

说明书

发明名称：事务上链方法、相关装置和介质

本申请要求于 2023 年 03 月 31 日提交中国专利局，申请号为 2023103616550，申请名称为“事务上链方法、相关装置和介质”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

本申请涉及区块链领域，特别是涉及一种事务上链方法、相关装置和介质。

背景技术

现有的区块链分层共识体系，包括局部共识网络和全局共识网络。局部共识网络中的共识节点针对局部产生的事务进行区块链上链操作，全局共识网络针对从局部事务归纳出的全局事务进行区块链上链操作。局部共识网络和全局共识网络上链操作的区块链不同，从而实现层级化治理，且全局共识网络可以专注于全局治理。

分层共识体系中，虽然在不同局部共识网络之间实现了数据隔离，但事务在区块链上是以明文存储，从而，针对不希望区块链上被第三方访问的目标事务，已有技术不能够满足目标事务的上链需求，目标事务上链安全性差。

发明内容

本申请实施例提供了一种事务上链方法、相关装置和介质。

根据本申请的一方面，提供了一种事务上链方法，由第一中继节点执行，包括：

在第一共识节点接收到局部事务的情况下，确定所述局部事务的父类型；

在所述父类型为第一类型的情况下，将所述局部事务发送到第二共识节点，所述局部事务用于指示所述第二共识节点执行所述局部事务，将所述局部事务记录到第二区块链，生成所述局部事务的第一上链验证信息，并将所述局部事务的第一上链验证信息发送到第三共识节点，所述第一上链验证信息，用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到所述局部事务的上链验证结果，其中，所述第二区块链禁止由所述第二共识节点以外的节点访问；及，

从所述第三共识节点获取所述局部事务的上链验证结果。

根据本申请的一方面，提供了一种事务上链方法，由第二共识节点执行，包括：

接收第一中继节点的局部事务，所述局部事务的父类型为第一类型；

执行所述局部事务，将所述局部事务记录到第二区块链，其中，所述第二区块链被禁止由所述第二共识节点以外的节点访问；

获取所述局部事务的第一上链验证信息；及，

将所述第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到上链验证结果。

根据本申请的一方面，提供了一种事务上链装置，包括：

第一确定单元，用于在第一共识节点接收到局部事务的情况下，确定所述局部事务的父类型；

第一发送单元，用于在所述父类型为第一类型的情况下，将所述局部事务发送到第二共识节点，所述局部事务用于指示所述第二共识节点执行所述局部事务，将所述局部事务记录到第二区块链，生成所述局部事务的第一上链验证信息，并将所述局部事务的第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到所述局部事务的上链验证结果，其中，所述第二区块链禁止由所述第二共识节点以外的节点访问；及，

第一获取单元，用于从所述第三共识节点获取所述局部事务的上链验证结果。

根据本申请的一方面，提供了一种事务上链装置，包括：

第一接收单元，用于接收第一中继节点转发的局部事务，所述局部事务的父类型为第一类型；

第二上链单元，用于执行所述局部事务，将所述局部事务记录到第二区块链，其中，所述第二区块链被禁止由所述第二共识节点以外的节点访问；

第二获取单元，用于获取所述局部事务的第一上链验证信息；及，

第二发送单元，用于将所述第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到上链验证结果。

根据本申请的一方面，提供了一种电子设备，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，所述处理器执行所述计算机可读指令时实现如上所述的事务上链方法。

根据本申请的一方面，提供了一个或多个可读存储介质，所述存储介质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实现如上所述的事务上链方法。

根据本申请的一方面，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，所述计算机可读指令被计算机设备的一个或多个处理器读取并执行，使得该计算机设备执行如上所述的事务上链方法。

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中的技术方案，下面将对实施例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 1A 是一个实施例中分层区块链网络的体系架构示意图；

图 1B 是另一个实施例中分层区块链网络的体系架构示意图；
图 1C 是另一个实施例中分层区块链网络的体系架构示意图；
图 2 是一个实施例中事务上链方法应用在电子发票场景下的示意图；
图 3 是一个实施例中事务上链方法的流程图；
图 4 示出了图 3 中步骤 330a 利用队列进行打包发送的流程图；
图 5 示出了本申请实施例中利用不同子类型所属的队列进行打包发送的示意图；
图 6 示出了图 3 中步骤 330a 利用优先级和队列进行打包发送的流程图；
图 7 示出了图 6 中利用优先级和队列进行打包发送的示意图；
图 8 示出了图 3 中步骤 330a 和 330b 利用摘要算法进行签名验证的示意图；
图 9 示出了图 3 中步骤 330a 利用子类型进行第一全局共识网络选择的示意图；
图 10 示出了本申请实施例中区块链网络存在多个第一全局共识网络的情形的体系构架图；
图 11 示出了图 3 中步骤 330c 和 330d 生成第一树以及利用第一树进行验证的示意图；
图 12A 示出了图 11 中步骤 330c 的第一上链验证信息的数据结构示意图；
图 12B 示出了本申请实施例中生成第一树的示意图；
图 12C 示出了本申请实施例中第一树的第一路径的第一旁路节点的示意图；
图 13 示出了在图 11 的基础上步骤 330c 和 330d 生成第二树以及利用第二树进行验证的流程图；
图 14A 示出了图 13 中步骤 330c 的第一上链验证信息的数据结构示意图；
图 14B 示出了本申请实施例中生成第二树的示意图；
图 14C 示出了本申请实施例中第二树的第二路径的第二旁路节点的示意图；
图 15 示出了带有第一签名的第一上链验证信息的数据结构示意图；
图 16 示出了带有事务脱敏信息的第一上链验证信息的数据结构示意图；
图 17 示出了带有即时性信息的第一上链验证信息的数据结构示意图；
图 18 示出了上链验证结果请求的一个数据结构示意图；
图 19 是另一个实施例的事务上链方法的流程图；
图 20 是另一个实施例的事务上链方法的流程图；
图 21 是本申请的一个详细实施例的多端交互图；
图 22 是一个实施例的由第二共识节点执行的事务上链方法的流程图；
图 23 是一个实施例的位于第一中继节点的事务上链装置的模块图；
图 24 是一个实施例的位于第二共识节点的事务上链装置的模块图；
图 25 是一个实施例实施事务上链方法的终端结构图；及，
图 26 是一个实施例实施事务上链方法的服务器结构图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

对本申请实施例进行进一步详细说明之前，对本申请实施例中涉及的名词和术语进行说明，本申请实施例中涉及的名词和术语适用于如下的解释：

分层区块链：是在区块链网络中的点对点传输的基础上，将共识网络和见证网络分开（如图 1A 所示）。共识网络的共识节点主要进行共识算法。见证网络又称业务网络，见证网络的见证节点进行数据的清分同步，并在见证节点的基础上完成相关具体业务。

清分同步：共识节点收到见证节点同步数据的请求后，将见证节点有权限读取的数据同步给见证节点。

分层区块链的分层共识体系：是在上述分层区块链将见证网络和共识网络分开的基础上，再将共识网络分为局部共识网络和全局共识网络。局部共识网络中的共识节点针对局部产生的事务（例如，某集团下属分公司产生的事务）进行区块链上链操作，全局共识网络针对从局部事务归纳出的全局事务（例如，从分公司事务归纳出的集团性事务）进行区块链上链操作。局部共识网络和全局共识网络上链操作的区块链不同，从而实现层级化治理。这样，全局共识网络不需要处理大量的局部事务，可以专注于全局治理。

在分层共识体系中，虽然在不同局部共识网络之间实现了数据隔离，但事务在区块链上还是以明文存储。某些事务出于某种需要并不希望暴露给第三方，因此已有技术不能够满足不希望暴露给第三方的目标事务的上链需求。目标事务上链安全性差。而且，分层共识体系比较大，各个局部共识网络产生很多目标事务，由各个局部共识网络各自处理目标事务的上链安全性问题，存在开销大和难度大的问题。因此，急需一种能够提高目标事务上链安全性且更具有普适性的技术。

本申请实施例应用的系统体系构架及场景说明

参见图 1A 所示的区块链网络，它包括见证网络和共识网络。共识网络是指对待上链事务进行共识后在区块链上进行上链的网络，它包括多个共识节点。多个是指至少两个。见证网络是指产生待上链事务、不在区块链上进行上链、但对待上链事务的上链进行见证的网络，它包括多个见证节点。共识节点即区块链节点。

见证节点不需要参与上链共识，主要用于产生待上链事务，并对待上链事务的上链进行见证。共识节点一般是全节点。全节点是指维护区块链上每个区块的全部数据的节点。由于共识节点要对待上链事务生成区块后上链，其当然要维护整个区块链上所有区块的数据。见证节点一般是轻节点。轻节点是指维护区块链上每个区块的部分数据的节点，例如全节点完成上链后，仅将上链区块的区块头发给轻节点，由轻节点在需要验证是否正确上链时，利用区块头中的摘要值进行默克尔树（Merkle trees）验证。

共识节点或区块链节点可以为区块链网络中的服务器，也可以为接入区块链网络中的用户终端，这里对共识节点或区块链节点的具体形式不做限定。图 1A 所示的见证网络和共识网络可以处于不同的网络环境。例如，通常来说，见证节点部署在处于公网的见证网络中，而运行区块链共识协议的共识节点则部署在私网的共识网络中。见证节点和共识节点可以通过路由节点进行交互，见证节点和共识节点也可以不通过路由节点而直接进行数据传输。由于共识网络处于相对安全的私有云中，其相互访问本就有共识机制保证安全，不需要额外加入身份管理和网络控制。而见证节点处于公共网络中，可能会被其他不确定的网络终端访问，因此见证节点以及其他可能的节点接入共识网络中的行为需要被严格控制。

图 1A 示出了包括见证网络和共识网络的体系架构图，接下来以图 1B 为例，继续说明在图 1A 的基础上利用共识网络进行分层共识的体系架构。

参见图 1B 所示的区块链分层共识网络，区块链分层共识网络是指用于对事务进行分层共识的区块链网络，该区块链分层共识网络包括见证网络、局部共识网络、局部网络级见证节点、和全局共识网络。见证网络即图 1A 中的见证网络。局部共识网络是指对局部事务进行共识并上链的网络。它包括多个局部共识节点。局部事务是指仅对局部范围有影响的事务。例如，某集团的分公司的电子发票报销方面的事务，属于局部事务。全局共识网络是用于对从局部事务推演出的全局事务进行共识并上链的网络。它包括多个全局共识节点。全局事务是指对全局范围有影响的事务。例如，集团针对其分公司的电子发票报销进行汇总的事务，属于全局事务。局部网络级见证节点是局部共识节点和全局共识节点之间的接口节点，它用于：将局部共识网络产生的局部事务汇总成全局事务，通过全局共识网络入口发送到全局共识网络上链，并对全局共识网络的上链进行见证。图 1B 中的局部网络级见证节点有 2 个，它起到双备份作用。两个局部网络级见证节点同时工作，执行相同的动作。若其中一个局部网络级见证节点发生故障，也不会造成信息的丢失和工作流的中断。

注意，见证网络中的见证节点不对全局共识网络中的上链正确性进行验证，仅对局部共识网络中的上链正确性进行验证。当其需要验证其产生的局部事务是否由局部共识节点正确上链时，通过如上所述的清分同步的方式从局部共识节点中取得其验证需要的数据，局部共识节点不会向其发送全部上链数据。而局部网络级见证节点仅对全局共识网络中的上链正确性进行验证。当其需要验证从局部事务推演出的全局事务是否由全局共识节点正确上链时，通过如上所述的清分同步的方式从全局共识节点中取得其验证需要的数据，全局共识节点也不会向其发送全部上链数据。

图 1C 的体系构架与图 1B 的区别在于，它用第一中继节点取代了图 1B 的两个局部网络级见证节点，将全局共识网络进一步区分为第二全局共识网络和第一全局共识网络，且在第二全局共识网络和第一全局共识网络之间采用第二中继节点。第一全局共识网络是指对目标事务进行上链处理的区块链网络，它将目标事务记录到第二区块链上。目标事务是指不希望被第三方访问且知晓的事务。第二区块链用于专门记录不希望被第三方访问且知晓的事务的区块，第二区块链不希望被外界访问。第三方和外界均指第二共识节点以外的区块链节点，例如，第三方和外界包括见证节点、第一共识节点、第三共识节点、第一中继节点、第二中继节点。如果希望获取记录到该区块链上的区块的验证信息，只能够通过请求记录该区块链的第一全局共识网络中的区块链节点来进行。

由于目标事务是不希望被第三方访问且知晓的事务，因此，在对目标事务上链前，要征求产生该目标事务的对象的同意。具体地，在对象产生目标事务，发送到局部共识网络进行上链时，可以向对象显示询问框，询问对象是否同意将目标事务上链。如果对象不同意，则不能实施该实施方式，或者仅上链同意上链的那部分事务。

图 1C 的第一共识节点与图 1B 的局部共识节点的区别在于，它只针对第二类型的局部事务进行上链。对于第一类型的局部事务，它通过第一中继节点委托第一全局共识网络中的第二共识节点上链。第一类型是指不希望被第三方访问且知晓的事务类型。第二类型是指允许被第三方访问且知晓的事务类型。第二类型的局部事务上链到一条外界任何节点可以查看的区块链上，而第一类型的局部事务上链到只有第一全局共识网络内部可见的区块链上，从而提高目标事务上链安全性。

图 1C 的全局共识网络中的第二全局共识网络与图 1B 中的全局共识网络类似，主要用于进行从局部事务推演出来的全局事务的上链。该第二全局共识网络包括多个第三共识节点。图 1C 的全局共识网络中的第一全局共识网络是相对于图 1B 增加的网络。它的作用是完成第一类型的局部事务的上链。第一全局共识网络包括多个第二共识节点。当第一全局共识网络将第一类型的局部事务上链后，该上链的区块链外界不得查看。为了让外界对象能够验证是否正确上链，第一全局共识网络可以产生上链验证信息，发送到第二全局共识网络，由第二全局共识网络进行验证，通过第一中继节点向局部共识网络返回上链验证结果。第一中继节点是将第一类型的事务传递到第一全局共识网络上链的节点。第二中继节点是将第一全局共识网络产生的上链验证信息发送到第二全局共识网络验证的节点。

本申请实施例可以应用在多种场景下，包括但不限于是电子发票、股权登记、证券交易等场景，例如图 2 所示的税务电子发票区块链系统的场景等。

参见图 2，税务电子发票区块链系统包括业务层、路由代理层、共识网络层。

业务层即见证网络，包括至少一个见证节点。业务层可以接收来自电子税局、企业或消费者的局部事务请求，例如电子税局的电子发票发行事务上链请求、企业的电子发票领取事务上链请求、消费者的电子发票开票上链请求。业务层包括税务专网中地方税局的服务器、公有云中的开票服务器（用于非关键企业电子发票开票的服务器）、报销服务器（用于非关键企业电子发票报销的服务器）、关键企业服务器（用于关键企业电子发票各种事务的服务器）、私有云中的支付服务器（用于消费者在非关键企业支付过程中的发票有关事务的服务器）、流转服务器（用于物品在非关键企业流转过程中发票有关事务的服务器）、

关键企业服务器（用于消费者在关键企业的发票有关事务的服务器）。关键企业是指有一定规模、因而需要专用服务器为其提供发票有关事务的企业。其中，电子税局的全称为电子税务局，用于提供网上办税服务。税务电子发票，是指电子税局发放的电子发票。电子发票是指通过电子方式生成、存储、传输和管理的发票。税务专网是指为纳税人服务的网络，地方税局是主管地方税收工作的政府机构。

税务专网中地方税局的服务器针对电子税局的电子发票发行需求，生成电子发票发行事务，并请求共识网络层对该事务进行上链。公有云中的开票服务器针对非关键企业申领电子发票的需求，生成电子发票领取事务，并请求共识网络层对该事务进行上链。公有云中的报销服务器针对非关键企业报销电子发票的需求，生成电子发票报销事务，并请求共识网络层对该事务进行上链。公有云中的关键企业服务器针对关键企业领取或报销电子发票的需求，生成电子发票领取或报销事务，并请求共识网络层对该事务进行上链。私有云中的支付服务器针对消费者在非关键企业的支付动作，生成要求开出电子发票的事务，并请求共识网络层对该事务进行上链。私有云中的流转服务器根据非关键企业的消费者之间互换物品的需求，生成电子发票流转事务，并请求共识网络层对该事务进行上链。私有云中的关键企业服务器根据关键企业的消费者的支付或物品流转的要求，生成要求开票或流转的事务，并请求共识网络层对该事务进行上链。

注意，上述各种服务器针对对象的各种需求，生成事务并请求共识网络层进行上链时，要征得对象的同意。具体地，在生成事务并发送到共识网络层进行上链时，可以向对象显示询问框，询问对象是否同意将生成的事务上链。如果对象不同意，则不能实施该实施方式，或者仅上链同意上链的那部分事务。

路由代理层是指在节点之间起到路由作用的层。它用于业务层和共识网络层相关数据的路由。它包括认证服务、证书缓存、路由服务和点对点服务。路由服务用于将业务层产生的待上链事务路由到共识网络层。认证服务用于在将待上链事务路由到共识网络层之前，对待上链事务进行认证，例如根据密钥证书进行待上链事务的签名进行验签。证书缓存专门用于缓存认证服务中需要的公私钥证书。点对点服务提供节点之间的对等通信。将待上链事务通过共识网络层上链后，接收共识网络层返回的上链验证信息就是通过点对点服务进行的。

共识网络层包括与图 1C 相同的局部共识网络、第一全局共识网络和位于二者之间的第一中继节点。局部共识网络包括多个第一共识节点，每个第一共识节点包含用于判断自己是否有上链权限的权限合约、以及局部事务区块链上链处理中用到的存储器，并本地维护自己上链的区块。第一全局共识网络包括多个第二共识节点，每个第二共识节点包含用于判断自己是否有上链权限的权限合约、以及目标事务上链处理中用到的存储器，并在本地维护自己上链的区块。

图 2 中，共识网络层有 3 个分支。如果接收到代理节点转发过来的、地方税局服务器生成的电子发票发行事务上链请求，转发到分支 1 的第一共识节点。第一共识节点查询自己的权限合约，发现自己没有在局部事务区块链上链的权限（因为电子发票的发行是不希望被第三方知晓的事务，必须转给第一全局共识网络上链到第二区块链），于是通过第一中继节点将该请求转发到分支 1 中的第二共识节点。如果接收到代理节点转发过来的、公有云的各种服务器生成的电子发票开票、报销等事务上链请求，转发到分支 2 的第一共识节点。第一共识节点查询自己的权限合约，发现自己没有在局部事务区块链记账的权限（因为电子发票的开出和报销是不希望第三方知晓的事务，必须转给第一全局共识网络上链到第二区块链），于是通过第一中继节点将该请求转发到分支 2 中的第二共识节点。如果接收到代理节点转发过来的、私有云的各种服务器生成的要求电子发票开出、电子发票流转等事务上链请求，转发到分支 3 的第一共识节点。第一共识节点查询自己的权限合约，发现自己没有在局部事务区块链记账的权限（因为要求电子发票开出、电子发票流转是不希望第三方知晓的事务，必须转给第一全局共识网络上链到第二区块链），于是通过第一中继节点将该请求转发到分支 3 中的第二共识节点。分支 1-3 的第二共识节点将目标事务记录到第二区块链后，该第二区块链外界不可获得，提高了目标事务上链安全性。

本申请实施例的总体说明

根据本申请的一个实施例，提供了一种事务上链方法。

该事务上链方法一般应用在事务数据不希望被外界知晓的业务场景中，例如图 2 所示的税务电子发票区块链系统的场景。将不希望被外界知晓的事务称为目标事务。本申请实施例提供了一种统一执行并记录第一类型的局部事务的方案，能够提高目标事务上链安全性。同时，为了确保目标事务的真实上链，还提供了验证机制。该事务上链方法由区块链分层共识网络中的第一中继节点执行。

如图 3 所示，根据本申请一个实施例的事务上链方法可以包括：

步骤 310、在第一共识节点接收到局部事务的情况下，确定局部事务的父类型；

步骤 320、在局部事务的父类型为第二类型的情况下，指示第一共识节点执行局部事务，并将局部事务记录到第一区块链，第一区块链允许由第一共识节点以外的节点访问；及，

其中，第一共识节点以外的节点是指区块链系统中除局部共识网络中节点之外的节点，包括见证节点、第一中继节点、第二中继节点、第一全局共识网络中的节点、第二全局共识网络中的节点。

步骤 320 中，由于第一区块链允许由第一共识节点以外的节点访问，从而在局部事务的父类型为第二类型的情况下，指示第一共识节点执行局部事务，并将局部事务记录到第一区块链，可以使得外界任何节点查看的该局部事务。

步骤 330、在局部事务的父类型为第一类型的情况下，将局部事务发送到第二共识节点，局部事务用于指示第二共识节点执行局部事务，将局部事务记录到第二区块链，生成局部事务的第一上链验证信息，并将局部事务的第一上链验证信息发送到第三共识节点，第一上链验证信息用于指示第三共识节点根据第一上链验证信息对局部事务的上链进行验证，得到局部事务的上链验证结果，其中，第二区块链禁止由第二共识节点以外的节点访问；

步骤 340、从第三共识节点获取局部事务的上链验证结果。

下面对步骤 310-340 进行详细描述。

在步骤 310 中，第一中继节点确定局部共识网络中的第一共识节点接收到的局部事务的父类型。该父类型为第一类型或第二类型。第一类型是指事务不允许外界知晓的类型。第二类型是指事务允许外界知晓的类型。

第一中继节点是用于确定局部事务的父类型并将第一类型的局部事务进行转发的一个模块。第一中继节点可以是一个独立的设备，如单独的计算机或服务器，也可以是独立设备的一部分，例如服务器上划分出的一个虚拟机。父类型为第一类型的局部事务在本申请中称为目标事务。

第一共识节点处于局部共识网络中，是用于接收局部事务并执行第二类型的局部事务以及记录到第一区块链的一个模块。第一区块链记录局部事务，且能被第一共识节点以外的节点访问。第一共识节点可以是一个独立的设备，如单独的计算机或服务器，也可以是独立设备的一部分，例如服务器上划分出的一个虚拟机。

步骤 310 可以分为第一共识节点接收到局部事务、第一中继节点发现局部事务、第一中继节点确定局部事务的父类型的交互过程。局部事务是指需要被共识节点执行并记录到区块链的局部事务，例如某企业发票报销事务等。局部事务的父类型用于指示该局部事务是否允许被第三方获知。该局部事务的父类型可为第一类型（例如发票报销事务的父类型为第一类型）或第二类型（例如天气信息事务）中的一个，第一类型的局部事务需要由共识节点（例如，下文出现的第二共识节点）执行并记录到不可被外界访问的区块链。第二类型的局部事务需要由共识节点（例如，第一共识节点）执行并记录到可以被外界访问的区块链。

在一些实施例中，局部事务的父类型的确定周期的设置包括以下情形：

- (1) 在发现第一共识节点接收到局部事务之后，立即确定局部事务的父类型；及，
- (2) 根据第一中继节点预先设置的确定周期，在发现第一共识节点存在局部事务之后且过去该确定周期时，确定局部事务的父类型。例如，第一中继节点预先设置的确定周期为 1 小时，若发现第一共识节点接收到局部事务的时刻为当日上午七点，则在当日上午八点确定局部事务的父类型。

在一些实施例中，局部事务的父类型的确定方式包括但不限于以下方式：

- (1) 在发现第一共识节点接收到局部事务之后，从局部事务的内容中提取第一关键字段，根据第一关键字段查找字段父类型对照表，以确定局部事务的父类型。如下是一个字段与父类型对照表的例子：

表 1

第一关键字段	父类型
发票	第一类型
资源	第一类型
天气	第二类型

如表 1 所示，对于第一关键字段为发票来说，该局部事务不允许向外界透露，所以确定该局部事务的父类型为第一类型。对于第一关键字段为资源来说，该局部事务也不允许向外界透露，所以确定该局部事务的父类型为第一类型。而对于第一关键字段为天气来说，该局部事务允许向外界透露，所以确定该局部事务的父类型为第二类型。

例如，局部事务的内容包括“电子发票 0001 报销：数额 500、且用于外出住宿”，其包括的第一关键字段为“发票”，因此确定该局部事务的父类型为第一类型。又例如，局部事务为“100 个第一资源转换成 10 个第二资源”，其包括的第一关键字段为“资源”，因此确定该局部事务的父类型为第一类型。又例如，局部事务为“天气 10001：XX 月 XX 日天气晴”，其包括的第一关键字段为“天气”，因此确定该局部事务的父类型为第二类型。

- (2) 在发现第一共识节点接收到局部事务之后，从局部事务的内容中获取类型标识，根据类型标识确定局部事务的父类型。

类型标识分为两种情形，一种情形是以字符代表是否为第一类型，例如“1”作为类型标识来代表第一类型、且以“0”作为类型标识来代表第二类型。另一种情形是直接将第一类型或第二类型作为类型标识。

例如，局部事务的内容包括“电子发票 0001 报销，数额 500、且用于外出住宿；【第一类型】”，则根据内容中包括的“【第一类型】”确定该局部事务的父类型为第一类型。又例如，局部事务的内容包括“电子发票 0001 报销，数额 500、且用于外出住宿；【1】”，则根据内容中包括的“【1】”确定该局部事务的父类型为第一类型。

在步骤 310 确定局部事务的父类型之后，存在两种情况。第一种情况是确定出局部事务的父类型为第二类型，则会执行步骤 320。第二种情况是确定出局部事务的父类型为第一类型，则会执行步骤 330。

先对步骤 310 之后产生的第一种情况展开描述。

在步骤 320 中，响应于确定出局部事务的父类型为第二类型，由第一共识节点执行局部事务，并将局部事务记录到第一区块链。

第一共识节点上运行普通业务智能合约（例如下文的订单智能合约），业务逻辑在合约代码中公开体现。与该普通业务智能合约交互的局部事务在第一共识节点上执行，执行结果也记录在第一共识节点维护的第一区块链上。此外，这些执行结果也可以通过第一中继节点回传到全局共识网络中第二全局共识网络。

例如，假定第二类型的局部事务为“订单 10001：购买办公用品 50 件”。则第一共识节点调用订单智

能合约执行该局部事务，执行结果为“已完成：订单 10001：购买办公用品 50 件”。该执行结果由第一共识节点记录在第一区块链上，且除了第一共识节点以外的节点均可访问该第一区块链。

对于上述提及的将局部事务记录到第一区块链的具体过程如下所述：

一般地，见证节点基于对象的操作行为产生局部事务，将局部事务以及见证节点的数字签名发送至局部共识网络上邻近的第一共识节点，便于第一共识节点对局部事务的真实性进行验证。在进行验证时，第一共识节点利用见证节点的公钥对数字签名进行验证，得到局部事务的第一摘要值，并根据摘要算法对局部事务进行摘要计算，得到局部事务的第二摘要值，比对第一摘要值和第二摘要值，若第一摘要值和第二摘要值相同，则验证通过，局部事务为见证节点产生的真实事务。

验证通过后，将局部事务和见证节点发送的其它局部事务进行积累。当积累达到一定程度（例如积累的事务数目达到某个阈值，或积累时间达到某个阈值），将这些局部事务打包成区块，发送到局部共识网络中的其它第一共识节点，进行共识，共识成功后，由各第一共识节点将该区块记录到第一共识节点各自维护的第一区块链上。

接着，对步骤 310 之后产生的第二种情况展开描述。

继续参照图 3，步骤 330 可以分为：

步骤 330a（由第一中继节点执行），响应于局部事务的父类型为第一类型，将局部事务发送到第一全局共识网络中的第二共识节点；

步骤 330b（由第二共识节点执行），执行局部事务，将局部事务记录到第二区块链；

步骤 330c（由第二共识节点执行），将局部事务的第一上链验证信息发送到第二全局共识网络中的第三共识节点；及，

步骤 330d（由第三共识节点执行），根据第一上链验证信息对局部事务的上链进行验证。

下面对步骤 330a-330d 进行详细描述。

在步骤 330a 中，第一中继节点在确定出局部事务的父类型为第一类型之后，由于目标事务是不希望被第三方访问且知晓的事务，因此，在对目标事务上链前，要征求产生该目标事务的对象的同意。具体地，可以向对象显示询问框，询问对象是否同意将目标事务上链。如果对象不同意，则不能实施该实施方式，或者仅上链同意上链的那部分事务。

然后，将局部事务发送到第一全局共识网络中的第二共识节点。

第一中继节点在确定出局部事务的父类型为第一类型之后，说明该局部事务需要被执行和记录到不可被外界访问的第二区块链，因此需要由第二共识节点执行该局部事务。

第二共识节点位于第一全局共识网络中，是用于接收并执行第一类型的局部事务以及记录到第二区块链的一个模块。该第二区块链被禁止由第二共识节点以外的节点访问，保证目标事务上链的安全性。第二共识节点可以是一个独立的设备，如单独的计算机或服务器，也可以是独立设备的一部分，例如服务器上划分出的一个虚拟机。

在步骤 330b 中，对于第二共识节点执行局部事务，以及将局部事务记录到第二区块链的具体过程，可以参照上述第一共识节点执行局部事务并记录到第一区块链的具体过程。

在第二共识节点将局部事务记录到第二区块链之后，为了能够验证第二共识节点将局部事务真实上链，第二共识节点还产生了第一上链验证信息。

在步骤 330c 中，第一上链验证信息由第二共识节点发送到第二全局共识网络中的第三共识节点。

在步骤 330d 中，第三共识节点位于第二全局共识网络中，是用于接收并根据第一上链验证信息进行验证的一个模块。该第三共识节点所维护的第三区块链能被由第三共识节点以外的节点访问。在第三共识节点对第一上链验证信息进行验证时，该第三共识节点运行部署目标状态验证智能合约，该合约中维护了对于第一全局共识网络发送的第一上链验证信息的验证代码。第三共识节点可以是一个独立的设备，如单独的计算机或服务器，也可以是独立设备的一部分，例如服务器上划分出的一个虚拟机。

接着，在步骤 330 之后，在步骤 340 中，第一中继节点从第三共识节点获取局部事务的上链验证结果。

在一实施例中，步骤 340 包括，第一中继节点从第三共识节点获取上链验证结果、第一中继节点将上链验证结果发送到局部共识网络的交互过程。通过上链验证结果获知第一类型的局部事务已上链成功。

通过上述步骤 310-340，本申请实施例将全局共识网络分为第二全局共识网络 and 第一全局共识网络，利用局部共识网络能够同步第二全局共识网络的信息，通过第一中继节点回传局部共识网络中的局部事务的能力，实现了目标事务的安全上链。也就是说，局部事务在第一全局共识网络中执行和记录，在第二全局共识网络中确认上链验证结果。具体的计算过程和计算逻辑以及中间结果，都在第一全局共识网络中完成，同时第一全局共识网络本身的共识以及在主区块链链中的验证，可以有效地利用区块链的不可篡改特性保证事务的正确可信。

以上是对步骤 310-340 进行的总体描述。由于步骤 320 和步骤 330b 已在上述总体描述中详尽，下面将针对步骤 330a、330c-330d 和步骤 340 的具体实现展开详细描述。

步骤 330a 的详细描述

在步骤 330a 中，第一中继节点在确定出局部事务的父类型为第一类型之后，将局部事务发送到第一全局共识网络中的第二共识节点。

在一些实施例中，局部事务的发送周期的设置包括以下情形：

（1）在确定出局部事务的父类型为第一类型之后，立即发送局部事务；及，

（2）根据第一中继节点预先设置的第一发送周期，在确定出局部事务的父类型为第一类型之后且过去该第一发送周期时，发送局部事务。例如，第一中继节点预先设置的第一发送周期为 2 小时，若确定出

局部事务的父类型为第一类型的时刻为当日下午七点，则发送局部事务的时刻为当日下午九点。

针对步骤 330a 的分解，本申请实施例给出了三种分解方式。每一种分解方式以不同的角度展开对步骤 330a 的详细描述。先来描述第一种分解方式。

参照上述对局部事务的发送周期的描述，无论是立即发送还是过去第一发送周期再发送的方式，相当于每次遇到一个第一类型的局部事务，就与第一全局共识网络建立一次连接，开销太大。为了减少开销，降低网络资源损耗，在一实施例中可以先排队，满足预定条件时再打包发送一次。

本申请实施例中，对于第一类型的局部事务，将局部事务发送到第二共识节点，以指示第二共识节点将局部事务记录到第二区块链。由于第二区块链不允许被第二共识节点之外的其它节点访问，从而使得第一类型的局部事务的安全性得到了保证。同时，第二共识节点完成局部事务的上链后，把上链后的第一上链验证信息发送给第三共识节点，由第三共识节点进行上链验证得到上链验证结果，并从第三共识节点获取上链验证结果，确保了虽然局部事务不可被外部查看，但是它的上链是真实可信的，从而提高了局部事务上链的安全性。

在一些实施例中，第一共识节点属于局部共识网络，第二共识节点属于全局共识网络中的第一全局共识网络，第三共识节点属于全局共识网络中的第二全局共识网络，第一中继节点，用于将第一类型的局部事务发送至第一全局共识网络中的第二共识节点。

本申请实施例，将全局共识网络分为第二全局共识网络和第一全局共识网络，利用局部共识网络能够同步第二全局共识网络的信息，通过第一中继节点回传局部共识网络中的局部事务的能力，实现了第一类型的局部事务的安全上链。也就是说，局部事务在第一全局共识网络中执行和记录，在第二全局共识网络中确认上链验证结果。具体的计算过程和计算逻辑以及中间结果，都在第一全局共识网络中完成，同时第一全局共识网络本身的共识以及在主区块链链中的验证，可以有效地利用区块链的不可篡改特性保证事务的正确可信。本申请实施例，提高了区块链分层共识体系中的目标事务上链安全性。本申请实施例可应用于区块链、结构化信息处理、安全技术等各种场景。

在该实施例具体实现时，参照图 4，步骤 330a（由第一中继节点执行）具体包括：

步骤 410、将局部事务放置在队列中排队；及，

步骤 420、响应于队列满足预定条件，将队列中的局部事务打包，发送到第二共识节点。

下面对步骤 410-420 进行详细描述。

在步骤 410 中，第一中继节点中设置一个队列，队列是一种用于存储局部事务的事务存储容器。每次第一中继节点确定一个局部事务的父类型为第一类型时，将该局部事务放置在队列中排队。

放置在队列中一般包括两种放置方式：

（1）直接将局部事务放置在队列尾部；及，

（2）先确定局部事务在队列中要插入的位置，局部事务在队列中要插入的位置称为目标位置，将目标位置上的局部事务以及排在目标位置后面的局部事务向后移动，然后将局部事务放置在队列的目标位置处。

在步骤 420 中，响应于队列满足预定条件，第一中继节点将队列中的局部事务打包，发送到第二共识节点。

预定条件包括以下至少之一：局部事务数目达到第一阈值、以及当前时间与上一个打包的时间的时间差达到第二阈值。例如，响应于队列中局部事务数目达到第一阈值，第一中继节点将队列中的局部事务打包，发送到第二共识节点。又例如，响应于队列中当前时间与上一个打包的时间的时间差达到第二阈值，第一中继节点将队列中的局部事务打包，发送到第二共识节点。又例如，响应于队列中局部事务数目达到第一阈值、且响应于队列中当前时间与上一个打包的时间的时间差达到第二阈值，第一中继节点将队列中的局部事务打包，发送到第二共识节点。

本实施例中，将所有第一类型的局部事务均放在同一个队列进行打包发送，提高了打包效率。

在上述预定条件下，若仅考虑数目达到第一阈值，会影响打包发送的时效性，从而导致一些局部事务长期得不到上链。若是仅考虑时间差达到第二阈值，虽是保证了时效性，但可能会导致每次打包的数目太少，浪费网络资源。同理，若是同时考虑数目达到第一阈值、且时间差达到第二阈值，则会存在时间差已满足第二阈值，但数目一直无法达到第一阈值的可能，仍然影响打包发送的时效性。因此，在一些实施例中，步骤 420 具体包括：

响应于队列中局部事务的数目达到第一阈值，将队列中的局部事务打包。

本实施例中，将局部事务的数目确定作为打包的条件，从而避免每次打包的数目太少，浪费网络资源。

在一些实施例中，步骤 420 具体还包括：响应于队列中局部事务的数目未达到第一阈值，确定当前时间与上一个打包时间之间的时间差；

响应于时间差达到第二阈值，将队列中的局部事务打包。

本实施例中，结合数目和时间差，既不会每次打包的数目太少，浪费网络资源，又兼顾了时效性，不会让一些局部事务长期得不到上链。

由于各个第一类型的局部事务的子类型并不相同，考虑到将同一种子类型的局部事务打成一个包一起上链，有助于第一全局共识网络上链的效率。因此，在另一些实施例中，每个子类型分别对应各自的队列，以便将同一子类型的局部事务放在同一个队列中。例如，图 5 中示出了两个队列，分别是 M 和队列 N。队列 M 用于存储子类型 a 的局部事务。队列 N 用于存储子类型 b 的局部事务。

在该实施例的具体实现时，步骤 410 包括：确定第一类型的局部事务的子类型；确定局部事务的子类型对应的队列；及，将局部事务放置在与子类型对应的队列中排队。

继续参照图 5，局部事务 1-8 已根据子类型分别放置入了对应的队列，也就是子类型 a 的局部事务 1、

3、5 和 7 放置在队列 M 中，子类型 b 的局部事务 2、4、6 和 8 放置在队列 N 中。在需要将局部事务 9 放置在队列时，先确定局部事务 9 的子类型。若局部事务 9 的子类型为 a，则放置入队列 M 的尾部（图 5 所示的队列 M 的虚线框处），若局部事务 9 的子类型为 b，则放置入队列 N 的尾部（图 5 所示的队列 N 的虚线框处）。

本实施例中，将同一子类型的局部事务子进行打包发送，第二共识节点可以使用同一种子类型的目标智能合约（目标智能合约或目标合约是指对某个子类型的目标事务进行上链处理的智能合约，其中包含有用于对该子类型的目标事务进行上链处理的代码）对这些局部事务进行统一执行，减少来回调用不同子类型的目标智能合约执行，从而提高执行效率。例如，第二共识节点接收到了一个打包好的局部事务，其中全部局部事务都是使用目标智能合约 T 进行执行，那么第二共识节点在处理这些局部事务时，可以全部使用目标智能合约 T 进行处理，缓解了因为需要多次更换目标智能合约而降低第二共识节点的处理效率的问题。

步骤 420 包括：如果一个队列中的局部事务数目达到第三阈值，将队列中的局部事务打包。以局部事务 9 放置在队列 M 为例，在放置局部事务 9 之后，队列 M 中局部事务的数目达到第三阈值（例如第三阈值为 5），将队列 M 中的局部事务打包，发送给第二共识节点。

本实施例中，将局部事务的数目确定作为打包的条件，从而避免每次打包的数目太少，浪费网络资源。以上是对步骤 330a 的第一种分解方式的详细描述，接下来描述第二种分解方式。

在上述步骤 330a 分解为步骤 410-420 时，是直接将局部事务放置在队列中进行排队。但对于某些需要紧急上链的局部事务而言，若是直接被放置在队列中排队，无法满足不同局部事务的紧急上链需求。因此，在一实施例中，步骤 330a 结合局部事务的优先级，将优先级高的局部事务先发送到第一全局共识网络进行上链，满足紧急上链需求。

在该实施例的具体实现时，参照图 6，步骤 330a（由第一中继节点执行）包括：

- 步骤 610、确定第一类型的局部事务的子类型；
- 步骤 620、根据子类型，确定局部事务的优先级；
- 步骤 630、将局部事务按照优先级从高到低的顺序，放置在队列中排队；及，
- 步骤 640、从队列中顺序取出局部事务，发送到第二共识节点。

下面对步骤 610-640 进行详细描述。

在步骤 610 中，第一中继节点确定第一类型的局部事务的子类型。

在对子类型进行说明之前，先再次强调，局部事务的父类型用于指示局部事务是否需要被执行和记录到不可被外界访问的区块链上。所以，第一类型的局部事务说明该局部事务需要被执行和记录到不可被外界访问的区块链（也就是由第二共识节点执行并记录至第二区块链上）。而与第一类型不同的是，子类型是指局部事务本身的事务类型。例如局部事务为发票报销事务，该发票报销事务本身的事务类型为发票类型，所以子类型为发票类型。又例如局部事务为企业采购事务，该企业采购事务本身的事务类型为订单类型，所以子类型为订单类型。以子类型为发票类型为例，第一中继节点确定该发票类型对应的优先级，从而根据优先级体现子类型为发票类型的企业开发票事务的紧急上链需求。

在一些实施例中，第一类型的局部事务的子类型的确定方式包括但不限于以下方式：

（1）从第一类型的局部事务的内容中提取第二关键字段，根据第二关键字段查找第二关键字段与子类型对照表，以确定局部事务的子类型。如下是一个第二关键字段与子类型对照表的例子：

表 2

第二关键字段	子类型
报销	发票报销类型
查发票	发票查询类型
开票	发票开票类型
换资源	资源互换类型
转资源	资源转移类型
统计资源	资源统计类型

如表 2 所示，对于局部事务包括的第二关键字段分别为报销、查发票和开票来说，确定局部事务的子类型分别为发票报销类型、发票查询类型和发票开票类型。同理，对于局部事务包括的第二关键字段分别为换资源、转资源和统计资源来说，确定该局部事务的子类型分别为资源互换类型、资源转移类型和资源统计类型。

需要注意的是，在表 1 中是利用第一关键字段确定局部事务的父类型是第一类型或是第二类型，而表 2 是在已经确定该局部事务是第一类型的基础上，再根据第二关键字段确定子类型。

例如，局部事务的内容包括“电子发票报销 0001，数额 500、且用于外出住宿”，其包括的第一关键字段为“发票”，因此确定该局部事务的父类型为第一类型，且根据包括的第二关键字段为“报销”确定子类型为发票报销类型。又例如，局部事务为“换资源，100 个第一资源换 10 个第二资源”，其包括的第一关键字段为“资源”，因此确定该局部事务的父类型为第一类型，且根据包括的第二关键字段为“换资源”确定子类型为资源互换类型。

(2) 在发现第一共识节点接收到局部事务之后，从局部事务的内容中获取子类型标识，根据子类型标识确定局部事务的子类型。

例如，局部事务的内容包括“电子发票报销 0001，数额 500、且用于外出住宿；【发票报销类型】”，根据类型标识为“【发票报销类型】”确定子类型为发票报销类型。

在确定子类型之后，在步骤 620 中，根据子类型确定优先级的方式包括：采取查找子类型与优先级对照表的方式，确定优先级。

子类型与优先级对照表列出了子类型与优先级的对应关系，如下是一个子类型与优先级对照表的例子：

表 3

子类型	优先级
发票报销类型	10
发票查询类型	9
发票开票类型	8
资源互换类型	7
资源转移类型	6
资源统计类型	5

如表 3 所示，对于子类型为发票报销类型来说，发票报销的事务对于紧急上链的需求较高，所以设置优先级为 10。同理，依据各个子类型对紧急上链的需求程度不同，分别设置了发票查询类型的优先级为 9、发票开票类型的优先级为 8、资源互换类型的优先级为 7、资源转移类型的优先级为 6、和资源统计类型的优先级为 5。

例如，局部事务的内容包括“电子发票报销 0001，数额 500、且用于外出住宿”，确定子类型为发票报销类型，则优先级为 10。又例如，局部事务为“100 个第一资源互换 10 个第二资源”，确定子类型为资源互换类型，则优先级为 7。

在确定优先级之后，在步骤 630 中，第一中继节点将局部事务按照优先级从高到低的顺序，放置在队列中排队。

参照图 7，图 7 中示出了在放置局部事务 5 之前的队列 L 以及放置了局部事务 5 之后的队列 L。在局部事务 5 未放置入队列 L 之前，该队列 L 已经存放有局部事务 1-4，且局部事务 1-4 的优先级依次为 9、8、7 和 6。在需要将局部事务放置入队列 L 时，先确定局部事务的优先级为 10，根据优先级从高到低的顺序，确定要将局部事务 5 放置入队列 L 的目标位置，也就是图 7 左边所示队列 L 的虚线框处。将目标位置上的局部事务 1 以及排在目标位置后面的局部事务 2-4 向后移动，然后将局部事务 5 放置在队列的目标位置处，放置后的结果如图 7 右边所示的队列 L。

在步骤 640 中，从队列中顺序取出局部事务，发送到第二共识节点。

步骤 640 从队列中取出局部事务的方式包括：

(1) 参照图 7，确定队列中的局部事务的数目达到第四阈值，则从队列中顺序取出局部事务进行打包，发送到第一全局共识网络中的第二共识节点；及，

(2) 确定当前时间与上一个打包的时间的时间差达到第五阈值，则从队列中顺序取出局部事务进行打包，发送到第一全局共识网络中的第二共识节点。

通过步骤 610-640，实现了根据优先级满足目标事务的紧急上链需求，提高了上链灵活性。

以上是对步骤 330a 的第二种分解方式的详细描述，接下来描述第三种分解方式。

在上述第一种分解方式将步骤 330a 展开为步骤 410-420 时，或上述第二种分解方式将步骤 330a 展开为步骤 610-640 时，第一中继节点仅将局部事务发送至第二共识节点。也就是说，第二共识节点无法确定接收到的局部事务是否是由第一中继节点产生的真实事务，安全性较低。因此，在一些实施例中，步骤 330a 结合第一中继节点的签名验证，使得步骤 330b 中的第二共识节点能够确保局部事务是由第一中继节点发送的真实事务，提高安全性。

在该实施例的具体实现时，参照图 8，步骤 330a（由第一中继节点执行）包括：

步骤 810、根据预定摘要算法，对局部事务生成第三摘要；

步骤 811、利用第一中继节点的私钥对第三摘要加密，得到第二签名；及，

步骤 812、将局部事务和第二签名发送到第二共识节点。

对应的，步骤 330b（由第二共识节点执行）包括：

步骤 820、利用第一中继节点的公钥，解密第二签名，得到第四摘要；

步骤 821、根据预定摘要算法，对局部事务生成第三摘要；及，

步骤 822、当第三摘要与第四摘要一致，则执行局部事务，将局部事务记录到第二区块链。

下面对步骤 810-812、步骤 820-822 进行详细描述。

在步骤 810-812 中，签名的过程包括，用摘要算法（例如哈希算法）对待签名主体求摘要，然后用签名者的私钥（或公钥）对摘要加密。签名算法的不同可以体现在采用不同的摘要算法等。所以，在第一中继节点生成第二签名时，用预定摘要算法对局部事务求第三摘要，并用第一中继节点的私钥对第三摘要进行加密。

在步骤 820-822 中，验证签名的过程包括，验签者利用签名者的公钥（或私钥）对签名进行解密，然后用与签名过程相同的摘要算法对待验签主体生成摘要，如果解密后的摘要和生成的摘要相同，则验签成功。所以，在第二共识节点进行验签时，利用第一中继节点的公钥对第二签名进行解密，得到第三摘要，再用同样的预定摘要算法对局部事务生成第四摘要，且将第三摘要与第四摘要进行对比。如果第三摘要与第四摘要一致，则对第二签名的验签成功。

上述是对步骤 330a 的三种分解方式的总体描述，而在上述分解方式中，均是以全局共识网络包括一个第二区块链为基础（如图 1C 所示），由第一中继节点将各个第一类型的局部事务发送到同一个第一全局共识网络。但在另一实施例中，第一全局共识网络选自多个候选全局共识网络（如图 10 所示的多个候选全局共识网络），且每个候选全局共识网络分别对应于不同局部事务的子类型。例如，处理子类型为发票类型的专门有一个第一全局共识网络，处理子类型为订单类型的专门有一个第一全局共识网络，有助于提高事务上链效率。

在该实施例的具体实现时，参照图 9，步骤 330a（由第一中继节点执行）具体包括：

- 步骤 910、确定第一类型的局部事务的子类型；
- 步骤 920、确定与子类型对应的候选全局共识网络，作为第一全局共识网络；及，
- 步骤 930、将局部事务发送到第一全局共识网络中的第二共识节点。

下面对步骤 910-930 进行详细描述。

在步骤 910 中，子类型的定义、以及确定子类型的方式已在上述的步骤 610 中描述。

在步骤 920 中，如图 10 所示，全局共识网络中包括多个候选全局共识网络（图 10 仅示出 4 个候选全局共识网络，但也可以小于 4 个也还可以大于 4 个）。每个候选全局共识网络对应一个子类型。

事先根据子类型的目标智能合约需求，制定子类型与第一全局共识网络的对照表，例如下表所示：

表 4

子类型	第一全局共识网络
发票报销类型	候选全局共识网络 1
发票开票类型	候选全局共识网络 2
资源互换类型	候选全局共识网络 3
资源统计类型	候选全局共识网络 4

如表 4 所示，局部事务的子类型具体可以为发票报销类型、发票开票类型、资源互换类型和资源统计类型。对于发票报销类型来说，需要关于报销的目标智能合约，所以选择候选全局共识网络 1 作为第一全局共识网络，由候选全局共识网络 1 统一调用关于报销的目标智能合约执行发票报销类型的局部事务。对于发票开票类型的事务来说，则是需要关于开票的目标智能合约，所以选择候选全局共识网络 2 作为第一全局共识网络，由候选全局共识网络 2 统一调用关于开票的目标智能合约执行发票开票类型的局部事务。同理，对于资源互换类型来说，由候选全局共识网络 3 统一调用关于互换的目标智能合约执行该子类型为资源互换类型的局部事务。同理，对于资源统计类型来说，由候选全局共识网络 4 统一调用关于统计的目标智能合约执行该子类型为资源统计类型的局部事务。

上述对照表制定好后，就可以根据子类型，查找上述对照表，确定第一全局共识网络。

在确定第一全局共识网络之后，在步骤 930 中，第一中继节点将局部事务发送到第一全局共识网络中的第二共识节点。

以子类型为发票报销类型为例，则第一全局共识网络为候选全局共识网络 1。第一中继节点将局部事务发送到候选全局共识网络 1 中的第二共识节点，由第二共识节点调用关于报销的目标智能合约执行该局部事务，并将局部事务记录到候选第二区块链 1 中的第二区块链。

对于由第二共识节点执行局部事务以及记录到第二区块链的具体过程，可参照上述实施例中由第一共识节点执行第二类型的局部事务以及记录到第一区块链的描述。但有所区别的是，第一区块链能被第一共识节点以外的节点访问，而第二区块链被禁止由第二共识节点以外的节点访问。

步骤 910-930 的实施例，通过子类型与第一全局共识网络的对照关系，有效地将同一子类型的局部事务发送到相同的候选全局共识网络上，使得候选第二区块链能够统一调用相同类型的目标智能合约执行局部事务，提高了第一全局共识网络处理局部事务的处理效率。

以上是对步骤 330a 的详细描述。

步骤 330c-330d 的详细描述

在步骤 330c 中，（第二共识节点）将局部事务的第一上链验证信息发送到第二全局共识网络中的第三共识节点。在步骤 330d 中，第三共识节点根据第一上链验证信息对局部事务的上链进行验证。

第二共识节点所处的执行环节分为两种情形。一种情形是第二共识节点具有可信执行环境，另一种情形是第二共识节点不具有可信执行环境。

在描述第二共识节点具有可信执行环境之前，先对可信执行环境的相关内容解释。

可信执行环境（Trusted Execution Environment，TEE）：是一种基于硬件的安全计算方案。通过软硬件方法在 CPU 中构建了一个安全区域，保证其内部加载的程序和数据在机密性与完整性上得到保护。TEE 将系统的硬件资源与软件资源划分成两个执行环境——可信部分与不可信部分（普通部分）。这两个环境是隔离的，不可信部分无法访问可信部分的存储、内存。

可信执行环境方案包括：Intel SGX 方案、arm trustzone 方案和 amd sev 方案。其中，Intel SGX 方案是指 Intel 提出的可信执行环境方案，可以在 Intel 生产的特定型号的 CPU 上支持可信执行环境。本文如提及可信执行环境，如无特别说明，均指基于 Intel SGX 方案的可信执行环境。

可信执行环境硬件密钥：Intel 在生产 CPU 时，烧制在 CPU 中的硬件密钥。其私钥在任何情况下都无法导出，其公钥在特定使用场景下可以导出，但 Intel 并不推荐此种做法。

基于上述可信执行环境的内容，该实施例中，在第二共识节点具有可信执行环境的情形下，第二区块链用可信执行环境的密钥加密，第一上链验证信息是第二共识节点响应于第二中继节点发送的第一上链验证信息请求，而向第二中继节点发送的，第一上链验证信息请求，是第二中继节点响应于在第二区块链上增加加密区块发送的，加密区块采用可信执行环境的密钥加密，第一上链验证信息用于指示第二中继节点将第一上链验证信息转发到第三共识节点。

本实施例中，通过可信执行环境的密钥对区块加密，并通过第二中继节点实现第一上链验证信息转发的方式，进一步提高了第一全局共识网络的目标事务上链的安全性。

以上是对第二共识节点具有可信执行环境的描述，接下来是对第二共识节点不具有可信执行环境的详细描述。

在一些实施例中，如图 12A 所示，第一上链验证信息包括局部事务的摘要值、和根据第一树中第一路径确定出的第一旁路节点记录的摘要值，第一树中叶子节点记录第二区块链上所记录事务的摘要值，第一路径，是第一树中一个叶子节点到第一树中根节点的路径，且第一树中一个叶子节点记录局部事务的摘要值，第一旁路节点是第一路径中除根节点之外节点在第一树中的兄弟节点，第一上链验证信息还用于指示第三共识节点根据局部事务的摘要值和第一旁路节点中记录的摘要值确定第一比较摘要值，当第一树中根节点记录的摘要值和第一比较摘要值一致，则验证成功。

第一树是由第二共识节点生成的，参照图 11，步骤 330c（由第二共识节点执行）包括：

步骤 1110、生成第一树；

步骤 1111、确定第一路径的第一旁路节点；及，

步骤 1112、将局部事务的摘要值和第一旁路节点中记录的摘要值发送到第三共识节点。

对应的，步骤 330d（由第三共识节点执行）包括：

步骤 1120、根据局部事务的摘要值和第一旁路节点中记录的摘要值，确定第一比较摘要值；及，

步骤 1121、当第一树中根节点记录的摘要值与第一比较摘要值一致，则验证成功。

下面对步骤 1110-1112、步骤 1120-1121 进行详细描述。

在步骤 1110 中，第一树中叶子节点是第二区块链上记录的事务的摘要值，记录的事务包含局部事务。第一树中叶子节点的顺序可以是第二共识节点接收到局部事务的顺序。例如，第二共识节点首先接收到局部事务 1 “员工 A 在企业 B 报销 1000 个资源”，接着接收到局部事务 2 “员工 C 在企业 D 报销 500 个资源”，则将局部事务 1 作为第一个叶子节点，将局部事务 2 作为第二个叶子节点”。得到摘要值所采用的摘要算法可以是以下中的一种：

（1）第二共识节点预先指定的对每个局部事务所属的实体都采用相同的摘要算法。例如，对于企业 B 的电子发票报销事务和企业 D 的电子发票报销事务都采用相同的摘要算法；及，

（2）第二共识节点预先为每个局部事务所属的实体指定的不同的摘要算法。例如，预先为企业 B 和企业 D 指定不同的摘要算法。当判定局部事务属于企业 B 时，采用预先为企业 B 指定的摘要算法，当判定局部事务属于企业 D 时，采用预先为企业 D 指定的摘要算法。该实施例由于为不同的实体采用不同的摘要算法，增大了从摘要值破解局部事务的难度，提高局部事务上链安全性。

第三共识节点在根据局部事务的摘要值和第一旁路节点记录的摘要值进行验证时，采用的摘要算法与上述摘要算法一致。

该实施例中，第一树中叶子节点所在的层与根节点所在层之间存在至少一个中间层，中间层包括至少一个中间节点，第一树中相邻的两层中，上一层的节点由下一层的至少两个节点生成，且下一层中同一节点仅用于生成上一层中的一个节点。其中，节点包括根节点、中间节点、叶子节点。

本申请实施例的第一树通常是一种二叉树，也可以是多叉树。第一树拥有树结构的所有特点，树结构常常包含多个节点（图 12B 所示的节点），多个节点中至少包括至少一个叶子节点、一个根节点，通常情况下还包含叶子节点和根节点之间的多个中间节点。

参照图 12B 所示的第一树，第一树的叶子节点记录事务的是摘要值。第一树中相邻的两层中，上一层的节点由下一层的至少两个节点生成，且下一层中同一节点仅用于生成上一层中的一个节点。如图 12B 所示，第一层的叶子节点 1 和叶子节点 2 串联后通过摘要算法生成第二层的中间节点 7 中的摘要值，叶子节点 3 和叶子节点 4 串联后通过摘要算法生成中间节点 8 中的摘要值，叶子节点 5 和叶子节点 6 串联后通过摘要算法生成中间节点 9 中的摘要值，中间节点 7 和中间节点 8 串联后通过摘要算法生成第三层的中间节点 11 中的摘要值，中间节点 9 和中间节点 10 串联后通过摘要算法生成第三层的中间节点 12 中的摘要值，中间节点 11 和中间节点 12 串联后通过摘要算法生成第一树中的根节点中的摘要值。

在步骤 1111 中，第一路径为第一树中局部事务的摘要值对应的叶子节点到第一树中根节点之间的路径。第一旁路节点是第一路径中除根节点之外的节点在第一树中的兄弟节点。

如图 12C 所示，假定局部事务的摘要值记录于叶子节点 4，则第一路径为第一树中叶子节点 4 到第一树中根节点之间的路径，其中，该第一路径包括叶子节点 4、中间节点 8、中间节点 11 以及第一树中根节点。由于中间节点 8 需要基于叶子节点 3 和叶子节点 4 生成，在已知叶子节点 4 的情况下，还需要获取叶子节点 3，因此，将叶子节点 3 确定为第一旁路节点。同样地，由于中间节点 11 需要基于中间节点 7 和中

间节点 8 生成, 在根据叶子节点 3 和叶子节点 4 生成中间节点 8 之后, 还需要获取中间节点 7, 因此, 将中间节点 7 确定为第一旁路节点。同样地, 由于中间节点 13 需要基于中间节点 11 和中间节点 12 生成, 在根据中间节点 8 和中间节点 7 生成中间节点 11 之后, 还需要获取中间节点 12, 因此, 将中间节点 12 确定为第一旁路节点。因此, 第一旁路节点包括叶子节点 3、中间节点 7 以及中间节点 12, 第一旁路节点在图 12C 中以黑色粗实线框表示。第一树中除第一旁路节点和局部事务对应的叶子节点以外的其他节点不会提供给第三共识节点。这样做的好处是, 在第三共识节点进行验证时, 从局部事务的摘要值对应的叶子节点逐层向上生成根节点的相关信息已提供给第三共识节点, 保证第三共识节点能够进行正确的验证。同时, 与验证无关的信息尽量避免提供给第三共识节点, 减少其它事务的信息泄露。同时, 即使是第一旁路节点, 一般也只会以摘要值等形式提供, 减少相关事务的真实信息泄露。

在步骤 1111 确定第一旁路节点之后, 在步骤 1112 中, 第二共识节点将局部事务的摘要值和第一旁路节点中记录的摘要值发送到第三共识节点。

接着, 第三共识节点在接收到局部事务的摘要值和第一旁路节点中记录的摘要值之后, 在步骤 1120 中, 第三共识节点利用第一旁路节点中记录的摘要值以及局部事务的摘要值, 确定第一比较摘要值。

确定第一比较摘要值的过程包括: 可以确定局部事务的摘要值, 再根据第一旁路节点记录的摘要值和局部事务的摘要值, 层层推测第一路径中各个节点记录的摘要值 (如图 12C 曲线圈出的部分), 对第一路径中的根节点推测出的摘要值则为第一比较摘要值。

如图 12C 所示, 在利用第一旁路节点记录的摘要值和局部事务的摘要值, 确定第一比较摘要值时, 假定局部事务的摘要值记录于叶子节点 4, 第一旁路节点包括叶子节点 3、中间节点 7 以及中间节点 12。此时, 根据叶子节点 4 记录的摘要值和叶子节点 3 记录的摘要值推测中间节点 8 记录的摘要值。根据推测出的中间节点 8 的摘要值和中间节点 7 的摘要值推测中间节点 11 的摘要值。根据推测出的中间节点 11 的摘要值和中间节点 12 的摘要值推测根节点的摘要值。

在步骤 1120 得到第一比较摘要值之后, 第三共识节点将第一树的根节点中记录的摘要值与第一比较摘要值进行比较。在步骤 1121 中, 如果第一树的根节点中记录的摘要值与第一比较摘要值一致, 则验证成功。

通过上述步骤 1110-1112 和步骤 1120-1121, 本申请实施例, 确保第三共识节点能够对局部事务进行准确的验证, 能够验证事务是否已真实上链。并且由于仅向三共识节点分享局部事务的摘要值和第一旁路节点中记录的摘要值, 从而减少了对相关事务的真实信息的泄露, 提高了安全性。

在另一些实施例中, 除了对事务是否真实记录进行验证, 还可以对局部事务被执行之后产生的关联数据进行验证。关联数据是指事务被执行后可能会影响到的参数, 例如资源总额或物品数额。例如, 局部事务为“电子发票报销 0001, 数额 500、且用于外出住宿”。该事务执行并上链后, 会对企业资源总额产生影响。假设企业原资源总额为 500000, 报销该电子发票后, 资源总额变成 499500。该资源总额为发票报销产生的关联数据。再例如, 局部事务是“赠送企业 A 600 张电影票”, 该事务执行后会对电影院剩下的电影票数产生影响。假设电影院原有电影票 5000 张, 则该事务执行并上链后, 电影院的电影票数变成 4400 张。该电影票数是赠票事务产生的关联数据。为了对局部事务执行后的关联数据进行验证, 在另一实施例中, 第一上链验证信息除了包括局部事务的摘要值、和第一旁路节点记录的摘要值 (如图 12A 所示), 该第一上链验证信息还包括局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值 (如图 14A 所示)。

在一些实施例中, 第一上链验证信息还包括局部事务执行后所获得关联数据的摘要值和第二树中第二旁路节点记录的摘要值, 第二树中叶子节点记录第二区块链上所记录事务执行后所获得关联数据的摘要值, 第二路径, 是第二树中一个叶子节点到第二树中根节点的路径, 第二树中一个叶子节点记录局部事务执行后所获得关联数据的摘要值, 第二旁路节点是第二路径上除根节点之外节点在第二树中的兄弟节点, 第一上链验证信息还用于指示第三共识节点在第一树中根节点记录的摘要值和第一比较摘要值一致的情况下, 根据局部事务执行后所获得关联数据的摘要值和第二旁路节点中记录的摘要值, 确定第二比较摘要值, 当第二树中根节点记录的摘要值与第二比较摘要值一致, 则验证成功。

第二树是第二共识节点生成的, 在该实施例下, 参照图 13, 步骤 330c (由第二共识节点执行) 还包括:

步骤 1310、生成第二树;

步骤 1311、确定第二路径的第二旁路节点; 及,

步骤 1312、将局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值发送到第三共识节点。

对应的, 步骤 330d 中的步骤 1121 (由第三共识节点执行) 还包括:

步骤 1320、当第一树中根节点记录的摘要值与第一比较摘要值一致, 根据局部事务执行后的关联数据的摘要值和第二旁路节点记录的摘要值, 确定第二比较摘要值; 及,

步骤 1321、当第二树中根节点记录的摘要值与第二比较摘要值一致, 则验证成功。

下面对步骤 1310-1312、步骤 1320-1321 进行详细描述。

在步骤 1310 中, 第二树的叶子节点记录的是第二区块链上记录的事务执行后的关联数据的摘要值, 记录的事务包含局部事务。第二树的叶子节点的顺序可以是预先指定的关联数据顺序。例如, 将企业 A、B、C、D……的顺序作为第二树的叶子节点的顺序。当第二共识节点接收到局部事务 1“员工 X 在企业 B 报销 1000 个资源”, 该事务引起企业 B 的总资源数目的变化, 使企业 B 的总资源变化为 49000 个, 因此, 更改第二树中的叶子节点 2 中的摘要值, 使其为 49000 的摘要值。当第二共识节点接收到局部事务 2“员

工 Y 在企业 D 报销 500 个资源”，该事务引起企业 D 的总资源数目的变化，使企业 D 的总资源变化为 24500 个，因此，更改第二树中的叶子节点 4 的摘要值，使其为 24500 的摘要值。局部事务所属的实体可以对应各自的摘要算法，局部事务的摘要值可以是所属的实体对应的摘要算法生成的。不同的实体对应的摘要算法可以相同也可以不同。摘要算法可以是第二共识节点预先指定的。

在步骤 1311 中，第二路径为第二树中局部事务执行后的关联数据的摘要值对应的叶子节点到第二树中根节点之间的路径，第二旁路节点是第二路径中除根节点之外的节点在第二树中的兄弟节点。

如图 14C 所示，假定局部事务执行后的关联数据的摘要值记录于叶子节点 4，则第二路径为第二树中叶子节点 4 到第二树中根节点之间的路径，其中，该第二路径还包括叶子节点 4、中间节点 8、中间节点 11 以及第二树中根节点。第二路径的第二旁路节点包括叶子节点 3、中间节点 7 以及中间节点 12，第二旁路节点在图 14C 中以黑色粗实线框表示。第二树中除第二旁路节点记录的摘要值和局部事务执行后的关联数据的摘要值以外的其他摘要值，不会提供给第三共识节点。

在步骤 1311 确定第二旁路节点之后，在步骤 1312 中，第二共识节点将待局部事务执行后的关联数据的摘要值和第二旁路节点中记录的摘要值发送到第三共识节点。

接着，第三共识节点在接收到局部事务执行后的关联数据的摘要值和第二旁路节点中记录的摘要值之后，在步骤 1320 中，当第一树中根节点记录的摘要值与第一比较摘要值一致，根据局部事务执行后的关联数据的摘要值和第二旁路节点记录的摘要值，确定第二比较摘要值。

确定第二比较摘要值的过程包括：根据第二旁路节点记录的摘要值和事务执行后的关联数据的摘要值，推测第二路径中各个节点记录的摘要值（如图 14C 曲线圈出的部分），对第二路径中的根节点推测出的摘要值则为第二比较摘要值。

在步骤 1320 得到第二比较摘要值之后，第三共识节点将第二树中根节点记录的摘要值与第二比较摘要值进行比较。在步骤 1321 中，当第二树中根节点记录的摘要值与第二比较摘要值一致，则验证成功。

通过上述步骤 1310-1312 和步骤 1320-1321，本申请实施例，不仅能够通过局部事务本身验证局部事务是否已真实上链，还能够通过产生的关联数据验证局部事务是否已真实上链，双重验证进一步提高了验证准确率。

在一些实施例中，第一上链验证信息还包括第二旁路节点的第一签名，第一签名，是第二共识节点用第二共识节点的第一私钥对第一摘要进行加密得到的，第一摘要，是第二共识节点根据局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后所获得关联数据的摘要值以及第二旁路节点记录的摘要值生成的，第一签名用于指示第三共识节点在第二树中根节点与第二待比较根节点一致的情况下，用第二共识节点的第一公钥解密第一签名，得到第二摘要，根据局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后所获得关联数据的摘要值以及第二旁路节点记录的摘要值生成第三摘要，当第三摘要与第二摘要一致，则验证成功。

参照图 15，图 15 中示出的第一上链验证信息除了包括局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、第二旁路节点记录的摘要值，还包括了第一签名。

该第一签名由第二共识节点对局部事务的摘要值、第一旁路记录的摘要值、局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值进行签名得到，第二共识节点生成第一签名的方式如下：

将局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、第二旁路节点记录的摘要值进行串联，得到串联数据；

根据预定摘要算法对串联数据进行处理生成第一摘要；及，

用第二共识节点的第一私钥对第一摘要进行加密，得到第一签名。

则在第一上链验证信息还包括第一签名的情况下，步骤 1321 包括：

当第二树中根节点记录的摘要值与第二比较摘要值一致，用第二共识节点的第一公钥解密第一签名，得到第二摘要；

根据预定摘要算法对串联数据进行处理生成第三摘要；及，

如果第三摘要与第二摘要一致，则验证成功。

局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值的串联顺序可以是以下中的一种：

(1) 预先指定的顺序，例如预定指定局部事务的摘要值-第一旁路节点记录的摘要值-局部事务执行后的关联数据的摘要值-第二旁路节点记录的摘要值的顺序；及，

(2) 按照局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值的首字符字典顺序。例如，局部事务的摘要值的首字符为 t，第一旁路节点记录的摘要值的首字符为 m，局部事务执行后的关联数据的摘要值的首字符为 a，第二旁路节点记录的摘要值的首字符为 c，则按照局部事务执行后的关联数据的摘要值-第二旁路节点记录的摘要值-第一旁路节点记录的摘要值-局部事务的摘要值的属性串联。该实施例有助于提高验证复杂度，提高第一类型的局部事务的上链安全性。

上述步骤 1310-1312 和步骤 1320-1321，通过第二共识节点的第一签名和第三共识节点对第一签名的验证，确保串联的待上链局部事务的摘要值、第一旁路节点记录的摘要值、待上链局部事务执行后的关联数据的摘要值、和第二旁路节点记录的摘要值是第二共识节点真实发出的，进一步提高了第一类型的局部事务的上链安全性。

以上是对步骤 330c-330d 的详细描述。

步骤 340 的详细描述

在步骤 340 中，第一中继节点从第三共识节点获取局部事务的上链验证结果。

在第一中继节点获取上链验证结果之前，上链验证结果是由第三共识节点根据第一上链验证信息对局部事务的上链进行验证之后得到的结果。参照图 16，第一上链验证信息包括局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、第二旁路节点记录的摘要值和事务脱敏信息。事务脱敏信息，是第二共识节点对局部事务进行脱敏处理得到的，脱敏处理是根据目标合约中的脱敏字段进行的，目标合约与局部事务的子类型相对应。

在第一上链验证信息包括事务脱敏信息的情况下，步骤 340 包括：从第三共识节点获取事务脱敏信息，作为上链验证结果。事务脱敏信息是指目标事务中能够向第三方透露的信息，如“XX 类型的事务已完成并上链”。

事务脱敏信息是第二共识节点生成的，第二共识节点生成事务脱敏信息的方法如下：

获取第一类型的局部事务的子类型；

获取子类型对应的目标合约；及，

根据目标合约中的脱敏字段，对局部事务进行脱敏处理，得到事务脱敏信息。

在该实施例中，获取子类型的方式与上述实施例中确定子类型的方式类似。

目标合约是执行某种子类型的第一类型事务的上链的合约。例如，发票子类型的第一类型事务对应于发票子类型的目标合约，用于执行发票子类型的第一类型事务的上链。订单子类型的第一类型事务对应于订单子类型的目标合约，用于执行订单子类型的第一类型事务的上链。一般来说，目标合约需要所有第二共识节点执行。

目标合约可以通过以下方式确定：根据子类型，查找子类型与候选目标合约的对照表，确定目标合约。

子类型可以是前述的发票类型、订单类型、资源互换类型和资源统计类型等。事先根据各子类型的合约要求，制定子类型与目标合约的对照表，例如：

表 5

子类型	目标合约
发票报销类型	报销目标合约
发票开票类型	开票目标合约
资源互换类型	互换目标合约
资源统计类型	统计目标合约

如表 5 所示，对于子类型为发票报销类型来说，可以设置统一的报销目标合约。对于子类型为发票开票类型来说，可以设置统一的开票目标合约。同理，对于资源互换类型，设置统一的互换目标合约，对于资源统计类型设置统一的统计目标合约。

上述对照表制定好后，就可以根据子类型，查找上述对照表，确定子类型对应的目标合约。

在确定目标合约之后，将根据目标合约中的脱敏字段，对局部事务进行脱敏处理，得到事务脱敏信息。脱敏字段是指承载可以向第三方透露的信息的字段。例如，电子发票报销的事务中，事务子类型和编号不含有不能向第三方透露的内容，可以向第三方透露。

例如，第一类型的局部事务为“电子发票 0001 报销，数额 500、且用于外出住宿”。则先获取该局部事务的子类型为发票报销类型（例如根据第二关键字段包括发票报销，则确定子类型为发票类型）。其次，根据子类型为发票报销类型查找上述对照表，得到目标合约为报销目标合约（该报销目标合约的脱敏字段包括数额和用途）。然后，根据报销目标合约中的脱敏字段，即事务子类型和编号，将“电子发票报销 0001，数额 500、且用于外出住宿”中的数额以及用途去除，只保留事务子类型和编号，得到的事务脱敏信息为“电子发票报销 0001 已成功报销”。

该实施例的好处是，通过目标合约中的脱敏字段的处理，提高了脱敏的准确性，从而提高目标事务上链安全性。

上述实施例中的第一上链验证信息包括事务脱敏信息，但在另一实施例中的第一上链验证信息不包括事务脱敏信息，而是包括即时性信息。

在一些实施例中，第一上链验证信息还包括局部事务的即时性信息，即时性信息是第二共识节点根据局部事务的子类型确定的；及，从第三共识节点获取局部事务的上链验证结果，包括：当即时性信息指示局部事务为即时事务，在第三共识节点验证成功后，接收第三共识节点返回的上链验证结果。

参照图 17，图 17 中示出的第一上链验证信息包括局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后的关联数据的摘要值、第二旁路节点记录的摘要值和即时性信息。则在第一上链验证信息包括即时性信息的情况下，步骤 340 包括：

当即时性信息指示局部事务为即时事务，在第三共识节点验证成功后，接收第三共识节点返回的上链验证结果。

在该实施例具体实现时，即时性信息通过以下方式生成：

获取第一类型的局部事务的子类型；及，

根据子类型，确定即时性信息。

在该实施例中，获取子类型的方式与上述实施例中确定子类型的方式类似。

子类型可以是前述的发票报销类型、发票开票类型、资源互换类型和资源统计类型等。事先根据各子

类型的即时性要求，制定子类型与即时性信息的对照表，例如：

表 6

子类型	即时性信息
发票报销类型	即时
发票开票类型	即时
资源互换类型	非即时
资源统计类型	非即时

如表 6 所示，对于子类型为发票报销类型或发票开票来说，对于即时性要求较高，可以设置即时性信息为即时（以便子类型为发票类型的局部事务的上链验证结果能够即时返回给第一中继节点）。对于资源互换类型或资源统计类型来说，对于即时性要求相比发票报销类型较低，所以设置即时性信息为非即时。

上述对照表制定好后，就可以根据子类型，查找上述对照表，确定子类型对应的即时性信息。

例如，第一类型的局部事务为“电子发票报销 0001，数额 500、且用于外出住宿”。则先获取该局部事务的子类型为发票报销类型。其次，根据子类型为发票类型查找上述对照表，得到即时性信息为即时，则说明“电子发票 0001 报销，数额 500、且用于外出住宿”为即时事务。然后，在第三共识节点验证成功后，第三共识节点立即向第一中继节点返回上链验证结果，以提高即时事务处理的即时性。

该实施例的好处是，对于即时的局部事务即时返回上链验证结果，保证了即时性事务的即时处理。

在一些实施例中，当即时性信息指示局部事务为非即时事务，向第三共识节点发送上链验证结果请求，并从第三共识节点对上链验证结果请求的应答中获取上链验证结果。

例如，第一类型的局部事务为“100 个第一资源互换 10 个第二资源”。则先获取该局部事务的子类型为资源互换类型。其次，根据子类型为资源互换类型查找上述对照表，得到即时性信息为非即时，则说明“100 个的第一资源互换 10 个第二资源”为非即时事务。这时，在第三共识节点验证成功后，第三共识节点就不需要那么急迫向第一中继节点返回上链验证结果，可以等待第一中继节点向第三共识节点发送上链验证结果请求，并响应于该请求作出应答。第一中继节点从第三共识节点对上链验证结果请求的应答中获取上链验证结果。

该实施例的好处是，对于非即时的局部事务等待第一中继节点请求，减少了对传输资源的占用。

在上述即时性信息指示局部事务为非即时事务时，第一中继节点向第三共识节点发送上链验证结果请求，以便从第三共识节点对上链验证结果请求的应答中获取上链验证结果。接下来对上链验证结果请求展开描述。

参照图 18，图 18 中示出的上链验证结果请求包括区块标识、源地址和目的地地址。源地址是指第一中继节点的地址，而目的地地址是指第三共识节点的地址。至于区块标识，则是用于指示上链验证结果所在的区块（该区块在第三共识节点维护的第三区块链上）。

区块标识由第三共识节点产生且由第三共识节点发送到第一中继节点。例如，步骤 330d 包括，第三共识节点根据第一上链验证信息对局部事务的上链进行验证，生成上链验证结果，第三共识节点将上链验证结果记录到第三区块链，并将记录到第三区块链的区块标识返回第一中继节点。

在该实施例具体实现时，在第三共识节点向第一中继节点发送区块标识之前，第三共识节点根据上链验证结果生成区块，并将区块记录到第三区块链。区块包括区块主体与区块头。区块主体被分为了多个分块，上链验证结果可以只占用其中的一个分块，也可以占用其中的几个分块，也可以占用其中的全部分块。在仅占用其中的一个或几个分块的情况下，其余的分块记录其它第三共识节点的局部事务的上链验证结果。即，第三共识节点将上链验证结果占用的分块和其它第三共识节点需要上链的上链验证结果对应的分块打包成区块体，加上区块头组成一个区块，记录到区块链上。区块头指示了这个区块的相关信息，包括：版本号、特征值、时间戳、与难度值等。区块标识是能够使区块区分于其它区块的标识，如区块的高度、区块的特征值等。区块的特征值一般是区块的区块体经摘要算法生成的摘要值。由于区块体不同，摘要值就不同，因此摘要值能够唯一区分区块。区块的高度是指区块是区块链上记录的第几个区块。区块的高度也能唯一区分区块和其它区块。在将区块记录到第三区块链之后，并将记录到第三区块链的区块标识返回第一中继节点。

在第一中继节点接收到区块标识之后，在一些实施例中，步骤 340 包括：向第三共识节点发送上链验证结果请求，上链验证结果请求中具有区块标识，以便第三共识节点根据区块标识从第三区块链中获取上链验证结果，接收第三共识节点返回的上链验证结果。这样做的好处是，第三共识节点将上链验证结果记录到第三区块链上，便于其它节点检查，上链验证结果不易被篡改，提高上链验证结果的安全性。

确定发送上链验证结果请求的方式包括但不限于以下三种情形：

（1）在第一中继节点接收到区块标识之后，第一中继节点立即向第三共识节点发送上链验证结果请求。

（2）第一中继节点预先设置第二发送周期，在接收到区块标识之后且过去该第二发送周期，第一中继节点向第三共识节点发送上链验证结果请求。

（3）在第一中继节点接收到区块标识之后，由第一中继节点向局部共识网络发送提示消息“是否获取第一上链验证结果”，在接收到第一共识节点返回的“是”这一指示信息时，响应于第一共识节点返回的指示信息，第一中继节点向第三共识节点发送上链验证结果请求。

考虑到归纳出的全局事务的上链需求

上述实施例中的事务上链方法，仅是针对局部事务的上链需求，根据局部事务的父类型将局部事务执行并记录到相应的区块链上。例如由第二共识节点将第一类型的局部事务记录到第二区块链上，且该第二区块链被禁止由第二共识节点以外的节点访问。又例如由第一共识节点将第二类型的局部事务记录到第一区块链上，该第一区块链能够被处第一共识节点以外的节点访问。也就是说，第二类型的局部事务均是记录在局部共识网络中的第一共识节点上。但在区块链分层共识体系中，各个局部共识网络所记录的局部事务需要汇总至全局共识网络中，对于第二类型的局部事务将会汇聚形成的归纳出的全局事务，将由全局共识网络中的第二全局共识网络记录到第三区块链上。因此，在一个实施例中，在响应于确定出局部事务的父类型为第二类型，由第一共识节点执行局部事务，并将局部事务记录到第一区块链之后，还需要进一步针对局部事务生成的归纳出的全局事务进行记录到第三区块链。

如图 19 所示，在步骤 320 之后，根据本申请一个实施例的事务上链方法可以还包括：

步骤 1910、获取从多个第二类型的局部事务归纳出的全局事务；及，

步骤 1920、将该全局事务发送到第三共识节点，该全局事务用于指示第三共识节点执行该全局事务，将该全局事务记录到第三区块链。

下面对步骤 1910-1920 进行详细描述。

在步骤 1910 中，可以从一个局部共识网络中的多个局部事务中归纳出全局事务，也可以从多个局部共识网络中的局部事务归纳出全局事务。

归纳得到全局事务的方式包括：

(1) 在第一共识节点接收到满足预定数量的局部事务之后，根据预定数量的局部事务生成全局事务。

(2) 在第一共识节点当前时间与上一次发送归纳出的全局事务的时间差超过阈值时，根据已接收到的局部事务生成新的全局事务。

(3) 在第一共识节点接收到满足预定数量的局部事务之后，根据预定数量的局部事务生成全局事务。若未满足预定数量，但在第一共识节点当前时间与上一次发送归纳出的全局事务的时间差超过阈值时，根据已接收到的局部事务生成全局事务。

例如，假定存在 3 个第二类型的局部事务，分别为“订单 10001：购买办公用品 50 件”、“订单 10002：购买办公用品 150 件”、和“订单 10003：购买办公用品 200 件”。根据这 3 个局部事务，归纳出的全局事务可为“订单的总数为 3”，也可以为“订单购买总额为办公用品 400 件”等。

继续参照图 19，步骤 1920 具体可以分为 1920a 将归纳出的全局事务发送到第三共识节点，以及 1920b（由第三共识节点执行）执行归纳出的全局事务，将归纳出的全局事务记录到第三区块链。

在步骤 1920a 中，第一共识节点发送归纳出的全局事务的方式包括：

(1) 在第一共识节点获取局部事务之后，立即向第三共识节点发送归纳出的全局事务。

(2) 第一共识节点预先设置第三发送周期，在第一共识节点获取局部事务之后且过去该第三发送周期，第一共识节点向第三共识节点发送归纳出的全局事务。

在步骤 1920b 中，第三共识节点执行归纳出的全局事务，且将归纳出的全局事务记录到第三区块链上。第三区块链记录归纳出的全局事务，且能被第三共识节点以外的节点访问。

对于第三共识节点执行并记录到第三区块链的具体过程，可参照上述实施例中第一共识节点执行并记录到第一区块链的描述。

上述实施例的好处是，基于分层共识系统架构（如图 10），可以保障各局部共识网络相对独立地运行局部事务，便于层级化地业务治理。也不需要把整个见证网络中业务联盟的流量全部汇集到全局共识网络。在起到数据隔离，业务安全隔离，合法合规的前提下，通过步骤 1910-1920 能够保障第二全局共识网络不需要承载大量的细分业务，可以专注于关键任务和全局事务的治理。

另外，上述实施例中，在由第三共识节点将归纳出的全局事务记录到第三区块链之后，第一中继节点可从第三共识节点获取第二上链验证信息且发送到第一共识节点，以便由第一共识节点对第二上链验证信息进行验证，确保归纳出的全局事务已被真实执行并真实上链。

如图 20 所示，在步骤 1920 之后，根据本申请一个实施例的事务上链方法可以还包括：

步骤 2010、在第三共识节点将全局事务记录到第三区块链，以生成第二上链验证信息的情况下，从第三共识节点接收第二上链验证信息；及，

步骤 2020、将第二上链验证信息发送到第一共识节点，第二上链验证信息用于指示第一共识节点对归纳出的全局事务的上链进行验证。

例如，假定该第二上链验证信息包括归纳出的全局事务的摘要值和第三旁路节点记录的摘要值。该第三旁路节点由第三共识节点通过以下方式获取：

生成第三树，其中，第三树的叶子节点记录的是第三区块链上记录的事务的摘要值，记录的事务包含归纳出的全局事务，第三树中相邻的两层中，上一层的节点由下一层的至少两个节点生成，且下一层中同一节点仅用于生成上一层中的一个节点。

确定第三路径的第三旁路节点，其中，第三路径为第三树上归纳出的全局事务的摘要值对应的叶子节点到第三树中根节点之间的路径，第三旁路节点是第三路径中除根节点之外节点在第三树中的兄弟节点。

则对应的，步骤 2020 包括：

根据归纳出的全局事务的摘要值和第三旁路记录的摘要值，确定第三比较摘要值；及，

如果第三比较摘要值与第三树中根节点中记录的摘要值一致，则验证成功。

根据第二上链验证信息验证的具体方法，参考根据第一上链验证信息进行验证的具体方法。

通过步骤 2010-2020, 本申请实施例, 确保第一共识节点能够对归纳出的全局事务进行准确的验证, 能够验证归纳出的全局事务是真实记录的, 没有作弊。

本申请实施例的事务上链方法的实施细节图

下面参照图 21, 详细示例性说明本申请实施例的事务上链方法的实施细节。

在步骤 310 中, 第一中继节点确定局部事务的父类型为第一类型, 或确定局部事务的父类型为第二类型。

在步骤 320 中, 响应于确定出局部事务的父类型为第二类型, 由第一共识节点执行局部事务, 并将局部事务记录到第一区块链。

在步骤 330 中, 分为步骤 330a-330d。在步骤 330a 中, 第一中继节点将局部事务放置在队列中排队 (步骤 410), 响应于队列满足预定条件, 将队列中的局部事务打包, 发送到第二共识节点 (步骤 420)。在步骤 330b 中: 由第二共识节点执行局部事务, 将局部事务记录到第二区块链。在步骤 330c 中: 步骤 1110 生成第一树; 步骤 1111 确定第一路径的第一旁路节点; 和步骤 1112 将局部事务的摘要值和第一旁路节点中记录的摘要值发送到第三共识节点。在步骤 330d 中, 根据局部事务的摘要值和第一旁路节点中记录的摘要值, 确定第一比较摘要值 (步骤 1120); 及, 当第一树中根节点记录的摘要值与第一比较摘要值一致, 则验证成功 (步骤 1121)。

在步骤 340 中, 从第三共识节点获取局部事务的上链验证结果。例如, 当第一树中根节点记录的摘要值与第一比较摘要值一致, 则上链验证结果为验证成功, 当第一树中根节点记录的摘要值与第一比较摘要值不一致, 则上链验证结果为验证失败。

除了局部事务需要上链之外, 还有归纳出的全局事务需要记录到第三区块链。因此, 继续参照图 21, 在步骤 1910 中, 获取针对局部事务生成的归纳出的全局事务; 在步骤 1920 中, 将归纳出的全局事务发送到第三共识节点 (1920a); 由第三共识节点执行归纳出的全局事务, 将归纳出的全局事务记录到第三区块链 (1920b)。接着, 在步骤 1920 之后, 步骤 2010 从第三共识节点接收归纳出的全局事务的第二上链验证信息; 步骤 2020a 将第二上链验证信息发送到第一共识节点; 及, 步骤 2020b (由第一共识节点执行) 对归纳出的全局事务的上链进行验证。

该实施例的优点包括但不限于: 能够区分局部事务是第一类型或是第二类型, 满足目标事务的上链安全性要求; 通过将多个局部事务一起打包发送, 能够减少网络开销; 通过将摘要值和旁路节点记录的摘要值作为第一上链验证信息, 能够验证局部事务的上链真实性且减少其他相关事务真实信息的泄露; 通过由第三共识节点对归纳出的全局事务的执行和记录到第三区块链, 能够使得第三共识节点更加集中的处理全局事务; 及, 通过第二上链验证信息, 能够验证归纳出的全局事务的上链真实性, 提高安全性。

上述实施例主要以第一中继节点作为核心处理模块展开描述, 下面以第二共识节点作为核心处理模块展开描述另一实施例的事务上链方法。

参照图 22, 由第二共识节点执行的事务上链方法, 包括:

步骤 2210、接收第一中继节点转发的局部事务, 局部事务的父类型为第一类型;

其中, 局部事务来源于局部共识网络。

步骤 2220、执行局部事务, 将局部事务记录到第二区块链; 其中, 第二区块链被禁止由第二共识节点以外的节点访问;

步骤 2230、获取局部事务的第一上链验证信息; 及,

步骤 2240、将第一上链验证信息发送到第二全局共识网络中的第三共识节点 (步骤 2240a), 第一上链验证信息用于指示第三共识节点根据第一上链验证信息对局部事务的上链进行验证, 得到上链验证结果 (步骤 2240b)。

本实施例中, 对于第一类型的局部事务, 将局部事务发送到第二共识节点, 以指示第二共识节点将局部事务记录到第二区块链。由于第二区块链不允许被第二共识节点之外的其它节点访问, 从而使得第一类型的局部事务的安全性得到了保证。同时, 第二共识节点完成局部事务的上链后, 把上链后的第一上链验证信息发送给第三共识节点, 由第三共识节点进行上链验证得到上链验证结果, 并从第三共识节点获取上链验证结果, 确保了虽然局部事务不可被外部查看, 但是它的上链是真实可信的, 从而提高了局部事务上链的安全性。

在一些实施例中, 第二共识节点具有可信执行环境, 第二区块链用可信执行环境的密钥加密; 将第一上链验证信息发送到第三共识节点包括: 接收第二中继节点发送的第一上链验证信息请求; 及, 响应于第一上链验证信息请求, 将第一上链验证信息发送到第二中继节点, 第一上链验证信息用于指示第二中继节点将第一上链验证信息转发到第三共识节点。

具体地, 第二中继节点响应于在第二区块链上增加用可信执行环境的密钥加密的区块, 向第二共识节点发送第一上链验证信息请求。第二共识节点响应于第二中继节点发送的第一上链验证信息请求, 将第一上链验证信息发送到第二中继节点, 第二中继节点将第一上链验证信息转发到第二全局共识网络中的第三共识节点。

在该实施例中, 第一全局共识网络上的第二区块链记录的局部事务是不能被第一中继节点看到的, 因此, 采用可信执行环境中的密钥加密。但是, 在第二区块链中增加一个区块, 是可以被发现的。因此, 第二中继节点可以识别出第二区块链是否有增加的用密钥加密的区块, 在发现第二区块链上存在增加的用密钥加密的区块之后, 向第二共识节点发送第一上链验证信息请求。而在第二共识节点接收到该第一上链验证信息请求之后, 不能直接将第一上链验证信息返回第一中继节点, 而是要返回第二中继节点, 由第二中继节点转发到第三共识节点, 从而由第三共识节点根据第一上链验证信息进行验证。

本申请实施例,通过可信执行环境的密钥对区块加密,并通过第二中继节点实现第一上链验证信息转发的方式,进一步提高了第一全局共识网络的目标事务上链的安全性。

本申请实施例的装置和设备描述

可以理解的是,虽然上述各个流程图中的各个步骤按照箭头的表征依次显示,但是这些步骤并不是必然按照箭头表征的顺序依次执行。除非本实施例中有明确的说明,这些步骤的执行并没有严格的顺序限制,这些步骤可以以其它的顺序执行。而且,上述流程图中的至少一部分步骤可以包括多个步骤或者多个阶段,这些步骤或者阶段并不必然是在同一时间执行完成,而是可以在不同的时间执行,这些步骤或者阶段的执行顺序也不必然是依次进行,而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

需要说明的是,在本申请的各个具体实施方式中,当涉及到需要根据目标对象属性信息或属性信息集合等与目标对象特性相关的数据进行相关处理时,都会先获得目标对象的许可或者同意,而且,对这些数据的收集、使用和处理等,都会遵守相关国家和地区的相关法律法规和标准。此外,当本申请实施例需要获取目标对象属性信息时,会通过弹窗或者跳转到确认页面等方式获得目标对象的单独许可或者单独同意,在明确获得目标对象的单独许可或者单独同意之后,再获取用于使本申请实施例能够正常运行的必要的目标对象相关数据。

图 23 为本申请实施例提供的事务上链装置 2300 的结构示意图。该事务上链装置 2300 包括:

第一确定单元 2310,用于在第一共识节点接收到的局部事务的情况下,确定局部事务的父类型。

第一发送单元 2330,用于在局部事务的父类型为第一类型的情况下,将局部事务发送到第二共识节点,局部事务用于指示第二共识节点执行局部事务,将局部事务记录到第二区块链,生成局部事务的第一上链验证信息,并将第一上链验证信息发送到第三共识节点,第一上链验证信息用于指示第三共识节点根据第一上链验证信息对局部事务的上链进行验证,得到局部事务的上链验证结果,其中,第二区块链禁止由第二共识节点以外的节点访问。

第一获取单元 2340,用于从第三共识节点获取局部事务的上链验证结果。

在一些实施例中,第一共识节点属于局部共识网络,第二共识节点属于全局共识网络中的第一全局共识网络,第三共识节点属于全局共识网络中的第二全局共识网络,第一中继节点,用于将第一类型的局部事务发送至第一全局共识网络中的第二共识节点。

在一些实施例中,事务上链装置 2300 还包括第一上链单元 2320,用于在父类型为第二类型的情况下,指示第一共识节点执行局部事务,并将局部事务记录到第一区块链,其中,第一区块链允许由第一共识节点以外的节点访问。

在一些实施例中,事务上链装置 2300 还包括:

第三获取单元,用于获取从多个第二类型的局部事务归纳出的全局事务;及,

第三发送单元,用于将全局事务发送到第三共识节点,全局事务用于指示第三共识节点执行全局事务,将全局事务记录到第三区块链,其中,第三区块链允许由第三共识节点以外的节点访问。

在一些实施例中,事务上链装置 2300 还包括:

第二接收单元,用于在第三共识节点将全局事务记录到第三区块链,以生成第二上链验证信息的情况下,从第三共识节点接收第二上链验证信息;及,

第三发送单元,用于将第二上链验证信息发送到第一共识节点,第二上链验证信息用于指示第一共识节点对全局事务的上链进行验证。

在一些实施例中,第一上链验证信息包括局部事务的摘要值、和根据第一树中第一路径确定出的第一旁路节点记录的摘要值,第一树中叶子节点记录第二区块链上所记录事务的摘要值,第一路径,是第一树中一个叶子节点到第一树中根节点的路径,且第一树中一个叶子节点记录局部事务的摘要值,第一旁路节点是第一路径中除根节点之外节点在第一树中的兄弟节点,第一上链验证信息还用于指示第三共识节点根据局部事务的摘要值和第一旁路节点中记录的摘要值确定第一比较摘要值,当第一树中根节点记录的摘要值和第一比较摘要值一致,则验证成功。

在一些实施例中,第一上链验证信息还包括局部事务执行后所获得关联数据的摘要值和第二树中第二旁路节点记录的摘要值,第二树中叶子节点记录第二区块链上所记录事务执行后所获得关联数据的摘要值,第二路径,是第二树中一个叶子节点到第二树中根节点的路径,第二树中一个叶子节点记录局部事务执行后所获得关联数据的摘要值,第二旁路节点是第二路径中除根节点之外节点在第二树中的兄弟节点,第一上链验证信息还用于指示第三共识节点在第一树中根节点记录的摘要值和第一比较摘要值一致的情况下,根据局部事务执行后所获得关联数据的摘要值和第二旁路节点记录的摘要值,确定第二比较摘要值,当第二树中根节点记录的摘要值与第二比较摘要值一致,则验证成功。

在一些实施例中,第一上链验证信息还包括事务脱敏信息,事务脱敏信息,是第二共识节点对局部事务进行脱敏处理得到的,脱敏处理是根据目标合约中的脱敏字段进行的,目标合约与局部事务的子类型相对应。

第一获取单元 2340 还具体用于:

从第三共识节点获取事务脱敏信息,作为上链验证结果。

在一些实施例中,第一上链验证信息还包括局部事务的即时性信息,即时性信息是第二共识节点根据局部事务的子类型确定的。

第一获取单元 2340 还具体用于:

当即时性信息指示局部事务为即时事务,在第三共识节点验证成功后,接收第三共识节点返回的上链

验证结果。

在一些实施例中，第一获取单元 2340 还用于：在即时性信息指示局部事务为非即时事务，向第三共识节点发送上链验证结果请求，并从第三共识节点对上链验证结果请求的应答中获取上链验证结果。

在一些实施例中，第一上链验证信息还包括第二旁路节点记录的摘要值的第一签名，第一签名，是第二共识节点用第二共识节点的第一私钥对第一摘要进行加密得到的，第一摘要，是第二共识节点根据局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后所获得关联数据的摘要值以及第二旁路节点记录的摘要值生成的，第一签名用于指示第三共识节点在第二树中根节点与第二待比较根节点一致的情况下，用第二共识节点的第一公钥解密第一签名，得到第二摘要，根据局部事务的摘要值、第一旁路节点记录的摘要值、局部事务执行后所获得关联数据的摘要值以及第二旁路节点记录的摘要值生成第三摘要，当第三摘要与第二摘要一致，则验证成功。

在一些实施例中，事务上链装置 2300 还用于：在第三共识节点将包括上链验证结果的区块记录到第三区块链后，接收第三共识节点返回的区块标识，区块标识是指包括上链验证结果的区块。

第一获取单元 2340 还用于：

向第三共识节点发送上链验证结果请求，上链验证结果请求中携带区块标识，上链验证结果请求，用于指示第三共识节点根据区块标识从第三区块链中获取上链验证结果；及，接收第三共识节点返回的上链验证结果。

在一些实施例中，第一发送单元 2330 还用于：

将局部事务放置在队列中排队；及，

响应于队列满足预定条件，将队列中的局部事务打包，发送到第二共识节点。

在一些实施例中，第一发送单元 2330 还具体用于：

响应于队列中局部事务的数目达到第一阈值，将队列中的局部事务打包。

在一些实施例中，第一发送单元 2330 还具体用于：响应于队列中局部事务的数目未达到第一阈值，确定当前时间与上一个打包的时间之间的时间差；及，

响应于时间差达到第二阈值，将队列中的局部事务打包。

在一些实施例中，

第一发送单元 2330 还具体用于：

确定局部事务的子类型；确定局部事务的子类型对应的队列；及，将局部事务放置于子类型对应的队列中排队。

在一些实施例中，第一发送单元 2330 还用于：响应于队列中的局部事务数目达到第三阈值，将队列中的局部事务打包。

在一些实施例中，第一发送单元 2330 还具体用于：

确定局部事务的子类型；

根据子类型，确定局部事务的优先级；

将局部事务按照优先级从高到低的顺序，放置在队列中排队；及，

从队列中顺序取出局部事务，发送到第二共识节点。

在一些实施例中，第二共识节点具有可信执行环境，第二区块链用可信执行环境的密钥加密；第一上链验证信息是第二共识节点响应于第二中继节点发送的第一上链验证信息请求，而向第二中继节点发送的，第一上链验证信息请求，是第二中继节点响应于在第二区块链上增加加密区块发送的，加密区块采用可信执行环境的密钥加密，第一上链验证信息用于指示第二中继节点将第一上链验证信息转发到第三共识节点。

图 24 为本申请实施例提供的事务上链装置 2400 的结构示意图。该事务上链装置 2400 包括：

第一接收单元 2410，用于接收第一中继节点转发的局部事务，局部事务的父类型为第一类型；

第二上链单元 2420，用于执行局部事务，将局部事务记录到第二区块链，其中，第二区块链被禁止由第二共识节点以外的节点访问；

第二获取单元 2430，用于获取局部事务的第一上链验证信息；及，

第二发送单元 2440，用于将第一上链验证信息发送到第三共识节点，第一上链验证信息用于指示第三共识节点根据第一上链验证信息对局部事务的上链进行验证，得到上链验证结果。

在一些实施例中，第二共识节点具有可信执行环境，第二区块链用可信执行环境的密钥加密；第二发送单元 2440，还用于：接收第二中继节点发送的第一上链验证信息请求；第一上链验证信息请求，是第二中继节点响应于在第二区块链上增加加密区块发送的，加密区块采用可信执行环境的密钥加密；及，响应于第一上链验证信息请求，将第一上链验证信息发送到第二中继节点，第一上链验证信息用于指示第二中继节点将第一上链验证信息转发到第三共识节点。

参照图 25，图 25 为实现本申请实施例的事务上链方法的终端的部分的结构框图，该终端包括：射频 (Radio Frequency，简称 RF) 电路 2510、存储器 2515、输入单元 2530、显示单元 2540、传感器 2550、音频电路 2560、无线保真 (wireless fidelity，简称 WiFi) 模块 2570、处理器 2580、以及电源 2590 等部件。本领域技术人员可以理解，图 25 示出的终端结构并不构成对手机或电脑的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

RF 电路 2510 可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，给处理器 2580 处理。另外，将设计上的数据发送给基站。

存储器 2515 可用于存储软件程序以及模块，处理器 2580 通过运行存储在存储器 2515 的软件程序以及模块，从而执行对象终端的各种功能应用以及数据处理。

输入单元 2530 可用于接收输入的数字或字符信息, 以及产生与对象终端的设置以及功能控制有关的键信号输入。具体地, 输入单元 2530 可包括触控面板 2531 以及其他输入装置 2532。

显示单元 2540 可用于显示输入的信息或提供的信息以及对象终端的各种菜单。显示单元 2540 可包括显示面板 2541。

音频电路 2560、扬声器 2561, 传声器 2562 可提供音频接口。

在本实施例中, 该终端所包括的处理器 2580 可以执行前面实施例的事务上链方法。

本申请实施例的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。本发明实施例可应用于各种场景, 包括但不限于数据安全、区块链、数据存储、信息技术等。

图 26 为实施本申请实施例的事务上链方法的服务器的部分的结构框图。服务器可因配置或性能不同而产生比较大的差异, 可以包括一个或一个以上中央处理器(Central Processing Units, 简称 CPU) 2622(例如, 一个或一个以上处理器)和存储器 2632, 一个或一个以上存储应用程序 2642 或数据 2644 的存储介质 2130(例如一个或一个以上海量存储装置)。其中, 存储器 2632 和存储介质 2630 可以是短暂存储或持久存储。存储在存储介质 2630 的程序可以包括一个或一个以上模块(图示没标出), 每个模块可以包括对服务器中的一系列指令操作。更进一步地, 中央处理器 2622 可以设置为与存储介质 2630 通信, 在服务器上执行存储介质 2630 中的一系列指令操作。

服务器还可以包括一个或一个以上电源 2626, 一个或一个以上有线或无线网络接口 2650, 一个或一个以上输入输出接口 2658, 和/或, 一个或一个以上操作系统 2641, 例如 Windows Server™, Mac OS X™, Unix™, Linux™, FreeBSD™ 等等。

服务器中的中央处理器 2622 可以用于执行本申请实施例的事务上链方法。

本申请实施例还提供一种计算机可读存储介质, 计算机可读存储介质用于存储计算机可读指令, 计算机可读指令用于执行前述各个实施例的事务上链方法。

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程序。计算机设备的处理器读取该计算机程序并执行, 使得该计算机设备执行实现上述的事务上链。

本申请的说明书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等(如果存在)是用于区别类似的对象, 而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换, 以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外, 术语“包括”和“包含”以及他们的任何变形, 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、系统、产品或装置不必限于清楚地列出的那些步骤或单元, 而是可包括没有清楚地列出的或对于这些过程、方法、产品或装置固有的其它步骤或单元。

应当理解, 在本申请中, “至少一个(项)”是指一个或者多个, “多个”是指两个或两个以上。“和/或”, 用于描述关联对象的关联关系, 表示可以存在三种关系, 例如, “A 和/或 B”可以表示: 只存在 A, 只存在 B 以及同时存在 A 和 B 三种情况, 其中 A, B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达, 是指这些项中的任意组合, 包括单项(个)或复数项(个)的任意组合。例如, a, b 或 c 中的至少一项(个), 可以表示: a, b, c, “a 和 b”, “a 和 c”, “b 和 c”, 或“a 和 b 和 c”, 其中 a, b, c 可以是单个, 也可以是多个。

应了解, 在本申请实施例的描述中, 多个(或多项)的含义是两个以上, 大于、小于、超过等理解为不包括本数, 以上、以下、以内等理解为包括本数。

在本申请所提供的几个实施例中, 应该理解到, 所揭露的系统, 装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个系统, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外, 在本申请各个实施例中的各功能单元可以集成在一个处理单元中, 也可以是各个单元单独物理存在, 也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。

集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用, 可以存储在一个计算机可读存储介质中。基于这样的理解, 本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来, 该计算机软件产品存储在一个存储介质中, 包括若干指令用以使得一台计算机装置(可以是个人计算机, 服务器, 或者网络装置等)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器(Read-Only Memory, 简称 ROM)、随机存取存储器(Random Access Memory, 简称 RAM)、磁碟或者光盘等各种可以存储计算机可读指令的介质。

还应了解, 本申请实施例提供的各种实施方式可以任意进行组合, 以实现不同的技术效果。

以上是对本申请的实施方式的具体说明, 但本申请并不局限于上述实施方式, 熟悉本领域的技术人员在不违背本申请精神的条件下还可作出种种等同的变形或替换, 这些等同的变形或替换均包括在本申请权利要求所限定的范围内。

权利要求书

1、一种事务上链方法，其特征在于，由第一中继节点执行，包括：

在第一共识节点接收到局部事务的情况下，确定所述局部事务的父类型；

在所述父类型为第一类型的情况下，将所述局部事务发送到第二共识节点，所述局部事务用于指示所述第二共识节点执行所述局部事务，将所述局部事务记录到第二区块链，生成所述局部事务的第一上链验证信息，并将所述第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到所述局部事务的上链验证结果，其中，所述第二区块链禁止由所述第二共识节点以外的节点访问；及，

从所述第三共识节点获取所述局部事务的上链验证结果。

2、根据权利要求1所述的方法，其特征在于，所述第一共识节点属于局部共识网络，第二共识节点属于全局共识网络中的第一全局共识网络，第三共识节点属于所述全局共识网络中的第二全局共识网络，所述第一中继节点，用于将第一类型的局部事务发送至第一全局共识网络中的第二共识节点。

3、根据权利要求1或2所述的方法，其特征在于，所述方法还包括：

在所述父类型为第二类型的情况下，指示所述第一共识节点执行所述局部事务，并将所述局部事务记录到第一区块链，其中，所述第一区块链允许由所述第一共识节点以外的节点访问。

4、根据权利要求3所述的方法，其特征在于，所述方法还包括：

获取从多个第二类型的局部事务归纳出的全局事务；及，

将所述全局事务发送到所述第三共识节点，所述全局事务用于指示所述第三共识节点执行所述全局事务，将所述全局事务记录到第三区块链，其中，所述第三区块链允许由所述第三共识节点以外的节点访问。

5、根据权利要求4所述的方法，其特征在于，所述方法还包括：

在所述第三共识节点将所述全局事务记录到所述第三区块链，以生成第二上链验证信息的情况下，从所述第三共识节点接收所述第二上链验证信息；及，

将所述第二上链验证信息发送到所述第一共识节点，所述第二上链验证信息用于指示所述第一共识节点对所述全局事务的上链进行验证。

6、根据权利要求1至5中任一所述的方法，其特征在于，所述第一上链验证信息包括所述局部事务的摘要值、和根据第一树中第一路径确定出的第一旁路节点记录的摘要值，所述第一树中叶子节点记录所述第二区块链上所记录事务的摘要值，所述第一路径，是所述第一树中一个叶子节点到所述第一树中根节点的路径，且所述第一树中一个叶子节点记录所述局部事务的摘要值，所述第一旁路节点是所述第一路径中除根节点之外节点在所述第一树中的兄弟节点，所述第一上链验证信息还用于指示所述第三共识节点根据所述局部事务的摘要值和所述第一旁路节点中记录的摘要值确定第一比较摘要值，当所述第一树中根节点记录的摘要值和所述第一比较摘要值一致，则验证成功。

7、根据权利要求6所述的方法，其特征在于，所述第一上链验证信息还包括所述局部事务执行后所获得关联数据的摘要值和第二树中第二旁路节点记录的摘要值，所述第二树中叶子节点记录所述第二区块链上所记录事务执行后所获得关联数据的摘要值，所述第二路径，是所述第二树中一个叶子节点到所述第二树中根节点的路径，所述所述第二树中一个叶子节点记录所述局部事务执行后所获得关联数据的摘要值，所述第二旁路节点是所述第二路径中除根节点之外节点在所述第二树中的兄弟节点，所述第一上链验证信息还用于指示所述第三共识节点在所述第一树中根节点记录的摘要值和所述第一比较摘要值一致的情况下，根据局部事务执行后所获得关联数据的摘要值和第二旁路节点记录的摘要值，确定第二比较摘要值，当所述第二树中根节点记录的摘要值与所述第二比较摘要值一致，则验证成功。

8、根据权利要求7所述的方法，其特征在于，所述第一上链验证信息还包括事务脱敏信息，所述事务脱敏信息，是所述第二共识节点对所述局部事务进行脱敏处理得到的，所述脱敏处理是根据目标合约中的脱敏字段进行的，所述目标合约与所述局部事务的子类型相对应；及，

所述从所述第三共识节点获取所述局部事务的上链验证结果，包括：

从所述第三共识节点获取所述事务脱敏信息，作为所述上链验证结果。

9、根据权利要求7所述的方法，其特征在于，所述第一上链验证信息还包括所述局部事务的即时性信息，所述即时性信息是所述第二共识节点根据所述局部事务的子类型确定的；及，

所述从所述第三共识节点获取所述局部事务的上链验证结果，包括：

当所述即时性信息指示所述局部事务为即时事务，在所述第三共识节点验证成功后，接收所述第三共识节点返回的所述上链验证结果。

10、根据权利要求9所述的方法，其特征在于，所述方法还包括：

当所述即时性信息指示所述局部事务为非即时事务，向所述第三共识节点发送上链验证结果请求，并从所述第三共识节点对所述上链验证结果请求的应答中获取所述上链验证结果。

11、根据权利要求7所述的方法，其特征在于，所述第一上链验证信息还包括所述第二旁路节点的第一签名，所述第一签名，是所述第二共识节点用所述第二共识节点的第一私钥对第一摘要进行加密得到的，所述第一摘要，是所述第二共识节点根据所述局部事务的摘要值、所述第一旁路节点记录的摘要值、所述局部事务执行后所获得关联数据的摘要值以及所述第二旁路节点记录的摘要值生成的；

所述第一签名用于指示所述第三共识节点在所述第二树中根节点与所述第二待比较根节点一致的情

况下,用所述第二共识节点的第一公钥解密所述第一签名,得到第二摘要,根据所述局部事务的摘要值、所述第一旁路节点记录的摘要值、所述局部事务执行后所获得关联数据的摘要值以及所述第二旁路节点记录的摘要值生成第三摘要,当所述第三摘要与所述第二摘要一致,则验证成功。

12、根据权利要求1所述的方法,其特征在于,所述方法还包括:

在所述第三共识节点将包括所述上链验证结果的区块记录到第三区块链后,接收所述第三共识节点返回的区块标识,所述区块标识是指包括所述上链验证结果的区块;

所述从所述第三共识节点获取所述局部事务的上链验证结果,包括:

向所述第三共识节点发送上链验证结果请求,所述上链验证结果请求中携带所述区块标识,所述上链验证结果请求,用于指示所述第三共识节点根据所述区块标识从所述第三区块链中获取所述上链验证结果;

及,接收所述第三共识节点返回的所述上链验证结果。

13、根据权利要求1至12中任一所述的方法,其特征在于,所述将所述局部事务发送到第二共识节点,包括:

将所述局部事务放置在队列中排队;及,

响应于所述队列满足预定条件,将所述队列中的局部事务打包,发送到所述第二共识节点。

14、根据权利要求13所述的方法,其特征在于,所述响应于所述队列满足预定条件,将所述队列中的所述局部事务打包,包括:

响应于所述队列中局部事务的数目达到第一阈值,将所述队列中的局部事务打包。

15、根据权利要求13所述的方法,其特征在于,所述响应于所述队列满足预定条件,将所述队列中的所述局部事务打包,包括:

响应于所述队列中局部事务的数目未达到第一阈值,确定当前时间与上一个打包时间之间的时间差;

及,响应于所述时间差达到第二阈值,将所述队列中的局部事务打包。

16、根据权利要求13所述的方法,其特征在于,所述将所述局部事务放置在队列中排队,包括:

确定所述局部事务的子类型;

确定所述局部事务的子类型对应的队列;及,

将所述局部事务放置在所述子类型对应的队列中排队。

17、根据权利要求16所述的方法,其特征在于,所述响应于所述队列满足预定条件,将所述队列中的所述局部事务打包,包括:

响应于所述队列中的局部事务数目达到第三阈值,将所述队列中的局部事务打包。

18、根据权利要求1至17中任一所述的方法,其特征在于,所述将所述局部事务发送到第二共识节点,包括:

确定所述局部事务的子类型;

根据所述子类型,确定所述局部事务的优先级;

将所述局部事务按照优先级从高到低的顺序,放置在队列中排队;及,

从所述队列中顺序取出所述局部事务,发送到第二共识节点。

19、根据权利要求1至18中任一所述的方法,其特征在于,所述第二共识节点具有可信执行环境,所述第二区块链用所述可信执行环境的密钥加密;所述第一上链验证信息是所述第二共识节点响应于所述第二中继节点发送的第一上链验证信息请求,而向所述第二中继节点发送的,所述第一上链验证信息请求,是所述第二中继节点响应于在所述第二区块链上增加加密区块发送的,所述加密区块采用所述可信执行环境的密钥加密,所述第一上链验证信息用于指示所述第二中继节点将所述第一上链验证信息转发到所述第三共识节点。

20、一种事务上链方法,其特征在于,由第二共识节点执行,包括:

接收第一中继节点转发的局部事务,所述局部事务的父类型为第一类型;

执行所述局部事务,将所述局部事务记录到第二区块链,其中,所述第二区块链被禁止由所述第二共识节点以外的节点访问;

获取所述局部事务的第一上链验证信息;及,

将所述第一上链验证信息发送到第三共识节点,所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证,得到上链验证结果。

21、根据权利要求20所述的方法,其特征在于,所述第二共识节点具有可信执行环境,所述第二区块链用所述可信执行环境的密钥加密;

所述将所述第一上链验证信息发送到第三共识节点包括:

接收第二中继节点发送的第一上链验证信息请求;所述第一上链验证信息请求,是所述第二中继节点响应于在所述第二区块链上增加加密区块发送的,所述加密区块采用所述可信执行环境的密钥加密;及,响应于所述第一上链验证信息请求,将所述第一上链验证信息发送到所述第二中继节点,所述第一上链验证信息用于指示所述第二中继节点将所述第一上链验证信息转发到所述第三共识节点。

22、一种事务上链装置,其特征在于,包括:

第一确定单元,用于在第一共识节点接收到的局部事务的情况下,确定所述局部事务的父类型;

第一发送单元,用于在所述父类型为第一类型的情况下,将所述局部事务发送到第二共识节点,所述

局部事务用于指示所述第二共识节点执行所述局部事务，将所述局部事务记录到第二区块链，生成所述局部事务的第一上链验证信息，并将所述局部事务的第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到所述局部事务的上链验证结果，其中，所述第二区块链禁止由所述第二共识节点以外的节点访问；及，

第一获取单元，用于从所述第三共识节点获取所述局部事务的上链验证结果。

23、一种事务上链装置，其特征在于，包括：

第一接收单元，用于接收第一中继节点转发的局部事务，所述局部事务的父类型为第一类型；

第二上链单元，用于执行所述局部事务，将所述局部事务记录到第二区块链，其中，所述第二区块链被禁止由所述第二共识节点以外的节点访问；

第二获取单元，用于获取所述局部事务的第一上链验证信息；及，

第二发送单元，用于将所述第一上链验证信息发送到第三共识节点，所述第一上链验证信息用于指示所述第三共识节点根据所述第一上链验证信息对所述局部事务的上链进行验证，得到上链验证结果。

24、一种电子设备，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，其特征在于，所述处理器执行所述计算机可读指令时实现根据权利要求 1 至 21 任意一项所述的事务上链方法。

25、一个或多个可读存储介质，所述存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被一个或多个处理器执行时实现根据权利要求 1 至 21 任意一项所述的事务上链方法。

26、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，所述计算机可读指令被计算机设备的一个或多个处理器读取并执行，使得该计算机设备执行根据权利要求 1 至 21 任意一项所述的事务上链方法。