

发明名称：一种基于区块链的数据处理方法、设备以及可读存储介质

本申请要求于 2022 年 07 月 05 日提交中国专利局，申请号为 202210783272.8，申请名称为“一种基于区块链的数据处理方法、设备以及可读存储介质”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。

技术领域

本申请涉及互联网技术领域，尤其涉及一种基于区块链的数据处理方法、装置、计算机设备、可读存储介质和程序产品。

背景技术

随着网络技术的快速发展以及企业对数据安全的重视，区块链得到了重视和应用。

现有技术中，对于一个有公信力的区块链而言，区块链资源通常是有限的，区块链资源可以包括区块链的计算资源和存储资源，区块链的计算资源以及储存空间均是有限的，所以在区块数量不断增加时，该有公信力的区块链就会面临区块链资源不足的困境。

发明内容

本申请实施例提供一种基于区块链的数据处理方法、装置、计算机设备、可读存储介质和程序产品。

根据本申请提供的各种实施例，提供了一种基于区块链的数据处理方法，该方法由侧链节点执行，侧链节点属于联盟链中的侧区块链，联盟链还包括主区块链，该方法包括：

获取业务设备发送的携带业务交易的交易上链请求，根据交易上链请求，确定业务交易对应的交易执行结果，对交易执行结果以及业务交易进行上链处理；

当交易执行结果以及业务交易成功存储至侧区块链时，根据交易序号、业务类型标识以及交易执行结果，生成业务交易对应的业务交易摘要信息；交易序号用于表征业务交易在侧区块链中的序号，业务类型标识用于表征侧区块链所处理业务的业务类型；

将业务交易摘要信息传输至主区块链，以使主区块链存储业务交易摘要信息。

本申请实施例一方面提供了一种基于区块链的数据处理方法，由验证设备执行，包括：

发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链，以使主区块链将业务交易摘要信息返回至验证设备；交易序号用于表征业务交易在侧区块链中的序号；侧区块链属于联盟链；业务交易摘要信息是侧区块链传输至主区块链的；业务交易摘要信息，是侧区块链中的第一侧链节点在交易执行结果以及业务交易成功存储至侧区块链的情况下生成的，业务交易摘要信息，是根据交易序号、业务类型标识以及交易执行结果所生成的；交易执行结果是第一侧链节点在获取到业务设备所发送的交易上链请求时，根据交易上链请求所确定的；交易上链请求携带业务交易；业务类型标识用于表征侧区块链所处理业务的业务类型；

发送携带交易序号的第二数据获取请求至侧区块链，以使侧区块链中的第二侧链节点将与交易序号相关联的交易执行结果返回至验证设备；

根据交易执行结果，验证业务交易摘要信息的合法性。

本申请实施例一方面提供了一种基于区块链的数据处理装置，该装置运行于侧链节点，侧链节点属于联盟链中的侧区块链，联盟链还包括主区块链，该装置包括：

交易执行模块，用于获取业务设备发送的携带业务交易的交易上链请求，根据交易上链请求，确定业务交易对应的交易执行结果，对交易执行结果以及业务交易进行上链处理；

第一生成模块，用于当交易执行结果以及业务交易成功存储至侧区块链时，根据交易序号、业务类型标识以及交易执行结果，生成业务交易对应的业务交易摘要信息；交易序号用于表征业务交易在侧区块链

中的序号，业务类型标识用于表征侧区块链所处理业务的业务类型；

摘要传输模块，用于将业务交易摘要信息传输至主区块链，以使主区块链存储业务交易摘要信息。

本申请实施例一方面提供了一种基于区块链的数据处理装置，该装置运行于验证设备，该装置包括：

第一发送模块，用于发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链，以使主区块链将业务交易摘要信息返回至验证设备；交易序号用于表征业务交易在侧区块链中的序号；侧区块链属于联盟链；业务交易摘要信息是侧区块链传输至主区块链的；业务交易摘要信息，是侧区块链中的第一侧链节点在交易执行结果以及业务交易成功存储至侧区块链的情况下生成的，业务交易摘要信息，是根据交易序号、业务类型标识以及交易执行结果所生成的；交易执行结果是第一侧链节点在获取到业务设备所发送的交易上链请求时，根据交易上链请求所确定的；交易上链请求携带业务交易；业务类型标识用于表征侧区块链所处理业务的业务类型；

第二发送模块，用于发送携带交易序号的第二数据获取请求至侧区块链，以使侧区块链中的第二侧链节点将与交易序号相关联的交易执行结果返回至验证设备；

信息验证模块，用于根据交易执行结果，验证业务交易摘要信息的合法性。

本申请一方面提供了一种计算机设备，计算机设备包括存储器和一个或多个处理器，存储器存储有计算机可读指令，计算机可读指令被处理器执行时，使得一个或多个处理器执行本申请实施例中的方法。

本申请实施例一方面提供了一个或多个非易失性计算机可读存储介质，上述计算机可读存储介质中存储有计算机可读指令，上述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行本申请实施例中的方法。

本申请实施例一方面提供了一种计算机程序产品，该计算机程序产品包括计算机可读指令，计算机可读指令被处理器执行时行实现本申请实施例中的方法。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其他特征、目的和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1是本申请实施例提供的一种系统架构示意图；

图2是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图；

图3是本申请实施例提供的一种基于区块链的数据处理的场景示意图；

图4是本申请实施例提供的另一种基于区块链的数据处理的场景示意图；

图5是本申请实施例提供的一种业务交易摘要信息的结构示意图；

图6是本申请实施例提供的另一种基于区块链的数据处理的场景示意图；

图7是本申请实施例提供的另一种基于区块链的数据处理方法的流程示意图；

图8是本申请实施例提供的另一种基于区块链的数据处理的场景示意图；

图9是本申请实施例提供的另一种基于区块链的数据处理方法的流程示意图；

图10是本申请实施例提供的一种基于区块链的数据处理方法的交互流程图；

图11是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图；

图12是本申请实施例提供的另一种基于区块链的数据处理装置的结构示意图；

图13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

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

为了便于理解，首先对部分名词进行以下简单解释：

1、区块链：狭义上，区块链是一种以区块为基本单位的链式数据结构，区块中利用数字摘要对之前获取的交易历史进行校验，适合分布式记账场景下防篡改和可扩展性的需求；广义上，区块链还指代区块链结构实现的分布式记账技术，包括分布式共识、隐私与安全保护、点对点通信技术、网络协议、智能合约等。区块链的目标是实现一个分布的数据记录账本，此账本只允许添加，不允许删除。账本底层的基本结构是一个线性的链表。链表由一个个“区块”串联组成，后继区块中记录前继区块的哈希(Hash)值，每个区块（以及区块中的交易）是否合法，可通过计算哈希值的方式进行快速检验。若网络中的节点提议添加一个新的区块，必须经过共识机制对区块达成共识确认。

对于一个有公信力的区块链而言，其计算资源以及储存空间是有限的，所以当区块数量不断增加时，可能会导致该有公信力的区块链所对应的可用存储空间不够，以及响应慢于请求，这时就需要进行扩容，如扩容得到扩容区块链，为了保证扩容的效率，通常会采用私有链作为扩容区块链，在本申请中，将具有公信力的区块链称为主区块链，将扩容区块链称为侧区块链，即侧区块链的作用是为了扩容主区块链。其中，主区块链以及侧区块链可以组成联盟链。

2、区块(block)：是在区块链网络上承载交易数据的数据包，是一种被标记上时间戳和前继区块对应的哈希值的数据结构，区块经过网络的共识机制验证并确认区块中的交易。区块包括区块头(Block Header)以及区块体(Block Body)，区块头可以记录当前区块的元信息，包含当前版本号、前继区块对应的哈希值、时间戳、随机数、默克尔树根(Merkle Root)的哈希值等数据。区块体可以记录一段时间内所生成的详细数据，包括当前区块经过验证的、区块创建过程中生成的所有交易记录或是其他信息，可以理解为账本的一种表现形式。此外，区块体的详细数据可以包括通过默克尔树(Merkle Tree)的哈希过程，生成唯一的Merkle Root记录于区块头。

前继区块，也称父区块(Parent Block)，区块链通过在区块头记录区块对应的哈希值以及父区块对应的哈希值实现时间上的排序。

3、哈希值(hash)：也称作信息特征值或特征值，哈希值是通过哈希算法将任意长度的输入数据转换为密码并进行固定输出而生成的，不能通过解密哈希值来检索原始输入数据，它是一个单向的加密函数。在区块链中，每个区块（除了初始区块）都包含前继区块的哈希值，哈希值是区块链技术中的潜力核心基础和最重要的方面，它保留了记录和查看数据的真实性，以及区块链作为一个整体的完整性。

4、区块链节点：区块链网络将节点区分为共识节点（也可以称作核心节点）以及同步节点（可以包括数据节点以及轻节点）。其中，共识节点负责区块链全网的共识业务；同步节点负责同步共识节点的账本信息，即同步最新的区块数据。无论是共识节点还是同步节点，其内部构造都包括网络通信组件，因为区块链网络本质是一个点对点(Peer to Peer, P2P)网络，需通过P2P组件与区块链网络中的其他节点进行通信。区块链网络中的资源和服务都分散在各个节点上，信息的传输和服务的实现都直接在节点之间进行，无需中间环节或中心化的服务器（第三方）介入。

在本申请实施例中，主区块链所包括的区块链节点称为主链节点，侧区块链所包括的区块链节点称为侧链节点，侧链节点又可以分为侧链同步节点（其功能同上述的同步节点），以及侧链共识节点（其功能同上述的共识节点）。

5、写集合：共识节点在执行交易后，会计算写集合并填入交易的结构体内。写集合不参与交易哈希的计算，一笔交易的写集合记录了该交易所有落盘操作。通过写集合可以在不执行交易的前提下，快速更新链状态。本申请实施例提出历史写集合，历史写集合是指交易执行前，落盘对象的初始状态。

6、读集合：与写集合类似，记录一笔交易在执行过程中所有的读盘操作。

7、默克尔(Merkle)树、Merkle根：Merkle树是一种典型的二叉树结构，由一个根结点(Merkle根)，一组中间节点和一组叶子节点构成。最下层的叶子节点存储数据或其哈希值，其他节点存储其两个子节点内容的哈希值。

8、非对称签名：该算法包括两个密钥，公开密钥（简称公钥，public key）和私有密钥（简称私钥，private key）。公钥与私钥是一对，如果用私钥对数据进行签名，只有用对应的公钥才能验签。因为签名过程和验签过程分别使用两个不同的密钥，所以这种算法称作非对称签名。非对称签名实现机密信息交换的基本过程可以是：甲方生成一对密钥并将公钥公开，甲方需要向其他角色(乙方)发送信息时，使用自己的私钥对机密信息进行签名后再发送给乙方；乙方再用甲方的公钥对签名后的信息进行验签。

9、智能合约(Smart Contract)：是一种旨在以信息化方式传播、验证或执行合同的计算机协议。在区块链系统当中，智能合约（简称合约）是一种区块链各节点可以理解并执行的代码，可以执行任意逻辑并得到结果。在实际应用中，智能合约通过区块链上的交易来管理与试用。每条交易相当于对区块链系

统的一个远程过程调用（Remote Procedure Call，RPC）请求。如果说智能合约相当于可执行程序，区块链就相当于提供运行环境的操作系统。区块链可以包含多个合约（如本申请中的资源融合函数、资源发行函数等），以合约账号（Identity，ID）、标识号或名称来区分。

图 1 是本申请实施例提供的一种系统架构示意图。如图 1 所示，该系统架构可以包括终端设备集群以及联盟链 100 中的区块链节点集群，终端设备集群可以包括终端设备 10g、终端设备 10h、终端设备 10i 以及终端设备 10j。区块链节点集群可以包括区块链节点 10a、区块链节点 10b、区块链节点 10c、区块链节点 10d、区块链节点 10e 以及区块链节点 10f。本申请实施例不对终端设备集群的数量进行限制，可以包括一个或多个终端设备，同理，不对区块链节点集群的属性进行限制，可以包括一个或多个区块链节点。

其中，终端设备集群之间可以存在通信连接，例如终端设备 10i 与终端设备 10g 之间存在通信连接。其中，区块链节点集群之间可以存在通信连接，例如区块链节点 10a 与区块链节点 10c 之间存在通信连接，区块链节点 10a 与区块链节点 10d 之间存在通信连接。其中，区块链节点集群中的任一区块链节点可以与终端设备集群中的任一终端设备存在通信连接，例如区块链节点 10a 与终端设备 10h 之间存在通信连接，区块链节点 10d 与终端设备 10j 之间存在通信连接，区块链节点 10c 与终端设备 10g 之间存在通信连接，区块链节点 10e 与终端设备 10i 之间存在通信连接；其中，上述的通信连接不限定连接方式，可以通过有线通信方式进行直接或间接地连接，也可以通过无线通信方式进行直接或间接地连接，还可以通过其他方式。

区块链节点之间可以通过上述通信连接进行数据或者区块传输。上述区块链节点之间的通信连接可以基于节点标识，对于区块链网络中的每个区块链节点，均具有与其对应的节点标识，而且上述每个区块链节点均可以存储与自身有相连关系的其他区块链节点的节点标识，以便后续根据其他区块链节点的节点标识，将获取到的数据或生成的区块广播至其他区块链节点，例如区块链节点 10a 可以维护一个节点标识列表，该节点标识列表保存着其他区块链节点的节点名称和节点标识，如表 1 所示。

表 1

节点名称	节点标识
区块链节点 10b	AAAAA
区块链节点 10c	BBBBB
...	...
区块链节点 10d	CCCCC
区块链节点 10e	DDDDD
区块链节点 10f	EEEEEE
...	...

其中，节点标识可为网络之间互联的协议（Internet Protocol，IP）地址以及其他任意一种能够用于标识区块链网络中区块链节点的信息。

假设区块链节点 10a 的节点标识为 FFFFFFFF，则区块链节点 10a 可以通过节点标识 CCCCC，向区块链节点 10d 发送摘要信息上传请求，且区块链节点 10d 通过节点标识 FFFFFFFF，可以知道该摘要信息上传请求是区块链节点 10a 所发送的；同理，区块链节点 10d 可以通过节点标识 BBBBBB，向区块链节点 10c 发送区块共识请求，且区块链节点 10c 通过节点标识 CCCCCC，可以知道该区块共识请求是区块链节点 10d 所发送的，其他节点之间的数据传输亦如此。

本申请实施例将区块链网络划分成一个主区块链网络以及一个或多个侧区块链网络，形成联盟链 100，本申请实施例不对联盟链 100 中的区块链的数量进行限制。请再参见图 1，联盟链 100 可以包括主区块链 100a、侧区块链 100b、...、侧区块链 100c。其中，区块链节点 10a、...、区块链节点 10b 属于主区块链 100a 中的节点，即为区块链网络集群中的主链节点，区块链节点 10c、...、区块链节点 10d 属于侧区块链 100b 中的节点，即为侧区块链 100b 中的侧链节点，区块链节点 10e、...、区块链节点 10f 属于侧区块链 100c 中的节点，即为侧区块链 100c 中的侧链节点。区块链节点（也包括区块链节点 10a、区块链节点 10b、区块链节点 10c、区块链节点 10d、区块链节点 10e 以及区块链节点 10f）可以用于维护其所属的区块链。上述的主区块链 100a、侧区块链 100b、...、侧区块链 100c 均可以理解成分布式系统，在分布式系统中，任何设备如服务器、用户终端等都可以加入而成为区块链节点。

企业可以包括多种类型的业务数据，例如企业税务数据、社保数据以及工商数据等，不同类型的业务数据，被存储于不同的区块链，例如终端设备 10g 以及终端设备 10h 分别将企业税务数据存储于联盟链 100 中的侧区块链 100b，终端设备 10i 以及终端设备 10j 将社保数据存储于联盟链 100 中的侧区块链 100c，终端设备 10g 以及终端设备 10i 分别将工商数据存储于联盟链 100 中的其他侧区块链。在本申请实施例中，侧区块链中的侧链节点在进行正常工作时，可以接收到客户端发送的业务交易，并基于接收到的业务交易生成区块，然后进行区块上链处理，即在自己所维护的区块链中进行上链处理。在本申请的具体实施方式中，涉及到用户信息（例如业务交易）等相关的数据，当本申请实施例运用到具体产品或技术中时，需要

获得用户许可或者同意,且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

上述可知,本申请实施例中的每个侧区块链均分别独立维护一种全量数据,即所存储的全量业务数据不相同,维护的区块也均不相同。同理,主区块链 100a 所维护的区块也与侧区块链(例如图 1 中的侧区块链 100b)所维护的区块不同。

图 1 中的联盟链 100 中的区块链节点包括但不限于移动终端或服务器。上述服务器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、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络(Content Delivery Network,简称 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。上述移动终端包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端、飞行器等。其中,移动终端和服务器可以通过有线或无线方式进行直接或间接地连接。

图 2 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图。该基于区块链的数据处理方法可以由联盟链中的侧区块链 Z 中的侧链节点执行,联盟链可以为图 1 中的联盟链 100,侧区块链 Z 可以为上述图 1 中任意一个侧区块链。如图 2 所示,该基于区块链的数据处理方法至少可以包括以下步骤 S101-步骤 S103。

步骤 S101,获取业务设备发送的携带业务交易的交易上链请求,根据交易上链请求,确定业务交易对应的交易执行结果,对交易执行结果以及业务交易进行上链处理。

本申请实施例中的业务设备是指生成业务交易并将业务交易传输至侧区块链的设备。业务设备包括但不限于终端设备或业务服务器。其中,业务服务器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,还可以是提供云数据库、云服务、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、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。终端设备包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端、飞行器等。图 3 是本申请实施例提供的一种基于区块链的数据处理的场景示意图。如图 3 所示,业务对象 20a 操作业务设备 201a,生成业务交易 202a 即“在对象 201b 的当前资源中转移 30 资源至对象 202b”,若业务对象 20a 授权业务设备 201a 将业务交易 202a 发送至侧区块链 201c(即侧区块链 Z),则业务设备 201a 生成携带该业务交易 202a 的交易上链请求,然后将交易上链请求发送至属于侧区块链 201c 的侧链节点 20c。

步骤 S102,当交易执行结果以及业务交易成功存储至侧区块链时,根据交易序号、业务类型标识以及交易执行结果,生成业务交易对应的业务交易摘要信息。

其中,交易序号用于表征业务交易在侧区块链中的序号,业务类型标识用于表征侧区块链所处理业务的业务类型。

步骤 S103,将业务交易摘要信息传输至主区块链,以使主区块链存储业务交易摘要信息。

在本申请实施例中,当侧链节点获取到业务设备发送的携带业务交易的交易上链请求时,可以根据交易上链请求,确定业务交易对应的交易执行结果,其中,侧链节点属于联盟链中的侧区块链,且该联盟链还包括主区块链;进一步,侧链节点对交易执行结果以及业务交易进行上链处理,即存储至侧区块链;进一步,根据交易序号、业务类型标识以及交易执行结果,侧链节点可以生成业务交易对应的业务交易摘要信息,将业务交易摘要信息传输至主区块链,以使主区块链存储业务交易摘要信息;其中,存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备;验证设备用于根据从侧区块链中所获取的交易执行结果,验证业务交易摘要信息的合法性。上述可知,属于侧区块链中的侧链节点,可以执行与侧区块链所处理业务的业务类型相匹配的业务交易,并将交易执行结果以及业务交易存储至侧区块链,故可以避免区块链网络中主区块链执行业务交易的负荷过重缺陷,进而可以减轻主区块链的计算资源;由于主区块链只存储业务交易摘要信息,故可以减轻主区块链的存储资源。

在一些实施例中,根据交易上链请求,确定业务交易对应的交易执行结果,包括:确定业务交易的业务类型,若业务交易的业务类型与业务类型标识相匹配,则根据交易上链请求,调用智能合约中与业务交易的业务类型相匹配的交易执行函数;根据交易执行函数,获取针对业务交易中的第二业务对象的历史状态值,将第二业务对象的历史状态值组合成业务交易的读集合;根据业务交易以及读集合执行交易执行函数,获取交易执行函数被执行时所生成的针对业务交易中的第一业务对象的更新状态值;将第一业务对象的更新状态值确定为业务交易的写集合,获取在未执行交易执行函数之前第一业务对象的状态值,将获取到的状态值确定为业务交易的历史写集合;根据写集合、历史写集合以及读集合,确定业务交易对应的交易执行结果。

侧链节点 20c 获取到交易上链请求后,首先对业务交易 202a 进行业务类型验证,故确定业务交易 202a 的业务类型 20d,图 3 示例业务交易 202a 的业务类型 20d 为资源转移类型。进一步,侧链节点 20c 将业务类型 20d(即资源转移类型),与侧区块链 201c 所处理的业务类型进行匹配,业务类型可以用业务类型标识表示,若业务类型 20d 与业务类型标识不匹配,例如业务类型标识表明侧区块链 201c 所处理的业务类型为数字产品确权类型,此时,侧链节点 20c 可以拒绝处理业务设备 201a 发送的交易上链请求。若业

务类型 20d 与业务类型标识相匹配,此时,侧链节点 20c 根据交易上链请求,调用智能合约中与资源转移类型相匹配的交易执行函数 20e,交易执行函数 20e 例如如图 3 所示的资源转移函数。

侧链节点 20c 根据交易执行函数 20e,可以确定业务交易“在对象 201b 的当前资源中转移 30 资源至对象 202b”的读盘数据,即对象 201b 的当前资源以及对象 202b 的当前资源,图 3 示例对象 201b 的当前资源为 30,对象 202b 的当前资源为 50,侧链节点 20c 将读取到的状态数据确定为读集合 20f。进一步,侧链节点 20c 根据读集合 20f 以及业务交易 202a 执行交易执行函数 20e,业务交易 202a 执行后,获取对象 201b 的更新状态值以及对象 202b 的更新状态值,对象 201b 的更新状态值例如为图 3 所示的对象 201b 的更新资源:0,对象 202b 的更新状态值例如为图 3 所示的对象 202b 的更新资源:80,将业务交易 202a 执行后需要落盘的状态数据,确定为写集合 20g。进一步,侧链节点 20c 获取需要落盘的状态数据的历史状态数据,将获取到的状态数据确定为历史写集合 20h。第一业务对象是指业务交易执行后,需要落盘的状态数据所对应的业务对象,第二业务对象是指执行业务交易时需读盘的状态数据所对应的业务对象。在图 3 中,第一业务对象与第二业务对象相同,即侧链节点 20c 读取了对象 201b 以及对象 202b 分别对应的历史状态值,如图 3 中的对象 202b 的当前资源:50,对象 201b 当前资源:30;同时,侧链节点 20c 也写入了对象 201b 以及对象 202b 分别对应的更新状态值,如图 3 中的对象 202b 的更新资源:80,对象 201b 的更新资源:0。在上述场景下,历史写集合 20h 为对象 202b 的历史资源:50,对象 201b 的历史资源:30。实际应用中,第一业务对象可能与第二业务对象不同,例如交易“新建对象 202z,在对象 204b 的当前资源中转移 30 资源至对象 202b”,此时,第一业务对象包括对象 204b 以及对象 202z,第二业务对象包括对象 204b。

请再参见图 3,侧链节点 20c 根据写集合 20g、历史写集合 20h 以及读集合 20f,确定业务交易 202a 对应的交易执行结果。本申请实施例不对交易执行结果的内容进行限定,可以根据实际应用场景进行设定,具体的,交易执行结果还可以包括业务交易执行时的相关参数,例如错误码、交易所在高度或交易哈希值中的至少一个。

本实施例中,若业务交易的业务类型与业务类型标识相匹配,则根据交易上链请求,调用智能合约中与业务交易的业务类型相匹配的交易执行函数,以确定业务交易对应的交易执行结果,使得在业务交易的业务类型与业务类型标识相匹配的情况下,才调用交易执行函数生成交易执行结果,保证了交易执行结果的正确性。

在一些实施例中,该方法还包括:根据交易执行结果对历史状态树进行更新,得到更新状态树;历史状态树是基于侧区块链中的全量历史状态值所生成的默克尔树;根据交易序号、业务类型标识以及交易执行结果,生成业务交易对应的业务交易摘要信息,包括:根据交易序号、业务类型标识、交易执行结果、历史状态树以及更新状态树,生成业务交易对应的业务交易摘要信息。

其中,侧区块链 201c 维护一个包括所有业务对象分别对应的状态数据的状态树,图 4 是本申请实施例提供的另一种基于区块链的数据处理的场景示意图。如图 4 所示,在执行业务交易 202a 之前,侧区块链 201c 维护历史状态树 20i。需要强调的是,本申请实施例为了便于叙述以及理解,全量业务对象的总数量为 4 个,分别为对象 201b、对象 202b、对象 203b 以及对象 204b,实际应用时,全量业务对象对应的总数量可以为任意正整数。

历史状态树 20i 包括对象 201b 对应的历史状态值 1 (即图 4 中的 30)、对象 202b 对应的历史状态值 2 (即图 4 中的 50)、对象 203b 对应的历史状态值 3 (即图 4 中的 40),以及对象 204b 对应的历史状态值 4 (即图 4 中的 80);此外,历史状态树 20i 还包括历史状态值 1 对应的哈希值 1 (即图 4 中的 H (1))、历史状态值 2 对应的哈希值 2 (即图 4 中的 H (2))、历史状态值 3 对应的哈希值 3 (即图 4 中的 H (3)),以及历史状态值 4 对应的哈希值 4 (即图 4 中的 H (4));进一步,历史状态树 20i 还包括的 H (1) 以及 H (2) 对应的哈希值 (如图 4 中的 H (12)),以及, H (3) 以及 H (4) 对应的哈希值 (如图 4 中的 H (34));此外,历史状态树 20i 还包括 H (12) 以及 H (34) 对应的哈希值 (如图 4 中的 H (1234)),该哈希值为历史状态树 20i 的默克尔树根。

侧链节点 20c 执行完业务交易 202a,得到交易执行结果,根据交易执行结果,对历史状态树 20i 进行更新,具体为根据写集合 20g 中的状态数据对历史状态树 20i 进行更新,如图 4 所示,侧链节点 20c 将对对象 201b 的历史状态值更新为对象 201b 的更新状态值,即将 30 更新为 0;将对对象 202b 的历史状态值更新为对象 202b 的更新状态值,即将 50 更新为 80。此时,侧链节点 20c 生成对象 201b 的更新状态值对应的哈希值 (如图 4 中的 H' (1)),以及对象 202b 的更新状态值对应的哈希值 (如图 4 中的 H' (2)),进一步,对 H' (1) 以及 H' (2) 进行哈希计算,得到 H' (12),进一步,对 H' (12) 以及 H (34) 进行哈希计算,得到 H' (1234),此时,侧链节点 20c 可以得到更新状态树 20j。

本实施例中,根据交易序号、业务类型标识、交易执行结果、历史状态树以及更新状态树,生成业务交易对应的业务交易摘要信息,从而业务交易摘要信息包括了历史状态树以及更新状态树,提高了业务交易摘要信息的合理性。

在一些实施例中,对交易执行结果以及业务交易进行上链处理,包括:当侧链节点具有共识权限时,从侧区块链 Z 中获取具有最大生成时间戳的区块,作为父区块,将父区块的区块头哈希值作为父区块哈希值;基于父区块哈希值、携带交易序号的业务交易、交易执行结果以及基于交易执行结果所生成的更新状态树,生成侧链区块;侧链区块的生成时间戳用于更新侧区块链 Z 的最大生成时间戳;利用侧链节点对应的节点私钥,对侧链区块进行签名,得到签名信息,将携带签名信息的侧链区块广播至侧区块链 Z 中的共识节点;在确定侧区块链 Z 中的共识节点针对侧链区块达成共识通过时,将侧链区块添加至侧区块链 Z 中,将交易序号返回至业务设备。

举例说明,若侧链节点 20c 为侧区块链 201c 中具有共识权限以及出块权限的节点,即为侧区块链 201c 中的共识节点,则从侧区块链 201c 中获取具有最大生成时间戳的区块,作为父区块,请再参见图 4,侧链节点 20c 将具有最高区块高度的区块作为父区块,将父区块的区块头哈希值作为父区块哈希值;基于父区块哈希值、携带交易序号的业务交易 202a、交易执行结果以及更新状态树 20j,生成侧链区块 20k。例如,图 4 中业务交易 202a 在侧区块链 201c 中的序号为 100。进一步,侧链节点 20c 利用侧链节点 20c 对应的节点私钥 203c,对侧链区块 20k 进行签名,得到签名信息 201k,将携带签名信息 201k 的侧链区块 20k 广播至侧区块链 201c 中的共识节点,以使侧区块链 201c 中的共识节点对侧链区块 20k 进行共识处理。在确定侧区块链 201c 中的共识节点针对侧链区块 20k 达成共识通过时,侧链节点 20c 将侧链区块 20k 添加至侧区块链 201c 中,得到侧区块链 202c,同时,将交易序号返回至业务设备 201a。

本实施例中,侧区块链是一条独立的区块链,可以对与自己处理的业务类型相关联的业务交易进行共识处理,并存储全量数据,故可以减轻主区块链的共识负荷,进而可以缓解主区块链的存储压力。

在一些实施例中,根据交易序号、业务类型标识、交易执行结果、历史状态树以及更新状态树,生成业务交易对应的业务交易摘要信息,包括:获取历史状态树的历史状态根哈希,在历史状态根哈希中获取第一目标字段值;获取更新状态树的更新状态根哈希,在更新状态根哈希中获取第二目标字段值;根据交易序号、业务类型标识、交易执行结果、第一目标字段值以及第二目标字段值,生成业务交易对应的业务交易摘要信息。其中,更新状态树属于默克尔树,根哈希是指默克尔树根,更新状态根哈希是指更新状态树的根节点。

若包含交易执行结果以及业务交易的侧链区块存储于侧区块链 Z 时,则侧链节点会生成业务交易对应的业务交易摘要信息,图 5 是本申请实施例提供的一种业务交易摘要信息的结构示意图。如图 5 所示,侧链节点获取历史状态树 20i 的历史状态根哈希,如图 4 以及图 5 中的 H (1234),在历史状态根哈希中获取第一目标字段值 30e,本申请实施例不对第一目标字段值 30e 的取值范围进行限定,可以根据实际应用进行设定,例如为历史状态根哈希的前 16 位,或后 8 位,或前 8 位加后 8 位,本申请实施例为了便于叙述以及理解,以历史状态根哈希的前 16 位进行示例,如图 5 中的 abababababababab。进一步,侧链节点获取更新状态树 20j 的更新状态根哈希,如图 4 以及图 5 中的 H' (1234),在更新状态根哈希中获取第二目标字段值 30f,其中,第二目标字段值对应的含义,参见第一目标字段值的释义;图 5 以 cdcdcdcdcdcdcdcd 示例第二目标字段值 30f。

本实施例中,考虑到业务交易的全量数据(包括交易执行结果)的存储容量大,本申请实施例生成针对业务交易的业务交易摘要信息,其对应的存储容量小于业务交易的全量数据的存储容量,将该业务交易摘要信息传输至主区块链,以使其存储,既可以让主区块链存储与业务交易相关的数据,又可以减轻主区块链的存储压力。

在一些实施例中,根据交易执行结果对历史状态树进行更新,得到更新状态树,包括:根据交易执行结果中的写集合对历史状态树进行更新,得到更新状态树;全量历史状态值包括交易执行结果中的历史写集合;写集合包括业务交易中的第一业务对象的更新状态值;历史写集合包括第一业务对象的历史状态值;根据交易序号、业务类型标识、交易执行结果、第一目标字段值以及第二目标字段值,生成业务交易对应的业务交易摘要信息,包括:生成写集合的第一哈希值,在第一哈希值中获取第三目标字段值;生成历史写集合的第二哈希值,在第二哈希值中获取第四目标字段值;生成交易执行结果中的读集合的第三哈希值,在第三哈希值中获取第五目标字段值;读集合包括业务交易中的第二业务对象的历史状态值;将交易序号、业务类型标识、第三目标字段值、第四目标字段值、第五目标字段值、第一目标字段值以及第二目标字段值,组合成业务交易对应的业务交易摘要信息。

其中,第三目标字段值、第四目标字段值以及第五目标字段值分别对应的含义,均参见第一目标字段值的释义。

进一步,由步骤 S101 可知,交易执行结果可以包括写集合、历史写集合以及读集合。侧链节点生成写集合的第一哈希值,在第一哈希值中获取第三目标字段值 30b,图 5 以 efefefefefefefef 示例第三目标字段值 30b;侧链节点生成历史写集合的第二哈希值,在第二哈希值中获取第四目标字段值 30c,图 5 以 ghghghghghghghgh 示例第四目标字段值 30c;侧链节点生成读集合的第三哈希值,在第三哈希值中获取第五目标字段值 30d,图 5 以 ijijijijijijij 示例第五目标字段值 30d。进一步,侧链节点将交易序号(图 5 以

序号 100 示例)、业务类型标识、第三目标字段值 30b、第四目标字段值 30c、第五目标字段值 30d、第一目标字段值 30e 以及第二目标字段值 30f, 组合成业务交易对应的业务交易摘要信息。

本实施例中, 考虑到业务交易的全量数据(包括交易执行结果)的存储容量大, 本申请实施例生成针对业务交易的业务交易摘要信息, 其对应的存储容量远远小于业务交易的全量数据的存储容量, 将该业务交易摘要信息传输至主区块链, 以使其存储, 故既可以主区块链存储与业务交易相关的数据, 又可以减轻主区块链的存储压力。

在一些实施例中, 将业务交易摘要信息传输至主区块链, 包括: 利用主区块链的主链公钥, 对业务交易摘要信息进行加密, 得到加密摘要信息; 调用主区块链中与业务类型标识相对应的信息上传函数, 通过信息上传函数, 将加密摘要信息上传至主区块链, 以使主区块链中的主链节点利用主区块链的主链私钥, 对加密摘要信息进行解密, 在解密结果为解密通过结果时, 存储解密通过结果所对应的业务交易摘要信息。

考虑到业务交易摘要信息在传输过程中, 可能被非法设备获取, 且被非法设备修改, 在传输业务交易摘要信息之前, 侧链节点利用主区块链的主链公钥, 对业务交易摘要信息进行加密, 得到加密摘要信息。进一步, 侧链节点调用主区块链中与业务类型标识相对应的信息上传函数, 通过信息上传函数, 将加密摘要信息上传至主区块链, 图 6 是本申请实施例提供的另一种基于区块链的数据处理的场景示意图。侧链节点 401b 维护其所属的侧区块链 401c, 侧链节点 402b 维护其所属的侧区块链 402c, 侧区块链 401c 所处理业务的业务类型, 不同于侧区块链 402c 所处理的业务类型, 且两条区块链均独立进行上链处理, 故侧区块链 401c 所存储的区块不同于侧区块链 402c 所存储的区块。主区块链 40d 所存储的区块亦不同于侧区块链 401c 以及侧区块链 402c。其中, 业务设备 401a 发送交易上链请求至侧链节点 401b 的过程, 侧链节点 401b 执行业务交易 1 的过程, 侧链节点 401b 生成业务交易 1 对应的加密摘要信息(图 6 中称为加密摘要信息 1)的过程, 业务设备 402a 发送交易上链请求至侧链节点 402b 的过程, 侧链节点 402b 执行业务交易 2 的过程, 侧链节点 402b 生成业务交易 2 对应的加密摘要信息(图 6 中称为加密摘要信息 2)的过程, 请参见上文步骤 S101-步骤 S102 的描述。

如图 6 所示, 信息上传函数 1 用于传输侧区块链 401c 所上传的加密摘要信息 1, 信息上传函数 2 用于传输侧区块链 402c 所上传的加密摘要信息 2。主链节点获取到加密摘要信息 1 时, 利用主区块链的主链私钥, 对加密摘要信息 1 进行解密, 在解密结果为解密通过结果时, 主链节点存储解密通过结果所对应的业务交易摘要信息。其中, 主链节点对加密摘要信息 2 的处理过程, 与对加密摘要信息 1 的处理过程相同。

其中, 主区块链发送业务交易摘要信息至验证设备的过程, 以及验证设备根据从侧区块链 Z 中所获取的交易执行结果, 验证业务交易摘要信息的合法性的过程, 请参见下文图 9 所对应的实施例中的描述。

本实施例中, 由于业务交易摘要信息在传输过程中, 可能被非法设备获取, 且被非法设备修改, 通过将业务交易摘要信息加密传输至主区块链, 提高了信息传输的安全性。

图 7 是本申请实施例提供的另一种基于区块链的数据处理方法的流程示意图。该基于区块链的数据处理方法可以由联盟链中的侧区块链 Z 中的侧链节点执行, 联盟链可以为图 1 中的联盟链 100, 侧区块链 Z 可以为上述图 1 中任意一个侧区块链。如图 7 所示, 该方法至少可以包括以下步骤。

步骤 S201, 获取业务设备发送的携带业务交易的交易上链请求, 根据交易上链请求, 确定业务交易对应的交易执行结果, 对交易执行结果以及业务交易进行上链处理。

步骤 S202, 当交易执行结果以及业务交易成功存储至侧区块链时, 根据交易序号、业务类型标识以及交易执行结果, 生成业务交易对应的业务交易摘要信息; 交易序号用于表征业务交易在侧区块链中的序号, 业务类型标识用于表征侧区块链所处理业务的业务类型。

步骤 S203, 将业务交易摘要信息传输至主区块链, 以使主区块链存储业务交易摘要信息; 存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备; 验证设备用于根据从侧区块链中所获取的交易执行结果, 验证业务交易摘要信息的合法性。

步骤 S204, 基于更新状态树, 生成针对更新状态值的默克尔路径, 基于历史状态树, 生成针对历史状态值的默克尔路径。

具体的, 基于更新状态树, 生成针对更新状态值 B_c 的默克尔路径, 基于历史状态树, 生成针对历史状态值 D_c 的默克尔路径。交易执行结果包括业务交易对应的写集合, 以及业务交易对应的历史写集合; 写集合包括更新状态值 B_c , c 为正整数且 c 小于或等于写集合中的更新状态值的总数量; 历史写集合包括历史状态值 D_c 。

当交易执行结果以及业务交易成功存储至侧区块链时, 侧链节点额外维护写集合中所有状态值分别对应的 merkle 路径, 以及历史写集合中所有状态值的 merkle 路径, 上述两种类型的 merkle 路径的不存储于链上, 故无需由侧区块链的共识节点进行共识。图 8 是本申请实施例提供的另一种基于区块链的数据处理的场景示意图。如图 8 所示, 历史写集合 20h、写集合 20g、历史状态树 20i 以及更新状态树 20j 分别对应的含义, 请参见上文图 3-图 5 中的描述。针对历史写集合 20h 的历史资源值 50, 其对应的默克尔路径 1 包括 $H(1)$ 以及 $H(34)$, 针对历史写集合 20h 的历史资源值 30, 其对应的默克尔路径 2 包括 $H(2)$ 以

及 H (34); 针对写集合 20g 的更新资源值 80, 其对应的默克尔路径 3 包括 H' (1) 以及 H (34), 针对写集合 20g 的更新资源值 0, 其对应的默克尔路径 4 包括 H' (2) 以及 H (34)。

步骤 S205, 将写集合中的每个更新状态值对应的默克尔路径, 与写集合进行关联存储; 将历史写集合中的每个历史状态值对应的默克尔路径, 与历史写集合进行关联存储。

具体的, 请再参见图 8, 侧链节点将写集合 20g 中的每个更新状态值 (如图 8 中的每个更新资源值) 分别对应的默克尔路径, 与写集合 20g 关联存储至数据库 70a; 侧链节点将历史写集合 20h 中的每个历史状态值 (如图 8 中的每个历史资源值) 分别对应的默克尔路径, 与历史写集合 20h 关联存储至数据库 70a。

可选的, 步骤 S204-步骤 S205 的执行过程, 可以先于步骤 S202-步骤 S203 的执行过程。可选的, 步骤 S204-步骤 S205 的执行过程与步骤 S202-步骤 S203 的执行过程同步。

在本申请实施例, 当侧链节点获取到业务设备发送的携带业务交易的交易上链请求时, 可以根据交易上链请求, 确定业务交易对应的交易执行结果, 其中, 侧链节点属于联盟链中的侧区块链 Z, 且该联盟链还包括主区块链; 进一步, 侧链节点对交易执行结果以及业务交易进行上链处理, 即存储至侧区块链 Z; 进一步, 根据交易序号、业务类型标识以及交易执行结果, 侧链节点可以生成业务交易对应的业务交易摘要信息, 将业务交易摘要信息传输至主区块链, 以使主区块链存储业务交易摘要信息; 其中, 存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备; 验证设备用于根据从侧区块链 Z 中所获取的交易执行结果, 验证业务交易摘要信息的合法性。上述可知, 属于侧区块链 Z 中的侧链节点, 可以执行与侧区块链 Z 所处理业务的业务类型相匹配的业务交易, 并将交易执行结果以及业务交易存储至侧区块链 Z, 故可以避免区块链网络中主区块链执行业务交易的负荷过重缺陷, 进而可以减轻主区块链的计算资源; 由于主区块链只存储业务交易摘要信息, 故可以减轻主区块链的存储资源。

在一些实施例, 存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备; 验证设备用于根据从侧区块链 Z 中所获取的交易执行结果, 验证业务交易摘要信息的合法性。

具体地, 存储在侧区块链 Z 中的交易执行结果以及存储在主区块链的业务交易摘要信息, 均可以发送至验证设备, 故验证设备可以对侧区块链 Z 所发送的交易执行结果以及主区块链发送的业务交易摘要信息进行验证。

本实施例中, 验证设备可以对侧区块链 Z 所发送的交易执行结果以及主区块链发送的业务交易摘要信息进行验证, 从而可以确定业务交易摘要信息的合法性, 故可以确保区块链网络的安全性。

图 9 是本申请实施例提供的另一种基于区块链的数据处理方法的流程示意图。该方法由验证设备执行, 如图 9 所示, 该方法至少可以包括以下步骤。

步骤 S301, 发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链, 以使主区块链将业务交易摘要信息返回至验证设备; 交易序号用于表征业务交易在侧区块链中的序号; 侧区块链属于联盟链; 业务交易摘要信息是侧区块链传输至主区块链的; 业务交易摘要信息, 是侧区块链中的第一侧链节点在交易执行结果以及业务交易成功存储至侧区块链的情况下生成的, 业务交易摘要信息, 是根据交易序号、业务类型标识以及交易执行结果所生成的; 交易执行结果是第一侧链节点在获取到业务设备所发送的交易上链请求时, 根据交易上链请求所确定的; 交易上链请求携带业务交易; 业务类型标识用于表征侧区块链所处理业务的业务类型。

其中, 业务交易摘要信息是侧区块链中的第一侧链节点在交易执行结果以及业务交易成功存储至侧区块链时, 根据交易序号、业务类型标识以及交易执行结果所生成的。

在本申请实施例, 验证设备可以为非区块链节点的设备, 且具有验证需求, 包括但不限于图 2 所述的业务设备。当验证设备不为业务设备时, 验证设备可以先从业务设备获取业务交易对应的交易序号, 或侧链节点将交易序号传输至交易序号。本申请实施例不对验证设备获取交易序号的方式进行限定, 可以根据实际应用场景进行设定。

图 10 是本申请实施例提供的一种基于区块链的数据处理方法的交互流程图。如图 10 所示, S1、验证设备发送第一数据获取请求至主链节点。其中, 主链节点所处的主区块链以及侧链节点所属的侧区块链, 构成联盟链, 本申请示例不对联盟链中侧区块链的数量进行限定, 可以根据实际应用场景进行设定。其中, 第一数据获取请求携带业务类型标识以及交易序号。步骤 S2、主链节点确定获取权限。主链节点根据业务类型标识以及交易序号, 对验证设备进行验证, 以确定其具有获取权限, 具体可以包括: 主链节点根据业务类型标识以及交易序号, 是否可以从主区块链中获取到相对应的业务交易摘要信息, 若可以获取到包括业务类型标识以及交易序号的业务交易摘要信息, 则确定验证设备具有第一获取权限。步骤 S3、在验证设备具有第一获取权限的场景下, 主链节点将包括业务类型标识以及交易序号的业务交易摘要信息, 返回至验证设备。

步骤 S302, 发送携带交易序号的第二数据获取请求至侧区块链, 以使侧区块链中的第二侧链节点将与交易序号相关联的交易执行结果返回至验证设备。

步骤 S303, 根据交易执行结果, 验证业务交易摘要信息的合法性。

其中，第一侧链节点以及第二侧链节点可以为侧区块链 Z 中的任一侧链节点，第一侧链节点与第二侧链节点可以是侧区块链 Z 中不同的侧链节点，也可以是侧区块链 Z 中同一个侧链节点，这里不做限制。

上述可知，属于侧区块链 Z 中的侧链节点，可以执行与侧区块链 Z 所处理业务的业务类型相匹配的业务交易，并将交易执行结果以及业务交易存储至侧区块链 Z，故可以避免区块链网络中主区块链执行业务交易的负荷过重缺陷，进而可以减轻主区块链的计算资源；由于主区块链只存储业务交易摘要信息，故可以减轻主区块链的存储资源；此外，存储在侧区块链 Z 中的交易执行结果以及存储在主区块链的业务交易摘要信息，均可以发送至验证设备，故验证设备可以对侧区块链 Z 所发送的交易执行结果以及主区块链发送的业务交易摘要信息进行验证，从而可以确定业务交易摘要信息的合法性，故可以确保区块链网络的安全性。

在一些实施例中，业务交易摘要信息，是主区块链确定验证设备具有针对业务交易摘要信息的第一获取权限的情况下返回的。

其中，第一获取权限，是指获取该业务交易摘要信息的权限。主区块链根据业务类型标识以及交易序号，来确定验证设备具有针对业务交易摘要信息的第一获取权限。

本实施例中，由于业务交易摘要信息是在确定验证设备具有第一获取权限的情况下返回的，从而提升了数据安全性。

在一些实施例中，交易执行结果，是第二侧链节点确定验证设备具有第二获取权限的情况下返回的。

其中，第二获取权限，是指获取该交易执行结果的权限。

本实施例中，由于交易执行结果是在确定验证设备具有第二获取权限的情况下返回的，从而提升了数据的安全性。

在一些实施例中，该方法还包括：获取第二侧链节点返回的与交易序号相关联的默克尔路径集合；默克尔路径集合，是在第二侧链节点确定验证设备具有第二获取权限的情况下返回的；根据交易执行结果，验证业务交易摘要信息的合法性，包括：根据交易执行结果以及默克尔路径集合，验证业务交易摘要信息的合法性。

，在确定验证设备具有第二获取权限时，第二侧链节点将与交易序号相关联的默克尔路径集合返回至验证设备。

如图 10 所示的步骤 S4、验证设备发送第二数据获取请求至侧链节点。其中，第二数据获取请求携带交易序号。步骤 S5、侧链节点确定获取权限。具体的，侧链节点对验证设备进行鉴权，本申请实施例不对验证设备进行鉴权的方式进行限定，可以根据实际应用场景进行设定，鉴权的主要目标在于防止验证设备获取其没有权限的数据，以确保侧区块链中的数据的可见性。S6、侧链节点返回交易执行结果以及默克尔路径集合。在验证设备具有第二获取权限的场景下，侧链节点将与交易序号相关联的交易执行结果，以及与交易序号相关联的默克尔路径集合返回至验证设备。其中，默克尔路径集合可以包括上文图 2 所对应的实施例中的写集合中的每个更新状态值所对应的默克尔路径，以及历史写集合中的每个历史状态值所对应的默克尔路径。默克尔路径集合可以提高业务交易摘要信息的验证准确性。

本实施例中，根据交易执行结果以及默克尔路径集合，验证业务交易摘要信息的合法性，通过默克尔路径集合提高了业务交易摘要信息的验证准确性。

在一些实施例中，根据交易执行结果以及默克尔路径集合，验证业务交易摘要信息的合法性，包括：生成交易执行结果中的写集合的第一哈希值，在第一哈希值中获取第三验证目标字段值；写集合包括业务交易中的第一业务对象的更新状态值；生成交易执行结果中的历史写集合的第二哈希值，在第二哈希值中获取第四验证目标字段值；历史写集合包括第一业务对象的历史状态值；生成交易执行结果中的读集合的第三哈希值，在第三哈希值中获取第五验证目标字段值；读集合包括业务交易中的第二业务对象的历史状态值；根据第三验证目标字段值、第四验证目标字段值、第五验证目标字段值、写集合、历史写集合、读集合以及默克尔路径集合，验证业务交易摘要信息的合法性。

其中，在第一哈希值中获取第三验证目标字段值的方法，与在第一哈希值中获取第三目标字段值的方法一致。在第二哈希值中获取第四验证目标字段值的方法，与在第二哈希值中获取第四目标字段值的方法一致。在第三哈希值中获取第五验证目标字段值的方法，与在第三哈希值中获取第五目标字段值的方法一致。

本实施例中，根据第三验证目标字段值、第四验证目标字段值、第五验证目标字段值、写集合、历史写集合、读集合以及默克尔路径集合，验证业务交易摘要信息的合法性，提高了合法性验证的准确度。

在一些实施例中，根据第三验证目标字段值、第四验证目标字段值、第五验证目标字段值、写集合、历史写集合、读集合以及默克尔路径集合，验证业务交易摘要信息的合法性的具体过程可以包括：将第三验证目标字段值与业务交易摘要信息中的第三目标字段值进行对比，得到第一对比结果；将第四验证目标字段值与业务交易摘要信息中的第四目标字段值进行对比，得到第二对比结果；将第五验证目标字段值与

业务交易摘要信息中的第五目标字段值进行对比,得到第三对比结果;根据历史写集合以及默克尔路径集合中与历史写集合相关联的默克尔路径,生成验证历史状态根哈希;根据写集合以及默克尔路径集合中与写集合相关联的默克尔路径,生成验证更新状态根哈希;根据读集合重新执行业务交易,得到验证写集合,根据第一对比结果、第二对比结果、第三对比结果、验证历史状态根哈希、验证更新状态根哈希以及验证写集合,验证业务交易摘要信息的合法性。

本实施例中,根据第一对比结果、第二对比结果、第三对比结果、验证历史状态根哈希、验证更新状态根哈希以及验证写集合,验证业务交易摘要信息的合法性,提高了合法性验证的准确度。在一些实施例中,根据第一对比结果、第二对比结果、第三对比结果、验证历史状态根哈希、验证更新状态根哈希以及验证写集合,验证业务交易摘要信息的合法性的具体过程可以包括:在验证历史状态根哈希中获取第一验证目标字段值,将第一验证目标字段值与业务交易摘要信息中的第一目标字段值进行对比,得到第四对比结果;在验证更新状态根哈希中获取第二验证目标字段值,将第二验证目标字段值与业务交易摘要信息中的第二目标字段值进行对比,得到第五对比结果;将验证写集合与写集合进行对比,得到第六对比结果;若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果中,存在对比结果为对比不同结果,则确定业务交易摘要信息为非法信息;若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果均为对比相同结果,则确定业务交易摘要信息为合法信息。

请再参见图 10,步骤 S7、验证设备生成验证目标字段值。已知业务交易摘要信息包括交易序号、业务类型标识、第三目标字段值、第四目标字段值、第五目标字段值、第一目标字段值,以及第二目标字段值。故验证设备根据交易执行结果中的写集合生成第三验证目标字段值、根据交易执行结果中的历史写集合生成第四验证目标字段值,根据交易执行结果中的读集合生成第五验证目标字段值。验证设备根据历史写集合以及历史写集合对应的默克尔路径,生成第一验证目标字段值,根据写集合以及写集合对应的默克尔路径,生成第二验证目标字段值。

步骤 S8、验证设备对比验证目标字段值以及目标字段值,得到对比结果。具体的,验证设备将第一目标字段值以及第一验证目标字段值进行对比,若两者相同,则确定交易业务摘要信息中第一目标字段值具有合法性;若两者不同,则确定第一目标字段值不具有合法性。验证设备将第二目标字段值以及第二验证目标字段值进行对比,若两者相同,则确定交易业务摘要信息中第二目标字段值具有合法性;若两者不同,则确定第二目标字段值不具有合法性。验证设备将第三目标字段值以及第三验证目标字段值进行对比,若两者相同,则确定交易业务摘要信息中第三目标字段值具有合法性;若两者不同,则确定第三目标字段值不具有合法性。剩余两个目标字段值的对比亦如此。

此外,验证设备根据交易执行结果中的读集合重新执行业务交易,得到验证写集合,将验证写集合与写集合进行对比,得到第六对比结果。根据第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果,验证设备确定业务交易摘要信息的合法性。

本实施例中,若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果中,存在对比结果为对比不同结果,则确定业务交易摘要信息为非法信息;若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果均为对比相同结果,则确定业务交易摘要信息为合法信息,准确的判定出业务交易摘要信息是否合法。

在一些实施例中,若验证业务交易摘要信息为非法信息,则根据业务类型标识、交易序号、交易执行结果以及默克尔路径集合,生成挑战侧链交易;将挑战侧链交易传输至主区块链,以使主区块链对挑战侧链交易进行共识,且在共识通过挑战侧链交易时,确认侧区块链 Z 为不可信链。

步骤 S9、若对比结果为对比不同结果,则生成挑战侧链交易。可理解的是,若上述的 6 个对比结果中存在一个对比结果为对比不同结果,则验证设备可以基于业务类型标识、交易序号、交易执行结果以及默克尔路径集合,生成挑战侧链交易。步骤 S10、验证设备发送挑战侧链交易至主链节点。步骤 S11、主链节点验证挑战侧链交易。若挑战侧链交易在主区块链上执行成功,则证明侧区块链为不可信链,此时,主区块链可以暂停该不可信链的数据交互。

本实施例中,通过挑战侧链交易判定侧区块链是否可行,以及时发现不可信的侧区块链,提高了区块链系统的安全性。

图 11 是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图。该基于区块链的数据处理装置可以运行于侧链节点,侧链节点属于联盟链中的侧区块链,联盟链还包括主区块链,上述基于区块链的数据处理装置 1 可以用于执行本申请实施例提供的方法中的相应步骤。如图 11 所示,该基于区块链的数据处理装置 1 可以包括:交易执行模块 11、第一生成模块 12 以及摘要传输模块 13。

交易执行模块 11,用于获取业务设备发送的携带业务交易的交易上链请求,根据交易上链请求,确定业务交易对应的交易执行结果,对交易执行结果以及业务交易进行上链处理;

第一生成模块 12,用于当交易执行结果以及业务交易成功存储至侧区块链时,根据交易序号、业务

类型标识以及交易执行结果,生成业务交易对应的业务交易摘要信息;交易序号用于表征业务交易在侧区块链中的序号,业务类型标识用于表征侧区块链所处理业务的业务类型;

摘要传输模块 13,用于将业务交易摘要信息传输至主区块链,以使主区块链存储业务交易摘要信息。

基于区块链的数据处理装置 1 还可以包括:状态更新模块 14。

状态更新模块 14,用于根据交易执行结果对历史状态树进行更新,得到更新状态树;历史状态树是基于侧区块链中的全量历史状态值所生成的默克尔树;

则第一生成模块 12,具体用于根据交易序号、业务类型标识、交易执行结果、历史状态树以及更新状态树,生成业务交易对应的业务交易摘要信息。

第一生成模块 12 可以包括:第一获取单元 121、第二获取单元 122 以及第一生成单元 123。

第一获取单元 121,用于获取历史状态树的历史状态根哈希,在历史状态根哈希中获取第一目标字段值;

第二获取单元 122,用于获取更新状态树的更新状态根哈希,在更新状态根哈希中获取第二目标字段值;

第一生成单元 123,用于根据交易序号、业务类型标识、交易执行结果、第一目标字段值以及第二目标字段值,生成业务交易对应的业务交易摘要信息。

状态更新模块 14,具体用于根据交易执行结果中的写集合对历史状态树进行更新,得到更新状态树;全量历史状态值包括交易执行结果中的历史写集合;写集合包括业务交易中的第一业务对象的更新状态值;历史写集合包括第一业务对象的历史状态值;

则第一生成单元 123 可以包括:第一生成子单元 1231、第二生成子单元 1232、第三生成子单元 1233 以及第四生成子单元 1234。

第一生成子单元 1231,用于生成写集合的第一哈希值,在第一哈希值中获取第三目标字段值;

第二生成子单元 1232,用于生成历史写集合的第二哈希值,在第二哈希值中获取第四目标字段值;

第三生成子单元 1233,用于生成交易执行结果中的读集合的第三哈希值,在第三哈希值中获取第五目标字段值;读集合包括业务交易中的第二业务对象的历史状态值;

第四生成子单元 1234,用于将交易序号、业务类型标识、第三目标字段值、第四目标字段值、第五目标字段值、第一目标字段值以及第二目标字段值,组合成业务交易对应的业务交易摘要信息。

交易执行结果包括业务交易对应的写集合,以及业务交易对应的历史写集合;写集合包括更新状态值;历史写集合包括历史状态值;

基于区块链的数据处理装置 1 还可以包括:第二生成模块 15 以及关联存储模块 16。

第二生成模块 15,用于基于更新状态树,生成针对更新状态值的默克尔路径,基于历史状态树,生成针对历史状态值的默克尔路径;

关联存储模块 16,用于将写集合中的每个更新状态值对应的默克尔路径,与写集合进行关联存储;

关联存储模块 16,还用于将历史写集合中的每个历史状态值对应的默克尔路径,与历史写集合进行关联存储。

交易执行模块 11 可以包括:第一确定单元 111、第三获取单元 112、第四获取单元 113、第二确定单元 114 以及第三确定单元 115。

第一确定单元 111,用于确定业务交易的业务类型,若业务交易的业务类型与业务类型标识相匹配,则根据交易上链请求,调用智能合约中与业务交易的业务类型相匹配的交易执行函数;

第三获取单元 112,用于根据交易执行函数,获取针对业务交易中的第二业务对象的历史状态值,将第二业务对象的历史状态值组合成业务交易的读集合;

第四获取单元 113,用于根据业务交易以及读集合执行交易执行函数,获取交易执行函数被执行时所生成的针对业务交易中的第一业务对象的更新状态值;

第二确定单元 114,用于将第一业务对象的更新状态值确定为业务交易的写集合,获取在未执行交易执行函数之前第一业务对象的状态值,将获取到的状态值确定为业务交易的历史写集合;

第三确定单元 115,用于根据写集合、历史写集合以及读集合,确定业务交易对应的交易执行结果。

交易执行模块 11 可以包括:第五获取单元 116、第二生成单元 117、区块广播单元 118 以及区块添加单元 119。

第五获取单元 116,用于当侧链节点具有共识权限时,从侧区块链中获取具有最大生成时间戳的区块,作为父区块,将父区块的区块头哈希值作为父区块哈希值;

第二生成单元 117,用于基于父区块哈希值、携带交易序号的业务交易、交易执行结果以及基于交易执行结果所生成的更新状态树,生成侧链区块;侧链区块的生成时间戳用于更新侧区块链的最大生成时间戳;

区块广播单元 118,用于利用侧链节点对应的节点私钥,对侧链区块进行签名,得到签名信息,将携

带签名信息的侧链区块广播至侧链区块链中的共识节点；

区块添加单元 119，用于在确定侧链区块链中的共识节点针对侧链区块达成共识通过时，将侧链区块添加至侧链区块链中，将交易序号返回至业务设备。

摘要传输模块 13 可以包括：摘要加密单元 131 以及信息上传单元 132。

摘要加密单元 131，用于利用主区块链的主链公钥，对业务交易摘要信息进行加密，得到加密摘要信息；

信息上传单元 132，用于调用主区块链中与业务类型标识相对应的信息上传函数，通过信息上传函数，将加密摘要信息上传至主区块链，以使主区块链中的主链节点利用主区块链的主链私钥，对加密摘要信息进行解密，在解密结果为解密通过结果时，存储解密通过结果所对应的业务交易摘要信息。

在一些实施例中，存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备；验证设备用于根据从侧链区块链中所获取的交易执行结果，验证业务交易摘要信息的合法性。

进一步地，图 12 是本申请实施例提供的另一种基于区块链的数据处理装置的结构示意图。上述基于区块链的数据处理装置 2 可以运行于验证设备，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。如图 12 所示，该基于区块链的数据处理装置 2 可以包括：第一发送模块 21、第二发送模块 22 以及信息验证模块 23。

第一发送模块 21，用于发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链，以使主区块链将业务交易摘要信息返回至验证设备；交易序号用于表征业务交易在侧链区块链中的序号；侧链区块链属于联盟链；业务交易摘要信息是侧链区块链传输至主区块链的；业务交易摘要信息，是侧链区块链中的第一侧链节点在交易执行结果以及业务交易成功存储至侧链区块链的情况下生成的，业务交易摘要信息，是根据交易序号、业务类型标识以及交易执行结果所生成的；交易执行结果是第一侧链节点在获取到业务设备所发送的交易上链请求时，根据交易上链请求所确定的；交易上链请求携带业务交易；业务类型标识用于表征侧链区块链所处理业务的业务类型；

第二发送模块 22，用于发送携带交易序号的第二数据获取请求至侧链区块链，以使侧链区块链中的第二侧链节点将与交易序号相关联的交易执行结果返回至验证设备；

信息验证模块 23，用于根据交易执行结果，验证业务交易摘要信息的合法性。

在一些实施例中，业务交易摘要信息，是主区块链确定验证设备具有针对业务交易摘要信息的第一获取权限的情况下返回的。

在一些实施例中，交易执行结果，是第二侧链节点确定验证设备具有第二获取权限的情况下返回的。

第二发送模块 22，还用于获取第二侧链节点返回的与交易序号相关联的默克尔路径集合；默克尔路径集合，是在第二侧链节点确定验证设备具有第二获取权限的情况下返回的；

则信息验证模块 23，具体用于根据交易执行结果以及默克尔路径集合，验证业务交易摘要信息的合法性。

信息验证模块 23 可以包括：第一哈希生成单元 231、第二哈希生成单元 232、第三生成单元 233 以及合法验证单元 234。

第一哈希生成单元 231，用于生成交易执行结果中的写集合的第一哈希值，在第一哈希值中获取第三验证目标字段值；写集合包括业务交易中的第一业务对象的更新状态值；

第二哈希生成单元 232，用于生成交易执行结果中的历史写集合的第二哈希值，在第二哈希值中获取第四验证目标字段值；历史写集合包括第一业务对象的历史状态值；

第三生成单元 233，用于生成交易执行结果中的读集合的第三哈希值，在第三哈希值中获取第五验证目标字段值；读集合包括业务交易中的第二业务对象的历史状态值；

合法验证单元 234，用于根据第三验证目标字段值、第四验证目标字段值、第五验证目标字段值、写集合、历史写集合、读集合以及默克尔路径集合，验证业务交易摘要信息的合法性。

合法验证单元 234 可以包括：第一对比子单元 2341、第二对比子单元 2342、第三对比子单元 2343、第一哈希生成子单元 2344、第二哈希生成子单元 2345 以及合法验证子单元 2346。

第一对比子单元 2341，用于将第三验证目标字段值与业务交易摘要信息中的第三目标字段值进行对比，得到第一对比结果；

第二对比子单元 2342，用于将第四验证目标字段值与业务交易摘要信息中的第四目标字段值进行对比，得到第二对比结果；

第三对比子单元 2343，用于将第五验证目标字段值与业务交易摘要信息中的第五目标字段值进行对比，得到第三对比结果；

第一哈希生成子单元 2344，用于根据历史写集合以及默克尔路径集合中与历史写集合相关联的默克尔路径，生成验证历史状态根哈希；

第二哈希生成子单元 2345，用于根据写集合以及默克尔路径集合中与写集合相关联的默克尔路径，

生成验证更新状态根哈希：

合法验证子单元 2346，用于根据读集合重新执行业务交易，得到验证写集合，根据第一对比结果、第二对比结果、第三对比结果、验证历史状态根哈希、验证更新状态根哈希以及验证写集合，验证业务交易摘要信息的合法性。

合法验证子单元 2346 可以包括：第一获取子单元 23461、第二获取子单元 23462、集合对比子单元 23463、第一确定子单元 23464 以及第二确定子单元 23465。

第一获取子单元 23461，用于在验证历史状态根哈希中获取第一验证目标字段值，将第一验证目标字段值与业务交易摘要信息中的第一目标字段值进行对比，得到第四对比结果；

第二获取子单元 23462，用于在验证更新状态根哈希中获取第二验证目标字段值，将第二验证目标字段值与业务交易摘要信息中的第二目标字段值进行对比，得到第五对比结果；

集合对比子单元 23463，用于将验证写集合与写集合进行对比，得到第六对比结果；

第一确定子单元 23464，用于若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果中，存在对比结果为对比不同结果，则确定业务交易摘要信息为非法信息；

第二确定子单元 23465，用于若第一对比结果、第二对比结果、第三对比结果、第四对比结果、第五对比结果以及第六对比结果均为对比相同结果，则确定业务交易摘要信息为合法信息。

基于区块链的数据处理装置 2 还可以包括：交易生成模块 24 以及交易传输模块 25。

交易生成模块 24，用于若验证业务交易摘要信息为非法信息，则根据业务类型标识、交易序号、交易执行结果以及默克尔路径集合，生成挑战侧链交易；

交易传输模块 25，用于将挑战侧链交易传输至主区块链，以使主区块链对挑战侧链交易进行共识，且在共识通过挑战侧链交易时，确认侧区块链 Z 为不可信链。

图 13 是本申请实施例提供的一种计算机设备的结构示意图。如图 13 所示，该计算机设备 1000 可以包括：至少一个处理器 1001，例如 CPU，至少一个网络接口 1004，用户接口 1003，存储器 1005，至少一个通信总线 1002。其中，通信总线 1002 用于实现这些组件之间的连接通信。其中，在一些实施例中，用户接口 1003 可以包括显示屏（Display）、键盘（Keyboard），网络接口 1004 可选地可以包括标准的有线接口、无线接口（如 WI-FI 接口）。存储器 1005 可以是高速 RAM 存储器，也可以是非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。存储器 1005 可选地还可以是至少一个位于远离前述处理器 1001 的存储装置。如图 13 所示，作为一种计算机存储介质的存储器 1005 可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

在图 13 所示的计算机设备 1000 中，网络接口 1004 可提供网络通讯功能；而用户接口 1003 主要用于为用户提供输入的接口；而处理器 1001 可以用于调用存储器 1005 中存储的设备控制应用程序，以实现：

获取业务设备发送的携带业务交易的交易上链请求，根据交易上链请求，确定业务交易对应的交易执行结果，对交易执行结果以及业务交易进行上链处理；

当交易执行结果以及业务交易成功存储至侧区块链 Z 时，根据交易序号、业务类型标识以及交易执行结果，生成业务交易对应的业务交易摘要信息；交易序号用于表征业务交易在侧区块链 Z 中的序号，业务类型标识用于表征侧区块链 Z 所处理业务的业务类型；

将业务交易摘要信息传输至主区块链，以使主区块链存储业务交易摘要信息；存储在主区块链中的业务交易摘要信息用于由主区块链发送至验证设备；验证设备用于根据从侧区块链 Z 中所获取的交易执行结果，验证业务交易摘要信息的合法性。

应当理解，本申请实施例中所描述的计算机设备 1000 可执行前文各实施例中对基于区块链的数据处理方法或装置的描述。另外，对采用相同方法的有益效果描述。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机可读指令，该计算机可读指令被处理器执行时实现前文各实施例中对基于区块链的数据处理方法或装置的描述。另外，对采用相同方法的有益效果描述。

上述计算机可读存储介质可以是前述任一实施例提供的基于区块链的数据处理装置或者上述计算机设备的内部存储单元，例如计算机设备的硬盘或内存。该计算机可读存储介质也可以是该计算机设备的外部存储设备，例如该计算机设备上配备的插接式硬盘，智能存储卡（smart media card，SMC），安全数字（secure digital，SD）卡，闪存卡（flash card）等。进一步地，该计算机可读存储介质还可以既包括该计算机设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机可读指令以及该计算机设备所需的其它程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机可读指令，该计算机可读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可读指令，处理器执行该计算机可读指令，使得该计算机设备可执行前文各实施例中对基于区块链的数据处理方法或

装置的描述。另外，对采用相同方法的有益效果描述。

本申请实施例的说明书和权利要求书及附图中的术语“第一”、“第二”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、装置、产品或设备没有限定于已列出的步骤或模块，而是可选地还包括没有列出的步骤或模块，或可选地还包括对于这些过程、方法、装置、产品或设备固有的其他步骤单元。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

以上所揭露的仅为本申请较佳实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

权利要求书

1、一种基于区块链的数据处理方法，其特征在于，所述方法由侧链节点执行，所述侧链节点属于联盟链中的侧区块链，所述联盟链还包括主区块链，所述方法包括：

获取业务设备发送的携带业务交易的交易上链请求，根据所述交易上链请求，确定所述业务交易对应的交易执行结果，对所述交易执行结果以及所述业务交易进行上链处理；

当所述交易执行结果以及所述业务交易成功存储至所述侧区块链时，根据交易序号、业务类型标识以及所述交易执行结果，生成所述业务交易对应的业务交易摘要信息；所述交易序号用于表征所述业务交易在所述侧区块链中的序号，所述业务类型标识用于表征所述侧区块链所处理业务的业务类型；

将所述业务交易摘要信息传输至所述主区块链，以使所述主区块链存储所述业务交易摘要信息。

2、根据权利要求1所述的方法，其特征在于，所述方法还包括：

根据所述交易执行结果对历史状态树进行更新，得到更新状态树；所述历史状态树是基于所述侧区块链中的全量历史状态值所生成的默克尔树；

所述根据交易序号、业务类型标识以及所述交易执行结果，生成所述业务交易对应的业务交易摘要信息，包括：

根据交易序号、业务类型标识、所述交易执行结果、所述历史状态树以及所述更新状态树，生成所述业务交易对应的业务交易摘要信息。

3、根据权利要求2所述的方法，其特征在于，所述根据交易序号、业务类型标识、所述交易执行结果、所述历史状态树以及所述更新状态树，生成所述业务交易对应的业务交易摘要信息，包括：

获取所述历史状态树的历史状态根哈希，在所述历史状态根哈希中获取第一目标字段值；

获取所述更新状态树的更新状态根哈希，在所述更新状态根哈希中获取第二目标字段值；

根据交易序号、业务类型标识、所述交易执行结果、所述第一目标字段值以及所述第二目标字段值，生成所述业务交易对应的业务交易摘要信息。

4、根据权利要求3所述的方法，其特征在于，所述根据所述交易执行结果对历史状态树进行更新，得到更新状态树，包括：

根据所述交易执行结果中的写集合对历史状态树进行更新，得到更新状态树；所述全量历史状态值包括所述交易执行结果中的历史写集合；所述写集合包括所述业务交易中的第一业务对象的更新状态值；所述历史写集合包括所述第一业务对象的历史状态值；

所述根据交易序号、业务类型标识、所述交易执行结果、所述第一目标字段值以及所述第二目标字段值，生成所述业务交易对应的业务交易摘要信息，包括：

生成所述写集合的第一哈希值，在所述第一哈希值中获取第三目标字段值；

生成所述历史写集合的第二哈希值，在所述第二哈希值中获取第四目标字段值；

生成所述交易执行结果中的读集合的第三哈希值，在所述第三哈希值中获取第五目标字段值；所述读集合包括所述业务交易中的第二业务对象的历史状态值；

将交易序号、业务类型标识、所述第三目标字段值、所述第四目标字段值、所述第五目标字段值、所述第一目标字段值以及所述第二目标字段值，组合成所述业务交易对应的业务交易摘要信息。

5、根据权利要求2所述的方法，其特征在于，所述交易执行结果包括所述业务交易对应的写集合，以及所述业务交易对应的历史写集合；所述写集合包括更新状态值；所述历史写集合包括历史状态值；

所述方法还包括：

基于所述更新状态树，生成针对所述更新状态值的默克尔路径，基于所述历史状态树，生成针对所述历史状态值的默克尔路径；

将所述写集合中的每个更新状态值对应的默克尔路径，与所述写集合进行关联存储；

将所述历史写集合中的每个历史状态值对应的默克尔路径，与所述历史写集合进行关联存储。

6、根据权利要求1-5中任一项所述的方法，其特征在于，所述根据所述交易上链请求，确定所述业务交易对应的交易执行结果，包括：

确定所述业务交易的业务类型，若所述业务交易的业务类型与所述业务类型标识相匹配，则根据所述交易上链请求，调用智能合约中与所述业务交易的业务类型相匹配的交易执行函数；

根据所述交易执行函数，获取针对所述业务交易中的第二业务对象的历史状态值，将所述第二业务对象的历史状态值组合成所述业务交易的读集合；

根据所述业务交易以及所述读集合执行所述交易执行函数，获取所述交易执行函数被执行时所生成

的针对所述业务交易中的第一业务对象的更新状态值；

将所述第一业务对象的更新状态值确定为所述业务交易的写集合，获取在未执行所述交易执行函数之前所述第一业务对象的状态值，将获取到的状态值确定为所述业务交易的历史写集合；

根据所述写集合、所述历史写集合以及所述读集合，确定所述业务交易对应的交易执行结果。

7、根据权利要求 1-6 中任一项所述的方法，其特征在于，所述对所述交易执行结果以及所述业务交易进行上链处理，包括：

当所述侧链节点具有共识权限时，从所述侧区块链中获取具有最大生成时间戳的区块，作为父区块，将所述父区块的区块头哈希值作为父区块哈希值；

基于所述父区块哈希值、携带所述交易序号的所述业务交易、所述交易执行结果以及基于所述交易执行结果所生成的更新状态树，生成侧链区块；所述侧链区块的生成时间戳用于更新所述侧区块链的最大生成时间戳；

利用所述侧链节点对应的节点私钥，对所述侧链区块进行签名，得到签名信息，将携带所述签名信息的所述侧链区块广播至所述侧区块链中的共识节点；

在确定所述侧区块链中的共识节点针对所述侧链区块达成共识通过时，将所述侧链区块添加至所述侧区块链中，将所述交易序号返回至所述业务设备。

8、根据权利要求 1-7 中任一项所述的方法，其特征在于，所述将所述业务交易摘要信息传输至所述主区块链，包括：

利用所述主区块链的主链公钥，对所述业务交易摘要信息进行加密，得到加密摘要信息；

调用所述主区块链中与所述业务类型标识相对应的信息上传函数，通过所述信息上传函数，将所述加密摘要信息上传至所述主区块链，以使所述主区块链中的主链节点利用所述主区块链的主链私钥，对所述加密摘要信息进行解密，在解密结果为解密通过结果时，存储所述解密通过结果所对应的所述业务交易摘要信息。

9、根据权利要求 1-8 中任一项所述的方法，其特征在于，存储在所述主区块链中的所述业务交易摘要信息用于由所述主区块链发送至验证设备；所述验证设备用于根据从所述侧区块链中所获取的所述交易执行结果，验证所述业务交易摘要信息的合法性。

10、一种基于区块链的数据处理方法，其特征在于，由验证设备执行，包括：

发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链，以使所述主区块链将业务交易摘要信息返回至所述验证设备；所述交易序号用于表征业务交易在侧区块链中的序号；所述侧区块链属于所述联盟链；所述业务交易摘要信息是所述侧区块链传输至所述主区块链的；所述业务交易摘要信息，是所述侧区块链中的第一侧链节点在交易执行结果以及所述业务交易成功存储至所述侧区块链的情况下生成的，所述业务交易摘要信息，是根据所述交易序号、所述业务类型标识以及所述交易执行结果所生成的；所述交易执行结果是所述第一侧链节点在获取到业务设备所发送的交易上链请求时，根据所述交易上链请求所确定的；所述交易上链请求携带所述业务交易；所述业务类型标识用于表征所述侧区块链所处理业务的业务类型；

发送携带所述交易序号的第二数据获取请求至所述侧区块链，以使所述侧区块链中的第二侧链节点将与所述交易序号相关联的所述交易执行结果返回至所述验证设备；

根据所述交易执行结果，验证所述业务交易摘要信息的合法性。

11、根据权利要求 10 所述的方法，其特征在于，所述业务交易摘要信息，是所述主区块链确定所述验证设备具有针对业务交易摘要信息的第一获取权限的情况下返回的。

12、根据权利要求 10-11 中任一项所述的方法，其特征在于，所述交易执行结果，是所述第二侧链节点确定所述验证设备具有第二获取权限的情况下返回的。

13、根据权利要求 10-11 中任一项所述的方法，其特征在于，所述方法还包括：

获取所述第二侧链节点返回的与所述交易序号相关联的默克尔路径集合；所述默克尔路径集合，是在所述第二侧链节点确定所述验证设备具有所述第二获取权限的情况下返回的；

所述根据所述交易执行结果，验证所述业务交易摘要信息的合法性，包括：

根据所述交易执行结果以及所述默克尔路径集合，验证所述业务交易摘要信息的合法性。

14、根据权利要求 13 所述的方法，其特征在于，所述根据所述交易执行结果以及所述默克尔路径集合，验证所述业务交易摘要信息的合法性，包括：

生成所述交易执行结果中的写集合的第一哈希值，在所述第一哈希值中获取第三验证目标字段值；所述写集合包括所述业务交易中的第一业务对象的更新状态值；

生成所述交易执行结果中的历史写集合的第二哈希值，在所述第二哈希值中获取第四验证目标字段值；所述历史写集合包括所述第一业务对象的历史状态值；

生成所述交易执行结果中的读集合的第三哈希值，在所述第三哈希值中获取第五验证目标字段值；所述读集合包括所述业务交易中的第二业务对象的历史状态值；

根据所述第三验证目标字段值、第四验证目标字段值、所述第五验证目标字段值、所述写集合、所述历史写集合、所述读集合以及所述默克尔路径集合，验证所述业务交易摘要信息的合法性。

15、根据权利要求14方法的方法，其特征在于，所述根据所述第三验证目标字段值、第四验证目标字段值、所述第五验证目标字段值、所述写集合、所述历史写集合、所述读集合以及所述默克尔路径集合，验证所述业务交易摘要信息的合法性，包括：

将所述第三验证目标字段值与所述业务交易摘要信息中的第三目标字段值进行对比，得到第一对比结果；

将所述第四验证目标字段值与所述业务交易摘要信息中的第四目标字段值进行对比，得到第二对比结果；

将所述第五验证目标字段值与所述业务交易摘要信息中的第五目标字段值进行对比，得到第三对比结果；

根据所述历史写集合以及所述默克尔路径集合中与所述历史写集合相关联的默克尔路径，生成验证历史状态根哈希；

根据所述写集合以及所述默克尔路径集合中与所述写集合相关联的默克尔路径，生成验证更新状态根哈希；

根据所述读集合重新执行所述业务交易，得到验证写集合，根据所述第一对比结果、所述第二对比结果、所述第三对比结果、所述验证历史状态根哈希、所述验证更新状态根哈希以及所述验证写集合，验证所述业务交易摘要信息的合法性。

16、根据权利要求15所述的方法，其特征在于，所述根据所述第一对比结果、所述第二对比结果、所述第三对比结果、所述验证历史状态根哈希、所述验证更新状态根哈希以及所述验证写集合，验证所述业务交易摘要信息的合法性，包括：

在所述验证历史状态根哈希中获取第一验证目标字段值，将所述第一验证目标字段值与所述业务交易摘要信息中的第一目标字段值进行对比，得到第四对比结果；

在所述验证更新状态根哈希中获取第二验证目标字段值，将所述第二验证目标字段值与所述业务交易摘要信息中的第二目标字段值进行对比，得到第五对比结果；

将所述验证写集合与所述写集合进行对比，得到第六对比结果；

若所述第一对比结果、所述第二对比结果、所述第三对比结果、所述第四对比结果、所述第五对比结果以及所述第六对比结果中，存在对比结果为对比不同结果，则确定所述业务交易摘要信息为非法信息；

若所述第一对比结果、所述第二对比结果、所述第三对比结果、所述第四对比结果、所述第五对比结果以及所述第六对比结果均为对比相同结果，则确定所述业务交易摘要信息为合法信息。

17、根据权利要求13所述的方法，其特征在于，所述方法还包括：

若验证所述业务交易摘要信息为非法信息，则根据所述业务类型标识、所述交易序号、所述交易执行结果以及所述默克尔路径集合，生成挑战侧链交易；

将所述挑战侧链交易传输至所述主区块链，以使所述主区块链对所述挑战侧链交易进行共识，且在共识通过所述挑战侧链交易时，确认所述侧区块链为不可信链。

18、一种基于区块链的数据处理装置，其特征在于，所述装置运行于侧链节点，所述侧链节点属于联盟链中的侧区块链，所述联盟链还包括主区块链，所述装置包括：

交易执行模块，用于获取业务设备发送的携带业务交易的交易上链请求，根据所述交易上链请求，确定所述业务交易对应的交易执行结果，对所述交易执行结果以及所述业务交易进行上链处理；

第一生成模块，用于当所述交易执行结果以及所述业务交易成功存储至所述侧区块链时，根据交易序号、业务类型标识以及所述交易执行结果，生成所述业务交易对应的业务交易摘要信息；所述交易序号用于表征所述业务交易在所述侧区块链中的序号，所述业务类型标识用于表征所述侧区块链所处理业务的业务类型；

摘要传输模块，用于将所述业务交易摘要信息传输至所述主区块链，以使所述主区块链存储所述业务交易摘要信息。

19、一种基于区块链的数据处理装置，其特征在于，所述装置运行于验证设备，所述装置包括：

第一发送模块，用于发送携带业务类型标识以及交易序号的第一数据获取请求至联盟链中的主区块链，以使所述主区块链将所述业务交易摘要信息返回至所述验证设备；所述交易序号用于表征业务交易在侧区块链中的序号；所述侧区块链属于所述联盟链；所述业务交易摘要信息是所述侧区块链传输至所述主区块链的；所述业务交易摘要信息，是所述侧区块链中的第一侧链节点在交易执行结果以及所述业务交易

成功存储至所述侧区块链的情况下生成的，所述业务交易摘要信息，是根据所述交易序号、所述业务类型标识以及所述交易执行结果所生成的；所述交易执行结果是所述第一侧链节点在获取到业务设备所发送的交易上链请求时，根据所述交易上链请求所确定的；所述交易上链请求携带所述业务交易；所述业务类型标识用于表征所述侧区块链所处理业务的业务类型；

第二发送模块，用于发送携带所述交易序号的第二数据获取请求至所述侧区块链，以使所述侧区块链中的第二侧链节点将与所述交易序号相关联的所述交易执行结果返回至所述验证设备；

信息验证模块，用于根据所述交易执行结果，验证所述业务交易摘要信息的合法性。

20、一种计算机设备，其特征在于，所述计算机设备包括存储器和一个或多个处理器，所述存储器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，使得所述一个或多个处理器执行权利要求 1 至 17 任一项所述的方法。

21、一个或多个非易失性计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机可读指令，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行权利要求 1-17 任一项所述的方法。

22、一种计算机程序产品，其特征在于，所述计算机程序产品包括计算机可读指令，所述计算机可读指令被处理器执行时实现权利要求 1-17 任一项所述的方法。