(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 9 月 23 日 (23.09.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/184970 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)

(21) 国际申请号: PCT/CN2021/074145

(22) 国际申请日: 2021 年 1 月 28 日 (28.01.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010190860.1 2020年3月18日 (18.03.2020) CN

(71) 申请人: 支付宝（杭州）信息技术有限公司 (**ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 吴行行 (**WU, Hanghang**); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 邱鸿霖 (**QIU, Honglin**); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 吴因佥 (**WU, Yinqian**); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** METHOD AND DEVICE FOR CALLING CONTRACT

(54) 发明名称: 调用合约的方法及装置

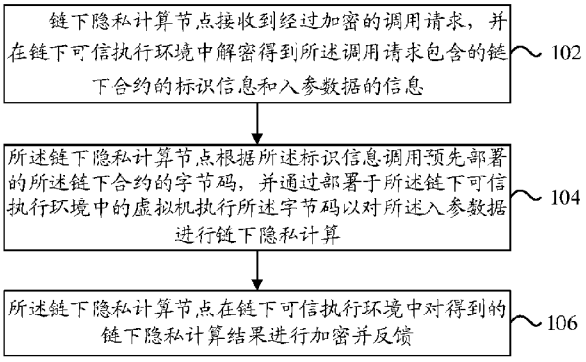

图 1

102 An off-chain privacy calculation node receives an encrypted calling request, and decrypts the encrypted calling request in an off-chain trusted execution environment to obtain identification information of an off-chain contract and information of incoming parameter data contained in the calling request

104 The off-chain privacy calculation node calls a pre-deployed byte code of the off-chain contract according to the identification information, and executes the byte code by means of a virtual machine deployed in the off-chain trusted execution environment so as to perform off-chain privacy calculation on the incoming parameter data

106 The off-chain privacy calculation node encrypts an obtained off-chain privacy calculation result in the off-chain trusted execution environment and feeds back the encrypted off-chain privacy calculation result

(57) **Abstract:** A method and device for calling a contract. The method comprises: an off-chain privacy calculation node receives an encrypted calling request, and decrypts the encrypted calling request in an off-chain trusted execution environment to obtain identification information of an off-chain contract and information of incoming parameter data contained in the calling request (102); the off-chain privacy calculation node calls a pre-deployed byte code of the off-chain contract according to the identification information, and executes the byte code by means of a virtual machine deployed in the off-chain trusted execution environment so as to perform off-chain privacy calculation on the incoming parameter data (104); and the off-chain privacy calculation node encrypts an obtained off-chain privacy calculation result in the off-chain trusted execution environment and feeds back the encrypted off-chain privacy calculation result (106). By means of the method, privacy protection can be implemented in a contract calling process.

WO 2021/184970 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种调用合约的方法及装置，该方法包括：链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息（102）；所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算（104）；所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈（106）。通过上述方法，可以在合约调用过程中实现隐私保护。

调用合约的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及可验证计算技术领域，尤其涉及一种调用合约的方法及装置。

背景技术

[02] 针对各种场景下的隐私需求，一种方式是通过同态加密（Homomorphic encryption）和零知识证明（Zero-knowledge proof）等加密技术实现隐私保护，但也随之带来了严重的性能损失。可信执行环境（Trusted Execution Environment，TEE）是另一种解决方式。TEE可以起到硬件中的黑箱作用，在TEE中执行的代码和数据操作系统层都无法偷窥，只有代码中预先定义的接口才能对其进行操作。在效率方面，由于TEE的黑箱性质，在TEE中进行运算的是明文数据，而不是同态加密中的复杂密码学运算，计算过程效率没有损失。

发明内容

[03] 有鉴于此，本说明书一个或多个实施例提供一种调用合约的方法及装置，能够在链下环境内安全实现调用合约的操作。

[04] 根据本说明书一个或多个实施例的第一方面，提出了一种调用合约的方法，包括：链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息；所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。

[05] 根据本说明书一个或多个实施例的第二方面，提出了一种调用合约的方法，包括：客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；所述客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[06] 根据本说明书一个或多个实施例的第三方面，提出了一种调用合约的方法，包括：区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[07] 所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。

[08] 根据本说明书一个或多个实施例的第四方面，提出了一种调用合约的方法，包括：控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点；所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。

[09] 根据本说明书一个或多个实施例的第五方面，提出了一种调用合约的方法，包括：隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息；所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算；所述隐私计算节点在可信执行环境中对得

到的隐私计算结果进行加密并反馈。

[10] 根据本说明书一个或多个实施例的第六方面，提出了一种调用合约的方法，包括：客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

[11] 根据本说明书一个或多个实施例的第七方面，提出了一种调用合约的方法，包括：控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点；所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

[12] 根据本说明书一个或多个实施例的第八方面，提出了一种调用合约的装置，包括：接收与解密单元，使链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息；调用与执行单元，使所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；反馈单元，使所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。

[13] 根据本说明书一个或多个实施例的第九方面，提出了一种调用合约的装置，包括：生成单元，使客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；发送单元，使所述客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[14] 根据本说明书一个或多个实施例的第十方面，提出了一种调用合约的装置，包括：获取单元，使区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；传输单元，使所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[15] 接收单元，使所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。

[16] 根据本说明书一个或多个实施例的第十一方面，提出了一种调用合约的装置，包括：接收单元，使控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；转发单元，使所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点；反馈单元，使所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。

[17] 根据本说明书一个或多个实施例的第十二方面，提出了一种调用合约的装置，包括：接收与解密单元，使隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息；调用与计算单元，使所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算；加密与反馈单元，使所述隐私计算节点在可信执行环境中对得到的隐私计算结果

进行加密并反馈。

[18] 根据本说明书一个或多个实施例的第十三方面，提出了一种调用合约的装置，包括：生成调用请求单元，使客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；发送调用请求单元，使所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

[19] 根据本说明书一个或多个实施例的第十四方面，提出了一种调用合约的装置，包括：接收调用请求单元，使控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；转发调用请求单元，使所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点；反馈隐私计算结果单元，使所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

[20] 根据本说明书一个或多个实施例的第十五方面，提出了一种电子设备，包括：处理器；用于存储处理器可执行指令的存储器；其中，所述处理器通过运行所述可执行指令以实现如第一方面、第二方面、第三方面、第四方面、第五方面、第六方面或第七方面所述的方法。

[21] 根据本说明书一个或多个实施例的第十六方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面、第二方面、第三方面、第四方面、第五方面、第六方面或第七方面所述方法的步骤。

[22] 综上所述，本说明书通过在链下隐私计算节点上实现链下可信执行环境，使得链下隐私计算节点可以提供安全可靠的运行环境，并且该链下可信执行环境的可靠性可以通过远程证明予以验证，从而能够安全可靠地调用部署于该链下隐私计算节点内的合约，确保链下隐私计算节点安全并且忠实地完成链下隐私计算。

附图说明

[23] 图 1 是本说明书一示例性实施例提供的一种链下隐私计算节点侧的调用合约的方法的流程图。

[24] 图 2 是本说明书一示例性实施例提供的一种调用合约的场景示意图。

[25] 图 3 是本说明书一示例性实施例提供的另一种调用合约的场景示意图。

[26] 图 4 是本说明书一示例性实施例提供的一种客户端侧的调用合约的方法的流程图。

[27] 图 5 是本说明书一示例性实施例提供的一种区块链节点侧的调用合约的方法的流程图。

[28] 图 6 是本说明书一示例性实施例提供的一种控制节点侧的调用合约的方法的流程图。

[29] 图 7 是本说明书一示例性实施例提供的另一种隐私节点侧的调用合约的方法的流程图。

[30] 图 8 是本说明书一示例性实施例提供的另一种客户端侧的调用合约的方法的流程图。

[31] 图 9 是本说明书一示例性实施例提供的另一种控制节点侧的调用合约的方法的流程图。

[32] 图 10 是一示例性实施例提供的一种设备的结构示意图。

[33] 图 11 是一示例性实施例提供的一种链下隐私计算节点侧的调用合约的装置的框图。

[34] 图 12 是一示例性实施例提供的一种客户端侧的调用合约的装置的框图。

[35] 图 13 是一示例性实施例提供的一种区块链节点侧的调用合约的装置的框图。

[36] 图 14 是一示例性实施例提供的一种控制节点侧的调用合约的装置的框图。

[37] 图 15 是一示例性实施例提供的另一种隐私计算节点侧的调用合约的装置的框图。

[38] 图 16 是一示例性实施例提供的另一种客户端侧的调用合约的装置的框图。

[39] 图 17 是一示例性实施例提供的另一种控制节点侧的调用合约的装置的框图。

具体实施方式

[40] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[41] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[42] 区块链一般被划分为三种类型：公有链（Public Blockchain）、私有链（Private Blockchain）和联盟链（Consortium Blockchain）。此外，还有多种类型的结合，比如私有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表，加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等，且各参与者（即节点）可自由加入以及退出网络。私有链则相反，该网络的数据写入权限由某个组织或者机构控制，数据读取权限受组织规定；简单来说，私有链可以为一个弱中心化系统，参与节点具有严格限制且少，因而私有链更适合于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织，参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。

[43] 在区块链网络中，通过向区块链节点提交相应的区块链交易（简称交易），并由区块链节点执行区块链交易，以实现相应的操作目的。对于上述任何类型的区块链而言，区块链节点均可以通过创建 TEE，并将 TEE 实现为区块链交易的安全执行环境。TEE 是基于 CPU 硬件的安全扩展，且与外部完全隔离的可信执行环境。TEE 最早是由 Global Platform 提出的概念，用于解决移动设备上资源的安全隔离，平行于操作系统为应用程序提供可信安全的执行环境。目前工业界十分关注 TEE 的方案，几乎所有主流的芯片和软件联盟都有自己的 TEE 解决方案，比如软件方面的 TPM（Trusted Platform Module，可信赖平台模块）以及硬件方面的 Intel SGX（Software Guard Extensions，软件保护扩展）、ARM Trustzone（信任区）和 AMD PSP（Platform Security Processor，平台安全处理器）等。

[44] 以 Intel SGX（以下简称 SGX）技术为例。区块链节点可以基于 SGX 技术创建 enclave（围圈或飞地），以作为用于执行区块链交易的 TEE。其中，区块链节点利用 CPU 中新增的处理器指令，在内存中可以分配一部分区域 EPC（Enclave Page Cache，围圈页面缓存或飞地页面缓存），以用于驻留上述的 enclave。上述 EPC 对应的内存区域被 CPU 内部的内存加密引擎 MEE（Memory Encryption Engine）加密，该内存区域中的内容（enclave 中的代码和数据）只有在 CPU 内核中才能够被解密，且用于加解密的密钥只有在 EPC 启动时生成并存储在 CPU 中。可见，enclave 的安全边界只包含其自身和 CPU，无论是特权或非特权软件都无法访问 enclave，即便是操作系统管理员和 VMM（virtual machine monitor，虚拟机监视器；或称为，Hypervisor）也无法影响 enclave 中的代码和数据，因而具有极高的安全性，并且在上述安全性保障的前提下，CPU 能够在 enclave 中对明文形式的区块链交易进行处理，具有极高的运算效率，从而兼顾了数据安全性和计算效率。

[45] 基于区块链网络的去中心化架构，使得区块链上的每笔区块链交易都需要在区块

链网络内的所有区块链节点上执行，以确保每个区块链节点所维护的区块链账本数据一致。如果交易逻辑较为简单，比如以比特币为例，区块链交易仅用于实现转账操作，此时即便区块链交易需要在所有区块链节点都执行，也不会导致过多的资源消耗。但是，如果区块链提供了智能合约的功能，而区块链交易调用了智能合约，那么情况可能大不相同。区块链上的智能合约是在区块链系统上可以被交易触发执行的合约，智能合约可以通过代码的形式定义。

[46] 以以太坊为例，支持用户在以太坊网络中创建并调用一些复杂的逻辑，这是以太坊区别于比特币区块链技术的最大挑战。以太坊作为一个可编程区块链的核心是以太坊虚拟机（EVM），每个以太坊节点都可以运行 EVM。EVM 是一个图灵完备的虚拟机，这意味着可以通过它实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在 EVM 上运行的。实际上，虚拟机直接运行的是虚拟机代码（虚拟机字节码，下简称“字节码”）。智能合约分为部署和调用两个阶段。

[47] 在部署阶段，用户将一个包含创建智能合约信息的交易发送至以太坊网络，该交易的 data 字段包含智能合约的代码（如字节码），该交易的 to 字段为空。以太坊网络中的各个节点分别通过 EVM 执行这个交易，并生成对应的合约实例。在节点间通过共识机制达成一致后，上述交易对应的智能合约创建成功，区块链上出现一个与该智能合约对应的合约账户，该合约账户拥有一个特定的合约地址，合约代码（即智能合约的代码）或合约代码的哈希值保存在该合约账户中，该合约代码用于控制相应的智能合约的行为。

[48] 在调用阶段，用户（可以与部署智能合约的用户相同或不同）将一个用于调用智能合约的交易发送到以太坊网络，该交易的 from 字段是该用户对应的外部账户的地址，to 字段是所需调用的智能合约的合约地址，data 字段包含调用智能合约的方法和参数。在节点间通过共识机制达成一致后，上述交易声明调用的智能合约以规定的方式在以太坊网络的每个节点上独立执行，所有执行记录和数据都保存在区块链上，所以当交易完成后，区块链上就保存了无法篡改、不会丢失的交易凭证。

[49] 如前所述，EVM 是一个图灵完备的虚拟机；类似地，其他区块链也可以采用其他类型的虚拟机，比如 WASM（WebAssembly）虚拟机等。总之，当交易调用的智能合约用于实现相对复杂的逻辑时，节点通过虚拟机执行该智能合约的代码的过程会消耗相对较多的计算资源，并且由于区块链网络内的所有节点都需要执行该智能合约的代码，因此随着节点数量的增加会导致计算资源的消耗量成倍增长。因此，虽然结合 TEE 技术可以相对减少单个区块链节点的资源消耗、加快交易执行效率，但就整个区块链网络而言，仍然会造成极大的资源消耗和浪费。

[50] 为此，本说明书提出了在链下部署隐私计算节点（即链下隐私计算节点），可以将原本需要在所有区块链节点上执行的计算操作转移至链下隐私计算节点处执行，区块链节点只需要从链下隐私计算节点处获取计算结果并基于该计算结果更新区块链账本数据即可。链下隐私计算节点上可以创建链下 TEE，而基于可验证计算（Verifiable Computation）技术能够证明上述的计算结果确实是在该链下 TEE 内按照预期执行，从而在确保可靠性的同时，极大地降低了链上的资源消耗。

[51] 如前所述，通过在区块链节点调用智能合约，使得区块链节点可以执行该智能合约的代码以实现相应的计算需求；类似地，可以将用于执行计算任务的代码部署于链下隐私计算节点处，并通过对所部署的代码进行调用以实现相应的计算需求。为了便于理解，本说明书中将部署于区块链节点的合约称为链上合约、将部署于链下隐私计算节点的合约称为链下合约；当然，无论是链上合约还是链下合约，其本质都是一段可以在虚拟机内执行的代码。

[52] 图 1 是本说明书示出的一种链下隐私计算节点侧的调用合约的方法的流程图。如图 1 所示，该方法可以包括步骤 102~步骤 103。

[53] 步骤 102，链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息。

[54] 在通过调用请求来调用链下隐私计算节点上部署的链下合约之前，客户端需要将链下合约安全部署至该链下隐私计算节点处。例如，客户端在确定链下隐私计算节点可信的情况下，可以向链下隐私计算节点部署链下合约。链下合约与区块链节点所执行的链上合约类似，均可以为运行于虚拟机中的字节码，此处不再赘述。

[55] 如前所述，链下隐私计算节点可以创建链下 TEE，而针对链下合约的部署操作和调用操作均通过该链下 TEE 实现，从而确保操作过程中的数据安全和隐私保护。在链下隐私计算节点上创建的链下 TEE,与前文所述的区块链节点上创建的链上 TEE 相似，都是基于 CPU 硬件实现的与外部完全隔离的可信执行环境。客户端通过获取针对链下隐私计算节点上创建的链下 TEE 的远程证明报告,验证该链下隐私计算节点是否可信，具体指该链下隐私计算节点上部署的链下 TEE 是否可信。

[56] 远程证明报告产生于针对链下隐私计算节点上的链下 TEE 的远程证明过程。远程证明报告由认证服务器对链下隐私计算节点产生的自荐信息进行验证后生成，该自荐信息与链下隐私计算节点上创建的链下 TEE 相关。链下隐私计算节点通过产生与链下 TEE 相关的自荐信息，并由认证服务器对该自荐信息进行验证后产生远程证明报告，使得远程证明报告可以用于表明链下隐私计算节点上的链下 TEE 可信任。例如，以 Intel SGX 技术为例，链下 TEE 为链下隐私计算节点上创建的用于实现链下隐私计算的 enclave，远程证明过程还涉及到链下隐私计算节点上另一个特殊的 enclave,即 quoting enclave(简称 QE），QE 是由英特尔提供并签名的架构型 enclave（Architectural Enclave）。上述 enclave 首先需要生成一用于本地认证的 REPORT(报告)结构,并由 QE 基于该 REPORT 结构验证该 enclave 是否与自身处于同一平台上，而后由 QE 将该 REPORT 结构封装为一结构体 QUOTE（即自荐信息），并使用 EPID(enhanced privacy identification) 密钥进行签名。EPID 密钥不仅代表链下隐私计算节点这一平台，还代表链下隐私计算节点的底层硬件的可信度，还可以绑定处理器固件的版本等信息，并且只有 QE 才能访问到 EPID 密钥，以用于对上述的结构体 QUOTE 进行签名。在 SGX 技术中，上述的认证服务器可以为英特尔公司提供的 IAS（Intel Attestation Service）服务器，链下隐私计算节点向 IAS 服务器发送经过签名的上述结构体 QUOTE，使得 IAS 服务器可以对签名进行验证，并向链下隐私计算节点返回相应的远程证明报告。

[57] 链下隐私计算节点创建链下 TEE 后，产生用于实现远程证明的自荐信息，该自荐信息可以用于锚定和固化链下 TEE 的信息，使得最终得到的包含该自荐信息的远程证明报告可以用于表征链下 TEE 的状态，并用于验证该链下 TEE 是否可信。例如，自荐信息中可以包含第一待检验哈希值，该第一待检验哈希值为链下 TEE 的预设信息的哈希值，比如该预设信息可以包括链下 TEE 内部署的所有代码、该链下 TEE 的开发者的公钥等。以 Intel SGX 技术为例，对应于链下 TEE 内部署的所有代码所生成的哈希值为 MREnclave，对应于链下 TEE 的开发者的公钥所生成的哈希值为 MRSigner，即第一待检验哈希值可以包括 MREnclave 和 MRSigner。

[58] 仍以 Intel SGX 技术为例。如前所述，链下隐私计算节点向 IAS 服务器发送经过签名的结构体 QUOTE 后，由 IAS 服务器根据所维护的公钥集合进行签名验证，并向链下隐私计算节点返回远程证明报告（即 AVR 报告），该远程证明报告中包含：结构体 QUOTE 和签名验证结果，并且 IAS 服务器采用自身持有的私钥对该远程证明报告进行签名。

[59] 相应地，客户端在获取远程证明报告后，可以首先根据 IAS 服务器的公钥对该远程证明报告进行签名验证，如果验证通过则表明该远程证明报告确实由 IAS 服务器生成，且在数据传输过程中未被篡改或丢失数据。客户端可以通过任意途径获得 IAS 服务器的公钥，譬如远程证明报告被提供至客户端时，还可以关联提供 IAS 的证书链，使得客户

端可以从该证书链中提取IAS服务器的公钥。然后，客户端可以从远程证明报告中提取结构体QUOTE和签名验证结果。客户端可以首先查看签名验证结果，如果签名验证结果为通过验证，表明链下隐私计算节点的CPU持有由Intel提供的私钥，因而链下TEE建立在可靠的硬件平台上，可以继续执行其他验证操作；如果签名验证结果为未通过验证，客户端可以判定链下隐私计算平台不可靠，无需继续其他验证操作。然后，客户端可以从结构体QUOTE内提取上述的哈希值MREnclave和MRSigner，即待检验MREnclave和待检验MRSigner；同时，客户端预先获得了链下TEE的MREnclave和MRSigner的可信值，比如称之为可信MREnclave和可信MRSigner，并将待检验MREnclave与可信MREnclave进行比较、将待检验MRSigner与可信MRSigner进行比较。那么，客户端可以将“待检验MREnclave与可信MREnclave一致，且待检验MRSigner与可信MRSigner一致”作为确认链下隐私计算节点可信的前提条件；换言之，如果待检验MREnclave与可信MREnclave不一致，或者待检验MRSigner与可信MRSigner不一致，客户端就判定链下隐私计算节点不可信，而如果客户端设定的所有前提条件都被满足，就可以确认链下隐私计算节点可信。此外，客户端对于签名验证结果进行验证的操作，与针对待检验MREnclave和待检验MRSigner进行验证的操作之间，并不存在必然的先后顺序，两者之间可以完全独立。

[60] 除了MREnclave和MRSigner之外，客户端还可以通过其他的前提条件对链下隐私计算节点的可信度进行验证。例如，链下隐私计算节点在创建链下TEE后，可以在链下TEE内生成代表自身的身份信息的密钥对，并且链下隐私计算节点在链下TEE中创建自身的节点身份信息，该节点身份信息与上述对应于身份信息的密钥对相关，比如该节点身份信息可以包含该密钥对中的公钥。其中，代表身份信息的密钥对可以存在一组或多组，比如一组密钥对为用于签名与验签的密钥对（即签名密钥对），一组密钥对为用于加密与解密的密钥对（即加密密钥对），则节点身份信息可以包括签名密钥对中的签名公钥和加密密钥对中的加密公钥。在一组密钥对中，对应于不同的加密算法，可能同时存在多个公钥，这些公钥均被包含于上述的节点身份信息中。此外，节点身份信息还可以包含其他与链下隐私计算节点相关的信息，比如软件版本、所在域名、所在分区名等，本说明书并不对此进行限制。那么，链下隐私计算节点在生成结构体QUOTE时，可以计算上述节点身份信息的哈希值，并将该哈希值作为第二待检验哈希值添加至结构体QUOTE中。

[61] 相应地，客户端在收到远程证明报告后，可以从该远程证明报告进行签名验证。在签名验证通过的情况下，客户端可以提取远程证明报告所含的签名验证结果和第二待检验哈希值，并分别予以验证，且对于两者的验证并不存在必然的先后顺序，两者之间可以完全独立。假定客户端首先验证签名验证结果，并在签名验证结果为通过验证的情况下，继续对第二待检验哈希值进行验证。为了对第二待检验哈希值进行验证，客户端需要获取链下隐私计算节点的节点身份信息，比如远程证明报告被提供至客户端的同时，可以关联提供节点身份信息，当然客户端也可以通过其他方式或在其他时刻获得该节点身份信息。然后，客户端可以对获得的节点身份信息进行哈希计算，将计算得到的哈希值与上述的第二待检验哈希值进行比较，并将比较结果一致作为确认链下隐私计算节点可信的前提条件。如果第二待检验哈希值通过验证，可以证明链下隐私计算节点的身份信息是在链下TEE内初始化生成，上述代表身份信息的密钥对中的私钥仅由链下隐私计算节点所拥有，且该链下隐私计算节点能够完成签名、加密通讯等操作。

[62] 以上列举了两种针对链下隐私计算节点进行验证时采用的判断条件，即针对第一待检验哈希值的验证、针对第二待检验哈希值的验证。还可以采用其他的判断条件，此处不再一一列举。在针对链下隐私计算节点进行可信验证时，可以选用上述的一个或多个判断条件。例如，可以同时针对第一待检验哈希值和第二待检验哈希值进行验证；或者，在一些情况下，可以仅验证第二待检验哈希值，而对第一待检验哈希值可以不验证

或者部分验证。例如，客户端上可以设置信任等级，并根据信任等级确定是否验证或部分验证第一待检验哈希值，比如信任等级为 0 时，不需要验证第一待检验哈希值，信任等级为 1 时，验证第一待检验哈希值中的 MRSigner，信任等级为 2 时，验证第一待检验哈希值中的 MREnclave 等。

[63] 在上述实施例中，节点身份信息包含了链下隐私计算节点的身份相关的信息，比如代表身份的公钥等。节点身份信息还可以包含与链下 TEE 相关的信息，那么对节点身份信息进行哈希计算，并将得到的待检验哈希值添加至结构体 QUOTE 时，该待检验哈希值相当于同时实现了上述第一待检验哈希值和第二待检验哈希值的作用。例如，节点身份信息除了包含签名公钥和加密公钥等信息之外，还可以包含 MREnclave 和 MRSigner 的值，使得对该节点身份信息进行哈希计算得到的待检验哈希值，同时与链下隐私计算节点的身份、链下 TEE 相关。相应的，客户端在收到远程证明报告后，可以从该远程证明报告进行签名验证。在签名验证通过的情况下，客户端可以提取远程证明报告所含的签名验证结果和待检验哈希值，并分别予以验证，且对于两者的验证并不存在必然的先后顺序，两者之间可以完全独立。假定客户端首先验证签名验证结果，并在签名验证结果为通过验证的情况下，继续对待检验哈希值进行验证。为了对待检验哈希值进行验证，客户端需要获取链下隐私计算节点的节点身份信息，此处不再赘述。然后，客户端可以对获得的节点身份信息进行哈希计算，将计算得到的哈希值与上述的待检验哈希值进行比较，并将比较结果一致作为确认链下隐私计算节点可信的前提条件。可见，本实施例仅需一次比较，即可实现前文中两方面的验证，有助于提升验证效率。

[64] 客户端对远程证明报告的验证过程，还可以包括其他操作，比如根据远程证明报告的内容确定链下 TEE 是否运行于测试模式（测试模式下存在数据泄露的风险）等，此处不再一一赘述。

[65] 客户端可以向链下隐私计算节点发起挑战，并接收链下隐私计算节点返回的远程证明报告，从而可以根据远程证明报告确定链下隐私计算节点是否可信。例如，客户端可以向链下隐私计算节点发起链下挑战，即发起挑战的过程与区块链网络无关，这样可以跳过区块链节点之间的共识过程、减少链上链下的交互操作，使得客户端向链下隐私计算节点的挑战具有更高的操作效率。再例如，客户端可以采用链上挑战的形式，比如客户端可以向区块链节点提交挑战交易，该挑战交易所含的挑战信息可由区块链节点通过预言机机制传输至链下隐私计算节点，且该挑战信息用于向链下隐私计算节点发起挑战。

[66] 本说明书中通过预言机机制实现将数据从链上传递至链下或者从链下传递至链上的操作。本说明书中将预言机合约与预言机服务器之间的配合机制称为预言机机制。比如，上文中基于预言机机制实现的链上挑战；以及，下文中基于预言机机制实现的链上调用等。其中，客户端向区块链节点提交的交易可以直接或间接调用预言机合约，以触发预言机机制。其中，如果将预言机合约的合约地址填入该交易的 to 字段，表明该交易直接调用了预言机合约；如果将某一链上合约的合约地址填入该交易的 to 字段，且该链上合约调用了预言机合约，表明该交易间接调用了预言机合约。链上合约调用预言机合约，一种情况下可以是在链上合约的字节码中预先写入了预言机合约的合约地址，另一种情况下可以是将预言机合约的合约地址作为调用该链上合约时的入参，并将该入参填入上述交易的 data 字段。除了将调用请求或其他数据从链上传递至链下，预言机机制还可以将数据从链下传递至链上，具体可由预言机服务器将链下数据传递至预言机合约，然后由预言机合约将链下数据传递至数据需求方，比如这里的链下数据可以包括调用链下合约所产生的隐私计算结果等。在上述的预言机机制中，将数据从链上传递至链下可以视为“请求”过程，将数据从链下传递至链上可以视为“响应”过程，这两个过程通常成对出现。

[67] 无论是链下挑战或链上挑战，链下隐私计算节点在收到客户端发起的挑战后，均

可以临时触发如前文所述的远程证明过程并产生相应的远程证明报告，然后将远程证明报告反馈至客户端。或者，链下隐私计算节点在收到客户端发起的挑战时，如果本地已经存在预先生成的远程证明报告，那么链下隐私计算节点将该远程证明报告提供至客户端，而无需临时触发远程证明过程。其中，链下隐私计算节点本地存在的远程证明报告，可以是该链下隐私计算节点响应于除客户端之外的其他挑战者的挑战而触发产生，比如该其他挑战者可以包括其他客户端、链下隐私计算节点所处的链下隐私计算集群中的控制节点、KMS 服务器等，本说明书并不对此进行限制。因此，链下隐私计算节点在收到客户端发起的挑战后，可以首先查看本地是否存在先前生成的远程证明报告，如果存在则将该远程证明报告反馈至客户端，否则临时触发远程证明过程。其中，远程证明报告可以具有一定的时限性，比如 30 分钟或其他时长，超时的远程证明报告可以被客户端认定为失效，链下隐私计算节点也可以主动清除已失效的远程证明报告以避免反馈至客户端。

[68] 基于上述方案，客户端在确定链下隐私计算节点可信的情况下，可以向链下隐私计算节点部署链下合约。与前述的挑战过程相类似的，客户端可以通过链下途径将链下合约的字节码加密传输至链下隐私计算节点，或者，客户端可以通过链上途径将链下合约的字节码加密传输至链下隐私计算节点，比如客户端生成链下合约部署交易，该链下合约部署交易中包含对字节码进行加密得到的字节码密文，客户端将链下合约部署交易加密后提交至区块链节点，加密后的链下合约部署交易可在区块链节点处创建的链上 TEE 内被解密、得到字节码密文，然后由区块链节点通过预言机机制将该字节码密文传输至链下隐私计算节点。

[69] 链下隐私计算节点可以在链下 TEE 中解密得到明文的字节码后，可以在链下 TEE 中对字节码进行重新加密后，存储至链下 TEE 之外的存储空间，比如链下隐私计算节点的硬盘中，从而完成对链下合约的部署。此处，链下隐私计算节点通常采用一对称密钥，通过对称加密的方式对字节码进行加密并存储，这样在后续调用该字节码时，相比于采用非对称加密的形式而言，可以更快地完成解密操作。该对称密钥可由链下隐私计算节点在链下 TEE 中生成，或者由其他对象通过加密传输的方式分发至链下隐私计算节点。例如，可由 KMS 服务器对链下隐私计算节点发起挑战，并通过远程证明验证该链下隐私计算节点可信的情况下，向该链下隐私计算节点分发上述的对称密钥。链下隐私计算节点可以将 KMS 服务器分发的对称密钥作为根密钥，并将基于该根密钥派生得到的衍生密钥应用于针对字节码的加密存储。再例如，基于 Intel SGX 技术，上述对称密钥可以为烧录于链下隐私计算节点的 CPU 内 e-fuses 存储电路中的 RSK（Root Seal Key）密钥，或者该 RSK 密钥派生得到的衍生密钥（即 Seal Key）。当然，链下隐私计算节点也可以采用非对称加密或者对称加密与非对称加密结合的方式，对字节码进行加密存储，本说明书并不对此进行限制。

[70] 客户端可以通过生成调用请求来调用链下隐私计算节点上部署的链下合约，其中，调用请求中，可以包含链下合约的标识信息和入参数据的信息。例如，客户端可以直接向链下隐私计算节点发送调用请求，即发送调用请求的过程与区块链网络无关，这样可以跳过区块链节点之间的共识过程、减少链上链下的交互操作，使得客户端向链下隐私计算节点的发送调用请求具有更高的操作效率。再例如，客户端可以采用链上的形式，比如客户端可以向区块链节点提交交易，该交易所含的调用请求可由区块链节点通过预言机机制传输至链下隐私计算节点。

[71] 以图 2 所示的场景为例。一种情况下，客户端 21 可以通过链下渠道直接向链下隐私计算节点 22 发送调用请求，即客户端 21 发送调用请求的过程与区块链网络无关。另一种情况下，客户端 21 可以向区块链网络 23 提交交易，即客户端 21 通过区块链网络 23 向链下隐私计算节点 22 发送链上调用请求，区块链网络 23 可以根据该交易获得调用请求，并通过预言机机制将调用请求传输至链下隐私计算节点 22。客户端通过链上渠道

向客户端发送调用请求时，可以包括三个步骤：步骤①，客户端 21 向区块链网络 23 提交一笔交易，该交易可由区块链网络 23 内的某一节点 23n 接收并执行，从而由区块链节点 23n 获得经过加密的调用请求；步骤②，节点 23n 调用预先部署的预言机智能合约（简称预言机合约），该预言机合约可以将上述调用请求传递至链下的预言机服务器 24，比如预言机合约可以产生包含该调用请求的事件，而预言机服务器 24 可以通过监听预言机合约产生的事件，从而获取上述的调用请求；步骤③，预言机服务器 24 将调用请求通过链下渠道发送至链下隐私计算节点 22。

[72] 以图 2 所示的场景为例，所涉及的数据交互可以包括：客户端 21 与链下隐私计算节点 22 之间的数据交互（客户端 21 直接向链下隐私计算节点 22 发送链下调用请求，链下隐私计算节点 22 直接向客户端 21 返回链下隐私计算结果）、客户端 21 与节点 23n 之间的数据交互（客户端 21 向节点 23n 提交交易、节点 23n 向客户端 21 返回链下隐私计算结果）、节点 23n 与预言机服务器 24 之间的数据交互（预言机服务器 24 从节点 23n 读取调用请求、预言机服务器 24 向节点 23n 反馈链下隐私计算结果）、预言机服务器 24 与链下隐私计算节点 22 之间的数据交互（预言机服务器 24 向链下隐私计算节点 22 发送调用请求、链下隐私计算节点 22 向预言机服务器 24 返回链下隐私计算结果）等。在实现上述任一数据交互的过程中，数据发送方与数据接收方之间传输的数据存在泄漏的可能性，并且节点 23n 会将交易上链导致该交易包含的调用请求被公开，因此可以通过对数据进行加密传输的方式，避免造成信息泄露。

[73] 客户端可以向链下隐私计算节点部署更多的链下合约；类似地，其他客户端也可以向链下隐私计算节点部署链下合约。为了便于管理，以及便于后续对链下合约进行调用，链下隐私计算节点可以为部署的链下合约生成相应的合约 ID，链下合约与合约 ID 之间一一对应，合约 ID 可以作为链下合约的标识信息。例如，链下隐私计算节点可以对该链下合约的字节码进行哈希运算，得到第一哈希值，并将该第一哈希值作为该链下合约的合约 ID。当然，链下隐私计算节点也可以通过其他方式生成合约 ID，本说明书并不对此进行限制。

[74] 因此，为了准确地指示链下隐私计算节点对链下合约的字节码进行调用，上述的调用请求中可以包含该链下合约的标识信息，比如上述的合约 ID。进一步地，调用请求还可以包括函数信息，在链下合约中包含多个函数的情况下，调用请求需要通过函数信息指明客户端需要调用的函数，该函数信息可以是函数名等，本说明书并不对此进行限制。当然，如果链下合约仅包含一个函数，或者客户端希望调用链下合约中的所有函数，那么调用请求中也可以省去函数信息。

[75] 调用请求还包括入参数据的信息。入参数据的信息可以为入参数据本身，或者入参数据的描述信息，比如该描述信息可以为存储地址等，使得链下隐私计算节点可以据此获取入参数据，尤其是当客户端本身并非数据拥有者的情况下，可以省去客户端与数据拥有者之间的交互，还可以降低调用请求的数据量、加快其传输速度。

[76] 部署在链下隐私计算节点的链下合约可以用于实现对某一对象的状态更新，比如使得该对象从第一状态更新至第二状态。但是，由于链下合约为无状态合约，即链下隐私计算节点并不维护上述对象的状态数据，使得链下合约无法主动获知第一状态，如果入参数据仅包含用于驱动该对象从第一状态向第二状态进行变化的数据，则针对上述对象的状态更新将无法顺利执行。因此，除了上述用于驱动该对象从第一状态向第二状态进行变化的数据之外，入参数据还应当包括第一状态的状态数据。例如，上述的对象可以是区块链账户，区块链账户的数据（即状态数据）仅维护于区块链节点处，链下隐私计算节点不会维护区块链账户的数据，即链下合约为无状态合约，那么在链下合约的执行逻辑与区块链账户相关的情况下，提供给链下合约的入参数据除了包含用于驱动区块链账户实现更新的数据之外，还应当包含区块链账户的历史状态的数据。由于链下合约为无状态合约，可以避免将状态数据存储于链下隐私计算节点处，尤其是不会对链上数

据进行存储，从而可以保证链上数据的隐私性和安全性。

[77] 调用请求中还可以包括指定对象的身份公钥的信息，该身份私钥由指定对象所维护。比如该指定对象可以为上述的客户端，或者由该客户端所指定的其他任意需求方，本说明书并不对此进行限制。因此，在获得链下隐私计算结果后，链下隐私计算节点可以采用接收到的指定对象的身份公钥对链下隐私计算结果进行加密，使得只有维护有身份私钥的指定对象才能对该链下隐私计算结果进行解密，保证了链下隐私计算结果的安全性。如果同时存在多个指定对象，调用请求中可以包含这些指定对象分别对应的多个身份公钥的信息，使得链下隐私计算节点分别用每个身份公钥对链下隐私计算结果进行加密。

[78] 如图 2 所示，以客户端 21 直接向链下隐私计算节点 22 发送链下调用请求为例。客户端 21 生成调用请求，并可以直接通过链下渠道发送至链下隐私计算节点 22，那么链下隐私计算节点 22 可以根据调用请求中包含的链下合约的标识信息调用预先部署的链下合约的字节码，并通过部署在链下 TEE 中的虚拟机执行该字节码以对调用请求中包含的入参数据进行隐私计算。但是，如果客户端 21 并不希望自己的调用请求被其他用户随意获知，可以对调用请求进行隐私保护。客户端 21 可以对发送的调用请求进行加密，而链下隐私计算节点可以接收经过加密的调用请求，这样可以确保传输过程中不会造成调用请求的内容泄露。同时，链下隐私计算节点 22 执行链下隐私计算后得到链下隐私计算结果，链下隐私计算节点 22 可以直接通过链下渠道将链下隐私计算结果反馈至客户端或者数据需求方。

[79] 如图 2 所示，以客户端 21 向节点 23n 提交交易为例。客户端 21 生成交易，并可以通过链上渠道向节点 23n 提交交易，使得节点 23n 可以将客户端 21 提交的交易与其他节点进行共识后上链，对客户端 21 提交的交易进行存证。但是，如果客户端 21 并不希望自己的行为被其他用户随意获知，可以对交易进行隐私保护。客户端 21 可以对提交的交易进行加密，而节点 23n 可以接收经过加密的交易，这样可以确保传输过程中不会造成交易的内容泄露。节点 23n 处可以部署链上 TEE，并且节点 23n 可以将经过加密的交易读入该链上 TEE 后，在链上 TEE 内解密，可以确保解密得到的挑战交易仅存在于链上 TEE 内、不会外泄。

[80] 其中，如果客户端 21 生成的交易中直接包含经过加密的调用请求，那么节点 23n 可以在链上 TEE 内解密交易、得到调用请求密文，然后节点 23n 可以通过预言机机制将该调用请求密文传输至链下隐私计算节点。

[81] 针对调用请求中链下合约的标识信息，客户端 21 可以直接将该标识信息添加在交易中，那么节点 23n 可以在链上 TEE 内解密交易、得到标识信息；或者，客户端 21 生成的交易所调用的链上合约中定义了链下合约的标识信息，那么节点 23n 在接收到该交易后，可以在链上 TEE 内执行被调用的链上合约，从而获得该标识信息。

[82] 针对调用请求中入参数据的信息，客户端 21 生成的交易中可以直接包含入参数据，那么节点 23n 可以在链上 TEE 内解密交易、得到入参数据。然后通过链上 TEE 内部署的虚拟机执行被调用的链上合约，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含入参数据的描述信息，比如该描述信息可以为存储地址等，那么节点 23n 可以通过执行链上合约查询到相应的入参数据，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含初始数据，那么节点 23n 可以通过执行链上合约对初始数据进行处理以获得相应的入参数据，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含初始数据的描述信息，比如该描述信息可以为存储地址等，那么节点 23n 可以通过执行链上合约查询到相应的初始数据，并由链上合约对初始数据进行处理，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调

用请求进行加密，因而客户端可以不直接将标识信息或者入参数据添加在交易中，客户端对于调用链下合约执行链下隐私计算的过程是透明的，客户端只需要获得反馈的链下隐私计算结果即可，而不需要关注调用的链下合约的标识信息或者入参数据的信息等。

[83] 针对调用请求的加密传输，可以采用对称加密或非对称加密的形式。通过对调用请求进行加密传输可以确保传输过程中不会造成调用请求的内容泄露。当采用对称加密时，客户端 21 和链下隐私计算节点 22 分别维护有相同的对称密钥，比如该对称密钥可由客户端 21 与链下隐私计算节点 22 通过诸如 DH（Diffie-Hellman）或 ECDH（Elliptic Curve Diffie–Hellman）等算法协商得到，或者由 KMS（Key Management Service，密钥管理服务）服务器分发至客户端 21 和节链下隐私计算节点 22，本说明书并不限制密钥来源。当密钥由 KMS 服务器分发时，KMS 服务器可以在客户端 21 对链下隐私计算节点进行远程证明的过程中，将密钥传输至客户端 21 处。那么，客户端 21 可以通过上述的对称密钥对调用请求进行加密，而链下隐私计算节点 22 将对称密钥维护于链下 TEE 中，因而链下隐私计算节点 22 接受到由节点 23n 传输的调用请求，链下隐私计算节点 22 将经过加密的调用请求读入链下 TEE 内，并通过该对称密钥执行解密操作得到上述的调用请求，并进行相关的计算。对称加密采用的加密算法，例如可以包括 DES 算法，3DES 算法，TDEA 算法，Blowfish 算法，RC5 算法，IDEA 算法等。

[84] 当采用非对称加密时，链下隐私计算节点 22 维护有节点非对称密钥的私钥，比如称之为节点私钥，而客户端 21 可以获得该链下隐私计算节点 22 的节点公钥。非对称密钥可由链下隐私计算节点 22 在链下 TEE 内生成，或者由 KMS 服务器分发至该链下隐私计算节点 22，本说明书并不限制密钥来源。类似地，当密钥由 KMS 服务器分发时，KMS 服务器可以在客户端 21 对链下隐私计算节点进行远程证明的过程中，将节点公钥传输至客户端 21 处。那么，客户端 21 可以通过节点公钥对调用请求进行加密，而链下隐私计算节点 22 将节点私钥维护于链下 TEE 中，因而将经过加密的调用请求读入链下 TEE 内，并通过节点私钥执行解密操作得到上述的调用请求。非对称加密采用的非对称加密算法，例如可以包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。

[85] 针对调用请求的加密传输，还可以采用对称加密与非对称加密相结合的形式。客户端 21 可以维护一对称密钥，比如该对称密钥可由客户端 21 随机生成，且客户端 21 可以获得上述节点非对称密钥中的公钥。客户端 21 可以通过对称密钥对调用请求进行加密、得到加密后调用请求，并通过非对称密钥加密该对称密钥、得到加密后密钥，然后客户端 21 同时将加密后挑战交易与加密后密钥传输至链下隐私计算节点 22。相应的，链下隐私计算节点 22 将加密后调用请求与加密后密钥读入链下 TEE 内，首先通过节点私钥对加密后密钥进行解密、得到对称密钥，然后通过对称密钥对加密后调用请求进行解密。相比较而言，对称加密的加解密效率相对更高、但安全性相对较低，而非对称加密的加解密效率相对较低、但安全性相对更高，因此基于对称加密与非对称加密相结合的形式，可以兼顾加解密效率与安全性。

[86] 针对调用请求进行加密时，可以采用对称加密、非对称加密或两者结合的方式，本说明书并不对此进行限制。当采用非对称加密或者对称加密与非对称加密结合的方式时，涉及到一组非对称密钥对，客户端 21 或节点 23n 需要获知该非对称密钥对的公钥，且该非对称密钥对的私钥需要由链下隐私计算节点 22 所维护，使得该链下隐私计算节点 22 可以基于该私钥对收到的调用请求进行解密。例如，该非对称密钥对可以为前文所述的、链下隐私计算节点 22 在链下 TEE 中产生的加密密钥对；相应地，链下隐私计算节点 22 在收到调用请求密文后，将该调用请求密文读入链下 TEE 中，并基于加密私钥对该调用请求密文进行解密，从而得到明文的调用请求。

[87] 类似地，在其他数据交互的过程中，通过使得数据发送方与数据接收方之间维护相同的对称密钥，或者使得数据发送方维护有非对称密钥的公钥、数据接收方维护有非

对称密钥的私钥，或者结合对称加密与非对称加密的形式，可以实现任意的数据发送方与数据接收方之间的数据加密传输，此处不再赘述。

[88] 链下隐私计算节点可能属于链下隐私计算集群，该链下隐私计算集群包含多个链下隐私计算节点。如果各个链下隐私计算节点之间完全独立，那么客户端与单个链下隐私计算节点之间的交互过程可以参考上文所述的实施例。而另一种方式下，链下隐私计算集群可以包含一控制节点，并由该控制节点对集群内的所有链下隐私计算节点进行统一管理。比如，客户端可以向控制节点发送调用请求，并接收控制节点返回的上述链下隐私计算节点的链下隐私计算结果。与前述实施例相类似的，客户端可以向控制节点发送调用请求，或者客户端可以向区块链节点提交交易，该交易所含的调用请求由区块链节点通过预言机机制传输至控制节点，使得控制节点向客户端返回由链下隐私计算节点的发送的链下隐私计算结果。

[89] 以图 3 所示的场景为例。一种情况下，客户端 31 可以通过链下渠道直接向控制节点 32 发送调用请求。另一种情况下，客户端 31 可以通过区块链网络 33 向控制节点 32 提交交易，即客户端 31 向控制节点 32 发送链上交易，区块链网络 33 可以根据该交易获得调用请求，并通过预言机机制将调用请求传输至控制节点 32。链上调用请求过程可以包括三个步骤：步骤①，客户端 31 向区块链网络 33 提交一笔交易，该交易可由区块链网络 33 内的某一节点例如节点 33n 接收并执行，从而由区块链节点 33n 获得经过加密的调用请求；步骤②，节点 33n 调用预先部署的预言机智能合约（简称预言机合约），该预言机合约可以将上述调用请求传递至链下的预言机服务器 34，比如预言机合约可以产生包含该调用请求的事件，而预言机服务器 34 可以通过监听预言机合约产生的事件，从而获取上述的调用请求；步骤③，预言机服务器 34 将调用请求通过链下渠道发送至控制节点 32。

[90] 客户端 31 可以直接向控制节点 32 发送调用请求，即发送调用请求的过程与区块链网络无关，这样可以跳过区块链节点之间的共识过程、减少链上链下的交互操作，使得客户端 31 向控制节点 32 的发送调用请求具有更高的操作效率。再例如，客户端 31 可以采用链上的形式，比如客户端 31 可以向区块链节点提交交易，该交易所含的调用请求可由区块链节点通过预言机机制传输至控制节点。

[91] 控制节点接收到上述调用请求，该调用请求中可以将目标节点设定为控制节点 32 所处集群内的某一链下隐私计算节点，比如链下隐私计算节点 32n，那么控制节点 32 将接收到的调用请求转发至链下隐私计算节点 32n，与上述实施例类似的，客户端 31 或者节点 33n 在针对调用请求进行加密时，只需要确保该链下隐私计算节点 32n 能够解密即可，例如，可以采用该链下隐私计算节点 32n 在链下 TEE 内生成的加密公钥对调用请求进行加密，而链下隐私计算节点 32n 在收到调用请求密文后，可以在链下 TEE 内通过加密私钥对该调用请求密文进行解密，从而获得该调用请求。或者，客户端 31 或节点 33n 也可以不设定调用请求中的目标节点，而调用请求可以采用控制节点 32 所处集群内的某一链下隐私计算节点在链下 TEE 内生成的加密公钥对调用请求进行加密，那么控制节点 32 将接收到该调用请求并将其转发至控制节点 32 所处集群内的所有链下隐私计算节点，那么只有维护有对应的加密私钥的链下隐私计算节点可以对该调用请求进行解密。

[92] 以及链下隐私计算节点可能属于链下隐私计算集群，该链下隐私计算集群包含多个链下隐私计算节点。那控制节点 32 在接收到该调用请求后可以根据负载均衡算法从链下隐私计算集群中选取某一链下隐私计算节点，调用请求可以被所述控制节点接收并转发至该链下隐私计算节点。此时，客户端 31 或者节点 33n 在针对调用请求进行加密时，需要采用集群的加密公钥进行加密，从而确保该链下隐私计算集群中的任一链下隐私计算节点都能对该调用请求进行解密。

[93] 而客户端在部署链下合约的过程中，首先将字节码加密传输至控制节点，然后由

控制节点转发至集群内的一个或多个链下隐私计算节点，从而将链下合约的字节码部署至集群内的一个或多个链下隐私计算节点，与前述链下合约的部署过程类似，此处不再赘述。如果部署至多个链下隐私计算节点，那么这些链下隐私计算节点可以同时向外提供针对同一链下合约的调用能力，从而实现并行的链下隐私计算，还可以在多个链下隐私计算节点之间实现负载均衡。

[94] 在链下隐私计算节点属于链下隐私计算集群的情况下，可以为这些链下隐私计算节点生成统一的身份信息，比如称为集群身份信息。集群身份信息可以包括集群加密密钥对和集群签名密钥对，上述的各个链下隐私计算节点均需在各自的链下 TEE 内维护集群加密私钥、集群签名私钥。那么客户端或区块链节点只要使用集群加密公钥对调用请求进行加密，即可确保上述的各个链下隐私计算节点均能够在各自的链下 TEE 内通过集群加密私钥进行解密，从而调用请求。基于集群身份，客户端并不需要关注对方为单个链下隐私计算节点或者链下隐私计算集群，只需要将其作为一个对象并与该对象进行交互即可，无需关注于背后的节点或集群的细节。

[95] 除了链下隐私计算节点可以存在统一的集群身份之外，可以为链下隐私计算节点上部署的链下合约生成合约身份。当集群内存在多个链下隐私计算节点时，每个链下隐私计算节点可以为自身已部署的链下合约建立合约身份，且不同链下隐私计算节点针对同一链下合约生成的合约身份相同。例如，链下隐私计算节点可以根据统一的集群身份和链下合约的合约 ID，为链下合约生成相应的合约身份，由于集群身份相同、而不同链下合约的合约 ID 必然不同，因而可以确保：同一链下隐私计算节点上部署的不同链下合约存在不同的合约身份，而不同链下隐私计算节点上部署的同一链下合约存在相同的合约身份。

[96] 合约身份可由合约身份密钥对所定义。例如，合约身份可以包括合约加密密钥对和合约签名密钥对。那么，客户端 31 或节点 33n 除了采用集群身份公钥对调用请求进行加密之外，还可以采用合约加密公钥对调用请求内所含的入参数据的信息进行加密。链下隐私计算节点 32n 在收到针对某一链下合约的调用请求后，采用该链下合约对应的合约加密私钥对调用请求内加密后的入参数据的信息进行解密，从而确保入参数据的信息只能由被调用的链下合约所获得，而不会被其他链下合约获得。以及，在得到调用结果后，链下隐私计算节点 32n 可以通过被调用的链下合约的合约签名私钥对调用结果进行签名，而客户端 31 或节点 33n 可以通过合约签名公钥进行验签，从而确定该调用结果确实是由被调用的链下合约所产生。

[97] 步骤 104，所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[98] 链下隐私计算节点可以在链下 TEE 中对调用请求进行解密得到标识信息和入参数据的信息等其他信息，链下隐私计算节点可以根据标识信息调用预先部署的链下合约的字节码，而在链下可信执行环境中部署有若干执行引擎的情况下，链下隐私计算节点可以根据字节码确定对应的执行引擎，并且通过确定出的执行引擎执行所述字节码以对入参数据进行链下隐私计算。

[99] 在链下隐私计算节点处创建的链下TEE中，可以部署有若干执行引擎，比如EVM、WASM 虚拟机等中的一个或多个，在同时部署了多种执行引擎的情况下，客户端除了在链下隐私计算节点处安全存储链下合约的字节码之外，还可以向链下隐私计算节点指明用于执行该字节码的执行引擎。链下隐私计算节点可以接收客户端发送的与链下合约的字节码相关联的执行引擎指定信息，并根据执行引擎指定信息为字节码设定相应的执行引擎。因而链下隐私计算节点可以在链下 TEE 中根据确定出的执行引擎对入参数据进行链下隐私计算。

[100] 以及本说明书中通过调用链下合约，可以实现用户定义的任何计算逻辑。例如，

链下合约可以用于验证区块链上存储的加密订单数据的金额是否正确，并将验证结果反馈至链上；再例如，链下合约可以用于根据预设算法对多方数据进行安全计算，即安全多方计算，并将计算结果反馈至链上等，此处不再一一赘述。
[101] 步骤 106，所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。
[102] 链下隐私计算节点在链下 TEE 中执行计算得到的链下隐私计算结果可以包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出，链下隐私计算节点可以根据调用请求返回相应的链下隐私计算结果，本说明书中并不对此进行限制。
[103] 在得到链下隐私计算结果后，链下隐私计算节点可以通过链下隐私计算节点的节点签名私钥对计算结果进行签名或者可以采用被调用的链下合约的合约签名私钥对计算结果进行签名，也可以同时采用节点签名私钥和合约签名私钥对链下隐私计算结果进行签名，本说明书中并不对此进行限制。客户端或者区块链节点可以通过节点签名公钥或者合约签名公钥进行验签，从而确定该链下隐私计算结果确实是由链下隐私计算节点调用相应的链下合约所产生，并且该计算结果没有被篡改。
[104] 在调用请求中还包括指定对象的身份公钥的信息的情况下，链下隐私计算节点可以采用身份公钥对链下隐私计算结果进行加密，使得只有维护有身份私钥的指定对象才能对该链下隐私计算结果进行解密，可以限制能够查看链下隐私计算结果的用户，而其他用户直接查看链下隐私计算结果时仅能够获得加密后的链下隐私计算结果，从而保证了链下隐私计算结果的隐私保护。
[105] 链下隐私计算节点除了对链下隐私计算结果进行反馈之外，链下隐私计算节点还可以对接收到的调用请求进行哈希运算得到第一哈希值，链下隐私计算节点将第一哈希值与上述链下隐私计算结果进行关联反馈。客户端或者区块链节点将接收到的第一哈希值与生成的调用请求的第二哈希值进行比较，根据比较结果确定链下隐私计算结果是否可靠。
[106] 若第一哈希值与第二哈希值的比较结果不一致，则表明与该第一哈希值关联反馈的链下隐私计算结果不可靠；若第一哈希值与第二哈希值的比较结果一致，则需要进一步验证链下隐私计算节点或者被调用合约的签名等其他参考信息，在参考信息均正确的情况下，才能确定该链下隐私计算结果可靠。
[107] 在一种情况下，链下隐私计算节点可以通过链下渠道将链下隐私计算结果反馈至客户端或者是数据需求方，即链下隐私计算节点反馈链下隐私计算结果的过程与区块链网络无关，使得链下隐私计算节点直接向客户端或者数据需求方反馈链下隐私计算结果，具有更高的效率。在链下隐私计算节点属于链下隐私计算集群的情况下，链下隐私计算节点可以将链下隐私计算结果发送至控制节点，并由控制节点通过链下渠道将链下隐私计算结果反馈至客户端。此外，客户端在接受到链下隐私计算节点反馈的链下隐私计算结果后，客户端还可以向区块链节点发起存证交易，该存证交易中包含链下隐私计算结果，使得区块链节点将客户端提交的存证交易与其他节点进行共识后上链。
[108] 在另一种情况下，链下隐私计算节点可以通过预言机机制将链下隐私计算结果传输至区块链节点，或者，链下隐私计算节点可以先将链下隐私计算结果发送至控制节点，并由控制节点通过预言机机制将链下隐私计算结果传输至区块链节点。
[109] 区块链节点可以根据计算结果对区块链账本数据进行更新，可以对计算结果进行固化存证，而且可以支持针对该计算结果的后期验证。同时，相比于区块链节点在执行链上合约后所产生的上链数据而言，基于链下合约产生的计算结果本身相对更加简短，因而将该计算结果上链时，有助于节省链上存储空间。
[110] 区块链节点根据计算结果更新区块链账本数据，或者称为对计算结果进行上链，其方式可以包括：生成一笔区块链交易，将计算结果添加至交易的 data 字段，当该区块链交易通过共识后，可被各个区块链节点添加至最新区块的区块体中，从而实现了区块

链账本数据的更新，亦即完成了对该计算结果的上链；或者，区块链节点根据计算结果对相关账户的状态进行更新，该相关账户譬如可以为用户对应的外部账户或者链上合约对应的合约账户，该相关账户的状态更新会导致状态树（state tree）的树根发生取值变化，而该状态树的树根会被包含于最新区块的区块头，从而实现了区块链账本数据的更新，亦即相当于将该计算结果上链。

[111] 由以上技术方案可见，本说明书提出了在链下隐私计算节点处预先部署了链下合约的字节码的情况下，可以通过链下隐私计算节点调用链下合约的字节码在链下 TEE 中执行计算操作，并且链下隐私计算节点可以通过链下隐私计算节点的节点签名私钥对计算结果进行签名或者可以采用被调用的链下合约的合约签名私钥对计算结果进行签名，从而可以确定链下隐私计算结果确实是由链下隐私计算节点调用相应的链下合约所产生，并且可验证计算结果没有被篡改，可以保证链下隐私计算结果的安全性和可靠性；同时，区块链节点无需执行计算操作，只需要从链下隐私计算节点处获得计算结果并且基于该计算结果更新区块链账本数据，可以降低区块链网络的资源消耗。

[112] 对应于上述链下隐私节点侧的实施例，本说明书还提出了客户端侧、区块链节点侧、控制节点侧等其他方面的实施例，在链下隐私计算节点侧实施例中所涉及的描述同样可以适用于这些侧的实施例，下文中不再对此进行赘述。

[113] 相应地，图 4 是一示例性实施例提供的一种客户端侧的调用合约的方法的流程图。如图 4 所示，该方法可以包括步骤 402~步骤 404。

[114] 步骤 402，客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息。

[115] 如前所述，客户端向区块链节点提交交易，交易触发区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点；其中，链下隐私计算节点产生的链下隐私计算结果被反馈至区块链节点，链下隐私计算结果用于驱动区块链节点更新区块链账本数据。

[116] 步骤 404，客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[117] 如前所述，客户端可以向链下隐私计算节点直接发起链下调用请求。客户端可以向区块链节点发起存证交易，存证交易包含链下隐私计算结果。

[118] 如前所述，客户端直接向链下隐私计算节点发送经过加密的调用请求；或者，在链下隐私计算节点属于链下隐私计算集群的情况下，客户端向链下隐私计算集群的控制节点发送经过加密的调用请求，以由控制节点转发调用请求。

[119] 如前所述，调用请求由节点非对称密钥对的公钥进行加密后传输，且节点非对称密钥对的私钥被链下隐私计算节点所维护。

[120] 如前所述，在链下隐私计算节点属于链下隐私计算集群的情况下，节点非对称密钥对的私钥仅被链下隐私计算节点所维护，或者节点非对称密钥对的私钥被链下隐私计算集群内的所有链下隐私计算节点共同维护。

[121] 如前所述，客户端获取链下隐私计算节点的远程证明报告，远程证明报告由认证服务器对链下隐私计算节点产生的自荐信息进行验证后生成，自荐信息与链下隐私计算节点上创建的链下可信执行环境相关；客户端根据远程证明报告确定链下隐私计算节点可信的情况下，向链下隐私计算节点发送经过加密的调用请求。

[122] 如前所述，入参数据的信息可以由合约非对称密钥对的公钥进行加密，合约非对称密钥由链下隐私计算节点在链下可信执行环境内预先生成且对应于链下合约的身份。客户端可以采用所述合约非对称密钥对的公钥对入参数据的信息进行加密后传输。

[123] 如前所述，不同链下隐私计算节点针对链下合约生成的合约非对称密钥对不同；

或者，不同链下隐私计算节点针对链下合约生成的合约非对称密钥对相同。

[124] 如前所述，客户端向调用请求中添加指定对象的身份公钥的信息；客户端接收链下隐私计算节点采用身份公钥对执行结果进行加密后返回的结果密文。

[125] 如前所述，客户端向调用请求中添加函数信息，函数信息用于指示所述链下隐私计算节点用于调用链下合约中对应于函数信息的的字节码。

[126] 如前所述，链下隐私计算结果包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出。

[127] 如前所述，客户端接收到链下隐私计算节点对调用请求进行哈希运算得到的第一哈希值与链下隐私计算结果；客户端生成调用请求的第二哈希值，并将第一哈希值与第二哈希值进行比较；客户端根据比较结果确定所述链下隐私计算结果是否可靠。

[128] 如前所述，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

[129] 相应地，图 5 是一示例性实施例提供的一种区块链节点侧的调用合约的方法的流程图。如图 5 所示，该方法可以包括步骤 502~步骤 506。

[130] 步骤 502，区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息。

[131] 如前所述，区块链节点从客户端提交的交易中提取得到调用请求；或者，区块链节点根据客户端提交的交易在自身创建的链上可信执行环境内执行链上合约而生成调用请求。

[132] 如前所述，区块链节点将计算结果直接反馈至客户端；或者，区块链节点根据接收到的计算结果更新区块链账本数据。

[133] 步骤 504，所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[134] 如前所述，区块链节点直接通过预言机机制将经过加密的调用请求传输至链下隐私计算节点；或者，在链下隐私计算节点属于链下隐私计算集群的情况下，区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算集群的控制节点，以由控制节点转发调用请求。

[135] 如前所述，调用请求由节点非对称密钥对的公钥进行加密后传输，且非对称密钥对的私钥被链下隐私计算节点所维护。

[136] 如前所述，在链下隐私计算节点属于链下隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被链下隐私计算节点所维护，或者节点非对称密钥对的私钥被链下隐私计算集群内的所有链下隐私计算节点共同维护。

[137] 如前所述，入参数据的信息由合约非对称密钥对的公钥进行加密，合约非对称密钥由链下隐私计算节点在链下可信执行环境内预先生成且对应于链下合约的身份。

[138] 步骤 506，所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。

[139] 如前所述，在调用请求中还包括所述指定对象的身份公钥的信息的情况下，区块链节点接收到链下隐私计算节点采用身份公钥对执行结果进行加密后返回的计算结果密文。

[140] 如前所述，区块链节点接收到链下隐私计算节点对调用请求进行哈希运算得到的第一哈希值与链下隐私计算结果；区块链节点将第一哈希值与链下隐私计算结果反馈至请求方，第一哈希值用于与请求方生成的调用请求的第二哈希值进行比较，比较结果用于确定链下隐私计算结果是否可靠。

[141] 如前所述，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

[142] 相应地，图 6 是一示例性实施例提供的一种控制节点侧的调用合约的方法的流程图。如图 6 所示，该方法可以包括步骤 602~步骤 606。

[143] 步骤 602，控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息。

[144] 如前所述，控制节点接收到区块链节点通过预言机机制传输的调用请求；或者，控制节点接收客户端直接发送的链下调用请求。

[145] 如前所述，调用请求由节点非对称密钥对的公钥进行加密后传输，且非对称密钥对的私钥被链下隐私计算节点所维护。

[146] 步骤 604，所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点。

[147] 如前所述，节点非对称密钥对的私钥可以仅被所述链下隐私计算节点所维护。在经过加密的调用请求的目标节点被设定为链下隐私计算节点的情况下，控制接节点将调用请求转发至链下隐私计算节点；在经过加密的调用请求的目标节点未设定的情况下，控制节点将调用请求转发至链下隐私计算集群中的所有链下隐私计算节点。

[148] 如前所述，节点非对称密钥对的私钥可以被链下隐私计算集群内的所有链下隐私计算节点共同维护。控制节点根据负载均衡算法从链下隐私计算集群中选取链下隐私计算节点，并将调用请求转发至链下隐私计算节点。

[149] 步骤 606，所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。

[150] 如前所述，控制节点直接将链下隐私计算结果反馈至客户端；或者，控制节点通过预言机机制对链下隐私计算结果进行反馈。

[151] 如前所述，控制节点接收到链下隐私计算节点对调用请求进行哈希运算得到的第一哈希值与链下隐私计算结果；控制节点将第一哈希值与链下隐私计算结果转发至请求方，第一哈希值用于与请求方生成的调用请求的第二哈希值进行比较，比较结果用于确定链下隐私计算结果是否可靠。

[152] 如前所述，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

[153] 在本说明书的技术方案中，还可由客户端直接与链下隐私计算节点或者控制节点进行交互以完成在隐私计算节点上部署智能合约、向智能合约发起挑战、验证智能合约和调用智能合约等操作，而无需通过区块链的预言机机制来完成上述操作，同时调用部署于隐私计算节点的智能合约得到的计算结果也无需反馈至区块链。在该情况下，由于不涉及链上和链下的区分，下文将“链下隐私计算节点”称为“隐私计算节点”，将“链下可信执行环境”称为“可信执行环境”，将“链下合约”称为“智能合约”。但是，技术方案的原理与上述实施例类似，所涉及的实施细节同样可参考上述实施例，因此下文不再进行详细描述。

[154] 相应地，图 7 是一示例性实施例提供的一种隐私计算节点侧的智能合约的调用方法的流程图。如图 7 所示，该方法可以包括步骤 702~步骤 706。

[155] 步骤 702，隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息。

[156] 如前所述，所述隐私计算节点直接从客户端处接收到经过加密的调用请求；或者，在所述隐私计算节点属于隐私计算集群的情况下，所述隐私计算节点接收所述隐私计算集群的控制节点转发的经过加密的调用请求。

[157] 如前所述，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。

[158] 如前所述，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护；在所述经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算集群中的所有隐私计算节点。

[159] 如前所述，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护；所述隐私计算节点被所述控制节点根据负载均衡算法从所述隐私计算集群中选取，且所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算节点。

[160] 步骤 704，所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

[161] 如前所述，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

[162] 步骤 706，所述隐私计算节点在可信执行环境中对得到的隐私计算结果进行加密并反馈。

[163] 如前所述，所述隐私计算节点对所述调用请求进行哈希运算得到第一哈希值；所述隐私计算节点将所述第一哈希值与隐私计算结果关联反馈，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，所述比较结果用于确定所述隐私计算结果是否可靠。

[164] 相应地，图 8 是一示例性实施例提供的一种客户端侧的智能合约的调用方法的流程图。如图 8 所示，该方法可以包括步骤 802~步骤 804。

[165] 步骤 802，客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息。

[166] 如前所述，所述客户端直接向隐私计算节点发送经过加密的调用请求；或者，在所述隐私计算节点属于隐私计算集群的情况下，所述客户端向所述隐私计算集群的控制节点发送经过加密的调用请求，以由所述控制节点转发所述调用请求。

[167] 如前所述，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。

[168] 如前所述，在所述隐私计算节点属于隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护。

[169] 步骤 804，所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

[170] 如前所述，所述客户端接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果；所述客户端生成所述调用请求的第二哈希值，并将所述第一哈希值与所述第二哈希值进行比较；所述客户端根据比较结果确定所述隐私计算结果是否可靠。

[171] 如前所述，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

[172] 相应地，图 9 是一示例性实施例提供的一种控制节点侧的智能合约的调用方法的流程图。如图 9 所示，该方法可以包括步骤 902~步骤 906。

[173] 步骤 902，控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息。

[174] 如前所述，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述隐私计算节点所维护。

[175] 如前所述，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护；所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点，包括：在经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述控制接节点将所述调用请求转发至所述隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，所述控制节点将所述调用请求转发至所述隐私计算集群中的所有隐私计算节点。

[176] 如前所述，所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护；所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点，包括：所述控制节点根据负载均衡算法从所述隐私计算集群中选取所述隐私计算节点，并将所述调用请求转发至所述隐私计算节点。

[177] 步骤 904，所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点。

[178] 如前所述，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

[179] 步骤 906，所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

[180] 如前所述，所述控制节点接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果；所述控制节点将所述第一哈希值与所述隐私计算结果转发至请求方，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述隐私计算结果是否可靠。

[181] 图 10 是一示例性实施例提供的一种设备的示意结构图。请参考图 10，在硬件层面，该电子设备包括处理器 1002、内部总线 1004、网络接口 1006、内存 1008 以及非易失性存储器 1010，当然还可能包括其他业务所需要的硬件。处理器 1002 从非易失性存储器 1010 中读取对应的计算机程序到内存 1008 中然后运行，在逻辑层面上形成命令的调用合约的装置。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[182] 请参考图 11，在链下隐私计算节点侧的软件实施方式中，该调用合约的装置可以包括：接收与解密单元 1102，使链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息；调用与执行单元 1104，使所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；反馈单元 1106，使所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。

[183] 可选的，接收与解密单元 1102 具体用于：使所述链下隐私计算节点接收到区块链节点通过预言机机制传输的调用请求；使所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈，包括：所述链下计算节点通过预言机机制对所述链下隐私计算结果进行反馈。

[184] 可选的，接收与解密单元 1102 具体用于：使所述经过加密的调用请求由所述区块链节点从所述客户端提交的交易中提取得到；或者，使所述经过加密的调用请求由所述区块链节点根据所述客户端提交的交易在自身创建的链上可信执行环境内执行链上合约而生成。

[185] 可选的，接收与解密单元 1102 具体用于：使所述链下隐私计算节点接收到客户端直接发起的链下调用请求；使所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈，包括：所述链下计算节点将所述链下隐私计算结果直

接反馈给客户端。

[186] 可选的，接收与解密单元 1102 具体用于：使所述链下隐私计算节点直接从请求方处接收到经过加密的调用请求；或者，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述链下隐私计算节点接收所述链下隐私计算集群的控制节点转发的经过加密的调用请求。

[187] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述链下隐私计算节点所维护。

[188] 可选的，所述链下隐私计算节点属于链下隐私计算集群，且所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护；在所述经过加密的调用请求的目标节点被设定为所述链下隐私计算节点的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述链下隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述链下隐私计算集群中的所有链下隐私计算节点。

[189] 可选的，所述链下隐私计算节点属于链下隐私计算集群，且所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护；所述链下隐私计算节点被所述控制节点根据负载均衡算法从所述链下隐私计算集群中选取，且所述经过加密的调用请求被所述控制节点接收并转发至所述链下隐私计算节点。

[190] 可选的，所述链下可信执行环境中部署有若干执行引擎；所述装置还包括：引擎确定单元 1108，使所述链下隐私计算节点确定所述字节码对应的执行引擎；引擎执行单元 1110，所述链下隐私计算节点通过确定出的执行引擎执行所述字节码。

[191] 可选的，还包括：远程证明报告提供单元 1112，使所述链下隐私计算节点向请求方提供远程证明报告，所述远程证明报告由认证服务器对所述链下隐私计算节点产生的自荐信息进行验证后生成，所述自荐信息与所述链下隐私计算节点上创建的链下可信执行环境相关；其中，所述调用请求由所述客户端在根据所述远程证明报告确定所述链下隐私计算节点可信的情况下发起。

[192] 可选的，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份；所述装置还包括：入参数据信息解密单元 1114，所述链下隐私计算节点根据所述合约非对称密钥对的私钥，在所述链下可信执行环境中解密得到所述入参数据的信息。

[193] 可选的，不同的链下隐私计算节点针对所述链下合约生成的合约非对称密钥对不同；或者，不同的链下隐私计算节点针对所述链下合约生成的合约非对称密钥对相同。

[194] 可选的，所述调用请求还包括指定对象的身份公钥的信息，反馈单元 1106 具体用于：使所述链下隐私计算节点根据所述身份公钥对所述执行结果进行加密后反馈。

[195] 可选的，所述调用请求还包含函数信息，调用与执行单元 1104 具体用于：使所述链下隐私计算节点调用所述链下合约中对应于所述函数信息的字节码。

[196] 可选的，所述链下隐私计算结果包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出。

[197] 可选的，还包括：运算单元 1116，使所述链下隐私计算节点对所述调用请求进行哈希运算得到第一哈希值；关联反馈单元 1118，使所述链下隐私计算节点将所述第一哈希值与所述链下隐私计算结果关联反馈，所述第一哈希值用于与请求方生成的所述调用请求的第二哈希值进行比较，所述比较结果用于确定所述链下隐私计算结果是否可靠。

[198] 可选的，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

[199] 请参考图 12，在客户端侧的软件实施方式中，该调用合约的装置可以包括：生成单元 1202，使客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据

的信息；发送单元 1204，使所述客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

[200] 可选的，发送单元 1204 具体用于：使所述客户端向区块链节点提交交易，所述交易触发所述区块链节点通过预言机机制将经过加密的调用请求传输至所述链下隐私计算节点；其中，所述链下隐私计算节点产生的链下隐私计算结果被反馈至所述区块链节点，所述链下隐私计算结果用于驱动所述区块链节点更新区块链账本数据。

[201] 可选的，使所述客户端向所述链下隐私计算节点直接发起链下调用请求；可选的，还包括：交易发起模块 1206，使所述客户端向所述区块链节点发起存证交易，所述存证交易包含所述链下隐私计算结果。

[202] 可选的，发送单元 1204 具体用于：使所述客户端直接向链下隐私计算节点发送经过加密的调用请求；或者，在所述链下隐私计算节点属于链下隐私计算集群的情况下，使所述客户端向所述链下隐私计算集群的控制节点发送经过加密的调用请求，以由所述控制节点转发所述调用请求。

[203] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述链下隐私计算节点所维护。

[204] 可选的，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

[205] 可选的，还包括：远程证明报告获取单元 1208，使所述客户端获取所述链下隐私计算节点的远程证明报告，所述远程证明报告由认证服务器对所述链下隐私计算节点产生的自荐信息进行验证后生成，所述自荐信息与所述链下隐私计算节点上创建的链下可信执行环境相关；使所述客户端根据所述远程证明报告确定所述链下隐私计算节点可信的情况下，向所述链下隐私计算节点发送经过加密的调用请求。

[206] 可选的，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份；所述装置还包括：入参数据信息加密单元 1210，使所述客户端采用所述合约非对称密钥对的公钥对所述入参数据的信息进行加密后传输。

[207] 可选的，不同链下隐私计算节点针对所述链下合约生成的合约非对称密钥对不同；或者，不同链下隐私计算节点针对所述链下合约生成的合约非对称密钥对相同。

[208] 可选的，还包括：身份公钥信息添加单元 1212，使客户端向调用请求中添加指定对象的身份公钥的信息，使客户端接收所述链下隐私计算节点采用所述身份公钥对所述执行结果进行加密后返回的结果密文。

[209] 可选的，还包括：函数信息添加单元 1214，使客户端向调用请求中添加函数信息，所述函数信息用于指示所述链下隐私计算节点用于调用所述链下合约中对应于所述函数信息的的字节码。

[210] 可选的，所述链下隐私计算结果包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出。

[211] 可选的，还包括：运算结果接收单元 1216，使所述客户端接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果；比较单元 1218，使所述客户端生成所述调用请求的第二哈希值，并将所述第一哈希值与所述第二哈希值进行比较；结果确定单元 1220，使所述客户端根据比较结果确定所述链下隐私计算结果是否可靠。

[212] 可选的，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括

所述链下合约中定义的合约状态的历史状态取值。
[213] 请参考图 13，在区块链节点侧的软件实施方式中，该调用合约的装置可以包括：获取单元 1302，使区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；传输单元 1304，使所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；接收单元 1306，使所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。
[214] 可选的，获取单元 1302 具体用于：使区块链节点从所述客户端提交的交易中提取得到调用请求；或者，使所述区块链节点根据所述客户端提交的交易在自身创建的链上可信执行环境内执行链上合约而生成调用请求。
[215] 可选的，还包括：直接反馈单元 1308，使所述区块链节点将所述计算结果直接反馈至客户端；或者，更新单元 1310，使所述区块链节点根据接收到的所述计算结果更新区块链账本数据。
[216] 可选的，传输单元 1304 具体用于：使区块链节点直接通过预言机机制将经过加密的调用请求传输至链下隐私计算节点；或者，在所述链下隐私计算节点属于链下隐私计算集群的情况下，使所述区块链节点通过预言机机制将经过加密的调用请求传输至所述链下隐私计算集群的控制节点，以由所述控制节点转发所述调用请求。
[217] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述链下隐私计算节点所维护。
[218] 可选的，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。
[219] 可选的，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份。
[220] 可选的，接收单元 1306 具体用于：在所述调用请求中还包括所述指定对象的身份公钥的信息的情况下，使所述区块链节点接收到所述链下隐私计算节点采用所述身份公钥对所述执行结果进行加密后返回的计算结果密文。
[221] 可选的，还包括：运算结果接收单元 1312，使所述区块链节点接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果；结果反馈单元 1314，使所述区块链节点将所述第一哈希值与所述链下隐私计算结果反馈至请求方，所述第一哈希值用于与所述请求方生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述链下隐私计算结果是否可靠。
[222] 可选的，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。
[223] 请参考图 14，在控制节点侧的软件实施方式中，该调用合约的装置可以包括：接收单元 1402，使控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；转发单元 1404，使所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点；反馈单元 1406，使所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。
[224] 可选的，接收单元 1402 具体用于：所述控制节点接收到区块链节点通过预言机机制传输的调用请求；或者，所述控制节点接收所述客户端直接发送的链下调用请求。
[225] 可选的，还包括：直接反馈单元 1408，使所述控制节点直接将所述链下隐私计算结果反馈至所述客户端；或者，预言机机制反馈单元 1410，使所述控制节点通过预言机

机制对所述链下隐私计算结果进行反馈。
[226] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述链下隐私计算节点所维护。
[227] 可选的，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护，转发单元 1404 具体用于：在经过加密的调用请求的目标节点被设定为所述链下隐私计算节点的情况下，使所述控制接节点将所述调用请求转发至所述链下隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，使所述控制节点将所述调用请求转发至所述链下隐私计算集群中的所有链下隐私计算节点。
[228] 可选的，所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护，转发单元 1404 具体用于：使所述控制节点根据负载均衡算法从所述链下隐私计算集群中选取所述链下隐私计算节点，并将所述调用请求转发至所述链下隐私计算节点。
[229] 可选的，还包括：结果接收单元 1412，使所述控制节点接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果；结果转发单元 1414，使所述控制节点将所述第一哈希值与所述链下隐私计算结果转发至请求方，所述第一哈希值用于与请求方生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述链下隐私计算结果是否可靠。
[230] 可选的，在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。
[231] 请参考图 15，在隐私计算节点侧的软件实施方式中，该智能合约的调用装置可以包括：接收与解密单元 1502，使隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息；调用与计算单元 1504，使所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算；加密与反馈单元 1506，使所述隐私计算节点在可信执行环境中对得到的隐私计算结果进行加密并反馈。
[232] 可选的，所述接收与解密单元 1502 具体用于：使所述隐私计算节点直接从客户端处接收到经过加密的调用请求；或者，在所述隐私计算节点属于隐私计算集群的情况下，所述隐私计算节点接收所述隐私计算集群的控制节点转发的经过加密的调用请求。
[233] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。
[234] 可选的，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护；在所述经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算集群中的所有隐私计算节点。
[235] 可选的，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护；所述隐私计算节点被所述控制节点根据负载均衡算法从所述隐私计算集群中选取，且所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算节点。
[236] 可选的，还包括：哈希运算单元 1508，所述隐私计算节点对所述调用请求进行哈希运算得到第一哈希值；比较单元 1510，所述隐私计算节点将所述第一哈希值与隐私计算结果关联反馈，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，所述比较结果用于确定所述隐私计算结果是否可靠。
[237] 可选的，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

[238] 请参考图 16，在客户端侧的软件实施方式中，该智能合约的调用装置可以包括：生成调用请求单元 1602，使客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；发送调用请求单元 1604，使所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

[239] 可选的，发送调用请求单元 1604 具体用于：使所述客户端直接向隐私计算节点发送经过加密的调用请求；或者，在所述隐私计算节点属于隐私计算集群的情况下，使所述客户端向所述隐私计算集群的控制节点发送经过加密的调用请求，以由所述控制节点转发所述调用请求。

[240] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。

[241] 可选的，在所述隐私计算节点属于隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护。

[242] 可选的，还包括：运算结果接收单元 1606，使得所述客户端接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果；比较单元 1608，所述客户端生成所述调用请求的第二哈希值，并将所述第一哈希值与所述第二哈希值进行比较；结果确定单元 1610，所述客户端根据比较结果确定所述隐私计算结果是否可靠。

[243] 可选的，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

[244] 请参考图 17，在控制节点侧的软件实施方式中，该智能合约的调用装置可以包括：接收调用请求单元 1702，使控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息；转发调用请求单元 1704，使所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点；反馈隐私计算结果单元 1706，使所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

[245] 可选的，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述隐私计算节点所维护。

[246] 可选的，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护，转发调用请求单元 1704 具体用于：在经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述控制接节点将所述调用请求转发至所述隐私计算节点；在所述经过加密的调用请求的目标节点未设定的情况下，所述控制节点将所述调用请求转发至所述隐私计算集群中的所有隐私计算节点。

[247] 可选的，所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护，转发调用请求单元 1704 具体用于：所述控制节点根据负载均衡算法从所述隐私计算集群中选取所述隐私计算节点，并将所述调用请求转发至所述隐私计算节点。

[248] 可选的，还包括：接收单元 1708，使所述控制节点接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果；结果转发单元 1710，使所述控制节点将所述第一哈希值与所述隐私计算结果转发至请求方，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述隐私计算结果是否可靠。

[249] 可选的，在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

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

[251] 在一个典型的配置中，计算机包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[252] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

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

[254] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[255] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[256] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[257] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[258] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1、一种调用合约的方法，包括:

链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息;

所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算;

所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。

2、根据权利要求 1 所述的方法，所述链下隐私计算节点接收到经过加密的调用请求，包括: 所述链下隐私计算节点接收到区块链节点通过预言机机制传输的调用请求;

所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈，包括: 所述链下计算节点通过预言机机制对所述链下隐私计算结果进行反馈。

3、根据权利要求 2 所述的方法，所述链下隐私计算节点接收到区块链节点通过预言机机制传输的调用请求，包括:

所述经过加密的调用请求由所述区块链节点从客户端提交的交易中提取得到; 或者，

所述经过加密的调用请求由所述区块链节点根据所述客户端提交的交易在自身创建的链上可信执行环境内执行链上合约而生成。

4、根据权利要求 1 所述的方法，所述链下隐私计算节点接收到经过加密的调用请求，包括: 所述链下隐私计算节点接收到客户端直接发起的链下调用请求;

所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈，包括: 所述链下计算节点将所述链下隐私计算结果直接反馈给客户端。

5、根据权利要求 1 所述的方法，所述链下隐私计算节点接收到经过加密的调用请求，包括:

所述链下隐私计算节点直接从请求方处接收到经过加密的调用请求; 或者，

在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述链下隐私计算节点接收所述链下隐私计算集群的控制节点转发的经过加密的调用请求。

6、根据权利要求 1 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述链下隐私计算节点所维护。

7、根据权利要求 6 所述的方法，所述链下隐私计算节点属于链下隐私计算集群，且所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护;

在所述经过加密的调用请求的目标节点被设定为所述链下隐私计算节点的情况下，所述经过加密的调用请求被所述链下隐私计算集群的控制节点接收并转发至所述链下隐私计算节点;

在所述经过加密的调用请求的目标节点未设定的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述链下隐私计算集群中的所有链下隐私计算节点。

8、根据权利要求 6 所述的方法，所述链下隐私计算节点属于链下隐私计算集群，且所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护;

所述链下隐私计算节点被所述链下隐私计算集群的控制节点根据负载均衡算法从所述链下隐私计算集群中选取，且所述经过加密的调用请求被所述控制节点接收并转发至所述链下隐私计算节点。

9、根据权利要求 1 所述的方法，所述链下可信执行环境中部署有若干执行引擎; 所述方法还包括:

所述链下隐私计算节点确定所述字节码对应的执行引擎;

所述链下隐私计算节点通过确定出的执行引擎执行所述字节码。

10、根据权利要求 1 所述的方法，还包括:

所述链下隐私计算节点向请求方提供远程证明报告，所述远程证明报告由认证服务器对所述链下隐私计算节点产生的自荐信息进行验证后生成，所述自荐信息与所述链下隐私计算节点上创建的链下可信执行环境相关；

其中，所述调用请求由客户端在根据所述远程证明报告确定所述链下隐私计算节点可信的情况下发起。

11、根据权利要求 1 所述的方法，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份；所述方法还包括：

所述链下隐私计算节点根据所述合约非对称密钥对的私钥，在所述链下可信执行环境中解密得到所述入参数据的信息。

12、根据权利要求 11 所述的方法，

不同的链下隐私计算节点针对所述链下合约生成的合约非对称密钥对不同；或者，

不同的链下隐私计算节点针对所述链下合约生成的合约非对称密钥对相同。

13、根据权利要求 1 所述的方法，所述调用请求还包括指定对象的身份公钥的信息；所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈，包括：

所述链下隐私计算节点根据所述身份公钥对所述执行结果进行加密后反馈。

14、根据权利要求 1 所述的方法，所述调用请求还包含函数信息；所述链下隐私计算节点调用所述链下合约的字节码，包括：

所述链下隐私计算节点调用所述链下合约中对应于所述函数信息的字节码。

15、根据权利要求 1 所述的方法，所述链下隐私计算结果包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出。

16、根据权利要求 1 所述的方法，还包括：

所述链下隐私计算节点对所述调用请求进行哈希运算得到第一哈希值；

所述链下隐私计算节点将所述第一哈希值与所述链下隐私计算结果关联反馈，所述第一哈希值用于与请求方生成的所述调用请求的第二哈希值进行比较，所述比较结果用于确定所述链下隐私计算结果是否可靠。

17、根据权利要求 1 所述的方法，还包括：

在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

18、一种调用合约的方法，包括：

客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；

所述客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

19、根据权利要求 18 所述的方法，所述客户端向链下隐私计算节点发送经过加密的调用请求，包括：

所述客户端向区块链节点提交交易，所述交易触发所述区块链节点通过预言机机制将经过加密的调用请求传输至所述链下隐私计算节点；

其中，所述链下隐私计算节点产生的链下隐私计算结果被反馈至所述区块链节点，所述链下隐私计算结果用于驱动所述区块链节点更新区块链账本数据。

20、根据权利要求 18 所述的方法，所述客户端向链下隐私计算节点发送经过加密的调用请求，包括：所述客户端向所述链下隐私计算节点直接发起链下调用请求；所述方法还包括：

所述客户端向区块链节点发起存证交易，所述存证交易包含所述链下隐私计算结果。

21、根据权利要求 18 所述的方法，所述客户端向链下隐私计算节点发送经过加密的调用

请求，包括:

所述客户端直接向链下隐私计算节点发送经过加密的调用请求；或者，

在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述客户端向所述链下隐私计算集群的控制节点发送经过加密的调用请求，以由所述控制节点转发所述调用请求。

22、根据权利要求 18 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述链下隐私计算节点所维护。

23、根据权利要求 22 所述的方法，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

24、根据权利要求 18 所述的方法，还包括:

所述客户端获取所述链下隐私计算节点的远程证明报告，所述远程证明报告由认证服务器对所述链下隐私计算节点产生的自荐信息进行验证后生成，所述自荐信息与所述链下隐私计算节点上创建的链下可信执行环境相关;

所述客户端根据所述远程证明报告确定所述链下隐私计算节点可信的情况下，向所述链下隐私计算节点发送经过加密的调用请求。

25、根据权利要求 18 所述的方法，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份；所述方法还包括:

所述客户端采用所述合约非对称密钥对的公钥对所述入参数据的信息进行加密后传输。

26、根据权利要求 25 所述的方法，

不同链下隐私计算节点针对所述链下合约生成的合约非对称密钥对不同；或者，

不同链下隐私计算节点针对所述链下合约生成的合约非对称密钥对相同。

27、根据权利要求 18 所述的方法，还包括:

客户端向调用请求中添加指定对象的身份公钥的信息;

客户端接收所述链下隐私计算节点采用所述身份公钥对所述执行结果进行加密后返回的结果密文。

28、根据权利要求 18 所述的方法，还包括:

客户端向调用请求中添加函数信息，所述函数信息用于指示所述链下隐私计算节点用于调用所述链下合约中对应于所述函数信息的的字节码。

29、根据权利要求 18 所述的方法，所述链下隐私计算结果包括以下至少之一：响应码、响应信息、合约调用的返回值、合约调用的过程输出。

30、根据权利要求 18 所述的方法，还包括:

所述客户端接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果;

所述客户端生成所述调用请求的第二哈希值，并将所述第一哈希值与所述第二哈希值进行比较;

所述客户端根据比较结果确定所述链下隐私计算结果是否可靠。

31、根据权利要求 18 所述的方法，还包括:

在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

32、一种调用合约的方法，包括:

区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息;

所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链

下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算;

所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。

33、根据权利要求 32 所述的方法，所述区块链节点获取经过加密的调用请求，包括:

区块链节点从客户端提交的交易中提取得到调用请求；或者，

所述区块链节点根据所述客户端提交的交易在自身创建的链上可信执行环境内执行链上合约而生成调用请求。

34、根据权利要求 32 所述的方法，还包括:

所述区块链节点将所述计算结果直接反馈至客户端；或者，

所述区块链节点根据接收到的所述计算结果更新区块链账本数据。

35、根据权利要求 32 所述的方法，所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，包括:

区块链节点直接通过预言机机制将经过加密的调用请求传输至链下隐私计算节点；或者，

在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述区块链节点通过预言机机制将经过加密的调用请求传输至所述链下隐私计算集群的控制节点，以由所述控制节点转发所述调用请求。

36、根据权利要求 32 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述链下隐私计算节点所维护。

37、根据权利要求 36 所述的方法，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

38、根据权利要求 32 所述的方法，所述入参数据的信息由合约非对称密钥对的公钥进行加密，所述合约非对称密钥由所述链下隐私计算节点在所述链下可信执行环境内预先生成且对应于所述链下合约的身份。

39、根据权利要求 32 所述的方法，所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的计算结果，包括:

在所述调用请求中还包括指定对象的身份公钥的信息的情况下，所述区块链节点接收到所述链下隐私计算节点采用所述身份公钥对所述执行结果进行加密后返回的计算结果密文。

40、根据权利要求 32 所述的方法，还包括:

所述区块链节点接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果;

所述区块链节点将所述第一哈希值与所述链下隐私计算结果反馈至请求方，所述第一哈希值用于与所述请求方生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述链下隐私计算结果是否可靠。

41、根据权利要求 32 所述的方法，还包括:

在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

42、一种调用合约的方法，包括:

控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息;

所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点;

所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。

43、根据权利要求 42 所述的方法，所述控制节点接收到经过加密的调用请求，包括:

所述控制节点接收到区块链节点通过预言机机制传输的调用请求；或者，

所述控制节点接收客户端直接发送的链下调用请求。

44、根据权利要求 42 所述的方法，还包括:

所述控制节点直接将所述链下隐私计算结果反馈至客户端；或者，

所述控制节点通过预言机机制对所述链下隐私计算结果进行反馈。

45、根据权利要求 42 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述链下隐私计算节点所维护。

46、根据权利要求 45 所述的方法，所述节点非对称密钥对的私钥仅被所述链下隐私计算节点所维护；所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点，包括：

在经过加密的调用请求的目标节点被设定为所述链下隐私计算节点的情况下，所述控制接节点将所述调用请求转发至所述链下隐私计算节点；

在所述经过加密的调用请求的目标节点未设定的情况下，所述控制节点将所述调用请求转发至所述链下隐私计算集群中的所有链下隐私计算节点。

47、根据权利要求 42 所述的方法，所述节点非对称密钥对的私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护；所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点，包括：

所述控制节点根据负载均衡算法从所述链下隐私计算集群中选取所述链下隐私计算节点，并将所述调用请求转发至所述链下隐私计算节点。

48、根据权利要求 42 所述的方法，还包括：

所述控制节点接收到所述链下隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述链下隐私计算结果；

所述控制节点将所述第一哈希值与所述链下隐私计算结果转发至请求方，所述第一哈希值用于与请求方生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述链下隐私计算结果是否可靠。

49、根据权利要求 42 所述的方法，还包括：

在所述链下合约为无状态合约的情况下，所述链下合约的入参数据包括所述链下合约中定义的合约状态的历史状态取值。

50、一种调用合约的方法，包括：

隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息；

所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算；

所述隐私计算节点在可信执行环境中对得到的隐私计算结果进行加密并反馈。

51、根据权利要求 50 所述的方法，所述隐私计算节点接收到经过加密的调用请求，包括：

所述隐私计算节点直接从客户端处接收到经过加密的调用请求；或者，

在所述隐私计算节点属于隐私计算集群的情况下，所述隐私计算节点接收所述隐私计算集群的控制节点转发的经过加密的调用请求。

52、根据权利要求 50 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。

53、根据权利要求 52 所述的方法，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护；

在所述经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述经过加密的调用请求被所述隐私计算集群的控制节点接收并转发至所述隐私计算节点；

在所述经过加密的调用请求的目标节点未设定的情况下，所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算集群中的所有隐私计算节点。

54、根据权利要求 52 所述的方法，所述隐私计算节点属于隐私计算集群，且所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护；

所述隐私计算节点被所述隐私计算集群的控制节点根据负载均衡算法从所述隐私计算集

群中选取，且所述经过加密的调用请求被所述控制节点接收并转发至所述隐私计算节点。

55、根据权利要求 50 所述的方法，还包括:

所述隐私计算节点对所述调用请求进行哈希运算得到第一哈希值;

所述隐私计算节点将所述第一哈希值与隐私计算结果关联反馈，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，所述比较结果用于确定所述隐私计算结果是否可靠。

56、根据权利要求 50 所述的方法，还包括:

在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的状态的历史状态取值。

57、一种调用合约的方法，包括:

客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息;

所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

58、根据权利要求 57 所述的方法，所述客户端向隐私计算节点发送经过加密的调用请求，包括:

所述客户端直接向隐私计算节点发送经过加密的调用请求；或者，

在所述隐私计算节点属于隐私计算集群的情况下，所述客户端向所述隐私计算集群的控制节点发送经过加密的调用请求，以由所述控制节点转发所述调用请求。

59、根据权利要求 57 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述节点非对称密钥对的私钥被所述隐私计算节点所维护。

60、根据权利要求 59 所述的方法，在所述隐私计算节点属于隐私计算集群的情况下，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护，或者所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护。

61、根据权利要求 57 所述的方法，还包括:

所述客户端接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果;

所述客户端生成所述调用请求的第二哈希值，并将所述第一哈希值与所述第二哈希值进行比较;

所述客户端根据比较结果确定所述隐私计算结果是否可靠。

62、根据权利要求 57 所述的方法，还包括:

在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

63、一种调用合约的方法，包括:

控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息;

所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点;

所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

64、根据权利要求 63 所述的方法，所述调用请求由节点非对称密钥对的公钥进行加密后传输，且所述非对称密钥对的私钥被所述隐私计算节点所维护。

65、根据权利要求 64 所述的方法，所述节点非对称密钥对的私钥仅被所述隐私计算节点所维护；所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点，包括:

在经过加密的调用请求的目标节点被设定为所述隐私计算节点的情况下，所述控制接节点将所述调用请求转发至所述隐私计算节点;

在所述经过加密的调用请求的目标节点未设定的情况下，所述控制节点将所述调用请求转发至所述隐私计算集群中的所有隐私计算节点。

66、根据权利要求 64 所述的方法，所述节点非对称密钥对的私钥被所述隐私计算集群内的所有隐私计算节点共同维护；所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点，包括：

所述控制节点根据负载均衡算法从所述隐私计算集群中选取所述隐私计算节点，并将所述调用请求转发至所述隐私计算节点。

67、根据权利要求 63 所述的方法，还包括：

所述控制节点接收到所述隐私计算节点对所述调用请求进行哈希运算得到的第一哈希值与所述隐私计算结果；

所述控制节点将所述第一哈希值与所述隐私计算结果转发至请求方，所述第一哈希值用于与客户端生成的所述调用请求的第二哈希值进行比较，比较结果用于确定所述隐私计算结果是否可靠。

68、根据权利要求 63 所述的方法，还包括：

在所述智能合约为无状态合约的情况下，所述智能合约的入参数据包括所述智能合约中定义的合约状态的历史状态取值。

69、一种调用合约的装置，包括：

接收与解密单元，使链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息；

调用与执行单元，使所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；

反馈单元，使所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈。

70、一种调用合约的装置，包括：

生成单元，使客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；

发送单元，使所述客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算。

71、一种调用合约的装置，包括：

获取单元，使区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；

传输单元，使所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算；

接收单元，使所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果。

72、一种调用合约的装置，包括：

接收单元，使控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息；

转发单元，使所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点；

反馈单元，使所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈。

73、一种调用合约的装置，包括:

接收与解密单元，使隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息;

调用与计算单元，使所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算;

加密与反馈单元，使所述隐私计算节点在可信执行环境中对得到的隐私计算结果进行加密并反馈。

74、一种调用合约的装置，包括:

生成调用请求单元，使客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息;

发送调用请求单元，使所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算。

75、一种调用合约的装置，包括:

接收调用请求单元，使控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息;

转发调用请求单元，使所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点;

反馈隐私计算结果单元，使所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈。

76、一种电子设备，包括:

处理器;

用于存储处理器可执行指令的存储器;

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-68 中任一项所述的方法。

77、一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求 1-68 中任一项所述方法的步骤。

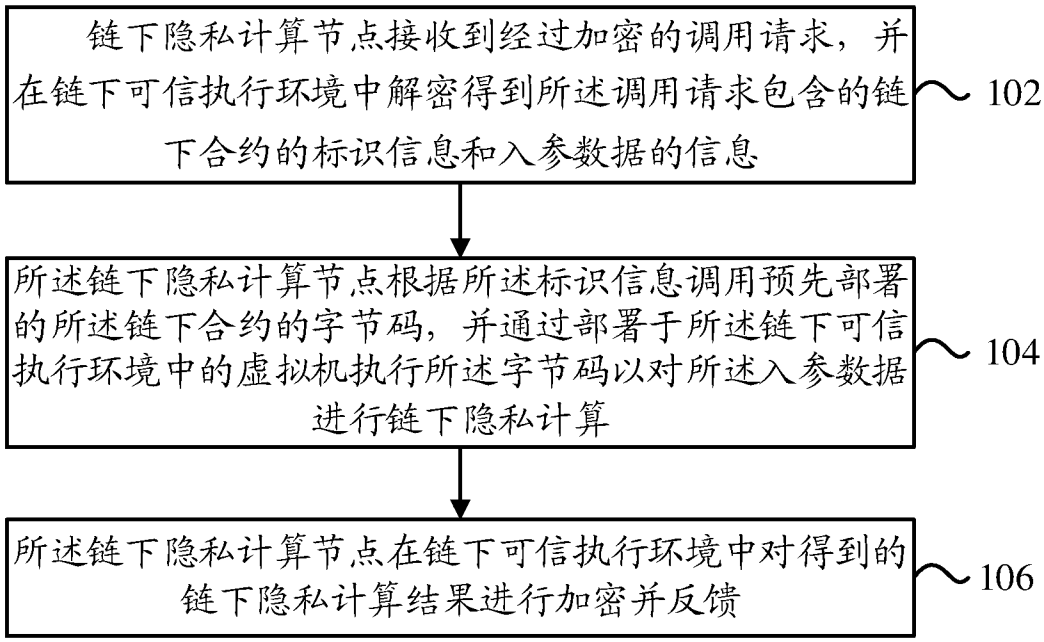
链下隐私计算节点接收到经过加密的调用请求，并在链下可信执行环境中解密得到所述调用请求包含的链下合约的标识信息和入参数据的信息
102
所述链下隐私计算节点根据所述标识信息调用预先部署的所述链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算
104
所述链下隐私计算节点在链下可信执行环境中对得到的链下隐私计算结果进行加密并反馈
106

图 1

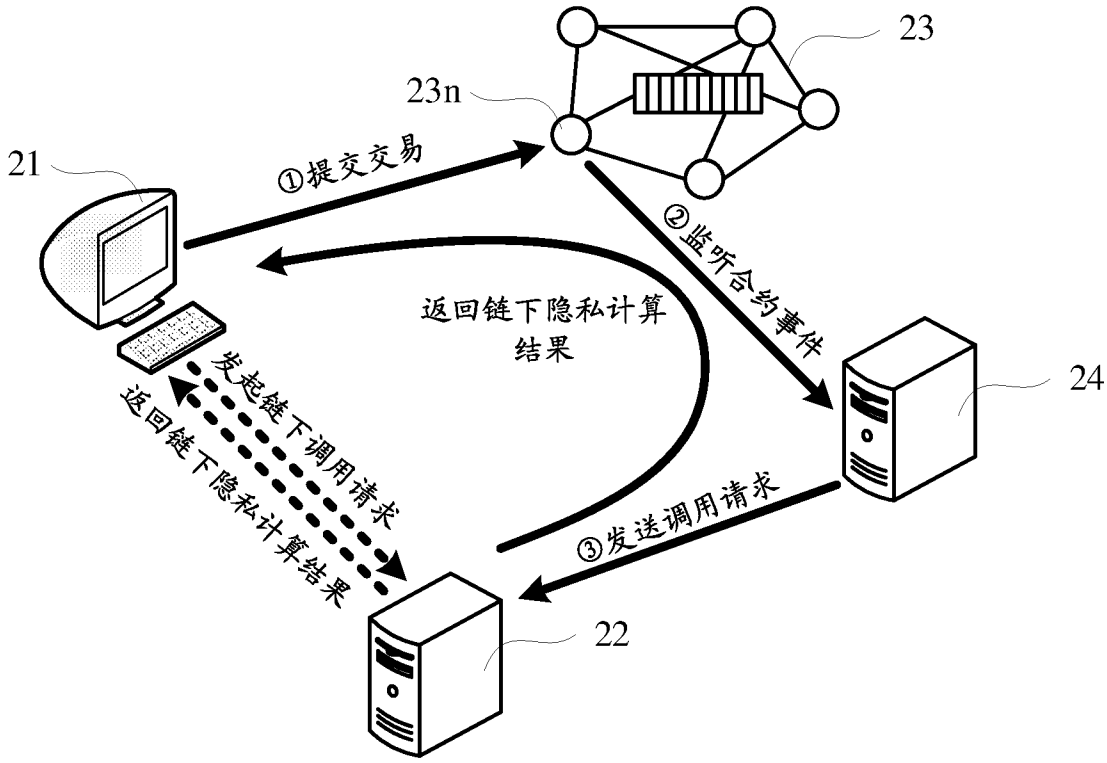
23
23n
21
①提交交易
②监听合约事件
返回链下隐私计算结果
发起链下调用请求
返回链下隐私计算结果
③发送调用请求
24
22

图 2

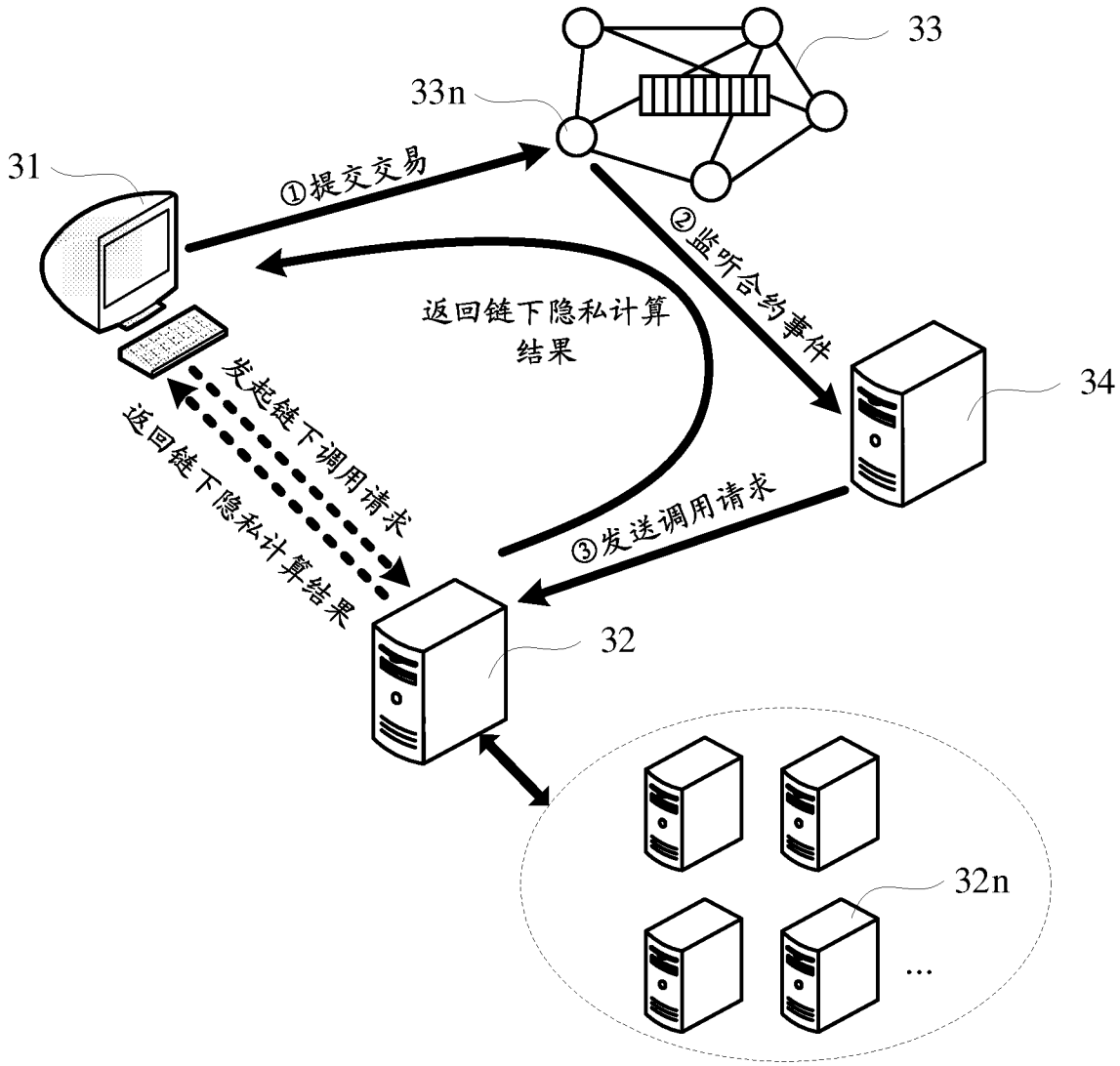
33
33n
31
①提交交易
②监听合约事件
返回链下隐私计算结果
发起链下调用请求
返回链下隐私计算结果
③发送调用请求
34
32
32n
...

图 3

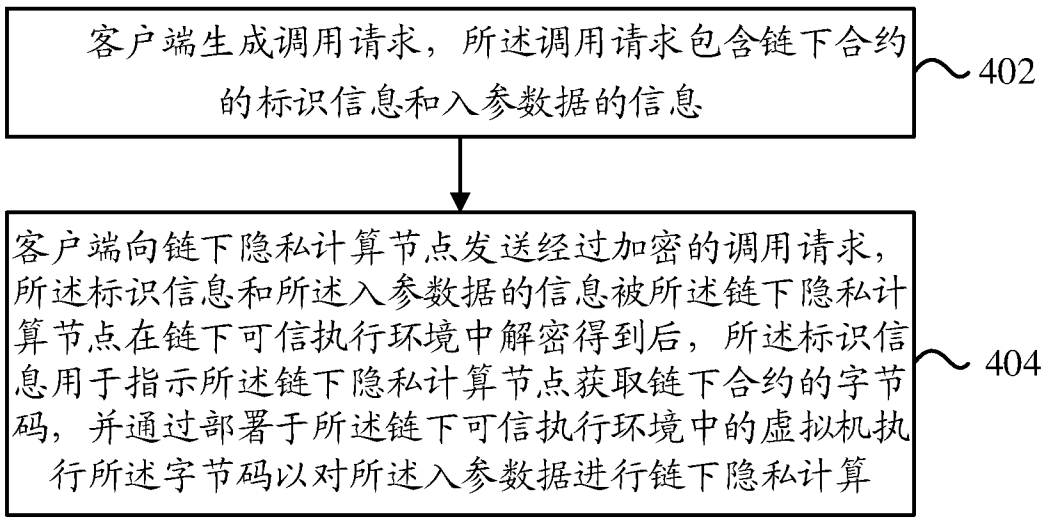
客户端生成调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息
402
客户端向链下隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算
404

图 4

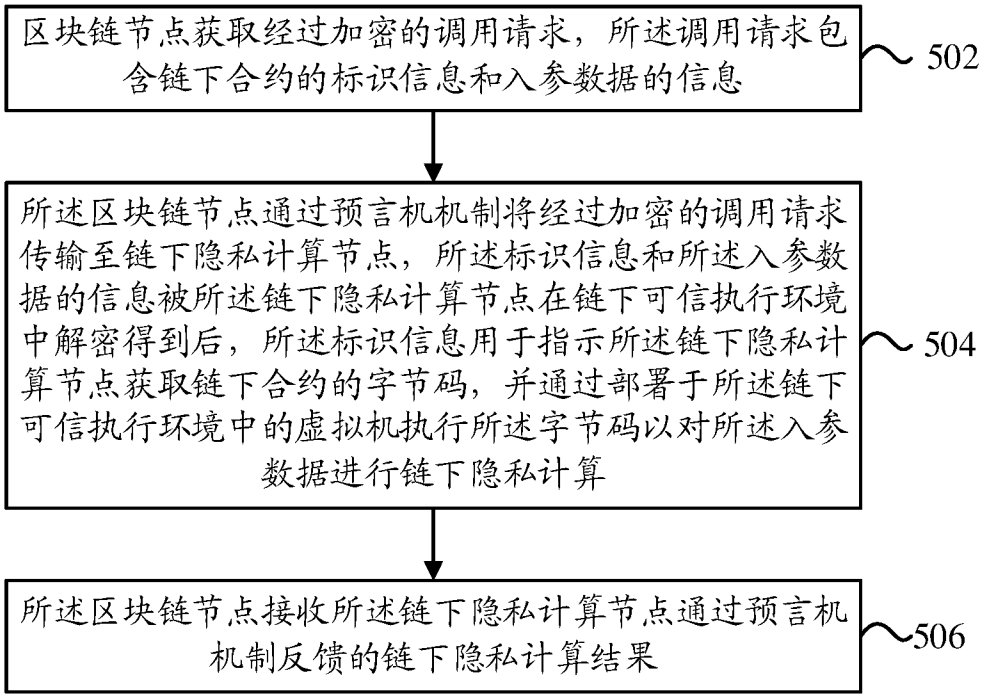
区块链节点获取经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息
502
所述区块链节点通过预言机机制将经过加密的调用请求传输至链下隐私计算节点，所述标识信息和所述入参数据的信息被所述链下隐私计算节点在链下可信执行环境中解密得到后，所述标识信息用于指示所述链下隐私计算节点获取链下合约的字节码，并通过部署于所述链下可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行链下隐私计算
504
所述区块链节点接收所述链下隐私计算节点通过预言机机制反馈的链下隐私计算结果
506

图 5

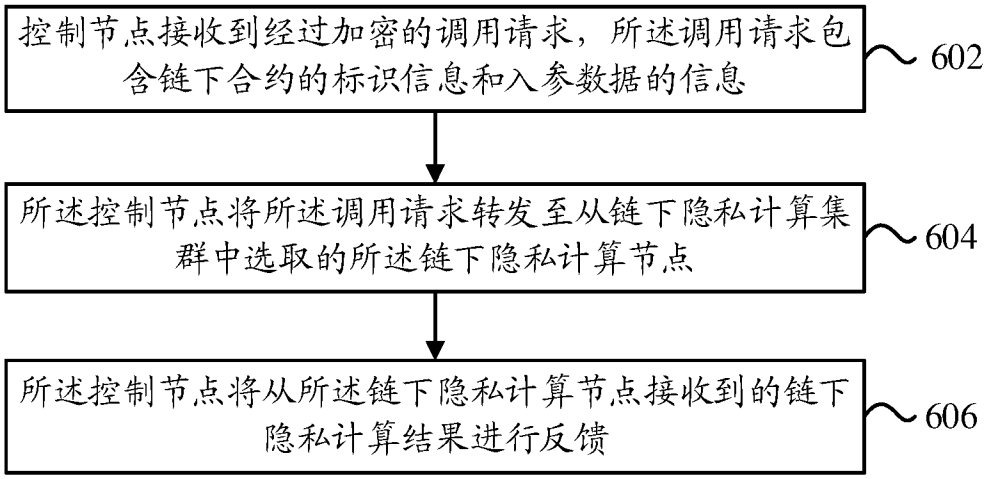
控制节点接收到经过加密的调用请求，所述调用请求包含链下合约的标识信息和入参数据的信息
602
所述控制节点将所述调用请求转发至从链下隐私计算集群中选取的所述链下隐私计算节点
604
所述控制节点将从所述链下隐私计算节点接收到的链下隐私计算结果进行反馈
606

图 6

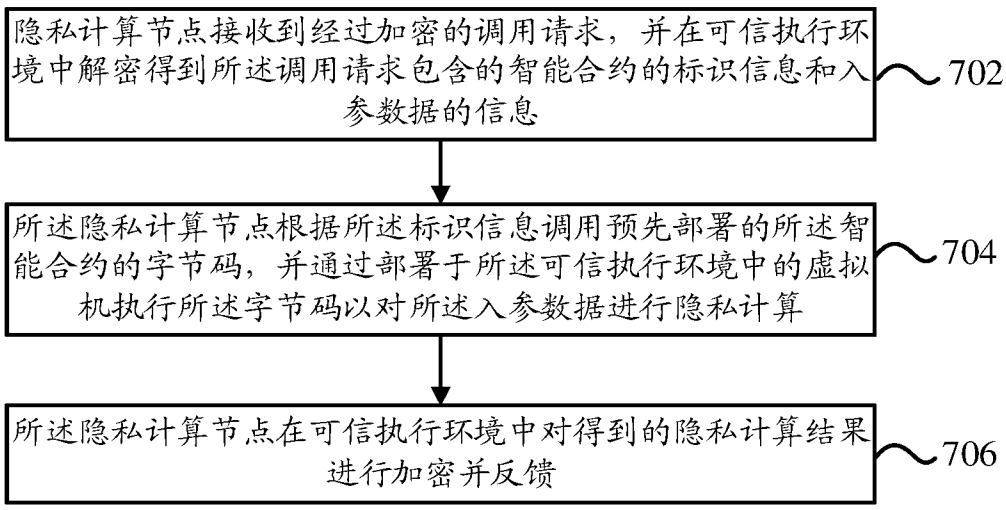
隐私计算节点接收到经过加密的调用请求，并在可信执行环境中解密得到所述调用请求包含的智能合约的标识信息和入参数据的信息
702
所述隐私计算节点根据所述标识信息调用预先部署的所述智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算
704
所述隐私计算节点在可信执行环境中对得到的隐私计算结果进行加密并反馈
706

图 7

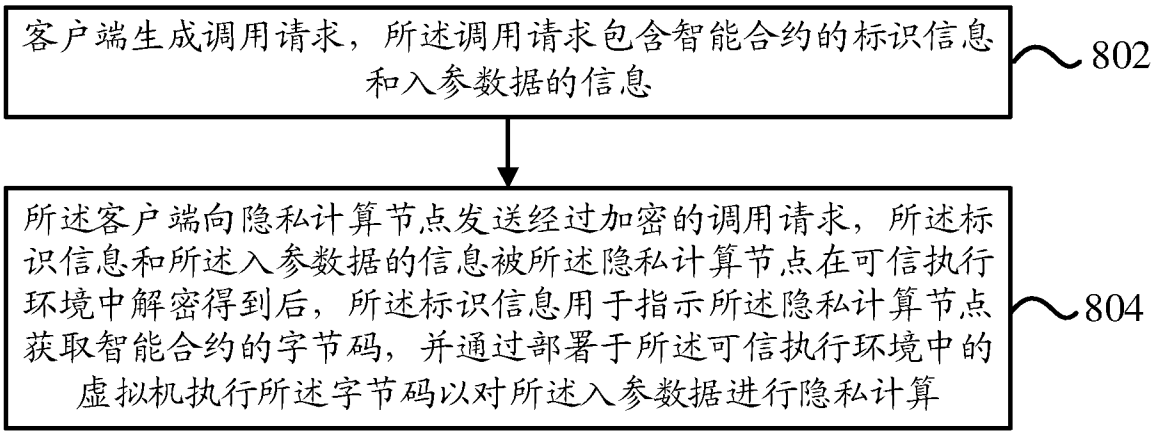
客户端生成调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息
802
所述客户端向隐私计算节点发送经过加密的调用请求，所述标识信息和所述入参数据的信息被所述隐私计算节点在可信执行环境中解密得到后，所述标识信息用于指示所述隐私计算节点获取智能合约的字节码，并通过部署于所述可信执行环境中的虚拟机执行所述字节码以对所述入参数据进行隐私计算
804

图 8

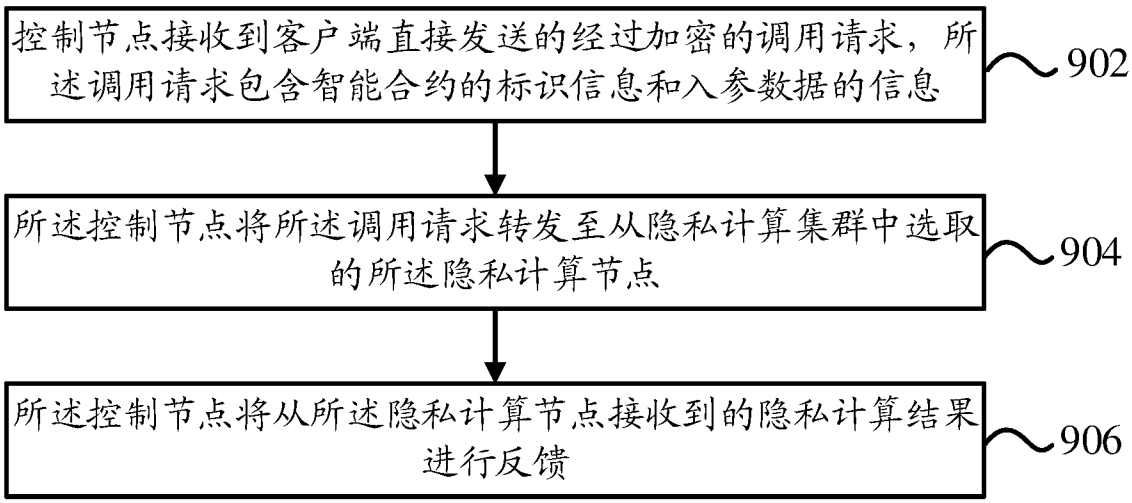
控制节点接收到客户端直接发送的经过加密的调用请求，所述调用请求包含智能合约的标识信息和入参数据的信息
902
所述控制节点将所述调用请求转发至从隐私计算集群中选取的所述隐私计算节点
904
所述控制节点将从所述隐私计算节点接收到的隐私计算结果进行反馈
906

图 9

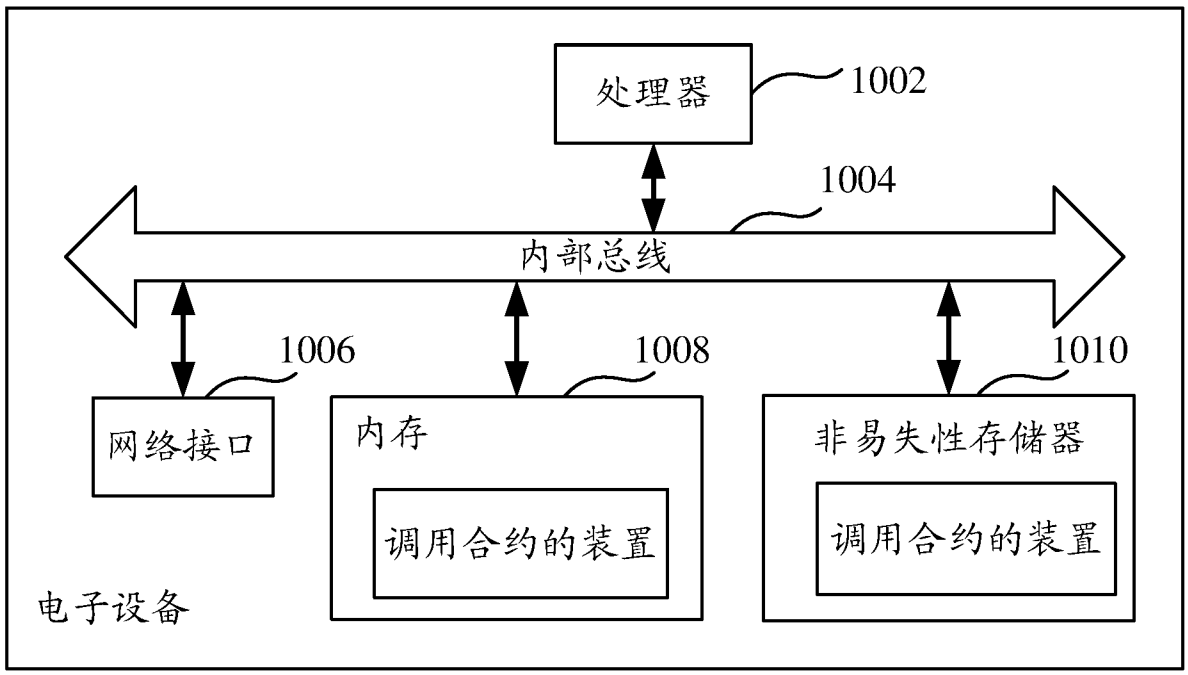
处理器
1002
1004
内部总线
1006
1008
1010
网络接口
内存
调用合约的装置
非易失性存储器
调用合约的装置
电子设备

图 10

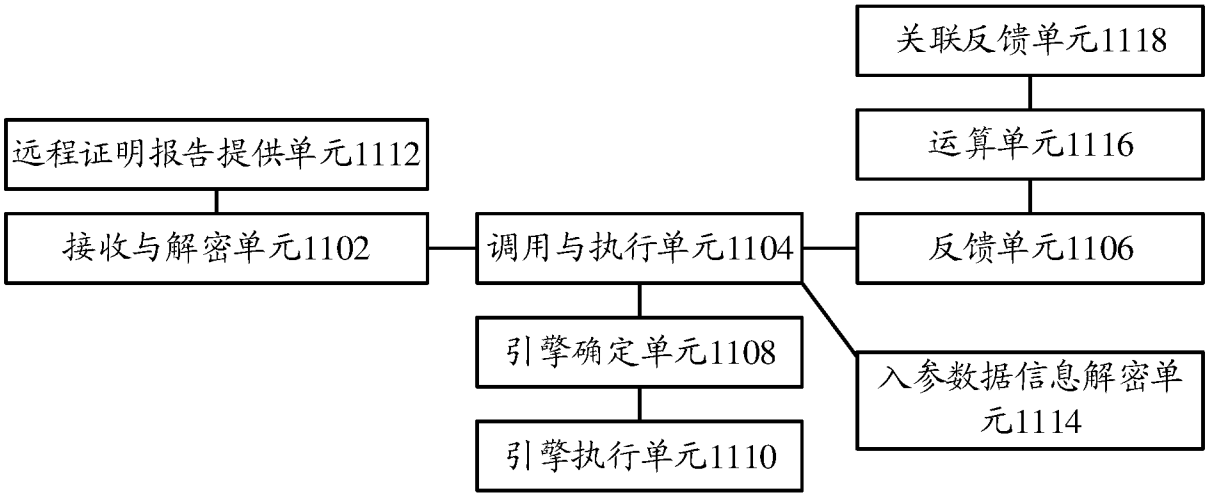
关联反馈单元1118
运算单元1116
远程证明报告提供单元1112
接收与解密单元1102
调用与执行单元1104
反馈单元1106
引擎确定单元1108
入参数据信息解密单元1114
引擎执行单元1110

图 11

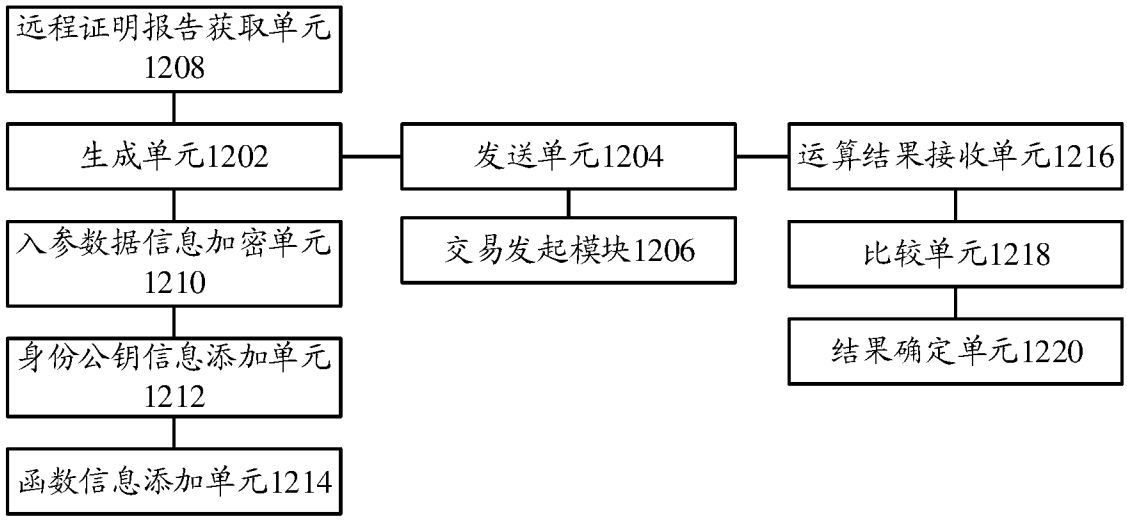
远程证明报告获取单元1208
生成单元1202
发送单元1204
运算结果接收单元1216
入参数据信息加密单元1210
交易发起模块1206
比较单元1218
身份公钥信息添加单元1212
结果确定单元1220
函数信息添加单元1214

图 12

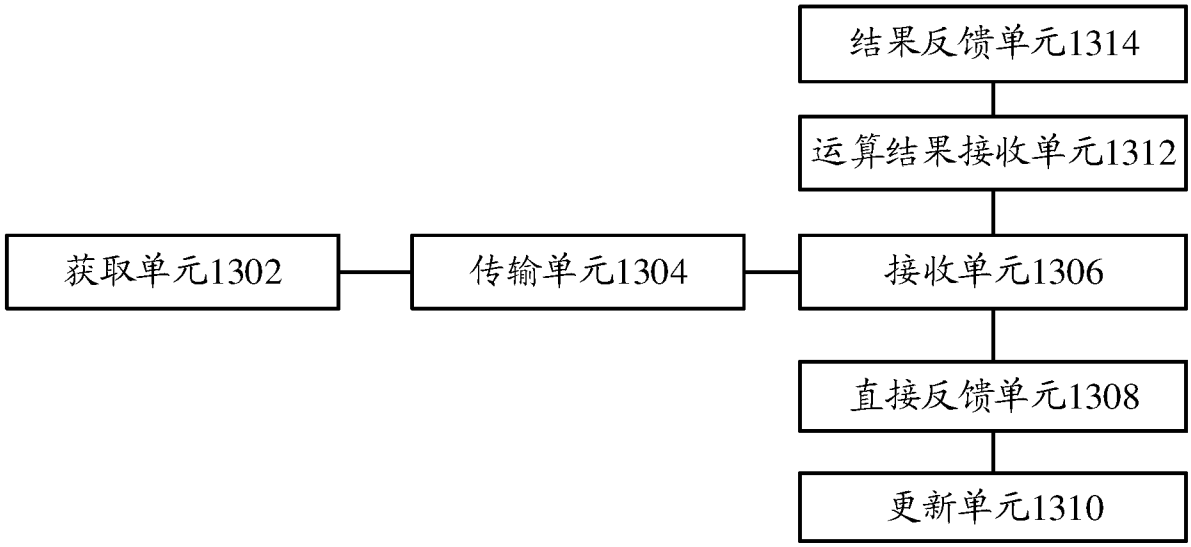
结果反馈单元1314
运算结果接收单元1312
获取单元1302
传输单元1304
接收单元1306
直接反馈单元1308
更新单元1310

图 13

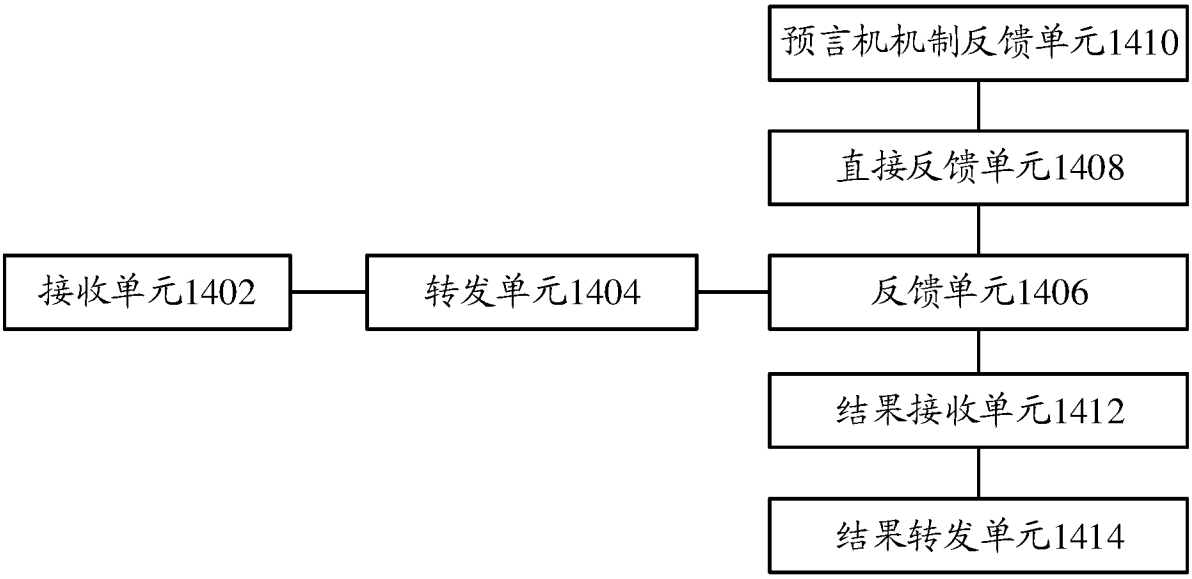

图 14

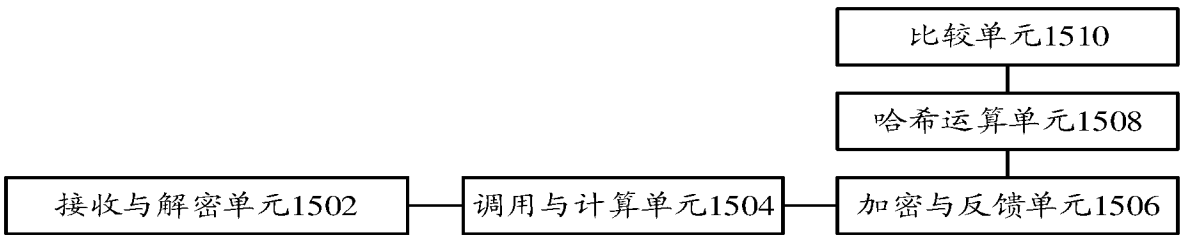

图 15

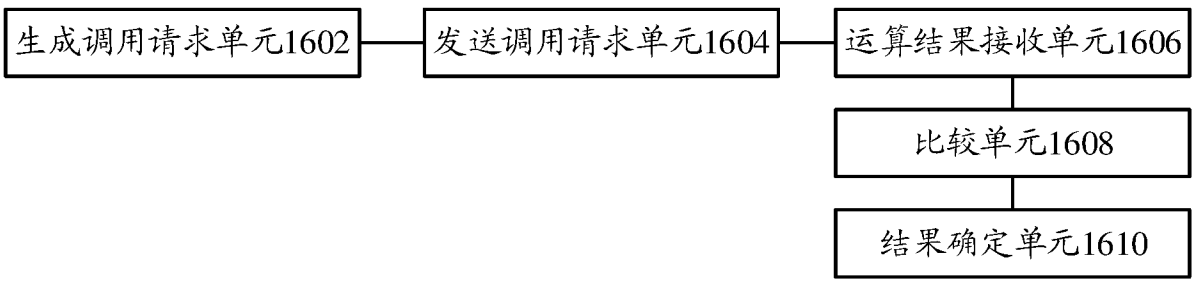

图 16

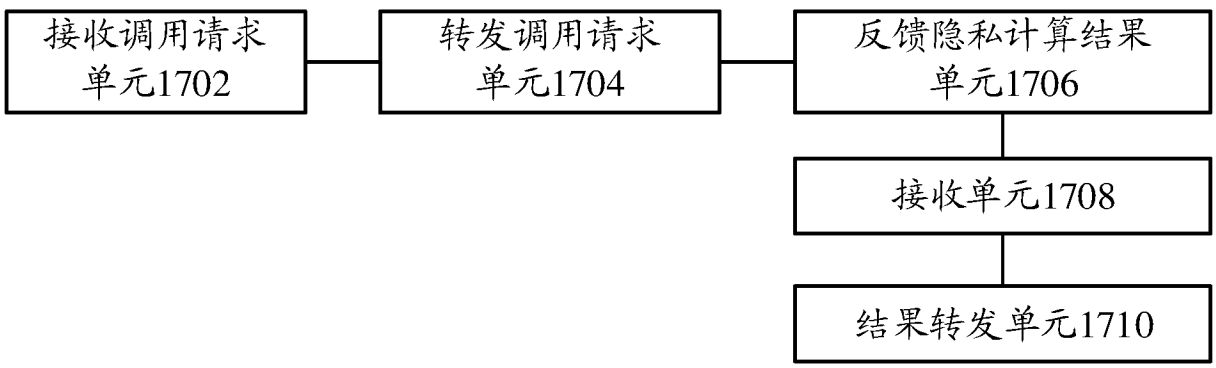

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/074145

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, GOOGLE, ISI: 区块链, 链下, 链外, 智能合约, 远程验证, 远程证明, 预言, 可信执行环境, block chain, offline, off-chain, smart contract, TEE, trusted execution environment, proof, verify, remote, predict

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111090874 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 01 May 2020 (2020-05-01) claims 1-77	1-77
Y	CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019 (2019-11-29) description paragraphs [0056]-[0112], [0160]-[0162], figures 1-4	1-77
Y	CN 110060158 A (ALIBABA GROUP HOLDING LIMITED) 26 July 2019 (2019-07-26) description, paragraphs [0062]-[0066], and figure 2	1-77
Y	CN 109727131 A (SUZHOU HONGLIAN INFORMATION TECHNOLOGY CO., LTD.) 07 May 2019 (2019-05-07) description paragraphs [0041]-[0056]	2, 3, 19, 32-41, 43, 44, 71, 76, 77
Y	CN 110580412 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 17 December 2019 (2019-12-17) description, paragraphs [0074]-[0087]	10, 24
A	WO 2018152519 A1 (ALPHAPOINT) 23 August 2018 (2018-08-23) entire document	1-77

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2021	**26 March 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/074145

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111090874	A	01 May 2020	CN	111090874	B	01 September 2020
CN	110520884	A	29 November 2019	US	2019279206	A1	12 September 2019
				WO	2019072297	A2	18 April 2019
				EP	3563329	A2	06 November 2019
				MX	2019008597	A	09 September 2019
				CA	3049924	A1	18 April 2019
				SG	11201906754 S	A	27 August 2019
				BR	112019014847	A2	14 April 2020
				KR	20200074910	A	25 June 2020
				PH	12019501714	A1	09 March 2020
				AU	2018347199	A1	02 July 2020
				JP	2020516104	A	28 May 2020
				RU	2729700	C1	11 August 2020
CN	110060158	A	26 July 2019	CN	110060158	B	09 June 2020
CN	109727131	A	07 May 2019		None		
CN	110580412	A	17 December 2019	CN	110580412	B	06 March 2020
				CN	111523110	A	11 August 2020
WO	2018152519	A1	23 August 2018	US	10691793	B2	23 June 2020
				US	2018239897	A1	23 August 2018

国际检索报告

国际申请号
PCT/CN2021/074145

A. 主题的分类

G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, GOOGLE, ISI: 区块链，链下，链外，智能合约，远程验证，远程证明，预言，可信执行环境，block chain, offline, off-chain, smart contract, TEE, trusted execution environment, proof, verify, remote, predict

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 111090874 A (支付宝杭州信息技术有限公司) 2020年 5月 1日 (2020-05-01) 权利要求1-77	1-77
Y	CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019-11-29) 说明书第[0056]-[0112]、[0160]-[0162]段、图1-4	1-77
Y	CN 110060158 A (阿里巴巴集团控股有限公司) 2019年 7月 26日 (2019-07-26) 说明书第[0062]-[0066]段、图2	1-77
Y	CN 109727131 A (苏州鸿链信息科技有限公司) 2019年 5月 7日 (2019-05-07) 说明书第[0041]-[0056]段	2，3，19，32-41，43，44，71，76，77
Y	CN 110580412 A (支付宝杭州信息技术有限公司) 2019年 12月 17日 (2019-12-17) 说明书第[0074]-[0087]段	10，24
A	WO 2018152519 A1 (ALPHAPOINT) 2018年 8月 23日 (2018-08-23) 全文	1-77

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 3月 17日	2021年 3月 26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张琳琳 电话号码 86-(10)-53961404

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/074145

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	111090874	A	2020年 5月 1日	CN	111090874	B	2020年 9月 1日
CN	110520884	A	2019年 11月 29日	US	2019279206	A1	2019年 9月 12日
				WO	2019072297	A2	2019年 4月 18日
				EP	3563329	A2	2019年 11月 6日
				MX	2019008597	A	2019年 9月 9日
				CA	3049924	A1	2019年 4月 18日
				SG	11201906754S	A	2019年 8月 27日
				BR	112019014847	A2	2020年 4月 14日
				KR	20200074910	A	2020年 6月 25日
				PH	12019501714	A1	2020年 3月 9日
				AU	2018347199	A1	2020年 7月 2日
				JP	2020516104	A	2020年 5月 28日
				RU	2729700	C1	2020年 8月 11日
CN	110060158	A	2019年 7月 26日	CN	110060158	B	2020年 6月 9日
CN	109727131	A	2019年 5月 7日		无		
CN	110580412	A	2019年 12月 17日	CN	110580412	B	2020年 3月 6日
				CN	111523110	A	2020年 8月 11日
WO	2018152519	A1	2018年 8月 23日	US	10691793	B2	2020年 6月 23日
				US	2018239897	A1	2018年 8月 23日