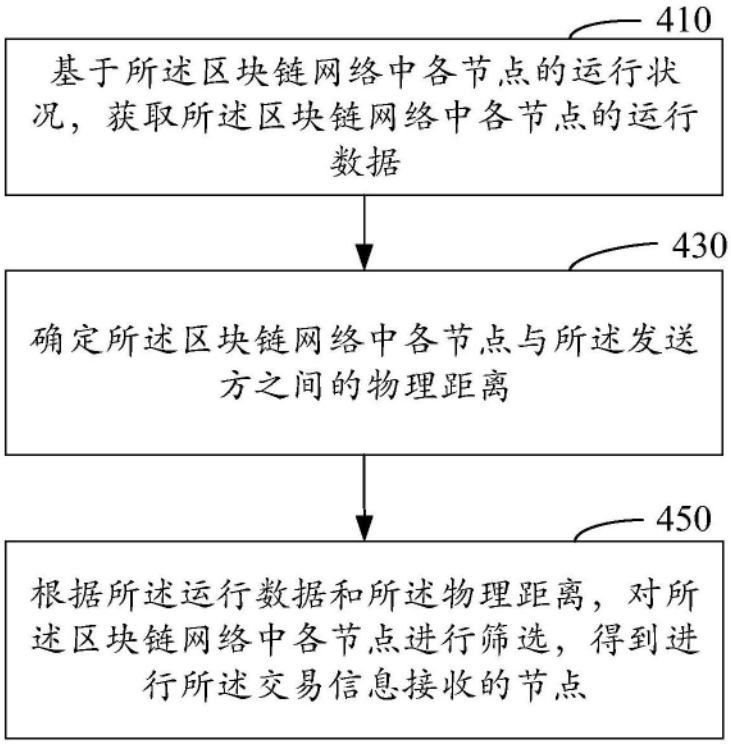

410
基于所述区块链网络中各节点的运行状况，获取所述区块链网络中各节点的运行数据
430
确定所述区块链网络中各节点与所述发送方之间的物理距离
450
根据所述运行数据和所述物理距离，对所述区块链网络中各节点进行筛选，得到进行所述交易信息接收的节点

图12

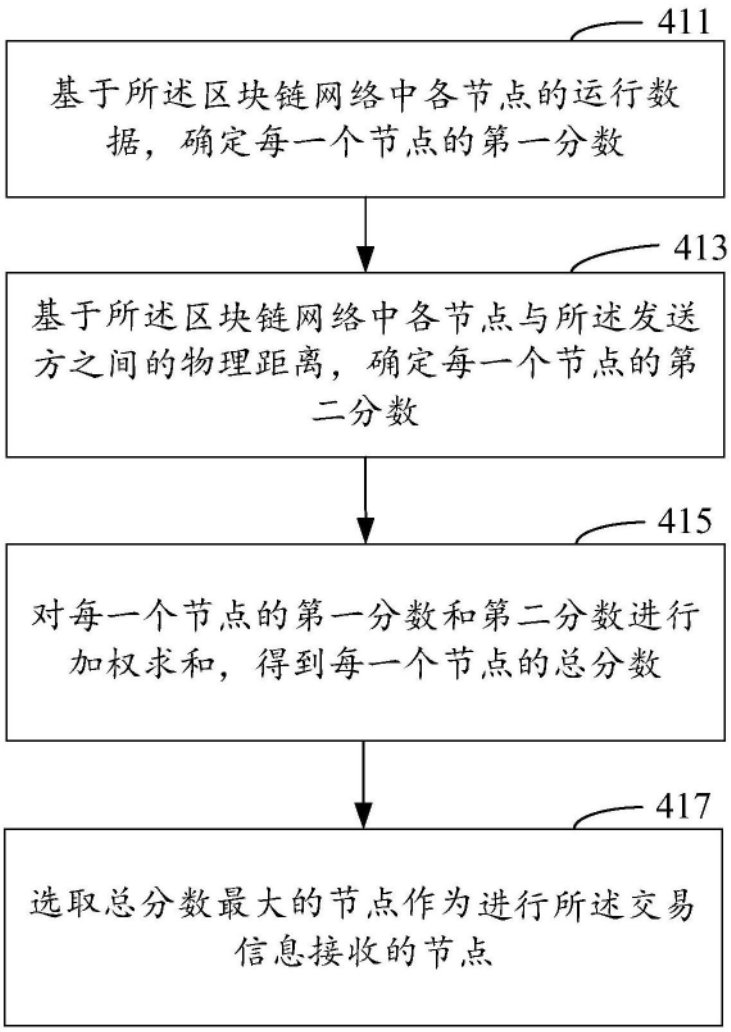

411
基于所述区块链网络中各节点的运行数据，确定每一个节点的第一分数
413
基于所述区块链网络中各节点与所述发送方之间的物理距离，确定每一个节点的第二分数
415
对每一个节点的第一分数和第二分数进行加权求和，得到每一个节点的总分数
417
选取总分数最大的节点作为进行所述交易信息接收的节点

图13

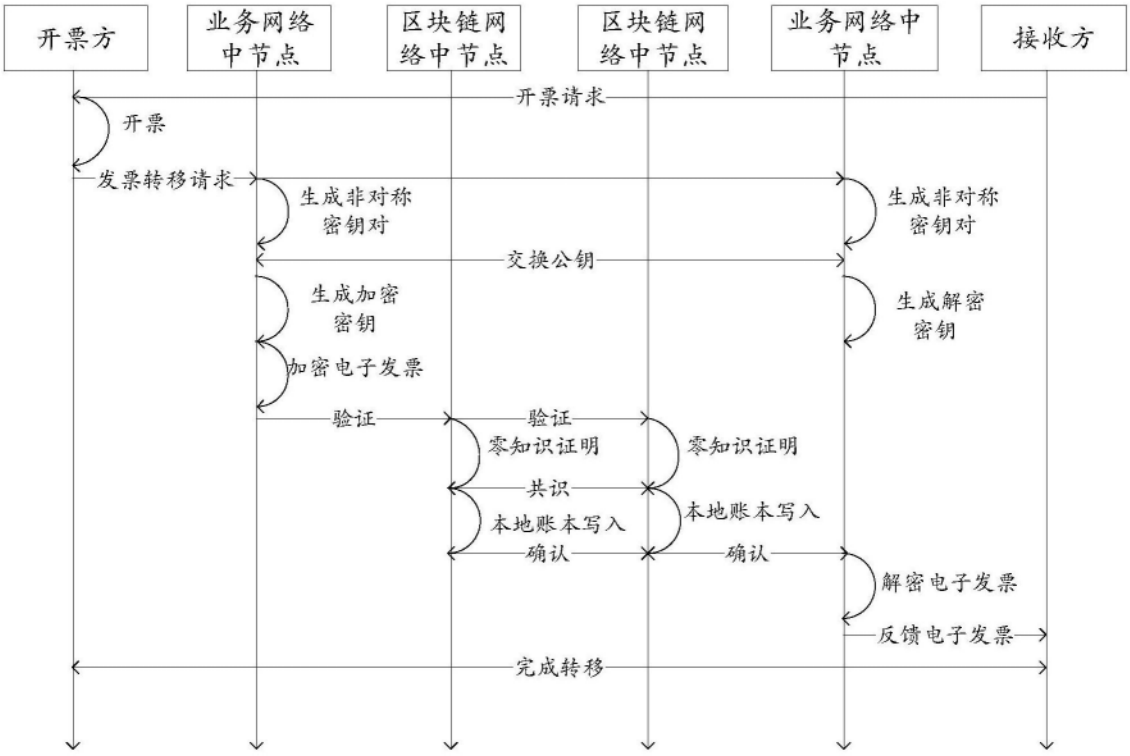

开票方
业务网络中节点
区块链网络中节点
区块链网络中节点
业务网络中节点
接收方
开票请求
开票
发票转移请求
生成非对称密钥对
生成非对称密钥对
交换公钥
生成加密密钥
生成解密密钥
加密电子发票
验证
验证
零知识证明
零知识证明
共识
本地账本写入
本地账本写入
确认
确认
解密电子发票
反馈电子发票
完成转移

图14

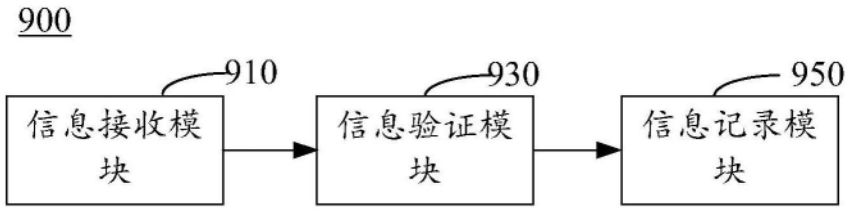

900
910
930
950
信息接收模块
信息验证模块
信息记录模块

图15

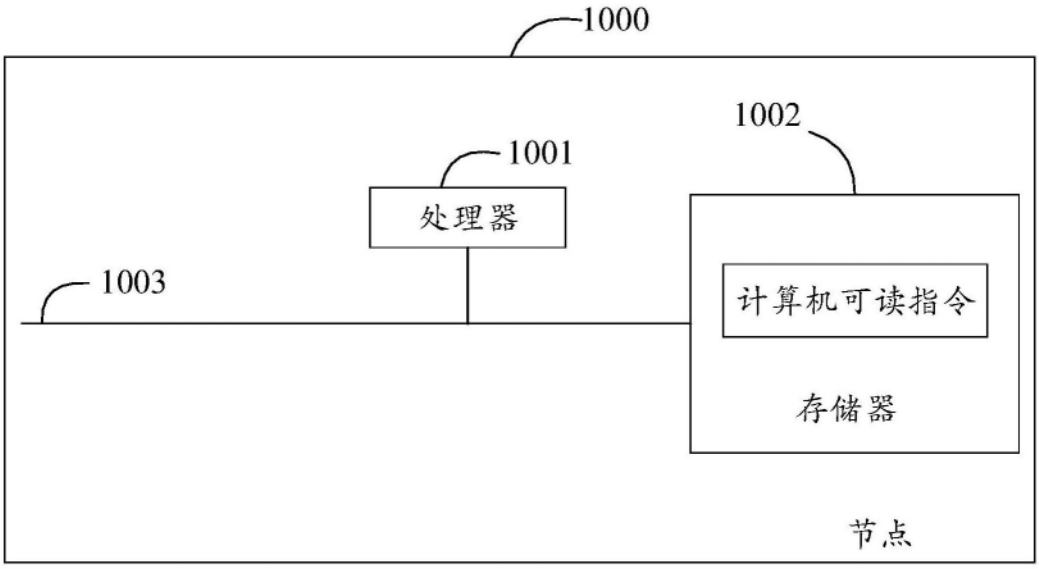


图16