

一种数据通信方法、装置、计算机设备及存储介质

本申请要求于 2020 年 11 月 16 日提交中国专利局、申请号为 2020112795166、申请名称为“一种数据处理方法、装置、计算机设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及互联网技术领域，具体涉及区块链数据通信技术。

背景技术

区块链是一种能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也就是分布式账本技术；区块链需要多方共同维护，并且使用密码学保证传输和访问安全。区块链分为三种类型：公有链、私有链和联盟链。

现有技术中的区块链普遍是节点之间组成的点对点(P2P, Peer To Peer)网络，例如，比特币、以太坊等公有链、以及 Fabric、Terdermint 等联盟链均是基于 P2P 网络形成的，P2P 网络中节点与节点之间是对等的，即现有的 P2P 网络是单层网络。

为了保护不同节点的数据隐私，就存在数据隔离的业务需求，业务节点向区块链网络中的共识节点发送数据同步请求后，业务节点只能从共识节点同步与自身相关的链上交易数据，并且业务节点只能无条件信任共识节点返回给自身的数据。在很多情况下，共识节点向业务节点发送的数据可能是不准确或者不完整的，即业务节点所接收的数据是无效的，那么如何验证业务节点同步的链上交易数据的有效性是当前研究热点。

发明内容

本申请实施例提出了一种数据通信方法、装置、计算机设备以及存储介质，能够验证轻量节点接收到的关联交易的有效性。

本申请实施例一方面提供了一种数据通信方法，由轻量节点执行，所述方法包括：

从与所述轻量节点具有关联关系的关联区块中接收数据，所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表，所述关联区块中包括多个交易以及所述统计证明交易列表，所述多个交易具有其各自对应的交易可见地址，所述统计证明交易列表包括多个统计证明交易，所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的；

在所述统计证明交易列表中识别所述轻量节点的目标索引；
基于所述关联交易获取加密路径集合，所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径；

根据所述统计证明交易列表、所述目标索引以及所述加密路径集合，确

定所述关联交易的有效程度;所述有效性程度用于表征所述关联交易的准确度以及完整度。

本申请实施例一方面提供了一种数据通信方法,由全量节点执行,所述方法包括:

- 5 接收轻量节点发送的数据同步请求,查找与所述轻量节点对应的关联区块;所述关联区块是与所述轻量节点具有关联关系的区块;所述关联区块中包括多个交易以及统计证明交易列表;所述多个交易具有其各自对应的交易可见地址;所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

10 从所述关联区块中提取所述统计证明交易列表,并在所述统计证明列表中识别所述轻量节点的目标索引;

- 15 从所述关联区块包括的所述多个交易中过滤出与所述轻量节点关联的关联交易,并基于所过滤出的关联交易确定加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

 将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点,以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效程度用于表征所述关联交易的准确度以及完整度。

- 20 本申请实施例一方面提供了一种数据通信装置,所述数据通信装置包括:

- 接收单元,用于从与所述轻量节点具有关联关系的关联区块中接收数据,所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表,所述关联区块中包括多个交易以及所述统计证明交易列表;所述多个交易具有其各自对应的交易可见地址,所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

 识别单元,用于在所述统计证明交易列表中识别所述轻量节点的目标索引;

- 30 获取单元,用于基于所述关联交易获取加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

 确定单元,用于根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效性程度用于表征所述关联交易的准确度以及完整度。

- 35 本申请实施例一方面提供了一种数据通信装置,所述数据通信装置包括:

 接收单元,用于接收轻量节点发送的数据同步请求,查找与所述轻量节

点对应的关联区块；所述关联区块是与所述轻量节点具有关联关系的区块；所述关联区块中包括多个交易以及统计证明交易列表；所述多个交易具有其各自对应的交易可见地址；所述统计证明交易列表包括多个统计证明交易，所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的；

提取单元，用于从所述关联区块中提取所述统计证明交易列表，并在所述统计证明列表中识别所述轻量节点的目标索引；

提取单元，还用于从所述关联区块中包括的所述多个交易中过滤出与所述轻量节点关联的关联交易，并基于所过滤出的关联交易确定加密路径集合，所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径；

发送单元，用于将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点，以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合，确定所述关联交易的有效程度；所述有效程度用于表征所述关联交易的准确度以及完整度。

本申请实施例一方面提供了一种计算机设备，包括存储器和处理器，存储器存储有计算机程序，计算机程序被处理器执行时，使得处理器执行上述各实施例中的方法。

本申请实施例一方面提供了一种计算机存储介质，计算机存储介质存储有计算机程序，计算机程序包括程序指令，程序指令当被处理器执行时，执行上述各实施例中的方法。

本申请实施例一方面提供了一种计算机程序产品或计算机程序，计算机程序产品或计算机程序包括计算机指令，计算机指令存储在计算机可读存储介质中，计算机指令被计算机设备的处理器执行时，执行上述各实施例中的方法。

通过本申请实施例的数据通信方法，轻量节点可以从关联区块中接收到统计证明交易列表，统计证明交易列表包括多个统计证明交易，统计证明交易是对关联区块包括的交易对应的交易可见地址、以及交易可见地址在关联区块中的数量进行加密处理得到的，轻量节点可以在统计证明交易列表中识别自身的目标索引，以及从关联区块包括的多个交易中过滤出与自身关联的关联交易，并基于所过滤出的关联交易确定加密路径集合，该加密路径集合中包括关联交易的加密路径、以及统计证明交易列表的加密路径，进而，轻量节点可以根据上述统计证明交易列表、目标索引以及加密路径集合，确定与自身相关的关联交易的有效程度，即确定与自身相关的关联交易的准确度以及完整度，关联交易的准确度用于表征关联交易是否准确，关联交易的完整度用于表征关联交易是否完整，所谓关联交易准确是指与关联交易相关的内容没有被篡改，所谓关联交易完整是指与关联交易相关的内容不存在缺

失。本申请中的轻量节点获取关联区块中与自身相关的明文关联交易、关联交易的加密路径以及该关联区块中加密的统计证明交易,并基于所获取的信息验证与自身相关的关联交易的有效程度,同时轻量节点不会获取与自身无关的明文交易,如此,在保证数据隔离即数据通信安全性的前提下,实现了对于与自身相关的关联交易的有效性的验证,保证了数据通信过程中传输的数据的有效性,提高了数据通信质量和效率。

附图说明

- 图 1A 是本申请实施例提供的一种区块链数据共享系统的结构示意图;
图 1B 是本申请实施例提供的一种区块链的结构示意图;
10 图 1C 是本申请实施例提供的一种区块生成的流程示意图;
图 2 是本申请实施例提供的一种数据通信系统的结构示意图;
图 3A 是本申请实施例提供的一种数据通信方法的场景示意图;
图 3B 是本申请实施例提供的另一种数据通信方法的场景示意图;
图 3C 是本申请实施例提供的另一种数据通信方法的场景示意图;
15 图 4 是本申请实施例提供的一种数据通信方法的流程示意图;
图 5 是本申请实施例提供的另一种数据通信方法的流程示意图;
图 6A 是本申请实施例提供的一种获取加密路径的流程示意图;
图 6B 是本申请实施例提供的一种统计证明交易列表的示意图;
图 7 是本申请实施例提供的另一种数据通信方法的流程示意图;
20 图 8 是本申请实施例提供的一种数据通信装置的结构示意图;
图 9 是本申请实施例提供的另一种数据通信装置的结构示意图;
图 10 是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

需要说明的是,本申请实施例涉及到区块链以及云技术,为了方便更好地理解本申请实施例,下面首先对区块链以及云技术相关术语以及技术进行详细说明。

云技术(Cloud technology)是基于云计算商业模式应用的网络技术、信息技术、整合技术、管理平台技术、应用技术等的总称,可以组成资源池,按需所用,灵活便利。云计算技术将变成重要支撑。技术网络系统的后台服务需要大量的计算、存储资源,如视频网站、图片类网站和更多的门户网站。伴随着互联网行业的高度发展和应用,将来每个物品都有可能存在自己的识别标志,需要传输到后台系统进行逻辑处理,不同程度级别的数据将会分开处理,各类行业数据皆需要强大的系统后盾支撑,只能通过云计算来实现。

云存储(cloud storage)是在云计算概念上延伸和发展出来的一个新的概念,分布式云存储系统(以下简称存储系统)是指通过集群应用、网格技术以及分布存储文件系统等功能,将网络中大量各种不同类型的存储设备(存

储设备也称之为存储节点)通过应用软件或应用接口集合起来协同工作,共同对外提供数据存储和业务访问功能的一个存储系统。

5 由于区块链中涉及到大量的数据计算以及数据存储服务,大量的数据计算以及数据存储服务需要花费大量的计算机运营成本,因此本申请涉及到的区块链中的统计证明交易列表、关联交易以及加密路径集合均可以通过云技术中的云存储技术实现。即,将区块链通过云存储技术存储在“云”上,当需要
10 要将统计证明交易列表、关联交易以及加密路径集合存储至区块链时,可以通过云存储技术将这些数据上传到“云”上的区块链中,且当需要读取这些数据时,也可以随时从“云”上的区块链中读取数据,如此可以降低对终端设备的存储要求,扩大区块链的应用范围。

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain),本质上是一个去中心化的数据库,是一串使用与密码学方法相关联的技术产生的数据块,每一个数据块中包含了一批网络交易的信息,用于验证其信息的有效性(防伪)和生成
15 下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层。

请参见图1A,图1A是本申请实施例提供的一种区块链数据共享系统的结构示意图,数据共享系统100是用于实现节点与节点之间数据共享的系统,该数据共享系统100中可以包括多个节点101和多个节点201,多个节点
20 点101可以是数据共享系统100中各个客户端,多个节点201可以是数据共享系统100中各个服务器。通常来说,节点201的存储空间和计算能力会大于节点101的存储空间和计算能力。为了保证数据共享系统内的信息互通,数据共享系统中各个节点之间可以存在信息连接,节点之间可以通过上述信息连接进行信息传输。例如,当数据共享系统100中的任意节点201接收到
25 输入信息时,数据共享系统100中的全部节点201便根据共识算法获取该输入信息,将该输入信息作为共享数据进行存储,使得数据共享系统100中全部节点201上存储的数据均一致。但是,由于节点101和节点201的存储空间不同或者业务需求等因素,对于数据共享系统100中的任意节点101来说,任意节点101接收到输入信息时,只会存储与节点自身相关的数据。

30 需要说明的是,本申请实施例提供的区块链数据共享系统100中每个节点201上可以存储完整的区块链,完整的区块链中包括与每个节点101和每个节点201相关的交易数据,而每个节点101中只会存储与自身相关的交易数据,每个节点101可以向任意节点201请求与自身相关的交易数据。

进一步地,图1A所示的区块链数据共享系统100中各节点涉及的功能
35 还包括:路由,路由是节点具有的基本功能,用于支持节点之间的通信。

具体的,每个节点101与每个节点201之间可以相互通信,节点101与节点201之间进行通信的方式可以为,通过节点101的路由功能实现通信,

或者通过节点 201 的路由功能实现通信。

数据共享系统 100 中的节点 201 可以是独立的物理服务器,也可以是多个物理服务器构成的服务器集群或者分布式系统,还可以是提供云服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。节点 101 可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表、车载终端等,但并不局限于此。

对于数据共享系统 100 中的每个节点 201,均存储一条相同的区块链。区块链由多个区块组成,请参见图 1B,图 1B 是本申请实施例提供的一种区块链的结构示意图。区块链由多个区块组成,各个区块中均包括区块头和区块主体,创始块的区块头中存储有输入信息特征值、版本号、时间戳和难度值,除创始块以外的其他区块的区块头中存储有输入信息特征值、版本号、时间戳、父区块的区块头特征值和难度值,各个区块的区块主体中均存储有输入信息,在本申请中输入信息除了可以包括节点发起的交易,还可以包括基于这些交易生成的统计证明交易列表,该统计证明交易列表也可以被认为是一个交易。

生成区块链中的各个区块时,请参见图 1C,图 1C 是本申请实施例提供的一种生成新区块的流程示意图。区块链所在的节点接收到发起的交易后,对该交易进行校验,完成校验后存储至内存池,基于内存池中的所有交易生成统计证明交易列表(内存池中所有的交易以及所生成的统计证明交易列表可以被统称为输入信息),并更新用于记录输入信息的哈希树。

之后,当计算得到小于随机数阈值的随机数时,便可将信息对应存储,生成区块头和区块主体,得到当前区块。随后,将新生成的区块分别发送给其所在的区块链数据共享系统中的其他节点,由其他节点对新生成的区块进行校验,并在完成校验后将新生成的区块添加至其存储的区块链中。

请参见图 2,图 2 是本申请实施例提供的一种数据通信系统的架构示意图。该系统架构包括:轻量节点集群 100 和全量节点集群 200,其中,轻量节点集群 100 包括轻量节点 101、轻量节点 102、轻量节点 103 以及轻量节点 104,全量节点集群 200 包括全量节点 201、全量节点 202、全量节点 203 以及全量节点 204。其中,轻量节点集群 100 处于第一区块链网络中,全量节点集群 200 处于第二区块链网络中,第一区块链网络不同于第二区块链网络,第一区块链网络为第二区块链网络的底层网络。

具体的,第一区块链网络中的节点只存储与自身相关的关联交易,第二区块链网络中的节点存储第一区块链网络中所有节点的关联交易。例如,第一区块链网络为公有网络,第二区块链网络为私有网络,并且第一区块链网络与第二区块链网络共同构成区块链网络。基于以上描述,本申请实施例涉及的区块链网络为双层区块链网络,可以实现节点与节点之间的数据隔离,

可以应用于资源数据发行机构等对保密性以及隐私性要求比较高的业务场景中，例如，商户 A 和商户 B 可以在区块链上开具电子发票，即将电子发票存储在链上，但只有维护区块链的机构服务器会存储所有商户的电子发票。当商户 A（或者商户 B）向机构服务器请求链上的电子发票时，机构服务器只会向商户 A（或者商户 B）返回商户 A（或者商户 B）自己开具的发票，如此实现商户之间的数据隔离性，即通过使得节点处于不同的区块链网络，实现不同数据的同步，从而达到隐私保密的需求。

需要说明的是，本申请实施例中的轻量节点集群 100 中的轻量节点的数量仅用于示例，在其他可行的实施例中，轻量节点集群 100 以及全量节点 200 中的节点数量可以根据具体业务场景进行调整，例如，轻量节点集群 100 中的节点数量还可以为五个、八个，全量节点集群 200 中的节点数量还可以为六个、七个等等，本申请对此不做具体限定。

具体实现时，轻量节点集群 100 中的每个轻量节点之间相互建立通信连接，具体的，轻量节点 101、轻量节点 102、轻量节点 103 以及轻量节点 104 之间可以通过无线网或者有线网的方式进行通信。同理，全量节点集群 200 中的每个全量节点之间也相互建立通信连接，具体的，全量节点 201、全量节点 202、全量节点 203 以及全量节点 204 之间可以通过无线网或者有线网的方式进行通信。并且，轻量节点集群 100 中的任意轻量节点可以与全量节点集群 200 中的任意全量节点之间通过网络路由的方式进行通信。

在一种可能的实现方式中，轻量节点可以将数据同步请求发送给全量节点集群 200 中与该轻量节点通信质量最好的全量节点；轻量节点也可以将数据同步请求发送给全量节点集群 200 中与该轻量节点距离最近的全量节点；轻量节点还可以将数据同步请求发送给全量节点集群 200 中所有全量节点通过共识算法选举出来的全量节点。其中，共识算法包括但不限于工作量证明（Proof of Work, PoW）算法、权益证明（Proof of Stake, PoS）算法、授权权益证明（Delegated Proof of Stake, DPoS）算法、实用拜占庭容错（Practical Byzantine Fault Tolerance, PBFT）算法等。

在一种可能的实现方式中，以轻量节点 101 与全量节点 201 进行通信为例进行具体说明。轻量节点 101 向全量节点 201 发送数据同步请求，全量节点 201 响应轻量节点 101 发送的数据同步请求，查找与轻量节点 101 对应的关联区块；该关联区块是在区块链中与轻量节点 101 具有关联关系的区块；其中包括多个交易以及统计证明交易列表；多个交易具有其各自对应的交易可见地址；统计证明交易列表包括多个统计证明交易，其中，任一统计证明交易是对关联区块包含的交易的任一交易可见地址、以及该交易可见地址在关联区块中的交易可见数量进行加密处理得到的。全量节点 201 从该关联区块中提取统计证明交易列表，并在统计证明交易列表中识别轻量节点 101 的目标索引。全量节点 201 从关联区块中过滤出与轻量节点 101 关联的关联

交易，并基于所过滤出的关联交易确定加密路径集合，该加密路径集合包括该关联交易的加密路径以及统计证明交易列表的加密路径；全量节点 201 将统计证明交易列表、目标索引、关联交易以及加密路径集合发送至轻量节点 101。

5 在一种可能的实现方式中，轻量节点 101 接收到全量节点 201 发送的统计证明交易列表、目标索引、关联交易以及加密路径集合之后，可以根据该加密路径集合，确定关联交易的准确度，即校验关联交易是否准确，关联交易是否被非法篡改；以及，可以根据该目标索引以及该统计证明交易列表，
10 确定关联交易的完整度，即校验关联交易是否完整，关联交易相关的内容是否存在缺失。

 需要说明的是，本申请实施例涉及的区块链网络中的所有节点均可以是手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备（MID，mobile internet device）、车辆、路边设备、飞行器、可穿戴设备，还可以是例如智能手表、智能手环、计步器等具有数据处理功能的智能设备，每个节点对应的
15 的设备类型可以相同，也可以不相同。

 可以理解的是，本申请实施例描述的数据通信系统是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着系统架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题同样适用。

20 请参见图 3A，图 3A 是本申请实施例提供的一种数据通信方法的场景示意图。本申请提供的数据通信方法可以应用于电子发票业务场景中。具体的，图 3A 实施例中涉及的业务节点可以是面向资源数据发行机构、企业或者消费者等的客户端。业务节点具体处于业务层中，业务节点可以属于安全
25 专网、公有云网络以及私有云网络等。其中，安全专网包括地方机构，公有云网络包括业务服务商、报销服务商以及 KA（Key Account），重点客户）企业等，私有云网络包括支付服务商、流转服务商以及 KA 企业等。代理节点可以处于路由代理层中，代理节点可以提供 P2P 服务、路由服务、证书缓存以及认证服务。核心网络共识层由一条或者多条核心区块链共同组成，
30 例如核心链 1、核心链 2 等等，每条核心链由区块链中的全量节点通过通信连接共同维护，并且不同的核心链可以包括不同的业务，例如，核心链 1 代表业务 1、核心链 2 代表业务 2 以及核心链 N 代表业务 N。每条核心链中可以包括若干个全量节点，全量节点可以生成并执行智能合约或者权限合约、缓存以及存储区块链中的数据以及发布区块至区块链网络中。

35 需要说明的是，代理节点可以起到对业务层以及核心共识网络层之间的隔离作用，并且业务层、路由代理层以及核心共识网络层共同组成一个区块链网络，该区块链网络可以应用于资源数据发行机构等具有高保密性的业务

场景中。

在一种可能的实现方式中,业务层中的业务节点可以通过路由代理层向核心共识网络层提交数据同步请求,以业务节点是业务服务商为例,业务服务商可以将数据同步请求(票据同步请求)发送至核心共识网络层中与该业务服务商通信质量最好的全量节点,或者业务服务商可以将数据同步请求(票据同步请求)发送至核心共识网络层中与该业务服务商距离最近的全量节点,或者业务服务商可以将获取请求(票据同步请求)发送至目标全量节点,该目标全量节点可以是核心共识网络层中对应票据业务的核心链上所有的全量节点通过共识算法选举出来的全量节点,需要说明的是,每条核心链上通过共识算法选举出来的目标全量节点可以周期性的更新,以实现区块链中区块数据的保密性以及公平性。票据同步请求包括业务服务商的身份信息,核心网络共识层中的全量节点接收到业务节点发送的票据同步请求之后,可以获取票据同步请求中业务服务商的身份信息,然后,对该业务服务商的身份信息进行校验。其中,业务服务商的身份信息可以是业务服务商从证书授权(Certificate Authority, CA)机构获取到的权威数字证书,全量节点可以对业务服务商的权威数字证书进行校验,若对该业务服务商的权威数字证书校验通过,则可以获取与业务服务商对应的关联区块。

在一种可能的实现方式中,如图 3B 所示,图 3B 是本申请实施例提供的另一种数据通信方法的场景示意图。轻量节点 1、轻量节点 2 和轻量节点 3 处于第一区块链网络中,全量节点 1、全量节点 2 和全量节点 3 处于第二区块链网络中。轻量节点 1 向全量节点 1 发起一笔交易 X(交易 X 的具体内容可以是轻量节点 1 的用户 1 转出一张电子票据),交易 X 包括多个交易可见地址(多个交易可见地址可以是轻量节点 1 的用户 1 指定的,例如用户 1 可以指定交易可见地址包括轻量节点 2 的节点地址,轻量节点 1 的节点地址通常会被默认为交易 X 的交易可见地址),全量节点 1 将交易 X 广播至第二区块链网络中,以使第二区块链网络中各个全量节点均将交易 X 存储在各自的交易池中(假设在存储交易 X 之前,交易池中已经存储了交易 1 和交易 2,且交易 1 和交易 2 的交易可见地址都包括轻量节点 2 的节点地址)。全量节点可以对交易池中的每个交易都进行区块链共识。共识通过之后,全量节点 1 分别统计交易池中每个交易对应的交易可见地址,即统计交易 1、交易 2 以及交易 X 各自对应的交易可见地址的交易可见数量;然后,全量节点 1 对每个交易可见地址以及每个交易可见地址的交易可见数量分别进行加密处理,得到统计证明交易列表。由于统计证明交易列表本身也是一笔交易,因此全量节点 1 可以根据统计证明交易列表、交易 1、交易 2 以及交易 X 生成关联区块,如图 3B 中区块 3,即为全量节点 1 统计证明交易列表、根据交易 1,交易 2、交易 X 和所统计的证明交易列表生成的关联区块。

此后,全量节点 1 如若接收到轻量节点 2 发送的数据同步请求,全量节

点 1 可以从关联区块中提取统计证明交易列表,并在该统计证明交易列表中识别轻量节点 2 的目标索引,由于上述区块 3 中存在的交易可见地址包括轻量节点 2 的节点地址,因此全量节点 1 可以将区块 3 作为轻量节点 2 的关联区块。然后,全量节点 1 可以确定区块 3 中统计证明交易列表的默克尔路径、交易 1 的默克尔路径、交易 2 的默克尔路径以及交易 X 的默克尔路径。具体的,可以将统计证明交易列表的默克尔路径,交易 1 的默克尔路径,交易 2 的默克尔路径和交易 X 的默克尔路径统称为加密路径集合。最后,全量节点 1 将统计证明交易列表、目标索引、关联交易(即交易 1、交易 2 以及交易 X)以及加密路径集合发送至轻量节点 2。由于区块 3 中交易 1、交易 2 以及交易 X 的交易可见地址均包括轻量节点 2 的节点地址,此处的交易 1、交易 2 以及交易 X 均是轻量节点 2 的关联交易。

在一种可能的实现方式中,如图 3C 所示,图 3C 是本申请实施例提供的另一种数据通信方法的场景示意图。轻量节点接收到全量节点发送的统计证明交易列表、目标索引、交易 1、交易 2、交易 X 以及加密路径集合后,可以根据统计证明交易列表、目标索引以及加密路径集合确定交易 1、交易 2 和交易 X 的有效性结果。其中,有效性结果可以包括准确性结果和完整性结果。具体的,轻量节点 2 可以根据加密路径集合,确定交易 1、交易 2 以及交易 X 的准确性结果,即校验交易 1、交易 2 以及交易 X 的内容是否被篡改;根据目标索引、统计证明交易列表以及统计证明交易列表的加密路径,确定交易 1、交易 2 以及交易 X 的完整性结果,即校验交易 1、交易 2 以及交易 X 的内容是否存在缺失。

需要说明的是,本申请实施例提供的数据通信方法可以应用于资源数据发行机构、公司等业务场景中,基于本申请实施例提供的双层区块链网络,可以实现数据之间的隔离性,可以在轻量节点向业务节点请求与该轻量节点本身相关的关联交易之后,通过统计证明交易列表证明轻量节点所获得的关联交易的有效性,既保障了区块链网络中存储的数据的安全性,又满足了轻量节点需要校验关联交易的有效性的应用需求。

请参见图 4,图 4 是本申请实施例提供的一种数据通信方法的流程示意图。该方法应用于区块链网络,区块链网络包括第一区块链网络和第二区块链网络,第一区块链网络包括轻量节点,第二区块链网络包括全量节点。该方法的操作步骤可由计算机设备执行,计算机设备可以是轻量节点,也可以是全量节点。本实施例主要描述轻量节点和全量节点之间的交互过程,该方法包括但不限于如下步骤 S410~S450:

步骤 S410: 轻量节点向全量节点发送数据同步请求。

具体实现时,轻量节点可以为简单支付验证(Simplified Payment Verification, SPV)节点,全量节点可以为共识节点。全量节点可以存储完

整区块链，其中，区块链包括第一区块链网络中所有节点的关联交易。轻量节点可以向全量节点发送数据同步请求，该数据同步请求用于向全量节点请求与该轻量节点自身相关的关联交易。

- 5 在一种可能的实现方式中，轻量节点可以将时间段、自身的节点地址、自身的身份信息、自身的数字签名以及自身所需同步的数据的业务类型打包并封装为数据同步请求，进而将数据同步请求发送至全量节点。

- 10 在区块链网络中，轻量节点的特点包括但不限于：不是一直在线；不用保存整个区块链，只要保存每个区块的块头；不用保存链上全部交易，只保存与自己相关的交易等。全量节点的特点包括但不限于：一直在线；在本地硬盘上维护完整的区块链信息；监听区块链网络上的交易信息，验证每个交易的合法性；决定哪些交易可以被打包到区块里；监听别的矿工挖出来的区块，验证其合法性以及挖矿等。

- 15 举例来说，在电子发票业务场景中，轻量节点可以为消费者所在的客户端，消费者可以包括个人消费者或者企业消费者等，全量节点可以为票据服务商所在的客户端，票据服务商所在的客户端中存储有所有消费者消费的电子发票。其中，票据服务商所在的客户端处于第二区块链网络中，第二区块链网络中可以包括一条或者多条区块链，当第二区块链网络包括多条区块链时，每条区块链可是根据业务或者地点的不同进行区分，例如，第二区块链网络包括区块链 1、区块链 2 以及区块链 3，区块链 1 可以负责业务 1 对应的电子发票业务 1，区块链 2 可以负责业务 2 对应的电子发票业务 2 以及区块链 3 可以负责业务 3 对应的电子发票业务 3。这种情况下，若企业向票据服务商发送数据同步请求，该数据同步请求包括业务类型，则票据服务商可以根据业务类型，确定该企业对应的业务服务商所在的客户端维护哪条区块链。

- 25 在一种可能的实现方式中，第一区块链网络中的轻量节点可以将数据同步请求发送至第二区块链网络中与该轻量节点通信质量最好的全量节点，或者第一区块链网络中的轻量节点可以将数据同步请求发送至第二区块链网络中与该轻量节点距离最近的全量节点，或者第一区块链网络中的轻量节点可以将数据同步请求发送至第二区块链网络中任一全量节点，或者，第一区块链网络中的轻量节点将数据同步请求发送至第二区块链网络中的目标全量节点，该目标全量节点是由第二区块链网络中所有全量节点通过共识算法选举出来的节点。

步骤 S420：全量节点接收轻量节点发送的数据同步请求，查找与所述轻量节点对应的关联区块。

- 35 其中，关联区块是在区块链中与轻量节点具有关联关系的区块；具有关联关系的区块可以是区块链网络中与该轻量节点具有关联关系的实时区块，也可以是区块链网络中与该轻量节点具有关联关系的历史区块。该关联区块

中包括多个交易以及统计证明交易列表；多个交易具有其各自对应的交易可见地址。

5 在一种可能的实现方式中，数据同步请求包括轻量节点的身份信息，则全量节点可以从该数据同步请求中获取轻量节点的身份信息，然后，全量节点可以对获取到的轻量节点的身份信息进行校验。具体实现时，身份信息可以包括轻量节点的数字签名，该数字签名是轻量节点根据轻量节点的私钥对数据同步请求进行签名处理得到的；全量节点接收来自轻量节点的身份信息之后，可以根据轻量节点的公钥，对轻量节点的数字签名进行校验，若校验成功，则表明轻量节点的身份校验通过。通过这种方式，对轻量节点身份的合法性进行校验，有利于提高轻量节点与全量节点之间的数据安全性，保证将数据传输给合法的轻量节点。

10 另外，身份信息还可以包含轻量节点的数字证书，该数字证书可以是公钥证书体系（Public Key Infrastructure, PKI），在公钥证书体系中，数字证书是一个公钥拥有者的身份证明，可以由权威机构例如 CA 机构颁发。全量节点可以校验轻量节点的数字证书，具体可以通过关键字提取算法获取数字证书中的关键字，以及通过图像识别算法识别数字证书中的目标图像，全量节点根据获取到的关键字以及目标图像等，对轻量节点的数字证书进行校验，若对轻量节点的数字证书校验通过，则表明轻量节点的身份校验通过。

15 在一种可能的实现方式中，全量节点可以获取轻量节点的节点地址，进而根据轻量节点的节点地址在区块链中获取与轻量节点对应的关联区块。若区块链上某个区块包含的交易中，存在至少一个交易的交易可见地址包括该轻量节点的节点地址，那么该区块就是与轻量节点具有关联关系的关联区块。

20 其中，节点地址的生成过程可以包括：基于密钥对生成节点地址，具体的，每个密钥对包括一个私钥和一个公钥。私钥是一个数字，通常是通过随机算法随机选出的。基于私钥，可以使用椭圆曲线乘法这个单向加密函数产生一个公钥。基于公钥，可以使用一个单向加密哈希函数生成比特币地址，即节点地址，其中，区块链网络中的每个节点对应一个唯一的节点地址。

25 步骤 S430：全量节点从所述关联区块中提取统计证明交易列表，并在所述统计证明交易列表中识别轻量节点的目标索引；以及，从关联区块包括的多个交易中过滤出与所述轻量节点关联的关联交易，并基于所过滤出的关联交易确定加密路径集合。

30 具体实现时，统计证明交易列表包括多个统计证明交易，每个统计证明交易是对关联区块包括的交易对应的交易可见地址、以及该交易可见地址在关联区块中的数量进行加密处理得到的，具体可以采用加密算法进行加密处理，加密算法包括但不限于：消息摘要算法第五版（Message-Digest Algorithm 5, MD5）、安全散列算法 256（Secure Hash Algorithm 256, SHA256）、安全

散列算法 512 (Secure Hash Algorithm512, SHA512)、安全散列算法 384 (Secure Hash Algorithm384, SHA384)、安全散列算法 1 (Secure Hash Algorithm 1, SHA-1) 等、哈希运算消息认证码算法 (Hash-based Message Authentication Code, HMAC)、AES 算法、DES 算法、3DES 算法、RSA 算法以及 ECC 算法等。

具体实现时,与轻量节点关联的关联交易的数量可以为一个,也可以为多个,并且,关联交易可以包括由轻量节点发起的交易,关联交易也可以包括由轻量节点接收的交易,关联交易还可以包括由轻量节点见证的交易。若关联区块中某个交易的交易可见地址包括轻量节点的节点地址,那么该交易就是与轻量节点关联的交易(交易可见地址可以是交易发起方人工指定的)。值得注意的是,若关联区块中某个交易是由轻量节点发起的,那么该轻量节点的节点地址必然是该交易的交易可见地址。

另外,加密路径集合包括关联交易的加密路径以及统计证明交易列表的加密路径,具体的,加密路径可以为默克尔路径。其中,统计证明交易列表中包括的多个统计证明交易是按照顺序排列的,具体是指,多个统计证明交易是按照交易可见地址在关联区块包含的交易的出现顺序排列的。同时,轻量节点在统计证明交易列表中的目标索引可以是 1、2、3...,通过目标索引,可以获取轻量节点在统计证明交易列表中对应的目标统计证明交易。

其中,任意一笔交易的交易可见地址可以由交易发起者人为设定,交易可见地址的数量可以为一个或者多个。交易可见地址的数量是指该交易可见地址在关联区块中所关联的多个交易的数量。

举例来说,假设轻量节点 A 的节点地址为 A,轻量节点 A 发起一笔交易 X,轻量节点 A 可以指定该交易 X 的交易可见地址,假设为 B、C,即轻量节点 A 指定轻量节点 B 以及轻量节点 C 可见交易 X,因此,对于轻量节点 A、轻量节点 B 和轻量节点 C 来说,交易 X 均是其的关联交易。对于交易 X 来说,交易 X 的交易可见地址包括 A、B 以及 C。

步骤 S440: 全量节点向轻量节点发送所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合。

在一种可能的实现方式中,若全量节点对轻量节点的身份信息校验通过,则全量节点将统计证明交易列表、目标索引、关联交易以及加密路径集合发送至该轻量节点。另外,全量节点还可以将关联区块的区块头也发送至该轻量节点,其中,关联区块的区块头包括但不限于:关联区块的版本号、输入信息特征值、时间戳、难度值以及区块默克尔根等。

步骤 S450: 轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效程度用于表征所述关联交易的准确度以及完整度。

具体实现时,关联交易的有效程度可以包括关联交易的准确度以及关联

交易的完整度。具体的，轻量节点可以根据加密路径集合，校验关联交易是否准确，即校验关联交易是否被篡改，从而得到准确度；轻量节点可以根据目标索引、统计证明交易列表以及统计证明交易列表的加密路径，校验关联交易是否完整，即校验关联交易的内容是否存在缺失，从而得到完整度。

- 5 在一种可能的实现方式中，轻量节点根据统计证明交易列表、目标索引、关联交易以及加密路径集合，确定关联交易的有效程度之前，可以获取全量节点的身份信息，该身份信息具体可以包括全量节点的数字签名，该数字签名是全量节点根据全量节点的私钥，对统计证明交易列表、目标索引、关联交易以及加密路径集合进行签名处理得到的。轻量节点获取全量节点的身份信息之后，可以根据全量节点的公钥，对全量节点的数字签名进行校验，若
10 校验成功，则表明该全量节点的身份信息校验通过。通过这种方式，能够提高轻量节点与全量节点之间的数据安全性。

- 本申请实施例提供的数据通信方法，可以应用于包括第一区块链网络和第二区块链网络的双层区块链网络，轻量节点处于第一区块链网络中，全量
15 节点处于第二区块链网络中，轻量节点与全量节点之间可以进行数据交流，具体的，轻量节点可以向全量节点发送数据同步请求，全量节点接收到轻量节点的数据同步请求之后，可以向该轻量节点发送其关联的关联交易。在本方案中，统计证明交易列表将每个交易可见地址的数量放入了区块中，但又没有将相关的交易明文放入，区块链网络中任一节点获得统计证明交易列表
20 时，由于没有全部交易信息，因此无法计算出每个节点地址对应的统计证明交易。加密路径集合保证了交易单体正确无篡改，统计证明交易列表保证了所得的关联交易总数和链上的一致，无篡改。两个证明叠加，可以完全相信所得到的数据就是区块中该节点可获得的数据，且应有的全部信息均完备。如此，在不泄露其他交易可见地址的数量的情况下，每个轻量节点可以验证
25 自身同步数据的正确性和完整性，保证了敏感业务数据的安全隔离以及安全隔离之后的有效性证明，实现了轻量节点与全量节点之间数据的隔离性，提高了数据的安全性。

- 请参见图 5，图 5 是本申请实施例提供的另一种数据处理方法的流程示意图。该方法应用于区块链网络，区块链网络包括第一区块链网络和第二区块链网络，第一区块链网络包括轻量节点，第二区块链网络包括全量节点。该方法的操作步骤可由计算机设备执行，计算机设备可以是轻量节点。本实施例主要描述轻量节点对关联交易的验证过程，该方法包括但不限于如下步骤 S510~S540：
30 步骤 S510：从与所述轻量节点具有关联关系的关联区块中接收数据，所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表，所述关联区块中包括多个交易以及所述统计证明交易列表，所

- 35 步骤 S510：从与所述轻量节点具有关联关系的关联区块中接收数据，所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表，所述关联区块中包括多个交易以及所述统计证明交易列表，所

述多个交易具有其各自对应的交易可见地址,所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的。

步骤 S520: 在所述统计证明交易列表中识别所述轻量节点的目标索引。

- 5 具体实现时,轻量节点接收全量节点发送的其从关联区块中提取的统计证明交易列表;以及接收全量节点发送的其在统计证明交易列表中识别出的该轻量节点的目标索引,或者,轻量节点也可以从所接收的统计证明交易列表中识别自身的目标索引。

- 其中,统计证明交易列表包括多个统计证明交易,多个统计证明交易按照交易可见地址的出现顺序进行排列,具体排列方式可以为顺位排列、逆位排列等等。例如,统计证明交易列表可以包括统计证明交易 1、统计证明交易 2 以及统计证明交易 3,其中,统计证明交易 1 是对关联区块包括的交易的交易可见地址 1、以及交易可见地址 1 在关联区块中的数量 m1 进行加密处理得到的,同理,统计证明交易 2 是对关联区块包括的交易的交易可见地址 2、以及交易可见地址 2 在关联区块中的数量 m2 进行加密处理得到的,统计证明交易 3 是对关联区块包括的交易的交易可见地址 3、以及交易可见地址 3 在关联区块中的数量 m3 进行加密处理得到的。若交易可见地址 1、交易可见地址 2 以及交易可见地址 3 在交易中的出现顺序依次为交易可见地址 1,交易可见地址 2,交易可见地址 3,那么,统计证明交易列表中统计证明交易的排列顺序可以为:统计证明交易 1,统计证明交易 2,统计证明交易 3。

此外,轻量节点还可以接收全量节点从关联区块中提取的、与该轻量节点关联的关联交易。关联交易的交易数量可以为一个或者多个。

- 25 步骤 S530: 基于所述关联交易获取加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径。

- 具体实现时,轻量节点接收全量节点发送的加密路径集合。其中,加密路径集合包括关联交易的加密路径,关联交易的交易数量可以为一个或者多个,由于统计证明交易列表本身也是一个交易,因此加密路径集合还包括统计证明交易列表的加密路径。举例来说,若关联交易的数量为 n 个,关联交易分别为 x1, x2, x3, ..., xn,则加密路径集合包括 x1 的加密路径, x2 的加密路径, x3 的加密路径, ..., xn 的加密路径和统计证明交易列表的加密路径。

- 35 在一种可能的实现方式中,如图 6A 所示,图 6A 是本申请实施例提供的一种获取加密路径的流程示意图。加密路径具体可以为是通过默克尔树得到的默克尔路径,对于交易 x1 来说,交易 x1 对应的加密路径为: N1 和 N5,交易 x2 对应的加密路径为: N0 和 N5,交易 x3 对应的加密路径为: N3 和 N4,交易 x4 对应的加密路径为: N2 和 N4。其中,关联交易和统计

证明交易列表可以为交易 x1, 交易 x2, 交易 x3 以及交易 x4 中的任一交易。

步骤 S540: 根据所述统计证明交易列表、所述目标索引以及所述加密路径集合, 确定所述关联交易的有效程度; 所述有效程度用于表征所述关联交易的准确度以及完整度。

- 5 具体实现时, 有效性程度可以包括准确度和完整度。轻量节点可以基于加密路径集合, 校验关联交易是否准确, 得到其准确度; 可以基于目标索引、统计证明交易列表以及统计证明交易列表的加密路径, 校验关联交易是否完整, 得到其完整度。

- 10 在一种可能的实现方式中, 关联交易的数量为多个, 多个关联交易包括第一关联交易和第二关联交易, 多个关联交易的加密路径包括第一关联交易对应的第一加密路径和第二关联交易对应的第二加密路径。轻量节点根据第一关联交易以及第一加密路径, 确定第一默克尔根, 轻量节点根据第二关联交易以及第二加密路径, 确定第二默克尔根。然后, 轻量节点接收关联区块的区块默克尔根, 若第一默克尔根、第二默克尔根以及区块默克尔根均相同,
15 则轻量节点确定关联交易准确。若第一默克尔根、第二默克尔根以及区块默克尔根中存在至少两个默克尔根不相同, 则轻量节点确定关联交易不准确。

- 举例来说, 如图 6A, 假设关联交易包括交易 x1, 交易 x2, 交易 x3 以及交易 x4, 交易 x1 对应的加密路径为: N1 和 N5, 交易 x2 对应的加密路径为: N0 和 N5, 交易 x3 对应的加密路径为: N3 和 N4, 交易 x4 对应的加密路径为: N2 和 N4。那么, 轻量节点根据交易 x1, N1 和 N5, 可以确定第一默克尔根, 具体为: 轻量节点通过哈希算法对交易 x1 进行哈希运算, 得到 hash(x1), 然后, 轻量节点再次对 hash(x1) 和 N1 进行哈希运算, 得到 hash[hash(x1)+N1], 最后, 轻量节点对 hash[hash(x1)+N1] 和 N5 进行哈希运算, 得到 hash{hash[hash(x1)+N1]+N5}, 即默克尔根 root1,
20 同理, 轻量节点可以得到交易 x2 对应的默克尔根 root2=hash{hash[hash(x2)+N0]+N5}, 轻量节点可以得到交易 x3 对应的默克尔根 root3=hash{hash[hash(x3)+N3]+N4}, 轻量节点可以得到交易 x4 对应的默克尔根 root4=hash{hash[hash(x4)+N2]+N4}。轻量节点获取区块默克尔根为 Root, 若 root1、root2、root3、root4 均与 Root 相同, 则轻量节点确定关联交易的准确性结果为具有准确性。若 root1 与 Root 相同, root2 与 Root 相同, root3 与 Root 不相同, root4 与 Root 不相同, 则轻量节点确定交易 x1 和交易 x2 的准确, 交易 x3 和交易 x4 不准确, 进而轻量节点确定关联交易的准确度为不准确。
30 轻量节点通过上述方式, 基于关联交易及其对应的加密路径, 确定关联交易对应的默克尔根, 进而根据关联交易对应的默克尔根和关联区块的区块默克尔根, 校验关联交易是否被篡改, 即确定关联交易的准确度。可以实现高效且准确地校验, 保证校验得到的准确性结果的可靠性。

- 35 轻量节点通过上述方式, 基于关联交易及其对应的加密路径, 确定关联交易对应的默克尔根, 进而根据关联交易对应的默克尔根和关联区块的区块默克尔根, 校验关联交易是否被篡改, 即确定关联交易的准确度。可以实现高效且准确地校验, 保证校验得到的准确性结果的可靠性。

在一种可能的实现方式中，轻量节点基于统计证明交易列表的加密路径，校验统计证明交易列表是否有效，统计证明交易列表是否有效相应地表征统计证明交易列表是否被篡改。具体的，轻量节点通过统计证明交易列表的加密路径，确定统计证明交易列表是否有效，具体可以参考以上轻量节点通过关联交易和关联交易的加密路径，确定关联交易的准确度的执行步骤，在此不再赘述。

在一种可能的实现方式中，若轻量节点校验确定统计证明交易列表有效，则从关联区块中接收关联交易的交易数量，以及在统计证明交易列表中查找与目标索引对应的目标统计证明交易。对交易数量和轻量节点的节点地址进行叠加运算，得到目标叠加值，并通过加密算法对目标叠加值进行加密运算，得到轻量节点的目标业务交易；若目标统计证明交易与目标业务交易相同，则轻量节点确定关联交易完整。

举例来说，假设关联交易的交易数量为 $m1$ 个，轻量节点的节点地址为 $address1$ 。轻量节点对交易数量和节点地址进行叠加运算，得到目标叠加值为： $address1+m1$ ，然后轻量节点通过哈希算法对目标叠加值进行哈希运算，得到 $hash(address1+m1)$ ，进一步地，轻量节点通过消息认证码算法(Message Authentication Code, MAC) 对 $hash(address1+m1)$ 进行加密，得到 $MAC[hash(address1+m1)]$ ，即轻量节点的目标业务交易。如图 6B，图 6B 为本申请实施例提供的一种统计证明交易列表的示意图，若目标索引为 1，则轻量节点根据目标索引 1 在统计证明交易列表中获取目标统计证明交易 $MAC[hash(address1+m1)]$ 。最后，若目标业务交易与目标统计证明交易相同，则可以确定关联交易完整，若目标业务交易与目标统计证明交易不相同，则可以确定关联交易不完整。

轻量节点通过上述方式，在校验统计证明交易列表有效的情况下，根据该统计证明交易列表、该统计证明交易列表中与自身相关的目标统计证明交易、交易数量和自身的节点地址，校验所接收的关联交易是否存在缺失，即校验关联交易的完整度。可以高效且准确地确定该完整度，即在仅需执行较简化的校验流程的情况下，即可准确地校验关联交易是否存在缺失。

通过本申请实施例提供的方法，在双层区块链网络的基础之上，轻量节点在向全量节点同步与自身相关的关联交易之后，可以通过关联交易、加密路径集合、统计证明交易列表以及统计证明交易列表的加密路径，确定关联交易是否准确以及是否完整。具体的，轻量节点可以根据加密路径集合，确定关联交易的准确度；以及可以根据目标索引、统计证明交易列表以及统计证明交易列表的加密路径，确定关联交易的完整度。轻量节点在确定关联交易具有有效程度之后，可以基于关联交易进行后续处理，相比于现有技术中轻量节点获得关联交易之后直接根据关联交易进行后续处理，可以进一步提高关联交易的准确性。

请参见图 7, 图 7 是本申请实施例所提供的另一种数据处理方法的流程示意图。该方法应用于区块链网络, 区块链网络包括第一区块链网络和第二区块链网络, 第一区块链网络包括轻量节点, 第二区块链网络包括全量节点。
5 该方法的操作步骤可由计算机设备执行, 计算机设备可以是全量节点。本实施例主要描述全量节点响应数据同步请求的过程, 该方法包括但不限于如下步骤 S710~S740:

步骤 S710: 接收轻量节点发送的数据同步请求, 查找与所述轻量节点对应的关联区块; 所述关联区块是与所述轻量节点具有关联关系的区块; 所述关联区块中包括多个交易以及统计证明交易列表; 所述多个交易具有其各自对应的交易可见地址; 所述统计证明交易列表包括多个统计证明交易, 所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的。
10

具体实现时, 数据同步请求包括轻量节点的身份信息, 全量节点接收到轻量节点发送的数据同步请求之后, 可以获取轻量节点的身份信息, 并对轻量节点的身份信息进行校验, 若全量节点对轻量节点的身份信息校验通过, 则可以获取轻量节点对应的关联区块。需要说明的是, 全量节点对轻量节点的身份信息进行校验的操作步骤具体可参见上述图 4 实施例的步骤 S420 中全量节点的具体操作过程, 本申请实施例在此不再赘述。
15

在一种可能的实现方式中, 全量节点接收待处理交易, 待处理交易包括多个交易可见地址; 全量节点统计待处理交易中每个交易可见地址的数量; 进而, 针对每个交易可见地址以及每个交易可见地址的交易可见数量进行加密处理, 得到统计证明交易列表。
20

举例来说, 全量节点获取第一区块链网络中任意轻量节点发起的待处理交易, 假设轻量节点 A 发起一笔待处理交易 x1, 轻量节点 A 可以指定第一区块链网络中哪些轻量节点可以看见这笔待处理交易 x1, 被指定的轻量节点对应的节点地址即为交易可见地址, 若轻量节点 A 指定轻量节点 B 和轻量节点 C 可见待处理交易 x1, 假设轻量节点 A 的节点地址为 address1, 轻量节点 B 的节点地址为 address2, 轻量节点 C 的节点地址为 address3, 则待处理交易 x1 的交易可见地址为 address1、address2 和 address3, 以此类推, 待处理交易的数量可以为多个。
25
30

全量节点通过上述方式, 根据待处理交易包括的交易可见地址以及交易可见地址的数量, 生成统计证明交易列表; 有效地将每个交易可见地址的数量放入了区块中, 但又没有将相关的交易明文放入, 当区块链网络中任一节点获得统计证明交易列表时, 由于没有全部交易信息, 因此无法计算出每个节点地址对应的统计证明交易, 保证了区块链网络中节点与节点之间数据通信的安全性, 并且有利于轻量节点基于该统计证明交易列表, 校验与其相关
35

的关联交易是否准确以及是否完整。

在一种可能的实现方式中,统计证明交易列表包括第一统计证明交易以及第二统计证明交易,多个交易可见地址包括第一交易可见地址和第二交易可见地址。全量节点对第一交易可见地址以及第一交易可见地址的数量进行加密处理,得到第一统计证明交易;对第二交易可见地址以及第二交易可见地址的数量进行加密处理,得到第二统计证明交易。进而,全量节点将第一统计证明交易以及第二统计证明交易组合为统计证明交易列表,其中,若第一交易可见地址在待处理交易中的出现顺序优先于第二交易可见地址在待处理交易中的出现顺序,则第一统计证明交易在统计证明交易列表中的排列顺序优先于第二统计证明交易在统计证明交易列表中的排列顺序。

需要说明的是,全量节点对第一交易可见地址和第一交易可见地址的数量进行加密处理,得到第一统计证明交易,以及对第二交易可见地址和第二交易可见地址的数量进行加密处理,得到第二统计证明交易,所采用的加密算法,应当与图 5 实施例轻量节点对目标叠加值进行加密处理得到目标统计证明交易时采用的加密算法一致,即先对叠加值进行哈希运算得到哈希值,然后再通过消息认证码算法对哈希值进行运算,得到每个统计证明交易。当然,此处的加密处理的方式不唯一,例如,还可以通过 HMAC 算法进行加密处理,只要与后续轻量节点对目标叠加值加密处理的方式一致即可,本申请实施例对此不作限定。

举例来说,全量节点可以按照出现顺序统计每个交易可见地址的数量,即全量节点依次统计交易可见地址 address1、address2、address3、address4 和 address5 各自对应数量,假设分别为 m1、m2、m3、m4 和 m5,交易可见地址和数量之间的对应关系可以如表 1.1 所示:

表 1.1

address1	m1
address2	m2
address3	m3
address4	m4
address5	m5

然后,全量节点将每个交易可见地址和及其数量进行叠加运算,得到多个叠加值,然后再对多个叠加值分别进行加密处理,得到统计证明交易列表,统计证明交易列表的数据结构可以是表格。在生成统计证明交易列表时,还需要确定每个统计证明交易对应的节点地址,并且确定每个节点地址在统计证明交易列表中的索引。

具体的,统计证明交易列表可以如表 1.2 所示:

表 1.2

Index1	MAC[hash(address1+m1)]
--------	------------------------

Index2	MAC[hash(address2+m2)]
Index3	MAC[hash(address3+m3)]
Index4	MAC[hash(address4+m4)]
Index5	MAC[hash(address5+m5)]

如表 1.2 所示，节点地址为“address1”的节点在统计证明交易列表中的索引为 1，节点地址为“address2”的节点在统计证明交易列表中的索引为 2，节点地址为“address3”的节点在统计证明交易列表中的索引为 3，节点地址为“address4”的节点在统计证明交易列表中的索引为 4，节点地址为“address5”的节点在统计证明交易列表中的索引为 5。

最后，全量节点根据统计证明交易列表和待处理交易生成关联区块，具体的，全量节点可以将统计证明交易列表作为第一笔交易，然后将待处理交易依次作为第一笔交易的下一笔交易，根据每笔交易生成关联区块，并将关联区块存储至区块链，其中，存储至区块链中的待处理交易均可称为交易。

全量节点通过上述方式生成统计证明交易列表，可以保证所生成的统计证明交易列表中各统计证明交易的排序合理，从而便于从中识别轻量节点对应的目标索引，有助于提高轻量节点确定关联交易的有效性结果的效率。

在一种可能的实现方式中，假设根据统计证明交易列表和待处理交易生成关联区块的全量节点为第一全量节点，第一全量节点根据统计证明交易列表和待处理交易生成关联区块之后，可以将该关联区块发布至第二区块链网络中的多个第二全量节点，以使每个第二全量节点对关联区块进行区块链共识。若区块链共识通过，则第一全量节点将关联区块发布至第二区块链网络中，并存储至区块链。其中，第二全量节点为第二区块链网络中除第一全量节点以外的所有节点。

在一种可能的实现方式中，全量节点获取与轻量节点对应的关联区块，可以通过区块高度的方式进行获取，具体的，全量节点接收到轻量节点发送的数据同步请求后，可以获取轻量节点的节点地址，进而确定该全量节点储存的区块链中包含全量节点的节点地址的区块，全量节点将包含轻量节点的节点地址的中的区块高度最大对应的区块，作为与轻量节点对应的关联区块。

步骤 S720：从所述关联区块中提取统计证明交易列表，并在所述统计证明列表中识别所述轻量节点的目标索引。

具体实现时，全量节点从关联区块中提取统计证明交易列表，可以将从关联区块的区块体中提取到的第一笔交易作为统计证明交易列表，全量节点从关联区块中提取轻量节点在统计证明交易列表中的目标索引，具体方式可以为，全量节点根据轻量节点的节点地址，在统计证明交易列表中查找轻量节点在统计证明交易列表中的目标索引。

步骤 S730：从所述关联区块包括的所述多个交易中过滤出与所述轻量

节点关联的关联交易，并基于所过滤出的关联交易确定加密路径集合，所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径。

具体实现时，全量节点从关联区块中提取与轻量节点关联的关联交易，与轻量节点关联的关联交易可以包括轻量节点发起的交易、轻量节点接收的交易以及轻量节点见证的交易。举例来说，交易 x1 假设是轻量节点发起的，则交易 x1 可以为轻量节点的关联交易，交易 x2 假设是轻量节点接收的，则交易 x2 可以为轻量节点的关联交易，交易 x3 是节点 1 发起的，但是交易 x3 的交易可见地址包括轻量节点，则交易 x3 也可以为轻量节点的关联交易。也就是说，全量节点可以将轻量节点的节点地址作为一个交易可见地址，在关联区块中获取到该交易可见地址所对应的交易，即为该轻量节点的关联交易，关联交易的数量可以为一个或者多个。

步骤 S740：将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点，以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合，确定所述关联交易的有效程度；所述有效程度用于表征所述关联交易的准确度以及完整度。

具体实现时，第二区块链网络中的全量节点通过区块链网络中的网络路由服务，将统计证明交易列表、目标索引、关联交易以及加密路径集合发送至第一区块链网络中的轻量节点。其中，轻量节点根据统计证明交易列表、目标索引以及加密路径集合，确定关联交易的有效程度的操作步骤具体可参见图 5 实施例中步骤 S540 中轻量节点的执行步骤，本申请在此不再赘述。

通过本申请实施例所提供的方法，第二区块链网络中的全量节点接收到第一区块链网络中的轻量节点发送的数据同步请求之后，可以对轻量节点进行身份校验，当全量节点对轻量节点身份校验通过后，全量节点才将轻量节点所需同步的数据，包括统计证明交易列表、目标索引、关联交易以及加密路径集合，发送至所述轻量节点。统计证明交易列表有效地将每个交易可见地址的数量放入了区块中，但又没有将相关的交易明文放入，当区块链网络中任一节点获得统计证明交易列表时，由于没有全部交易信息，因此无法计算出每个节点地址对应的统计证明交易。因此，可以提高区块链网络中节点与节点之间数据交流的安全性。

请参见图 8，图 8 是本申请实施例提供的一种数据通信装置的结构示意图。图 8 是本申请实施例所提供的一种数据通信装置的结构示意图。该数据通信装置可应用于图 5~图 6B 对应的方法实施例中的轻量节点。数据通信装置可以是运行于轻量节点中的一个计算机程序（包括程序代码），例如该数据通信装置为一个应用软件；该装置可以用于执行本申请实施例提供的方法中的相应步骤。该数据通信装置可包括：

接收单元 810, 用于从与所述轻量节点具有关联关系的关联区块中接收数据, 所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表, 所述关联区块中包括多个交易以及所述统计证明交易列表, 所述多个交易具有其各自对应的交易可见地址, 所述统计证明交易列表

5 包括多个统计证明交易, 所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

识别单元 820, 用于在所述统计证明交易列表中识别所述轻量节点的目标索引;

获取单元 830, 用于基于所述关联交易获取加密路径集合, 所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

10

确定单元 840, 用于根据所述统计证明交易列表、所述目标索引以及所述加密路径集合, 确定所述关联交易的有效程度; 所述有效程度用于表征所述关联交易的准确度以及完整度。

15 在一种可能的实现方式中, 确定单元 840 具体用于:

基于所述加密路径集合, 校验所述关联交易是否准确, 得到所述准确度;

基于所述目标索引、所述统计证明交易列表以及所述统计证明交易列表的加密路径, 校验所述关联交易是否完整, 得到所述完整度。

在一种可能的实现方式中, 关联交易的数量为多个, 所述多个关联交易

20 包括第一关联交易和第二关联交易, 所述多个关联交易的加密路径包括第一关联交易对应的第一加密路径和第二关联交易对应的第二加密路径;

确定单元 840 具体用于:

根据所述第一关联交易以及所述第一加密路径, 确定第一默克尔根, 根据所述第二关联交易以及所述第二加密路径, 确定第二默克尔根;

25 基于所述第一默克尔根和所述第二默克尔根, 校验所述关联交易是否准确, 得到所述准确度。

在一种可能的实现方式中, 确定单元 840 具体用于:

接收所述关联区块的区块默克尔根;

30 若所述第一默克尔根、所述第二默克尔根以及所述区块默克尔根均相同, 则确定所述关联交易准确;

若所述第一默克尔根、所述第二默克尔根以及所述区块默克尔根中存在至少两个默克尔根不相同, 则确定所述关联交易不准确。

在一种可能的实现方式中, 确定单元 840 具体用于:

35 根据所述统计证明交易列表的加密路径, 校验所述统计证明交易列表是否有效;

若校验确定所述统计证明交易列表有效, 则从所述关联区块中接收所述关联交易的交易数量;

在所述统计证明交易列表中查找所述目标索引对应的目标统计证明交易；

根据所述统计证明交易列表、所述目标统计证明交易、所述交易数量以及所述轻量节点的节点地址，校验所述关联交易是否完整，得到所述完整度。

5 在一种可能的实现方式中，确定单元 840 具体用于：

对所述交易数量和所述轻量节点的节点地址进行叠加运算，得到目标叠加值，并通过加密算法对所述目标叠加值进行加密运算，得到所述轻量节点的目标业务交易；

10 若所述目标统计证明交易与所述目标业务交易相同，则确定所述关联交易完整。

通过本申请实施例提供的数据通信装置，在双层区块链网络的基础上，轻量节点在向全量节点同步与自身相关的关联交易之后，可以通过关联交易、加密路径集合、统计证明交易列表以及统计证明交易列表的加密路径，确定关联交易的有效性结果。具体的，轻量节点可以根据加密路径集合，确定关联交易的准确度；根据目标索引、统计证明交易列表、以及统计证明交易列表的加密路径，确定关联交易的完整度。轻量节点确定出关联交易的有效程度之后，可以基于该有效程度根据关联交易进行后续处理，相比于现有技术中轻量节点获得关联交易之后直接根据关联交易进行后续处理，可以进一步提高关联交易的准确性。

20

请参见图 9，图 9 是本申请实施例提供的一种数据通信装置的结构示意图。图 9 是本申请实施例所提供的一种数据通信装置的结构示意图。该数据通信装置可应用于图 7 对应的方法实施例中的全量节点。数据通信装置可以是运行于全量节点中的一个计算机程序（包括程序代码），例如该数据通信装置为一个应用软件；该装置可以用于执行本申请实施例提供的方法中的相应步骤。该数据通信装置可包括：

25 接收单元 910，用于接收轻量节点发送的数据同步请求，查找与所述轻量节点对应的关联区块；所述关联区块是与所述轻量节点具有关联关系的区块；所述关联区块中包括多个交易以及统计证明交易列表；所述多个交易具有其各自对应的交易可见地址；所述统计证明交易列表包括多个统计证明交易，所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的。

30 提取单元 920，用于从所述关联区块中提取统计证明交易列表，并在所述统计证明列表中识别所述轻量节点的目标索引。

35 提取单元 920，还用于从所述关联区块包括的所述多个交易中过滤出与所述轻量节点关联的关联交易，并基于所过滤出的关联交易确定加密路径集合，所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易

列表的加密路径。

发送单元 930, 用于将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点, 以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合, 确定所述关联交易的有效程度; 所述有效程度用于表征所述关联交易的准确度以及完整度。

在一种可能的实现方式中, 该数据处理装置还包括: 获取单元 940、统计单元 950、处理单元 960。

获取单元 940, 用于接收待处理交易, 所述待处理交易包括多个交易可见地址;

统计单元 950, 用于统计所述待处理交易中每个交易可见地址的数量;

处理单元 960, 用于针对每个交易可见地址以及每个交易可见地址的数量分别进行加密处理, 得到统计证明交易列表;

处理单元 960, 还用于根据所述统计证明交易列表和所述待处理交易生成关联区块, 并将所述关联区块存储至区块链。

在一种可能的实现方式中, 统计证明交易列表包括第一统计证明交易以及第二统计证明交易, 所述多个交易可见地址包括第一交易可见地址和第二交易可见地址;

处理单元 960 具体用于:

对第一交易可见地址以及第一交易可见地址的数量进行加密处理, 得到所述第一统计证明交易;

对第二交易可见地址以及第二交易可见地址的数量进行加密处理, 得到所述第二统计证明交易;

将所述第一统计证明交易以及所述第二统计证明交易组合为所述统计证明交易列表, 若所述第一交易可见地址在所述待处理交易中的出现顺序优先于所述第二交易可见地址在所述待处理交易中的出现顺序, 则所述第一统计证明交易在所述统计证明交易列表中的排列顺序优先于所述第二统计证明交易在所述统计证明交易列表中的排列顺序。

在一种可能的实现方式中, 数据同步请求包括所述轻量节点的身份信息;

发送单元 930 将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点, 包括:

对所述轻量节点的身份信息进行校验;

若对所述身份信息校验通过, 则将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点。

在一种可能的实现方式中, 区块链对应的区块链网络包括第一区块链网络和第二区块链网络, 所述轻量节点是第一区块链网络中的节点, 所述轻量

节点用于存储所述轻量节点的关联交易，所述全量节点用于存储所述区块链，所述区块链包括所述第一区块链网络中所有节点的关联交易。

通过本申请实施例提供的数据通信装置，第二区块链网络中的全量节点响应第一区块链网络中的轻量节点发送的数据同步请求，可以对轻量节点进行身份校验，当全量节点对轻量节点身份校验通过后，全量节点将轻量节点需要同步的数据，包括统计证明交易列表、目标索引、关联交易以及加密路径集合发送至所述轻量节点。统计证明交易列表有效地将交易可见地址的数量放入了区块中，但又没有将相关的交易明文放入，区块链网络中任一节点获得统计证明交易列表，由于没有全部交易信息，因此无法计算出每个节点地址对应的统计证明交易。因此，可以提高区块链网络中节点与节点之间数据交流的安全性。

请参见图 10，图 10 是本申请实施例提供的一种计算机设备的结构示意图。上述图 4~图 7 对应实施例中的轻量节点可以为计算机设备 1000，如图 10 所示，计算机设备 1000 可以包括：用户接口 1002、处理器 1004、编码器 1006 以及存储器 1008。信号接收器 1016 用于经由蜂窝接口 1010、WIFI 接口 1012、...、或 NFC 接口 1014 接收或者发送数据。编码器 1006 将接收到的数据编码为计算机处理的数据格式。存储器 1008 中存储有计算机程序，处理器 1004 被设置为通过计算机程序执行上述任一项方法实施例中的步骤。存储器 1008 可包括易失性存储器（例如，动态随机存取存储器 DRAM），还可以包括非易失性存储器（例如，一次性可编程只读存储器 OTPROM）。在一些实例中，存储器 1008 可进一步包括相对于处理器 1004 远程设置的存储器，这些远程存储器可以通过网络连接至计算机设备 1000。用户接口 1002 可以包括：键盘 1018 和显示器 1020。

在图 10 所示的计算机设备 1000 中，处理器 1004 可以用于调用存储器 1008 中存储计算机程序，以实现上文方法实施例中的轻量节点侧的数据通信方法、或者上文方法实施例中的全量节点侧的数据通信方法。

应当理解，本申请实施例中所描述的计算机设备 1000 执行前文图 4 到图 7 所对应实施例中对数据通信方法的描述，也可执行前文图 8 和图 9 所对应实施例中对数据通信装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

本申请实施例还提供了一种计算机存储介质，且计算机存储介质中存储有前文提及的数据处理装置所执行的计算机程序，且该计算机程序包括程序指令，当处理器执行上述程序指令时，能够执行前文图 4 到图 7 所对应实施例中的方法，因此，这里将不再进行赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。对于本申请所涉及的计算机存储介质实施例中未披露的技术细节，请参照本申请方法实施例的描述。作为示例，程序指令可

以被部署在一个计算机设备上,或者在位于一个地点的多个计算机设备上执行,又或者,在分布在多个地点且通过通信网络互连的多个计算机设备上执行,分布在多个地点且通过通信网络互连的多个计算机设备可以组成区块链系统。

5 根据本申请的一个方面,提供了一种计算机程序产品或计算机程序,该计算机程序产品或计算机程序包括计算机指令,该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令,处理器执行该计算机指令,使得该计算机设备可以执行前文图 4 到图 7 所对应实施例中的方法,因此,这里将不再进行赘述。

10 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,上述程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,上述存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory, ROM)或随机存储记忆体(Random Access Memory, RAM)等。

15 以上所揭露的仅为本申请的部分实施例而已,当然不能以此来限定本申请之权利范围,本领域普通技术人员可以理解实现上述实施例的全部或部分流程,并依本申请权利要求所作的等同变化,仍属于发明所涵盖的范围。

权 利 要 求

1、一种数据通信方法，由轻量节点执行，所述方法包括：

从与所述轻量节点具有关联关系的关联区块中接收数据，所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表，
5 所述关联区块中包括多个交易以及所述统计证明交易列表，所述多个交易具有其各自对应的交易可见地址，所述统计证明交易列表包括多个统计证明交易，所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的；

在所述统计证明交易列表中识别所述轻量节点的目标索引；

10 基于所述关联交易获取加密路径集合，所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径；

根据所述统计证明交易列表、所述目标索引以及所述加密路径集合，确定所述关联交易的有效程度；所述有效性程度用于表征所述关联交易的准确度以及完整度。

15 2、根据权利要求 1 所述的方法，所述根据所述统计证明交易列表、所述目标索引以及所述加密路径集合，确定所述关联交易的有效程度，包括：

基于所述加密路径集合，校验所述关联交易是否准确，得到所述准确度；

基于所述目标索引、所述统计证明交易列表以及所述统计证明交易列表的加密路径，校验所述关联交易是否完整，得到所述完整度。

20 3、根据权利要求 2 所述的方法，所述关联交易的数量为多个，所述多个关联交易包括第一关联交易和第二关联交易，所述多个关联交易的加密路径包括所述第一关联交易对应的第一加密路径和所述第二关联交易对应的第二加密路径；

25 所述基于所述加密路径集合，校验所述关联交易是否准确，得到所述准确度，包括：

根据所述第一关联交易以及所述第一加密路径，确定第一默克尔根；

根据所述第二关联交易以及所述第二加密路径，确定第二默克尔根；

基于所述第一默克尔根和所述第二默克尔根，校验所述关联交易是否准确，得到所述准确度。

30 4、根据权利要求 3 所述的方法，所述基于所述第一默克尔根和所述第二默克尔根，校验所述关联交易是否准确，得到所述准确度，包括：

接收所述关联区块的区块默克尔根；

若所述第一默克尔根、所述第二默克尔根以及所述区块默克尔根均相同，则确定所述关联交易准确；

35 若所述第一默克尔根、所述第二默克尔根以及所述区块默克尔根中存在至少两个默克尔根不相同，则确定所述关联交易不准确。

5、根据权利要求 2 所述的方法，所述基于所述目标索引、所述统计证

明交易列表以及所述统计证明交易列表的加密路径,校验所述关联交易是否完整,得到所述完整度,包括:

根据所述统计证明交易列表的加密路径,校验所述统计证明交易列表是否有效;

- 5 若校验确定所述统计证明交易列表有效,则从所述关联区块中接收所述关联交易的交易数量;

在所述统计证明交易列表中查找所述目标索引对应的目标统计证明交易;

- 10 根据所述统计证明交易列表、所述目标统计证明交易、所述交易数量以及所述轻量节点的节点地址,校验所述关联交易是否完整,得到所述完整度。

6、根据权利要求5所述的方法,所述根据所述目标统计证明交易、所述交易数量以及所述轻量节点的节点地址,校验所述关联交易是否完整,得到所述完整度,包括:

- 15 对所述交易数量和所述轻量节点的节点地址进行叠加运算,得到目标叠加值,并通过加密算法对所述目标叠加值进行加密运算,得到所述轻量节点的目标业务交易;

若所述目标统计证明交易与所述目标业务交易相同,则确定所述关联交易完整。

7、一种数据通信方法,由全量节点执行,所述方法包括:

- 20 接收轻量节点发送的数据同步请求,查找与所述轻量节点对应的关联区块;所述关联区块是与所述轻量节点具有关联关系的区块;所述关联区块中包括多个交易以及统计证明交易列表;所述多个交易具有其各自对应的交易可见地址;所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

25 从所述关联区块中提取所述统计证明交易列表,并在所述统计证明列表中识别所述轻量节点的目标索引;

- 30 从所述关联区块包括的所述多个交易中过滤出与所述轻量节点关联的关联交易,并基于所过滤出的关联交易确定加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点,以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效程度用于表征所述关联交易的准确度以及完整度。

- 35 8、根据权利要求7所述的方法,所述方法还包括:

接收待处理交易,所述待处理交易包括多个交易可见地址;

统计所述待处理交易中每个交易可见地址的数量;

针对每个交易可见地址以及每个交易可见地址的数量分别进行加密处理,得到统计证明交易列表;

根据所述统计证明交易列表和所述待处理交易生成所述关联区块,并将所述关联区块存储至区块链。

- 5 9、根据权利要求 8 所述的方法,所述统计证明交易列表包括第一统计证明交易以及第二统计证明交易,所述多个交易可见地址包括第一交易可见地址和第二交易可见地址;

所述针对每个交易可见地址以及每个交易可见地址的数量分别进行加密处理,得到统计证明交易列表,包括:

- 10 对所述第一交易可见地址以及所述第一交易可见地址的数量进行加密处理,得到所述第一统计证明交易;

对所述第二交易可见地址以及所述第二交易可见地址的数量进行加密处理,得到所述第二统计证明交易;

- 15 将所述第一统计证明交易以及所述第二统计证明交易组合为所述统计证明交易列表,若所述第一交易可见地址在所述待处理交易中的出现顺序优先于所述第二交易可见地址在所述待处理交易中的出现顺序,则所述第一统计证明交易在所述统计证明交易列表中的排列顺序优先于所述第二统计证明交易在所述统计证明交易列表中的排列顺序。

- 20 10、根据权利要求 7 所述的方法,所述数据同步请求包括所述轻量节点的身份信息;

所述将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点,包括:

对所述轻量节点的身份信息进行校验;

- 25 若对所述身份信息校验通过,则将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点。

- 30 11、根据权利要求 7~10 中任一项所述的方法,所述区块链对应的区块链网络包括第一区块链网络和第二区块链网络,所述轻量节点是所述第一区块链网络中的节点,所述轻量节点用于存储所述轻量节点的关联交易,所述全量节点用于存储所述区块链,所述区块链包括所述第一区块链网络中所有节点的关联交易。

12、一种数据通信装置,所述数据处理装置包括:

- 35 接收单元,用于从与所述轻量节点具有关联关系的关联区块中接收数据,所述数据包括所述关联区块中与所述轻量节点关联的关联交易、以及统计证明交易列表,所述关联区块中包括多个交易以及所述统计证明交易列表,所述多个交易具有其各自对应的交易可见地址,所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

识别单元,用于在所述统计证明交易列表中识别所述轻量节点的目标索引;

获取单元,用于基于所述关联交易获取加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

- 5 确定单元,用于根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效程度用于表征所述关联交易的准确度以及完整度。

13、一种数据通信装置,所述数据处理装置包括:

- 10 接收单元,用于接收轻量节点发送的数据同步请求,查找与所述轻量节点对应的关联区块;所述关联区块是与所述轻量节点具有关联关系的区块;所述关联区块中包括多个交易以及统计证明交易列表;所述多个交易具有其各自对应的交易可见地址;所述统计证明交易列表包括多个统计证明交易,所述统计证明交易是对所述交易对应的交易可见地址、以及所述交易可见地址在所述关联区块中的数量进行加密处理得到的;

- 15 提取单元,用于从所述关联区块中提取所述统计证明交易列表,并在所述统计证明列表中识别所述轻量节点的目标索引;

- 提取单元,还用于从所述关联区块中包括的所述多个交易中过滤出与所述轻量节点关联的关联交易,并基于所过滤出的关联交易确定加密路径集合,所述加密路径集合包括所述关联交易的加密路径以及所述统计证明交易列表的加密路径;

- 发送单元,用于将所述统计证明交易列表、所述目标索引、所述关联交易以及所述加密路径集合发送至所述轻量节点,以使所述轻量节点根据所述统计证明交易列表、所述目标索引以及所述加密路径集合,确定所述关联交易的有效程度;所述有效程度用于表征所述关联交易的准确度以及完整度。

- 25 14、一种计算机设备,包括存储器以及处理器,所述存储器存储一组程序代码,所述处理器调用所述存储器中存储的程序代码,用于执行 1~6 或 7~11 中任一项所述的方法。

- 30 15、一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被处理器执行时使所述处理器执行如权利要求 1~6 或 7~11 中任一项所述的方法。

16、一种计算机程序产品,包括指令,当其在计算机上运行时,使得计算机实现如权利要求 1~6 或 7~11 中任一项所述的方法。