

(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)



(10) 国际公布号
WO 2021/184973 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2021/074240
- (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:
202010191190.5 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)。吴因金 (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,

(54) Title: EXTERNAL DATA ACCESSING METHOD AND DEVICE

(54) 发明名称: 访问外部数据的方法及装置

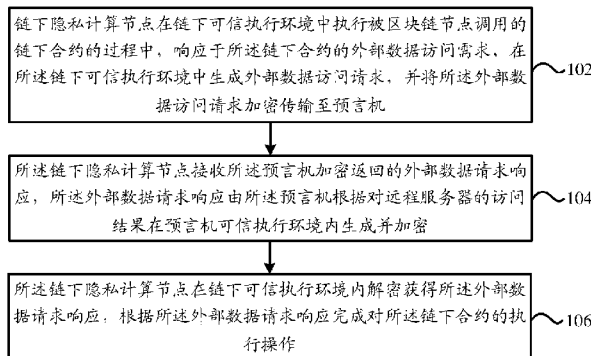


图 1

- 102 During executing, in an off-chain trusted execution environment, an off-chain contract invoked by a blockchain node, an off-chain privacy computing node creates, in response to an external data access requirement of the off-chain contract, an external data access request in the off-chain trusted execution environment, and transmits the external data access request to an oracle machine in an encrypted manner
- 104 The off-chain privacy computing node receives an external data request response returned by the oracle machine in an encrypted manner, the external data request response being created, according to the result of access to a remote server, and encrypted by the oracle machine in an oracle machine trusted execution environment
- 106 The off-chain privacy computing node performs decryption in the off-chain trusted execution environment to obtain the external data request response and completes execution of the off-chain contract according to the external data request response

(57) Abstract: Provided are an external data accessing method and device. The method is applied to an off-chain privacy computing node, a trusted execution environment being established in the off-chain privacy computing node. The method can comprises: executing an off-chain contract in the trusted execution environment upon the receipt of an off-chain contract invoking request sent from a blockchain node; if the off-chain contract has an external data access requirement, initiating, by means of an oracle machine, access to a remote server, and completing execution of the off-chain contract on the basis of an external data request response returned by the oracle machine and created according to the access result; and then returning the execution result to the blockchain node. The present method can achieve privacy protection during external data access.

(57) 摘要: 提供一种访问外部数据的方法及装置; 该方法应用于链下隐私计算节点, 该链下隐私计算节点中建立有可信执行环境, 该方法可以在接收到区块链节点发送的链下合约调用请求后, 在可信执行环境中执行链下合约, 并在链下合约存在外部数据访问需求的情况下, 通过预言机向远程服务器发起访问, 并基于预言机返回的基于访问结果创建的外部数据请求响应完成对链下合约的执行, 进而向区块链节点返回执行结果。本方法可以在访问外部数据的过程中实现隐私保护。

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。

- (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))。

访问外部数据的方法及装置

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，尤其涉及一种访问外部数据的方法及装置。

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访问外部数据的方法及装置。

[04] 根据本说明书一个或多个实施例的第一方面，提出了一种访问外部数据的方法，包括：链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求，在所述链下可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密；所述链下隐私计算节点在所述链下可信执行环境内解密获得所述外部数据请求响应，根据所述外部数据请求响应完成对所述链下合约的执行操作。

[05] 根据本说明书一个或多个实施例的第二方面，提出了一种访问外部数据的方法，包括：预言机接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起；所述链下合约在被区块链节点调用的情况下，由所述链下隐私计算节点在链下可信执行环境内执行；所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述链下隐私计算节点；所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

[06] 根据本说明书一个或多个实施例的第三方面，提出了一种访问外部数据的方法，包括：预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求而发起；所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问；所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述链下隐私计算节点。

[07] 根据本说明书一个或多个实施例的第四方面，提出了一种访问外部数据的方法，包括：隐私计算节点在节点可信执行环境中执行智能合约的过程中，在所述节点可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；所述隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密；所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请求响应，根据所述外部

数据请求响应完成对所述智能合约的执行操作。

[08] 根据本说明书一个或多个实施例的第五方面，提出了一种访问外部数据的方法，包括：预言机接收隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起；所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述隐私计算节点；所述外部数据请求响应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

[09] 根据本说明书一个或多个实施例的第六方面，提出了一种访问外部数据的方法，包括：预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起；所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问；所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述隐私计算节点。

[10] 根据本说明书一个或多个实施例的第七方面，提出了一种访问外部数据的装置，包括：请求单元，使链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求，在所述链下可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；响应单元，使所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密；反馈单元，使所述链下隐私计算节点在链下可信执行环境内解密获得所述外部数据请求响应，根据所述外部数据请求响应完成对所述链下合约的执行操作。

[11] 根据本说明书一个或多个实施例的第八方面，提出了一种访问外部数据的装置，包括：接收单元，使预言机接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起；所述链下合约在被区块链节点调用的情况下，由所述链下隐私计算节点在链下可信执行环境内执行；访问单元，使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；返回单元，使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述链下隐私计算节点；所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

[12] 根据本说明书一个或多个实施例的第九方面，提出了一种访问外部数据的装置，包括：请求接收单元，使预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求而发起；请求转发单元，使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问；结果返回单元，使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述链下隐私计算节点。

[13] 根据本说明书一个或多个实施例的第十方面，提出了一种访问外部数据的装置，包括：请求单元，使隐私计算节点在节点可信执行环境中执行智能合约的过程中，在所述节点可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至

预言机; 响应单元, 使所述隐私计算节点接收所述预言机加密返回的外部数据请求响应, 所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密; 反馈单元, 使所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请求响应, 根据所述外部数据请求响应完成对所述智能合约的执行操作。

[14] 根据本说明书一个或多个实施例的第十一方面, 提出了一种访问外部数据的装置, 包括: 接收单元, 使预言机接收隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起; 访问单元, 使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求, 并根据所述外部数据访问请求访问远程服务器; 返回单元, 使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密, 将加密后的外部数据请求响应返回所述隐私计算节点; 所述外部数据请求响应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

[15] 根据本说明书一个或多个实施例的第十二方面, 提出了一种访问外部数据的装置, 包括: 请求接收单元, 使预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起; 请求转发单元, 使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求, 并向集群内被选取的预言机节点转发所述外部数据访问请求, 所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问; 结果返回单元, 使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应, 并在控制节点可信执行环境内对所述外部数据请求响应进行加密后, 将经过加密的外部数据请求响应返回所述隐私计算节点。

[16] 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、第五方面或第六方面所述的方法。

[17] 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、第五方面或第六方面所述方法的步骤。

附图说明

[18] 图 1 是本说明书一示例性实施例示出的一种链下隐私计算节点侧的访问外部数据的方法的流程图。

[19] 图 2 是本说明书一示例性实施例示出的区块链节点调用链下合约过程中访问外部数据的流程图。

[20] 图 3 是本说明书一示例性实施例示出的一种预言机侧的访问外部数据的方法的流程图。

[21] 图 4 是本说明书一示例性实施例示出的一种预言机控制节点侧的访问外部数据的方法的流程图。

[22] 图 5 是本说明书一示例性实施例示出的一种隐私计算节点侧的访问外部数据的方法的流程图。

[23] 图 6 是本说明书一示例性实施例示出的另一种预言机侧的访问外部数据的方法的流程图。

[24] 图 7 是本说明书一示例性实施例示出的另一种预言机控制节点侧的访问外部数据的方法的流程图。

[25] 图 8 是本说明书一示例性实施例示出的一种基于单一预言机节点访问外部数据的示意图。

[26] 图 9 是本说明书一示例性实施例示出的一种基于单一预言机节点访问外部数据的

方法的交互图。

[27] 图 10 是本说明书一示例性实施例示出的一种对单一预言机节点进行远程证明的流程图。

[28] 图 11 是本说明书一示例性实施例示出的一种基于预言机集群访问外部数据的示意图。

[29] 图 12 是本说明书一示例性实施例示出的一种基于预言机集群访问外部数据的方法的交互图。

[30] 图 13 是本说明书一示例性实施例示出的一种预言机集群中的预言机节点进行远程证明的流程图。

[31] 图 14 是本说明书一示例性实施例示出的一种电子设备的示意结构图。

[32] 图 15 是本说明书一示例性实施例示出的一种链下隐私计算节点侧的访问外部数据的装置框图。

[33] 图 16 是本说明书一示例性实施例示出的一种预言机侧的访问外部数据的装置框图。

[34] 图 17 是本说明书一示例性实施例示出的一种预言机控制节点侧的访问外部数据的装置框图。

[35] 图 18 是本说明书一示例性实施例示出的一种隐私计算节点侧的访问外部数据的装置框图。

[36] 图 19 是本说明书一示例性实施例示出的另一种预言机侧的访问外部数据的装置框图。

[37] 图 20 是本说明书一示例性实施例示出的另一种预言机控制节点侧的访问外部数据的装置框图。

具体实施方式

[38] 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发明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、本发明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。

[39] 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。

[40] 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，私有链可以作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。

[41] 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。

[42] 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。

[43] 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。

[44] 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。

[45] 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。

[46] 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。

[47] 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。

[48] 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，并且可以基于可验证计算（Verifiable Computation）技术证明上述的计算结果确实是在可信执行环境内按照预期执行，从而在确保可靠性的同时，极大地降低了链上的资源消耗。

[49] 如前所述，通过在区块链节点部署智能合约，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在链下隐私计算节点处，使得链下隐私计算节点可以执行代码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。

[50] 链下合约在执行过程中，可能需要依赖于外部数据。这里的外部数据区别于链上数据，并且该外部数据不包括链下隐私计算节点维护的数据。因此，本说明书通过提供外部数据的访问方案，使得链下隐私计算节点能够安全、可靠地获得外部数据。

[51] 图 1 是本说明书一示例性实施例示出的一种链下隐私计算节点侧的访问外部数据的方法的流程图。如图 1 所示，该方法可以包括以下步骤。

[52] 步骤 102，链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求，在所述链下可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机。

[53] 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，需要将链下合约安全部署至该链下隐私计算节点处。链下合约可由某个客户端完成部署。上述的调用请求可能是区块链节点响应于某个客户端发起的交易而产生，这里发起交易的客户端与上述部署链下合约的客户端可以为同一客户端，或者不同的客户端。

[54] 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。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。

[55] 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。

[56] 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 MREncave, 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 MREncave 和 MRSigner。

[57] 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。

[58] 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 MREncave 和 MRSigner, 即待检验 MREncave 和待检验 MRSigner; 同时, 客户端预先获得了链下 TEE 的 MREncave 和 MRSigner 的可信值, 比如称之为可信 MREncave 和可信 MRSigner, 并将待检验 MREncave 与可信 MREncave 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 MREncave 与可信 MREncave 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 MREncave 与可信 MREncave 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 MREncave 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。

[59] 除了 MREncave 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。

[60] 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。

[61] 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。

[62] 在上述实施例，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。

[63] 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。

[64] 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。

[65] 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。

[66] 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起挑战，并接收控制节点返回的上述链下隐私计算节点的远程证明报告。与前述实施例相类似的，客户端可以向控制节点发起链下挑战，或者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链下隐私计算节点的远程证明报告。

[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。在将字节码加密传输至链下隐私计算节点时，与前述的挑战过程类似，可以直接加密传输至链下隐私计算节点，也可以通过控制节点实现转发。

[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] 针对链下隐私计算节点处已经部署的链下合约，区块链节点在执行客户端发起的交易的过程中，可以通过如前所述的调用请求，对该链下合约进行调用，以实现链下隐私计算。例如图 2 所示，调用链下合约的过程可以包括：步骤①，客户端 21 向区块链网络 22 提交一笔交易，该交易可由区块链网络中的某一节点例如节点 22n 接收并执行；步骤②，节点 22n 通过执行接收到的交易，形成链下合约调用请求；步骤③，预言机服务器 23 通过预言机机制获得调用请求，并发送至链下隐私计算节点 24。

[71] 针对客户端 21 提交的交易，节点 22n 可以将该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 22n 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 22n 处可以部署链上 TEE，并且节点 22n 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。

[72] 客户端 21 生成的交易中可以直接包含经过加密的调用请求，那么节点 22n 可以在链上 TEE 内解密交易、得到调用请求密文，然后节点 22n 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。或者，客户端 21 生成的交易中可以直接包含明文的调用请求，那么客户端 21 通常需要对交易进行加密传输，并确保节点 22n 在链上 TEE 内解密得到明文的调用请求后，再在链上 TEE 内对调用请求进行加密，然后通过预言机机制将加密后的调用请求传输至链下隐私计算节点 24。或者，客户端 21 生成的交易中并未包含调用请求，而节点 22n 在链上 TEE 内执行该交易调用的链上合约的过程中，主动在链上 TEE 内生成调用请求。

[73] 链下隐私计算节点处可以部署很多链下合约。调用请求中可以包含所需调用的链下合约的标识信息，以便链下隐私计算节点实现准确调用。调用请求中可以包含入参数据的信息，比如该入参数据本身或入参数据的存储地址等，使得链下隐私计算节点可以

通过链下 TEE 内部署的虚拟机执行链下合约，以针对入参数据进行处理。例如，入参数据的存储地址可能属于某一远程服务器，则链下隐私计算节点需要通过本说明书的外部数据访问方案，获取该入参数据以便完成链下合约的执行。再例如，链下隐私计算节点在执行链下合约以处理入参数据的过程中，可能需要某一远程服务器所提供的外部数据，则可以通过本说明书的外部数据访问方案来获取该外部数据。

[74] 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。假定调用请求由客户端生成并加密：

[75] 当采用对称加密时，客户端和链下隐私计算节点分别维护有相同的对称密钥，比如该对称密钥可由客户端与链下隐私计算节点通过诸如 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和链下隐私计算节点，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处。那么，客户端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将对称密钥维护于链下 TEE 中，因而链下隐私计算节点接受到由区块链节点传输的调用请求，链下隐私计算节点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。

[76] 当采用非对称加密时，链下隐私计算节点维护有节点非对称密钥的私钥，比如称之为链下节点私钥，而客户端可以获得该链下隐私计算节点的链下节点公钥。非对称密钥可由链下隐私计算节点在链下 TEE 内生成，或者由 KMS 服务器分发至该链下隐私计算节点，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对链下隐私计算节点进行远程证明的过程中，将链下节点公钥传输至客户端处。那么，客户端可以通过链下节点公钥对调用请求进行加密，而链下隐私计算节点将链下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，并通过链下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。

[77] 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。客户端可以维护一对称密钥，比如该对称密钥可由客户端随机生成，且客户端可以获得上述节点非对称密钥中的公钥。客户端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。相应的，链下隐私计算节点将加密后调用请求与加密后密钥读入链下 TEE 内，首先通过链下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。

[78] 类似地，在本说明书所涉及的其他数据交互过程中，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。

[79] 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。

[80] 在链下隐私计算节点属于链下隐私计算集群的情况下，这些链下隐私计算节点可以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。

[81] 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。

[82] 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，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，而客户端或区块链节点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。

[83] 链下隐私计算节点所创建的链下 TEE 与外部隔离，在链下 TEE 执行链下合约的过程中，链下 TEE 无法直接实现外部访问以获得所需的外部数据。因此，本说明书中可以通过预言机协助链下 TEE，使得链下 TEE 能够在确保安全性的前提下获得所需的外部数据。以图 2 为例，链下隐私计算节点 24 在执行链下合约的过程中，如果存在外部数据访问请求，可以通过步骤④创建外部数据访问请求，并发送至预言机 25，触发预言机 25 对远程服务器进行访问，并返回相应的外部数据请求响应。

[84] 链下合约的字节码中可以定义有外部数据访问接口。链下隐私计算节点在链下 TEE 中执行链下合约的过程中，通过调用该外部数据访问接口可以生成相应的外部数据访问请求。链下合约中可以包含多个函数，并非每个函数都必须调用外部数据访问接口。同时，即便某一函数能够调用外部数据访问接口，也并非在每次执行时都必然会调用，比如可以在上述的调用请求中包含用于指示是否调用外部数据访问接口的入参，从而基于该入参的取值来确定是否调用外部数据访问接口。

[85] 链下隐私计算节点可以对外部数据访问请求的访问行为进行限制。例如，可以将允许进行访问的 IP 地址写入预设的白名单中，并将外部数据访问请求的目标访问对象的 IP 地址与该白名单进行匹配，从而仅允许针对该白名单记录的 IP 地址进行访问；类似地，也可以将不允许进行访问的 IP 地址写入预设的黑名单，并将外部数据访问请求的目标访问对象的 IP 地址与该黑名单进行匹配，从而禁止针对该黑名单记录的 IP 地址进行访问。再例如，可以在配置文件中记录对外部数据访问请求的字段限制和内容限制，

从而避免外部数据访问请求中包含敏感字段或敏感内容等。因此，在生成外部数据访问请求后，可以对外部数据访问请求中的字段进行检查，在检测到外部数据访问请求中存在不符合访问要求的字段或请求内容，或者目的 IP 地址未处于预设白名单的情况下，禁止执行访问外部数据的操作。

[86] 链下隐私计算节点与预言机所支持的数据格式可能不同，造成链下隐私计算节点所生成的外部数据访问请求，可能无法被预言机顺利识别，进而造成对外部数据访问失败。因此，链下隐私计算节点在执行链下合约产生第一格式的外部数据访问请求后，可以主动将第一格式的外部数据访问请求转换为第二格式，而本步骤加密传输至预言机的即为转换为第二格式的外部数据访问请求。相应地，在预言机返回第二格式的外部数据请求响应后，链下隐私计算节点可以主动将第二格式的外部数据请求响应转换为第一格式，然后对该第一格式的外部数据请求响应予以处理。

[87] 在本说明书中，链下隐私计算节点向预言机发送外部数据访问请求的过程中，或者预言机向链下隐私计算节点返回外部数据请求响应的过程中，涉及到设备之间的数据交互。如前所述，可以通过对称加密、非对称加密或两者结合的方式，对外部数据访问请求和外部数据请求响应分别进行加密传输。其中，链下隐私计算节点处创建了链下 TEE，预言机处创建了预言机 TEE，可以确保对外部数据访问请求和外部数据请求响应的加密、解密操作均在 TEE 中实现，因而可以在数据交互的各个环节均确保了极高的安全性。

[88] 在实际应用中，预言机可以为单一的预言机节点，也可以为包含有多个预言机节点的预言机集群。其中，在预言机包含多个预言机节点的情况下，预言机集群中包含控制节点，以及控制节点以外的预言机节点。在基于非对称加密或数字信封（即对称加密与非对称加密结合）的方式进行数据交互的过程中，链下隐私计算节点用于加密的公钥可以为预言机加密公钥，而相应的预言机加密私钥可以由上述的单一预言机节点所持有、代表该单一预言机节点的身份，或者该预言机加密私钥可以由上述预言机集群中的某一预言机节点所持有、代表该预言机节点的身份，或者该预言机加密私钥可以由上述预言机集群中的所有预言机节点所共同持有、代表这些预言机节点的集群身份，或者该预言机加密私钥可以由上述预言机集群中的控制节点所持有、代表该控制节点的身份。

[89] 在上述预言机加密公钥对应于单一预言机节点，或者预言机集群中某一预言机节点的身份的情况下，链下隐私计算节点在链下 TEE 内基于该单一预言机节点的加密公钥对外部数据访问请求进行加密，并将加密后的外部数据访问请求发送至该预言机节点，以由该预言机节点基于维护的预言机加密私钥进行解密。

[90] 当预言机加密公钥对应于预言机集群中某一预言机节点的身份时，链下隐私计算节点与该预言机节点可以直接交互，那么其过程与单一预言机节点的情况无异。链下隐私计算节点可以根据自身的需求，从预言机集群中选取某一预言机节点；或者，链下隐私计算节点可以与预言机集群的控制节点进行协商，以确定由集群中哪一预言机节点对外部数据访问请求进行处理，而链下隐私计算节点采用该预言机节点对应的预言机加密公钥进行加密。在一种实施方式中，链下隐私计算节点可以在需要访问外部数据的情况下，先向控制节点请求一预言机节点用于处理本次外部数据访问请求，在接收到控制节点的请求响应后，基于响应中的信息确定分配的预言机节点，并基于该预言机节点对应的预言机加密公钥对外部数据访问请求进行加密。在另一实施方式中，可以由控制节点主动向链下隐私计算节点发送分配的预言机节点。比如，控制节点可以按照预设周期确定集群中预言机节点的性能状况，并基于负载均衡算法将性能状况较好的预言机节点作为该时间段用于处理外部数据访问请求的预言机节点，并主动将该预言机节点的信息告知链下隐私计算节点。在这种机制下，在该时间段内，所有外部数据访问请求均通过该预言机节点对应的预言机加密公钥进行加密，控制节点将所有接收到的外部数据访问请求发送至该预言机节点进行处理。当然，控制节点也可以同时确定出的多个预言机节点，

链下隐私计算节点可以从中选取一预言机节点,并采用被选取的预言机节点对应的预言机加密公钥对外部数据访问请求进行加密,并且链下隐私计算节点可以向控制节点告知被选取的预言机节点的信息,比如该预言机节点对应的预言机加密公钥或其哈希值,或者控制节点为该预言机节点分配的节点 ID 等,使得控制节点在接收到该外部数据访问请求后可以准确转发至上述被选取的预言机节点。

[91] 如前所述,在预言机集群场景下,预言机加密私钥可由该预言机集群的控制节点维护。在这种情况下,加密后的外部数据访问请求被发送至该控制节点,并由该控制节点解密后,转发至所述预言机集群内的预言机节点进行处理,使得链下隐私计算节点无需关注于预言机集群内的节点数量和各个节点的身份等,可以将预言机集群作为一个整体的“预言机”进行交互,可以简化交互过程。其中,控制节点在对外部数据访问请求解密后,可以随机或基于负载均衡算法从预言机集群内选取一预言机节点,采用对应于该被选取的预言机节点的身份的公钥在 TEE 内对外部数据访问请求进行重新加密,并将重新加密后的外部数据访问请求发送至该预言机节点,由该预言机节点在创建的预言机 TEE 内根据对应于自身身份的私钥进行解密和处理,且对应于该预言机节点的身份的公私钥对被创建于该预言机 TEE 内。

[92] 步骤 104,所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应,所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密。

[93] 预言机根据接收到的外部数据访问请求,对远程服务器予以访问,以获取相应的访问结果。例如图 2 所示,访问过程可以包括下述步骤:步骤③,预言机 25 基于外部数据访问请求向远程服务器 26 发起访问;步骤⑥,远程服务器 26 向预言机 25 返回访问结果;步骤⑦,预言机 25 基于访问结果创建外部数据请求响应,并返回至链下隐私计算节点 24。外部数据访问请求中可以包含目标数据和远程服务器 26 的信息,预言机 25 可以据此访问远程服务器 26 并获取相应的目标数据,以作为上述的访问结果;或者,外部数据访问请求中可以仅包含目标数据的信息,而预言机 25 可以根据该目标数据的信息确定相应的远程服务器 26,并针对该远程服务器 26 予以访问。预言机 25 在接收到远程服务器 26 返回的访问结果后,可以基于接收到的访问结果创建对应的外部数据请求响应。

[94] 链下隐私计算节点可以预先验证预言机是否可信,比如可以通过远程证明的方式对预言机创建的预言机 TEE 进行验证,如果验证通过则表明预言机具有可靠的硬件平台和软件环境,确定预言机可信。在此基础上,链下隐私计算节点可以在本地存储预言机的预言机签名公钥,以用于上述的验签操作;反之,如果预言机被验证为不可信,链下隐私计算节点不会在本地存储预言机签名公钥,那么上述的验签操作将无法实施,也就不会将收到的外部数据请求响应用于链下合约的后续操作。

[95] 上述的预言机可以为单个预言机节点,链下隐私计算节点可以直接与该预言机节点进行交互,以获取该预言机节点对应的远程证明报告。或者,上述的预言机可以为预言机集群,该预言机集群内的每个预言机节点分别创建预言机 TEE,而链下隐私计算节点可以获取集群内所有预言机节点分别对应的远程证明报告,以用于验证各个预言机节点所创建的预言机 TEE 是否可信。例如,可以由控制节点向各个预言机节点发起挑战的方式获得。具体的,控制节点可以向集群中的各个预言机节点发起挑战,各个预言机节点分别生成与预言机 TEE 相关的自荐信息并发送至认证服务器,以由认证服务器对自荐信息进行验证后生成相应的远程证明报告,并将该报告返回至对应的预言机节点,各个预言机节点在接收到远程证明报告后向控制节点转发,而控制节点将远程证明报告转发至链下隐私计算节点。

[96] 链下隐私计算节点可以分别对获取的每份远程证明报告进行验证,验证过程可以参考前文所述的远程证明过程的相关描述,差异仅在于挑战方与被挑战方的变化,此处

不再赘述。根据远程证明报告,如果链下隐私计算节点确认某一预言机节点可信,那么该链下隐私计算节点将在本地存储该预言机节点对应的预言机签名公钥;换言之,链下隐私计算节点在本地存储所有被验证为可信的预言机节点对应的预言机签名公钥,而不会存储被验证为不可信的预言机节点对应的预言机签名公钥。如前所述,预言机节点可以维护有代表自身身份的预言机加密私钥,而预言机签名私钥与预言机加密私钥类似,同样由预言机节点在自身创建的预言机 TEE 内生成,并且可以代表该预言机节点的身份。

[97] 预言机可以基于预言机签名私钥对创建的外部数据请求响应进行签名。相应地,链下隐私计算节点可以基于预先获取的预言机签名公钥对接收到的外部数据请求响应进行验签。如果验签成功,表明收到的外部数据请求响应确实来自预言机,并且在传输过程中未发生数据丢失等异常情况,即收到的外部数据请求响应可信,因而链下隐私计算节点可以在验签成功的情况下,根据外部数据请求响应完成对链下合约的后续操作。而在链下隐私计算节点仅在本地维护被验证为可信的预言机节点对应的预言机签名公钥的情况下,验签成功可以确保处理外部数据访问请求的预言机节点为预先验证过的可信节点,避免不可信的预言机节点进行冒充,有助于提升数据安全性。

[98] 对于同一预言机节点而言,如果该预言机节点存在对应的预言机加密密钥对和预言机签名密钥对,该预言机加密密钥对和预言机签名密钥对可以为同一密钥对,也可以为不同密钥对。而在本说明书的技术方案中,如果链下隐私计算节点在对外部数据访问请求进行加密的过程中,采用的公钥是预言机集群中的控制节点对应的预言机加密公钥,那么由于外部数据请求响应必然由某一预言机节点生成,因而此时所涉及的预言机加密密钥对与预言机签名密钥对必然不是同一密钥对。

[99] 预言机向链下隐私计算节点发送外部数据请求响应时,针对该外部数据请求响应进行加密传输。针对外部数据请求响应的加密传输过程,与前述的针对调用请求的加密传输过程类似,数据接收方均为链下隐私计算节点,只是数据发送方变为了预言机。与针对调用请求的加密传输过程相类似,针对外部数据请求响应进行加密传输时,可以采用对称加密、非对称加密或两者结合的数字信封等方式。并且,当采用非对称加密或数字信封的形式时,需要使用链下节点公钥,而相应的链下节点私钥可以仅由作为接收方的该链下隐私计算节点所维护、代表该链下隐私计算节点的节点身份,也可以代表该链下隐私计算节点所处的链下隐私计算集群的集群身份、由集群内的所有链下隐私计算节点共同维护。

[100] 步骤 106,所述链下隐私计算节点在所述链下可信执行环境内解密获得所述外部数据请求响应,根据所述外部数据请求响应完成对所述链下合约的执行操作。

[101] 在完成对链下合约的执行操作之后,还可以将执行结果加密反馈至区块链节点。例如图 2 所示,该过程可以包括以下步骤:步骤⑧,链下隐私计算节点 24 基于外部数据请求响应完成链下合约的执行操作,并将执行结果反馈至预言机服务器 23;步骤⑨,预言机服务器 23 将执行结果转发至区块链网络中的节点 22n,以由区块链节点 22n 基于该执行结果完成对链上合约的执行操作;步骤⑩,区块链节点 22n 完成链上合约的执行操作后,向客户端 21 返回链上合约的执行结果。在图 2 所示的实施例中,区块链节点 22n 用于实现链下交互的预言机服务器 23、链下隐私计算节点 24 用于访问外部数据的预言机 25 具有不同标识,这是为了便于体现出区块链节点 22n、链下隐私计算节点 24 所面临的交互对象、交互数据等所存在的差异,但实际上预言机服务器 23 与预言机 25 在物理结构上可以部署于同一设备,也可以部署于不同设备,本说明书并不对此进行限制。

[102] 由上述技术方案可知,本说明书的技术方案在检测到链下合约的执行过程中存在外部数据访问需求的情况下,可以通过预言机向远程服务器发起访问,进而获得需要的外部数据以完成链下合约的执行。通过在链下隐私计算节点处创建链下 TEE、在预言机

处创建预言机 TEE，并且在链下隐私计算节点与预言机之间实现加密的数据传输，使得链下合约、外部数据访问请求、外部数据请求响应都只在 TEE 内才处于明文状态，而在 TEE 外均处于密文状态，从而在实现外部数据访问的同时，能够确保数据安全性并满足隐私保护的需求。

[103] 对应于上述链下隐私节点侧的实施例，本说明书还提出了预言机侧、预言机集群中的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。

[104] 相应的，图 3 是本说明书一示例性实施例示出的一种预言机侧的访问外部数据的方法的流程图。如图 3 所示，该方法可以包括以下步骤。

[105] 步骤 302，预言机接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起；所述链下合约在被区块链节点调用的情况下，由所述链下隐私计算节点在链下可信执行环境内执行。

[106] 如前所述，该预言机可以为单一预言机节点，也可以为包含多个预言机节点的预言机集群（包含控制节点，以及控制节点以外的预言机节点）。链下隐私计算节点用于加密的预言机加密密钥可以为单一预言机节点的加密密钥或预言机集群中控制节点以外的预言机节点的加密密钥，也可以为预言机集群中控制节点的加密密钥。

[107] 如前所述，预言机可以接收链下隐私计算节点在链下 TEE 内基于预言机加密密钥加密的外部数据访问请求，并基于预言机加密私钥对接收到的外部数据访问请求进行解密。其中，上述预言机加密密钥可以为单一预言机节点的加密密钥，也可以为预言机集群中控制节点以外的预言机节点的加密密钥。

[108] 如前所述，在预言机加密密钥为单一预言机节点的情况下，链下隐私计算节点在链下 TEE 内基于该单一预言机节点的加密密钥对外部数据访问请求进行加密，并将加密后的外部数据访问请求发送至该单一预言机节点，以由该单一预言机节点基于维护的加密私钥进行解密。

[109] 如前所述，在预言机加密密钥为预言机集群中控制节点以外的预言机节点的加密密钥的情况下，链下隐私计算节点在链下 TEE 内基于任一预言机节点的加密密钥对外部数据访问请求进行加密，并将加密后的外部数据访问请求发送至预言机集群中的控制节点，并由控制节点将加密的外部数据访问请求转发至该任一预言机节点，以由该任一预言机节点基于维护的加密私钥进行解密。

[110] 如前所述，预言机集群中的控制节点可以接收链下隐私计算节点在链下 TEE 内基于预言机加密密钥加密的外部数据访问请求，并基于该控制节点维护有的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理。在该实施方式中，链下隐私计算节点用于加密外部数据访问请求的预言机加密密钥为控制节点的加密密钥；其中，基于控制节点维护有的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理可以包括：基于控制节点维护的加密私钥对接收到的外部数据访问请求进行解密，并基于任一预言机节点的加密密钥对外部数据访问请求进行重新加密，并向该任一预言机节点转发重新加密的外部数据访问请求。

[111] 如前所述，链下隐私计算节点与预言机可能支持不同的数据编码格式。因此，链下隐私计算节点在生成第一格式的外部数据访问请求后可以将其转换为第二格式。换言之，预言机接收到的链下隐私计算节点发送的第二格式的外部数据访问请求由链下隐私计算节点对第一格式的外部数据访问请求转换得到；而第一格式的外部数据访问请求在执行链下合约的情况下产生。

[112] 步骤 304，所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器。

[113] 步骤 306, 所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密, 将加密后的外部数据请求响应返回所述链下隐私计算节点; 所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

[114] 如前所述, 预言机在基于访问结果创建外部数据请求响应后, 还可以基于维护的预言机签名私钥对该外部数据请求响应进行签名, 以向链下隐私计算节点证明该外部数据请求响应的可靠性。

[115] 如前所述, 为了使链下隐私计算节点能够基于预先维护的预言机的签名公钥对带有签名的外部数据请求响应进行验签, 需要预先获取预言机签名公钥。为此, 还可以包括对预言机进行远程证明的过程。其中, 在该预言机为预言机节点的情况下, 预言机签名私钥由该预言机节点维护; 该预言机节点可以向链下隐私计算节点返回远程证明报告; 该远程证明报告由认证服务器对该预言机节点产生的自荐信息进行验证后生成, 该自荐信息与该预言机节点上创建的 TEE 相关; 在根据该远程证明报告确定预言机节点可信的情况下, 预言机签名公钥被所述链下隐私计算节点保存在本地。在该预言机为预言机集群的情况下, 预言机签名私钥由集群中响应于外部数据访问请求的预言机节点维护; 预言机集群中的控制节点向链下隐私计算节点返回集群中各个预言机节点的远程报告证明, 每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成, 所述自荐信息与相应预言机节点上创建的 TEE 相关; 在根据所述远程证明报告确定出可信预言机节点的情况下, 所述可信预言机节点的预言机签名公钥被所述链下隐私计算节点保存在本地。

[116] 如前所述, 在基于访问结果创建外部数据请求响应后, 预言机可以采用链下节点公钥对创建的外部数据请求响应进行加密, 并将加密的外部数据请求响应返回给所述链下隐私计算节点, 以由链下隐私计算节点基于链下节点私钥对加密的外部数据请求响应进行解密。其中, 在链下隐私计算节点属于链下隐私计算集群的情况下, 链下节点私钥仅被所述链下隐私计算节点所维护, 或者链下节点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。

[117] 如前所述由于预言机采用第二格式对数据进行编码, 因此, 基于访问结果创建的外部数据请求响应也采用第二格式; 该第二格式的外部数据请求响应在返回至链下隐私计算节点后, 将由链下隐私计算节点转换为第一格式的外部数据请求响应; 链下隐私计算节点可以基于所述第一格式的外部数据请求响应完成对所述链下合约的执行操作。

[118] 相应的, 图 4 是本说明书一示例性实施例示出的一种预言机控制节点侧的访问外部数据的方法的流程图。如图 4 所示, 该方法可以包括以下步骤。

[119] 步骤 402, 预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中, 响应于所述链下合约的外部数据访问需求而发起。

[120] 如前所述, 链下隐私计算节点基于控制节点的加密公钥对外部数据访问请求进行加密, 控制节点在接收到链下隐私计算节点发送的外部数据访问请求的情况下, 在控制节点 TEE 中基于维护的控制节点加密私钥对接收到的外部数据访问请求进行解密。

[121] 步骤 404, 所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求, 并向集群内被选取的预言机节点转发所述外部数据访问请求, 所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问。

[122] 如前所述, 控制节点在接收到外部数据访问请求后, 可以在集群中选取一可信节点作为处理本次外部数据访问请求的预言机节点 (该可信节点即为本步骤中被选取的预言机节点); 并可以在控制节点 TEE 中基于该可信节点的加密公钥对外部数据访问请求进行重新加密, 并将重新加密后的外部数据访问请求发送至该可信节点。

[123] 步骤 406, 所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应, 并在控制节点可信执行环境内对所述外部数据请求响应进行加密后, 将经

过加密的外部数据请求响应返回所述链下隐私计算节点。

[124] 如前所述，被选取的预言机节点在接收到控制节点发送的重新加密后的外部数据访问请求后，可以在被选预言机 TEE 中基于自身维护的加密私钥（即该可信节点的加密私钥）进行解密；并基于解密后的外部数据访问请求向相应的远程服务器发起访问。

[125] 如前所述，在接收到远程服务器返回的访问结果后，该被选取的预言机节点可以在 TEE 中基于该访问结果创建外部数据请求响应，并用该被选取的预言机的签名私钥进行签名；该签名后的外部数据访问请求在链下隐私计算节点基于预先获取的预言机公钥（即该被选取的预言机的加密公钥）验签后，用于完成对链下合约的执行操作。

[126] 如前所述，链下隐私计算节点可以通过多种方式获取被选取预言机的加密公钥。例如，可以由控制节点向链下隐私计算节点发送远程报告证明；远程证明报告由链下隐私计算节点进行验证后，将所述远程证明对应的预言机节点确定为可信节点；所述可信节点的公钥信息被链下隐私计算节点保存在本地。在一种实施方式中，链下隐私计算节点可以预先获取预言机集群中所有可信节点的公钥信息。此时，可以由控制节点向链下隐私计算节点发送集群中所有预言机节点对应的远程证明报告；由链下隐私计算节点对接收到远程证明报告进行验证，并将验证成功的远程证明报告对应的预言机节点确定为可信节点，并将所有可信节点的签名公钥信息在本地保存。

[127] 如前所述，可以由控制节点接收集群中预言机节点的远程证明报告，并基于远程证明报告确定预言机节点是否为可信节点；在接收到链下隐私计算节点发送的外部数据访问请求的情况下，控制节点可以基于负载均衡的原则分配一可信节点用于处理该外部数据访问请求。

[128] 在本说明书的技术方案中，还可以在隐私计算节点执行智能合约的过程中，执行对外部数据进行访问等操作，而无需在区块链通过预言机机制来调用隐私计算节点中的智能合约的情况下，才执行访问外部数据的操作，同时隐私计算节点对于智能合约的执行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“节点可信执行环境”，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，所涉及的实施细节比如隐私计算节点对可信执行环境的创建过程、隐私计算节点对远程证明报告的生成过程、客户端对远程证明报告的验证过程、对字节码的加解密方案、预言机访问外部数据等，同样可参考上述实施例，因此下文不再进行详细描述。

[129] 图 5 是本说明书一示例性实施例示出的一种隐私计算节点侧的访问外部数据的方法的流程图。如图 1 所示，该方法可以包括以下步骤。

[130] 步骤 502，隐私计算节点在节点可信执行环境中执行智能合约的过程中，在所述节点可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机。

[131] 如前所述，在隐私计算节点执行智能合约之前，需要将智能合约安全部署至该隐私计算节点处。智能合约可由某个客户端完成部署。上述的智能合约可能是响应于某个客户端发起的交易而执行，这里发起交易的客户端与部署智能合约的客户端可以为同一客户端，或者不同的客户端。

[132] 如前所述，隐私计算节点向预言机发送外部数据访问请求的过程中，或者预言机向隐私计算节点返回外部数据请求响应的过程中，涉及到设备之间的数据交互。可以通过对称加密、非对称加密或两者结合的方式，对外部数据访问请求和外部数据请求响应分别进行加密传输。

[133] 如前所述，隐私计算节点在将外部数据访问请求传输至预言机的过程中，可以在节点可信执行环境内基于预言机加密公钥对外部数据访问请求进行加密，并将加密后的外部数据访问请求发送至所述预言机。其中，该预言机可以包括维护有预言机加密私钥的预言机节点；或者，在该预言机为预言机集群的情况下，预言机加密私钥由预言机集

群的控制节点维护，加密后的外部数据访问请求被控制节点解密后转发至预言机集群内的预言机节点进行处理。

[134] 如前所述，隐私计算节点与预言机所支持的数据格式可能不同，造成隐私计算节点所生成的外部数据访问请求，可能无法被预言机顺利识别，进而造成对外部数据访问失败。因此，隐私计算节点在执行智能合约产生第一格式的外部数据访问请求后，可以主动将第一格式的外部数据访问请求转换为第二格式，而本步骤加密传输至预言机的即为转换为第二格式的外部数据访问请求。相应地，在预言机返回第二格式的外部数据请求响应后，隐私计算节点可以主动将第二格式的外部数据请求响应转换为第一格式，然后对该第一格式的外部数据请求响应予以处理。

[135] 如前所述，隐私计算节点可以对外部数据访问请求的访问行为进行限制。例如，可以将允许进行访问的 IP 地址写入预设的白名单中，并将外部数据访问请求的目标访问对象的 IP 地址与该白名单进行匹配，从而仅允许针对该白名单记录的 IP 地址进行访问；类似地，也可以将不允许进行访问的 IP 地址写入预设的黑名单，并将外部数据访问请求的目标访问对象的 IP 地址与该黑名单进行匹配，从而禁止针对该黑名单记录的 IP 地址进行访问。再例如，可以在配置文件中记录对外部数据访问请求的字段限制和内容限制，从而避免外部数据访问请求中包含敏感字段或敏感内容等。因此，在生成外部数据访问请求后，可以对外部数据访问请求中的字段进行检查，在检测到外部数据访问请求中存在不符合访问要求的字段或请求内容，或者目的 IP 地址未处于预设白名单的情况下，禁止执行访问外部数据的操作。

[136] 步骤 504，所述隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密。

[137] 如前所述，所述外部数据请求响应由预言机签名私钥进行签名；所述隐私计算节点在接收到所述外部数据访问请求后，可以基于预先获取的预言机签名公钥对所述外部数据请求响应进行验签。其中，所述隐私计算节点在确认验签成功的情况下，根据所述外部数据请求响应完成对所述智能合约的执行操作。

[138] 如前所述，在所述预言机为预言机节点的情况下，预言机签名私钥由所述预言机节点维护；所述隐私计算节点还可以获取针对所述预言机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预言机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预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定所述预言机节点可信的情况下，所述隐私计算节点将预言机签名公钥在本地保存；

[139] 如前所述，在所述预言机为预言机集群的情况下，预言机签名私钥由集群中响应于所述外部数据访问请求的预言机节点维护；所述隐私计算节点还可以分别获取针对集群中各个预言机节点的远程证明报告，每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成，所述自荐信息与相应预言机节点上创建的可信执行环境相关；所述隐私计算节点根据所述远程证明报告确定出可信的预言机节点，并将相应的预言机签名公钥在本地保存。

[140] 如前所述，预言机向隐私计算节点发送外部数据请求响应时，针对该外部数据请求响应进行加密传输。针对外部数据请求响应的加密传输过程，与前述的针对调用请求的加密传输过程类似，数据接收方均为隐私计算节点，只是数据发送方变为了预言机。与针对调用请求的加密传输过程相类似，针对外部数据请求响应进行加密传输时，可以采用对称加密、非对称加密或两者结合的数字信封等方式。并且，当采用非对称加密或数字信封的形式时，需要使用节点公钥，而相应的节点私钥可以仅由作为接收方的该隐私计算节点所维护、代表该链下隐私计算节点的节点身份，也可以代表该隐私计算节点所处的隐私计算集群的集群身份、由集群内的所有隐私计算节点共同维护。

[141] 步骤 506，所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请

求响应,根据所述外部数据请求响应完成对所述智能合约的执行操作。

[142] 如前所述,在所述隐私计算节点接收到外部数据访问请求后,可以将获取到的第二格式的外部数据请求响应转换为第一格式的外部数据请求响应;所述隐私计算节点基于所述第一格式的外部数据请求响应完成对所述智能合约的执行操作。

[143] 对应于上述隐私节点侧的实施例,本说明书还提出了预言机侧、预言机集群中的控制节点侧等其他方面的实施例,在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。

[144] 相应的,图 6 是本说明书一示例性实施例示出的另一种预言机侧的访问外部数据的方法的流程图。如图 6 所示,该方法可以包括以下步骤。

[145] 步骤 602,预言机接收隐私计算节点加密传输的外部数据访问请求,所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起。

[146] 如前所述,该预言机可以为单一预言机节点,也可以为包含多个预言机节点的预言机集群(包含控制节点,以及控制节点以外的预言机节点)。隐私计算节点用于加密的预言机加密公钥可以为单一预言机节点的加密公钥或预言机集群中控制节点以外的预言机节点的加密公钥,也可以为预言机集群中控制节点的加密公钥。

[147] 如前所述,预言机可以接收隐私计算节点在节点 TEE 内基于预言机加密公钥加密的外部数据访问请求,并基于预言机加密私钥对接收到的外部数据访问请求进行解密。其中,上述预言机加密公钥可以为单一预言机节点的加密公钥,也可以为预言机集群中控制节点以外的预言机节点的加密公钥。

[148] 如前所述,在预言机加密公钥为单一预言机节点的情况下,隐私计算节点在节点 TEE 内基于该单一预言机节点的加密公钥对外部数据访问请求进行加密,并将加密后的外部数据访问请求发送至该单一预言机节点,以由该单一预言机节点基于维护的加密私钥进行解密。

[149] 如前所述,在预言机加密公钥为预言机集群中控制节点以外的预言机节点的加密公钥的情况下,隐私计算节点在节点 TEE 内基于任一预言机节点的加密公钥对外部数据访问请求进行加密,并将加密后的外部数据访问请求发送至预言机集群中的控制节点,并由控制节点将加密的外部数据访问请求转发至该任一预言机节点,以由该任一预言机节点基于维护的加密私钥进行解密。

[150] 如前所述,预言机集群中的控制节点可以接收隐私计算节点在节点 TEE 内基于预言机加密公钥加密的外部数据访问请求,并基于该控制节点维护有的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理。在该实施方式中,隐私计算节点用于加密外部数据访问请求的预言机加密公钥为控制节点的加密公钥;其中,基于控制节点维护有的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理可以包括:基于控制节点维护的加密私钥对接收到的外部数据访问请求进行解密,并基于任一预言机节点的加密公钥对外部数据访问请求进行重新加密,并向该任一预言机节点转发重新加密的外部数据访问请求。

[151] 如前所述,隐私计算节点与预言机可能支持不同的数据编码格式。因此,隐私计算节点在生成第一格式的外部数据访问请求后可以将其转换为第二格式。换言之,预言机接收到的隐私计算节点发送的第二格式的外部数据访问请求由隐私计算节点对第一格式的外部数据访问请求转换得到;而第一格式的外部数据访问请求在执行智能合约的情况下产生。

[152] 步骤 604,所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求,并根据所述外部数据访问请求访问远程服务器。

[153] 步骤 606,所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密,将加密后的外部数据请求响应返回所述隐私计算节点;所述外部数据请求响

应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

[154] 如前所述，预言机在基于访问结果创建外部数据请求响应后，还可以基于维护的预言机签名私钥对该外部数据请求响应进行签名，以向隐私计算节点证明该外部数据请求响应的可靠性。

[155] 如前所述，为了使隐私计算节点能够基于预先维护的预言机的签名公钥对带有签名的外部数据请求响应进行验签，需要预先获取预言机签名公钥。为此，还可以包括对预言机进行远程证明的过程。其中，在该预言机为预言机节点的情况下，预言机签名私钥由该预言机节点维护；该预言机节点可以向隐私计算节点返回远程证明报告；该远程证明报告由认证服务器对该预言机节点产生的自荐信息进行验证后生成，该自荐信息与该预言机节点上创建的 TEE 相关；在根据该远程证明报告确定预言机节点可信的情况下，预言机签名公钥被所述隐私计算节点保存在本地。在该预言机为预言机集群的情况下，预言机签名私钥由集群中响应于外部数据访问请求的预言机节点维护；预言机集群中的控制节点向隐私计算节点返回集群中各个预言机节点的远程报告证明，每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成，所述自荐信息与相应预言机节点上创建的 TEE 相关；在根据所述远程证明报告确定出可信预言机节点的情况下，所述可信预言机节点的预言机签名公钥被所述隐私计算节点保存在本地。

[156] 如前所述，在基于访问结果创建外部数据请求响应后，预言机可以采用节点公钥对创建的外部数据请求响应进行加密，并将加密的外部数据请求响应返回给所述隐私计算节点，以由隐私计算节点基于节点私钥对加密的外部数据请求响应进行解密。其中，在隐私计算节点属于隐私计算集群的情况下，节点私钥仅被所述隐私计算节点所维护，或者节点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。

[157] 如前所述由于预言机采用第二格式对数据进行编码，因此，基于访问结果创建的外部数据请求响应也采用第二格式；该第二格式的外部数据请求响应在返回至隐私计算节点后，将由隐私计算节点转换为第一格式的外部数据请求响应；隐私计算节点可以基于所述第一格式的外部数据请求响应完成对所述智能合约的执行操作。

[158] 相应的，图 7 是本说明书一示例性实施例示出的另一种预言机控制节点侧的访问外部数据的方法的流程图。如图 7 所示，该方法可以包括以下步骤。

[159] 步骤 702，预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起。

[160] 如前所述，隐私计算节点基于控制节点的加密公钥对外部数据访问请求进行加密，控制节点在接收到隐私计算节点发送的外部数据访问请求的情况下，在控制节点 TEE 中基于维护的控制节点加密私钥对接收到的外部数据访问请求进行解密。

[161] 步骤 704，所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问。

[162] 如前所述，控制节点在接收到外部数据访问请求后，可以在集群中选取一可信节点作为处理本次外部数据访问请求的预言机节点（该可信节点即为本步骤中被选取的预言机节点）；并可以在控制节点 TEE 中基于该可信节点的加密公钥对外部数据访问请求进行重新加密，并将重新加密后的外部数据访问请求发送至该可信节点。

[163] 步骤 706，所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述隐私计算节点。

[164] 如前所述，被选取的预言机节点在接收到控制节点发送的重新加密后的外部数据访问请求后，可以在被选预言机 TEE 中基于自身维护的加密私钥（即该可信节点的加密私钥）进行解密；并基于解密后的外部数据访问请求向相应的远程服务器发起访问。

[165] 如前所述，在接收到远程服务器返回的访问结果后，该被选取的预言机节点可以在 TEE 中基于该访问结果创建外部数据请求响应，并用该被选取的预言机的签名私钥进行签名；该签名后的外部数据访问请求在隐私计算节点基于预先获取的预言机公钥（即该被选取的预言机的加密公钥）验签后，用于完成对智能合约的执行操作。

[166] 如前所述，隐私计算节点可以通过多种方式获取被选取预言机的加密公钥。例如，可以由控制节点向隐私计算节点发送远程报告证明；远程证明报告由隐私计算节点进行验证后，将所述远程证明对应的预言机节点确定为可信节点；所述可信节点的公钥信息被隐私计算节点保存在本地。在一种实施方式中，隐私计算节点可以预先获取预言机集群中所有可信节点的公钥信息。此时，可以由控制节点向隐私计算节点发送集群中所有预言机节点对应的远程证明报告；由隐私计算节点对接收到远程证明报告进行验证，并将验证成功的远程证明报告对应的预言机节点确定为可信节点，并将所有可信节点的签名公钥信息在本地保存。

[167] 如前所述，可以由控制节点接收集群中预言机节点的远程证明报告，并基于远程证明报告确定预言机节点是否为可信节点；在接收到隐私计算节点发送的外部数据访问请求的情况下，控制节点可以基于负载均衡的原则分配一可信节点用于处理该外部数据访问请求。

[168] 下面以单一预言机节点为例，结合图 8 和图 9 对本说明书的技术方案进行介绍。其中，图 8 是本说明书一示例性实施例示出的一种基于单一预言机节点访问外部数据的示意图，图 9 是本说明书一示例性实施例示出的一种基于单一预言机节点访问外部数据的交互图。如图 9 所示，将单一预言机节点称为预言（Oracle）节点，交互过程可以包括步骤 901~步骤 913。

[169] 步骤 901，链下隐私计算节点执行链下合约。

[170] 链下合约被预先部署于链下隐私计算节点处。链下隐私计算节点在链下 TEE 中对链下合约的字节码进行加密后，存储至链下 TEE 的外部，比如硬盘中。链下隐私计算节点可以响应于接收到的调用请求，从调用请求中读取需要调用的链下合约的合约 ID，并根据该合约 ID 查找相应的链下合约的加密后字节码，将该加密后字节码读入链下 TEE 内，然后在链下 TEE 内解密得到明文的字节码。

[171] 链下 TEE 中部署有链下合约的执行引擎，比如 EVM（以太坊虚拟机）、WASM 虚拟机或其他类型的虚拟机。链下隐私计算节点通过链下 TEE 内的虚拟机执行上述的字节码，即执行上述的链下合约。如果链下 TEE 中部署了多种类型的执行引擎，通常链下隐私计算节点在部署链下合约时，还会记录用于执行该链下合约的虚拟机的信息，以确保在该链下合约被调用时，采用正确的虚拟机执行该链下合约。链下合约可能包含多个函数。调用请求中可以包含函数名，以指示链下隐私计算节点通过虚拟机仅执行该函数名对应的函数，而非链下合约的所有字节码。

[172] 针对链下合约的调用请求，可以来源于区块链节点，比如区块链节点接收客户端提交的一笔交易，并在执行该交易的过程中产生链下隐私计算需求，从而通过预言机机制向链下隐私计算节点传输调用请求。或者，针对链下合约的调用请求还可以来源于客户端，比如客户端通过链下渠道直接将调用请求发送至链下隐私计算节点。

[173] 步骤 902，链下隐私计算节点创建外部数据访问请求。

[174] 在开发人员编译链下合约的过程中，可以在链下合约中定义外部数据访问接口，该外部数据访问接口可由链下合约中的一个或多个函数所调用。在执行链下合约的过程中，通过调用该外部数据访问接口，可使链下隐私计算节点创建上述的外部数据访问请求，以实现针对外部数据的访问操作。

[175] 外部数据访问请求中可以包含所要访问的远程服务器的 IP 地址，以及所要访问的内容（比如存储地址、关键词等）。出于安全性的考量，链下隐私计算节点处可以预先配置有安全文件，该安全文件用于对产生的外部数据访问请求进行安全过滤。比如，安

全文件中可以包含对外部数据访问请求的字段限制、访问内容限制、IP 地址限制等中的一种或多种。其中，字段限制和访问内容限制可以基于安全文件对外部数据访问请求中的字段进行检查实现，比如，当检测到外部数据访问请求中存在不符合访问要求的字段或请求内容时，不允许进行访问外部数据的执行操作；IP 地址限制可以基于 IP 白名单实现，比如当外部数据访问请求中的目的 IP 地址不在该 IP 白名单内时，不允许进行访问外部数据的执行操作。

[176] 开发人员可以根据预先定义的外部数据访问请求模型编译生成链下合约，使得链下合约可以支持符合该模型的外部数据访问请求。例如，当该模型为 HTTPS 请求模型时，链下合约所创建的外部数据访问请求为相应的 HTTPS 请求。HTTPS 模型包括 HTTP 模型和 SSL 模型。在 HTTP 模型中可以包含远程服务器地址、远程服务器的端口、请求方法（如 GET/POST）、访问资源的路径、版本协议、HTTPS 请求头、HTTPS 请求体等信息；在 SSL 模型中则可以包含信任的远程服务器的 CA 根证书、与远程服务器建立 TLS 连接所使用的客户端证书以及该证书对应的 Key 值等信息。其中，远程服务器的地址和端口等字段的取值，可以在链下合约中定义，使得相应生成的外部数据访问请求中必然包含链下合约中定义的上述远程服务器的地址和端口，即链下合约所定义的远程服务器为固定服务器；或者，远程服务器的地址和端口可以在链下合约中定义为空，并由调用请求中包含的参数所定义，使得相应生成的外部数据访问请求中包含由调用请求所指示的远程服务器的地址和端口，即链下合约所定义的远程服务器不固定。

[177] 如果预言节点并不支持上述的 HTTPS 协议或者链下隐私计算节点所产生的其他协议的外部数据访问请求，则链下隐私计算节点还需要对创建的外部数据访问请求进行格式转换，以使预言节点能够顺利处理接收到的外部数据访问请求。为实现格式转换的功能，可以预先设置一格式转换接口，并可以在需要进行格式转换时，通过调用该接口进行格式转换。举例而言，该格式转换接口可以用于指示预言（Oracle）编码模型，该编码模型中包含预言编码格式（即前文中的第二格式）的通用字节码，在转换过程中只需将创建的采用链下节点编码格式（即前文中的第一格式）的外部数据访问请求中的特定信息复制到该预言编码模型中即可。当然，该转换方式仅是示意性的，具体如何实现格式转换可以由本领域技术人员根据实际情况确定。

[178] 步骤 903，链下隐私计算节点创建的外部数据访问请求进行加密。

[179] 在本实施例中，由于只存在单一预言节点，因此链下隐私计算节点将该预言节点的加密公钥读入链下 TEE 内，并基于该加密公钥在链下 TEE 中对创建的外部数据访问请求进行加密。

[180] 步骤 904，链下隐私计算节点向预言节点发送加密后的外部数据访问请求。

[181] 步骤 905，预言节点对接收到的外部数据访问请求进行解密。

[182] 在本实施例中，预言节点基于自身维护的加密私钥，在该预言节点所创建的 TEE 内对接收到的外部数据访问请求进行解密。

[183] 步骤 906，预言节点基于外部数据访问请求创建远程服务器访问请求。

[184] 由于在步骤 902 中已经将外部数据访问请求转化为预言编码格式，因此，预言节点在步骤 905 对外部数据访问请求解密后，可以直接读取该外部数据访问请求中的数据，并根据该外部数据访问请求的内容向远程服务器发起访问。例如，预言节点可以包括基于读取的远程服务器的 IP 地址、端口等信息创建远程服务器访问请求，以向远程服务器发起请求。

[185] 远程服务器访问请求中可以包含外部数据的信息，用于指示远程服务器获取相应的外部数据。预言节点可以在自身创建的 TEE 内对远程服务器访问请求进行加密，以避免在传输过程中暴露请求中所含的外部数据的信息。

[186] 步骤 907，预言节点向远程服务器发送访问请求。

[187] 步骤 908，远程服务器向预言节点返回访问结果。

[188] 步骤 909, 预言节点基于返回的访问结果创建外部数据请求响应。

[189] 如果远程服务器访问请求被加密, 远程服务器需要将加密后的远程服务器访问请求读入自身创建的 TEE 内, 并在该 TEE 内执行解密操作, 以得到明文的远程服务器访问请求。

[190] 类似地, 远程服务器可以在自身创建的 TEE 内对访问结果进行加密, 然后将加密后的访问结果返回预言节点。在预言节点接收到远程服务器返回的访问结果后, 可以在该预言节点创建的 TEE 内对访问结果进行解密, 读取该访问结果中的数据, 并基于读取的数据创建外部数据请求响应。

[191] 步骤 910, 预言节点对创建的外部数据请求响应进行加密并签名。

[192] 预言节点在创建外部数据请求响应后, 还在 TEE 内通过预言节点的签名私钥进行签名, 以及基于链下隐私计算节点的加密公钥对外部数据请求响应进行加密, 然后传输至链下隐私计算节点。相应地, 链下隐私计算节点可以通过解密和验签, 确保得到的外部数据请求响应是否可靠。

[193] 为实现本步骤签名和加密的操作, 需要对预言节点进行远程证明。为方便理解该远程证明的过程可参考图 10。图 10 为本说明书一示例性实施例示出的一种对单一预言机节点进行远程证明的流程图。

[194] 由图 10 可知, 在单一预言机的情况下, 链下隐私计算节点对预言机节点进行远程证明主要包括以下几个步骤: 步骤①, 链下隐私计算节点向预言机节点发起挑战; 步骤②, 预言机节点接收到挑战信息后, 生成与预言机 TEE 相关的自荐信息并发送给认证服务器; 步骤③, 认证服务器对预言机的自荐信息进行验证, 并基于验证结果生成远程证明报告; 并返回给预言机; 步骤④, 预言机将该远程证明报告转发给链下隐私计算节点, 以由链下隐私计算节点基于该远程证明报告确定预言机节点是否可信。

[195] 在上述过程中, 认证服务器在用自身的签名私钥对远程证明报告签名后再返回, 以此证明该远程证明报告的可靠性(接收到该远程证明报告的设备可以基于该认证服务器的签名公钥验证该远程证明报告是否为认证服务器创建的)。其中, 远程证明报告可以由预言机转发至链下隐私节点, 也可以由认证服务器直接发送至链下隐私计算节点。链下隐私计算节点在接收到远程证明报告并基于认证服务器的公钥验签成功后, 便可将预言机节点的签名公钥保存在本地, 以用于对预言机返回的外部数据请求响应进行验签。

[196] 步骤 911, 预言节点向链下隐私计算节点返回加密的外部数据请求响应。

[197] 步骤 912, 链下隐私计算节点对接收到的外部数据请求响应进行验签并解密。

[198] 链下隐私计算节点接收到外部数据请求响应后, 可以基于预先获取的预言机公钥进行验签, 并在验签成功后基于自身维护的加密私钥对外部数据请求响应进行解密。在本步骤中, 由于步骤 910 中先加密后验签, 因此本步骤先进行验签后解密。本实施例采用这种顺序的原因在于, 在验签失败的情况下, 证明该请求响应本身不可靠, 无需再进行解密等步骤; 若步骤 910 中优先进行签名后进行加密, 那么, 本步骤中需要优先解密再进行验签, 这种情况下, 即使请求响应本身不可靠, 仍需要对请求响应进行解密和验签两个步骤。当然, 具体如何操作, 本领域技术人员可以根据实际需求确定。

[199] 步骤 913, 链下隐私计算节点基于解密并验签后的外部数据请求响应完成链下合约的执行操作。

[200] 在从外部数据请求响应中获取到外部数据后, 即可根据获取到的外部数据完成链下合约的执行操作。在链下合约执行完成后还可以通过图 2 中区块链下的预言机将执行结果反馈给区块链节点, 以由区块链节点完成对链上合约的执行操作。

[201] 链下隐私计算节点也可以属于链下隐私计算集群。在这种情况下, 区块链节点可以调用集群中任一可信的链下隐私计算节点执行链下合约。其中, 链下隐私计算集群中通常包含一控制节点, 也可以由该控制节点分配一可信节点作为执行链下合约的链下隐私计算节点, 此时, 若集群中任一可信节点需要访问外部数据即可通过控制节点与预言

机进行交互。

[202] 由上述技术方案可知，本说明书的技术方案可以在链下合约执行过程中检测到存在外部数据访问需求的情况下，可以由链下隐私计算节点通过单一预言机节点向远程服务器发起访问，并借助基于返回的访问结果创建的外部数据请求响应完成对链下合约的执行操作。

[203] 进一步的，在创建外部数据访问请求之前，链下隐私计算节点预先对预言机节点进行了远程证明，进而确保了预言机节点的可靠性。其次，链下隐私计算节点在基于远程证明确定预言机节点为可信节点的情况下，在本地保存有预言机节点的签名公钥，使得在接收到预言机节点返回的带有预言机签名的外部数据请求响应后，能够对其进行验签。通过这样的验签机制确保了数据的安全性和完整性。

[204] 再进一步的，在本实施例中，预言机节点的加密密钥对与签名密钥对可以为同一密钥对。这样的方式使得在保证数据安全性和完整性的前提下，简化了加解密以及签名验签的复杂程度。

[205] 下面以预言机为预言机集群为例，结合图 11 和图 12 对本说明书的技术方案进行介绍。其中，图 11 是本说明书一示例性实施例示出的一种基于预言机集群访问外部数据的示意图。图 12 是本说明书一示例性实施例示出的一种基于预言机集群访问外部数据的方法的交互图。如图 12 所示，在该方法中可以将预言机集群称为预言（Oracle）集群，集群中包含一控制节点，将集群中除控制节点以外的预言节点称为实体（Entity），该方法可以包括步骤 1201~步骤 1217。

[206] 步骤 1201，链下隐私计算节点执行链下合约。

[207] 本步骤与步骤 901 相类似，可参照步骤 901 的介绍，在此不作赘述。

[208] 步骤 1202，链下隐私计算节点创建外部数据访问请求。

[209] 本步骤与步骤 902 相类似，可参照步骤 902 的介绍，在此不作赘述。

[210] 步骤 1203，链下隐私计算节点创建的外部数据访问请求，并用预言控制节点的加密公钥进行加密。

[211] 在本实施例中，与上一实施例不同的是，在上一实施例中，链下隐私计算节点将单一预言节点的加密公钥读入链下 TEE 内，并基于该加密公钥在链下 TEE 中对创建的外部数据访问请求进行加密；而在本实施例中，链下隐私计算节点将控制节点的加密公钥读入链下 TEE 内，并基于控制节点的加密公钥在链下 TEE 中对创建的外部数据访问请求进行加密。换言之，在上一实施例中，链下隐私计算节点基于实际处理外部数据访问请求的预言节点的加密公钥对外部数据访问请求进行加密；而在本实施例中，基于控制节点的加密公钥对外部数据访问请求进行加密，但控制节点本申请并不对外部数据访问请求进行处理。

[212] 通过这样的方式，链下隐私计算节点无需与控制节点预先协商由集群中哪一实体对外部数据访问请求进行处理，同时也无需采用该实体对应的预言机加密公钥进行加密。

[213] 步骤 1204，链下隐私计算节点向预言控制节点发送加密后的外部数据访问请求。

[214] 步骤 1205，预言控制节点基于控制节点加密私钥对接收到的外部数据访问请求进行解密。

[215] 在本实施例中，预言控制节点基于自身维护的加密私钥，在该控制节点所创建的 TEE 内对接收到的外部数据访问请求进行解密。除此之外，预言控制节点在接收到外部数据访问请求后，还需要给本次外部数据访问请求分配一实体用于处理本次外部数据访问请求。具体的，可参考图 11 所述的设备架构图。如图 11 所示，预言机集群中包括预言控制节点以及 A、B、C...若干个实体。控制节点在接收到外部数据访问请求后，将实体 A 分配为处理本次外部数据访问请求的预言机节点，即向远程服务器发起访问等操作均由实体 A 执行，后续步骤中将以实体 A 为分配得到的实体对交互过程进行介绍。

[216] 其中，控制节点可以采用多种方式分配处理外部数据访问请求的实体。为方便表

述，后文中将该过程简称为分配实体。例如，可以随机或基于负载均衡算法从预言机集群中选取一实体用于处理本次外部数据访问请求。在本实施例中，控制节点基于负载均衡算法分配实体。具体的，控制节点可以在接收到外部数据访问请求的情况下，分别获取集群中每一实体的负载情况，并基于负载均衡算法将性能状况较好的实体作为负责本次处理外部数据访问请求的预言机节点。除此之外，控制节点也可以通过实时监控集群中各个实体负载情况，在接收到外部数据访问请求的情况下，基于负载均衡算法对已获取的负载情况确定出性能较好的实体。当然，上述举例仅是示意性的，具体的如何实现基于负载均衡算法分配实体可由本领域技术人员根据实际情况确定，在此不作限定。

[217] 在采用负载均衡算法分配实体之前，还需要确定集群中所有实体是否为可信节点。为此，需要预先对集群中各个实体进行远程证明。远程证明的方式可以通过多种方式实现。在本实施例中，可以采用如图 10 所述的方法对集群中的实体进行远程证明。

[218] 图 13 为本说明书一示例性实施例示出的一种对预言机集群中的预言机节点进行远程证明的流程图。该过程可以包括以下步骤：步骤①，由预言控制节点向集群中所有实体发起挑战；步骤②，集群中任一实体在接收到挑战信息后，生成与实体中 TEE 相关的自荐信息并发送给认证服务器；步骤③，认证服务器在接收到任一实体发送的自荐信息后，对自荐信息进行验证，并基于验证结果生成相应的远程证明报告并返回给该任一实体；步骤④，所有接收到认证服务器返回的远程证明报告的实体，将该远程证明报告返回给预言控制节点。预言控制节点在接收到所有远程证明报告后，对所有远程证明报告进行验证，并将验证成功的远程证明报告对应的实体确定为可信节点，在本实施例中，可以将所有确定为可信节点的实体组成的集群确定为可信集群。进一步的，链下隐私计算节点可以向预言控制节点请求获取远程证明报告，以由链下隐私计算节点验证预言集群中的实体是否可信；当链下隐私计算节点基于远程证明报告确定任一实体可信时，可以将该任一实体的签名公钥保存在本地。关于认证服务器如何证明远程证明报告可靠性的内容可参照步骤 910 中的介绍，在此不作赘述。

[219] 当然，除了由控制节点对集群中的实体发起挑战，也可以由链下隐私计算节点向控制节点发起挑战，再由控制节点向各个实体转发该挑战信息。具体获取远程证明报告的过程与控制节点发起挑战一致，在此不作赘述。

[220] 在通过上述方式确定集群中的实体均为可信节点的情况下，预言控制节点即可采用负载均衡算法分配实体。通过这样的方式，能够较好地平衡各个实体的负载情况，避免了单个实体负载过高的情况，进而提高整个集群性能的稳定性。

[221] 预言控制节点在基于控制节点加密私钥对外部数据访问请求解密并且分配实体后，预言控制节点可以基于分配得到的实体的加密公钥（在本实施例中，即为实体 A 的加密公钥）对外部数据访问请求进行加密。通过这样的方式，预言控制节点无需预先与链下隐私计算节点协商用于处理本次外部数据访问请求的实体，减少了交互次数，进而提高了访问效率。

[222] 步骤 1206，预言控制节点基于实体 A 的加密公钥对外部数据访问请求重新加密。

[223] 为保证数据以密文的形式进行传输，并且能够被实体 A 解密，需要由预言控制节点基于预先获取的实体 A 的加密公钥对外部数据访问请求重新加密。

[224] 步骤 1207，预言控制节点将重新加密后的外部数据访问请求发送至实体 A。

[225] 步骤 1208，实体 A 基于自身加密私钥对接收到的外部数据访问请求进行解密。

[226] 实体 A 基于自身维护的加密私钥，在实体 A 所创建的 TEE 内对接收到的外部数据访问请求进行解密。

[227] 步骤 1209，实体 A 基于解密后的外部数据访问请求创建远程访问请求。

[228] 本步骤与步骤 906 相类似，可参照步骤 906 的介绍，在此不作赘述。

[229] 步骤 1210，实体 A 向远程服务器发起访问。

[230] 步骤 1211，远程服务器向实体 A 返回访问结果。

[231] 步骤 1212, 实体 A 基于接收到的访问结果创建外部数据请求响应。

[232] 本步骤除执行主体为实体 A 以外, 与步骤 909 相类似, 可参照步骤 909 的介绍, 在此不作赘述。

[233] 步骤 1213, 实体 A 对创建的外部数据请求响应进行加密并签名。

[234] 实体 A 在创建外部数据请求响应后, 还在 TEE 内通过实体 A 的签名私钥进行签名, 以及基于链下隐私计算节点的加密公钥对外部数据请求响应进行加密, 然后通过预言控制节点传输至链下隐私计算节点。相应地, 链下隐私计算节点可以通过解密和验签, 确保得到的外部数据请求响应是否可靠。

[235] 与上一实施例相类似, 链下隐私计算节点需要预先对实体 A 进行远程证明。在实际操作中, 链下隐私计算节点通常只与预言集群的控制节点交互, 即链下隐私计算节点将预言机集群作为一个整体的“预言机”进行交互。因此, 通常情况下, 需要预先对预言集群中的所有实体进行远程证明。由于在本实施例中, 预言控制节点可能已经预先对集群中的实体进行了远程证明(如步骤 1205 所述)。在这种情况下, 当控制节点接收到链下隐私计算节点发送的远程证明报告获取请求时, 只需将保留于控制节点中的所有实体对应的远程证明报告发送至链下隐私计算节点, 链下隐私计算节点可以在接收到所有远程证明报告后验证预言集群中所有实体是否为可信节点, 并将验证成功的可信节点的签名公钥保存在本地。换言之, 在远程证明后, 链下隐私计算节点中保存有所有可信实体的签名公钥。因此, 无论外部数据请求响应由哪一实体返回, 链下隐私计算节点均可以基于保存的签名公钥对接收到的外部数据请求响应进行验签。

[236] 值得注意的是, 在链下隐私计算节点属于链下隐私计算集群的情况下, 上述远程证明的过程可由链下隐私计算集群中的控制节点发起, 在验证成功后, 将信息同步至集群中所有链下隐私计算节点。当然, 也可以由集群中任一链下隐私计算节点执行上述验证过程后, 将验证信息同步至其他链下隐私计算节点; 为了进一步确保验证的可靠性, 还可以由集群中所有链下隐私计算节点分别进行验证。

[237] 步骤 1214, 实体 A 将加密后的外部数据请求响应发送至预言控制节点。

[238] 步骤 1215, 预言控制节点将加密的外部数据请求响应转发至链下隐私计算节点。

[239] 在链下隐私计算节点属于链下隐私计算集群的情况下, 通常需要将该外部数据请求响应发送至链下隐私计算集群的控制节点, 再由该控制节点转发至发送对应外部数据访问请求的链下隐私计算节点。

[240] 步骤 1216, 链下隐私计算节点对接收到的外部数据请求响应验签并解密。

[241] 在链下隐私计算节点本地保留有所有可信实体的签名公钥信息, 可以利用其中实体 A 的签名公钥对接收到外部数据请求响应进行验签; 以及基于自身维护的链下节点私钥对该外部数据请求响应进行解密。与上一实施例相类似, 在实体 A 先对外部数据请求响应进行加密、后进行签名的情况下, 在本步骤优先对外部数据请求响应进行验签, 后进行解密。关于签名加密, 以及验签解密的顺序介绍可参照步骤 912 的介绍, 在此不作赘述。

[242] 步骤 1217, 链下隐私计算节点基于解密并验签后的外部数据请求响应完成链下合约的执行操作。

[243] 本步骤内容与步骤 913 相类似, 可参照步骤 913 中相关介绍, 在此不作赘述。值得注意的是, 在本实施例中, 链下隐私计算节点用于对外部数据访问请求进行加密的预言机加密公钥(属于控制节点), 与链下隐私计算节点用于对外部数据请求响应进行验签的预言机签名私钥(属于实体 A)一定不属于同一密钥对。

[244] 与上一实施例相比, 由于本实施例引入了预言机集群的概念, 使得链下隐私计算节点在访问外部数据的情况下, 有更多可选择预言机节点。可以理解的是, 在预言机集群中, 若单一节点发生故障, 仍可以通过预言机节点实现外部数据的访问。换言之, 本实施例通过设置预言机集群的方式提高了传输的可靠性。

[245] 进一步的, 在本实施例中, 由于链下隐私计算节点基于控制节点的加密公钥对外部数据访问请求进行加密, 使得链下隐私计算节点存在外部数据访问需求的情况下, 无需预先与预言机控制节点协商 (由集群中哪一预言机节点负责本次外部数据访问请求的处理), 进而减少了交互的次数, 提高了访问效率。

[246] 再进一步的, 由于预言机控制节点预先对预言机集群中的所有预言机节点进行了远程证明, 使得集群 (前述可信预言机集群) 中的预言机节点均为可信节点。这样的方式, 使得在链下隐私计算节点有外部数据访问需求的情况下, 预言机控制节点可以基于负载均衡原则分配用于处理本次外部数据访问请求的预言机节点。

[247] 图 14 是一示例性实施例提供的一种电子设备的示意结构图。请参考图 14, 在硬件层面, 该设备包括处理器 1402、内部总线 1404、网络接口 1406、内存 1408 以及非易失性存储器 1410, 当然还可能包括其他业务所需要的硬件。处理器 1402 从非易失性存储器 1410 中读取对应的计算机程序到内存 1408 中然后运行, 在逻辑层面上形成访问外部数据的装置。当然, 除了软件实现方式之外, 本说明书一个或多个实施例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。

[248] 请参考图 15, 在链下隐私计算节点侧的软件实施方式中, 该访问外部数据的装置可以包括: 请求单元 1501, 使链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中, 响应于所述链下合约的外部数据访问需求, 在所述链下可信执行环境中生成外部数据访问请求, 并将所述外部数据访问请求加密传输至预言机; 响应单元 1502, 使所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应, 所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密; 反馈单元 1503, 使所述链下隐私计算节点在所述链下可信执行环境内解密获得所述外部数据请求响应, 根据所述外部数据请求响应完成对所述链下合约的执行操作。

[249] 可选的, 所述请求单元 1501 进一步用于: 使所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥对所述外部数据访问请求进行加密, 并将加密后的外部数据访问请求发送至所述预言机; 其中, 所述预言机包括维护有预言机加密私钥的预言机节点; 或者, 在所述预言机为预言机集群的情况下, 所述预言机加密私钥由所述预言机集群的控制节点维护, 加密后的外部数据访问请求被所述控制节点解密后转发至所述预言机集群内的预言机节点进行处理。

[250] 可选的, 所述外部数据请求响应由预言机签名私钥进行签名; 还包括: 验签单元 1504, 使所述链下隐私计算节点基于预先获取的预言机签名公钥对所述外部数据请求响应进行验签; 其中, 所述链下隐私计算节点在确认验签成功的情况下, 根据所述外部数据请求响应完成对所述链下合约的执行操作。

[251] 可选的, 还包括: 认证单元 1505, 在所述预言机为预言机节点的情况下, 预言机签名私钥由所述预言机节点维护; 使所述链下隐私计算节点获取针对该预言机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预言机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预言机节点上创建的可信执行环境相关; 在根据所述远程证明报告确定所述预言机节点可信的情况下, 使所述链下隐私计算节点将预言机签名公钥在本地保存; 在所述预言机为预言机集群的情况下, 预言机签名私钥由集群中响应于所述外部数据访问请求的预言机节点维护; 使所述链下隐私计算节点分别获取针对集群中各个预言机节点的远程证明报告, 每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成, 所述自荐信息与相应预言机节点上创建的可信执行环境相关; 使所述链下隐私计算节点根据所述远程证明报告确定出可信的预言机节点, 并将相应的预言机签名公钥在本地保存。

[252] 可选的, 所述外部数据请求响应由预言机在预言机可信执行环境内采用链下节点

公钥进行加密；所述响应单元 1502 进一步用于：使所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，并在链下可信执行环境中通过链下节点私钥对接收到的外部数据请求响应进行解密。

[253] 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，链下节点私钥仅被所述链下隐私计算节点所维护，或者链下节点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。

[254] 可选的，所述请求单元 1501 进一步用于：使所述链下隐私计算节点获取执行所述链下合约产生的第一格式的外部数据访问请求，并将获取到的外部数据访问请求转换为第二格式；使所述链下隐私计算节点将转换为第二格式的外部数据访问请求加密传输至预言机；所述反馈单元 1503 进一步用于：使所述链下隐私计算节点将获取到的第二格式的外部数据请求响应转换为第一格式的外部数据请求响应；使所述链下隐私计算节点基于所述第一格式的外部数据请求响应完成对所述链下合约的执行操作。

[255] 可选的，还包括：检查单元 1506，使所述链下隐私计算节点对所述外部数据访问请求中的字段进行检查；在检测到所述外部数据访问请求中存在不符合访问要求的字段或请求内容，或者目的 IP 地址未处于预设白名单的情况下，禁止执行访问外部数据的操作。

[256] 请参考图 16，在预言机侧的软件实施方式中，该访问外部数据的装置可以包括：接收单元 1601，使预言机接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起；所述链下合约在被区块链节点调用的情况下，由所述链下隐私计算节点在链下可信执行环境内执行；访问单元 1602，使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；返回单元 1603，使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述链下隐私计算节点；所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

[257] 可选的，所述接收单元 1601 进一步用于：在所述预言机为预言机节点的情况下，使所述预言机接收所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥加密的外部数据访问请求，并基于预言机加密私钥对接收到的外部数据访问请求进行解密；或者，在所述预言机为预言机集群的情况下，使所述预言机集群中的控制节点接收所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥加密的外部数据访问请求，并基于该控制节点维护有的预言机加密私钥请求集群内的节点对所述加密后的外部数据访问请求进行处理。

[258] 可选的，还包括：签名单元 1604，使所述预言机基于预言机签名私钥对所述外部数据请求响应进行签名。

[259] 可选的，在所述预言机为预言机节点的情况下，预言机签名私钥由该预言机节点维护；所述返回单元 1603 进一步用于：使所述预言机向所述链下隐私计算节点返回远程证明报告；所述远程证明报告由认证服务器对该预言机节点产生的自荐信息进行验证后生成，所述自荐信息与该预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定预言机节点可信的情况下，预言机签名公钥被所述链下隐私计算节点保存在本地；在所述预言机为预言机集群的情况下，预言机签名私钥由集群中响应于所述外部数据访问请求的预言机节点维护；所述返回单元 1603 进一步用于：使所述预言机集群中的控制节点向所述链下隐私计算节点返回集群中各个预言机节点的远程报告证明，每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成，所述自荐信息与相应预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定出可信预言机节点的情况下，所述可信预言机节点的预言机签名公钥被所述链下隐私计算节点保存在本地。

[260] 可选的, 所述返回单元 1603 进一步用于: 使所述预言机采用链下节点公钥对创建的外部数据请求响应进行加密, 并将加密的外部数据请求响应返回给所述链下隐私计算节点; 所述加密的外部数据请求响应由所述链下隐私计算节点在接收后基于链下节点私钥进行解密。

[261] 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, 链下节点私钥仅被所述链下隐私计算节点所维护, 或者链下节点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。

[262] 可选的, 所述接收单元 1601 进一步用于: 使所述预言机接收链下隐私计算节点加密传输的外部数据访问请求, 包括: 使所述预言机接收所述链下隐私计算节点发送的第二格式的外部数据访问请求; 所述第二格式的外部数据访问请求由所述链下隐私计算节点在执行所述链下合约的情况下产生的第一格式的外部数据访问请求转换得到; 所述返回单元 1603 进一步用于, 使所述将加密后的外部数据请求响应返回所述链下隐私计算节点, 包括: 使所述预言机将第二格式的外部数据请求响应返回所述链下隐私计算节点; 所述第二格式的外部数据请求响应由所述链下隐私计算节点转换为第一格式的外部数据请求响应; 所述链下隐私计算节点基于所述第一格式的外部数据请求响应完成对所述链下合约的执行操作。

[263] 请参考图 17, 在预言机控制节点侧的软件实施方式中, 该访问外部数据的装置可以包括: 请求接收单元 1701, 使预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中, 响应于所述链下合约的外部数据访问需求而发起; 请求转发单元 1702, 使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求, 并向集群内被选取的预言机节点转发所述外部数据访问请求, 所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问; 结果返回单元 1703, 使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应, 并在控制节点可信执行环境内对所述外部数据请求响应进行加密后, 将经过加密的外部数据请求响应返回所述链下隐私计算节点。

[264] 可选的, 所述外部数据请求响应由所述被选取的预言机节点在预言机可信执行环境内创建, 并由所述被选取的预言机通过预言机私钥进行签名; 所述签名后的外部数据请求响应在所述链下隐私计算节点基于预先获取的预言机公钥验签后, 用于完成对所述链下合约的执行操作。

[265] 可选的, 还包括: 报告发送单元 1704, 使所述控制节点向所述链下隐私计算节点发送远程证明报告; 所述远程证明报告由所述链下隐私计算节点验证通过后, 将所述远程证明对应的预言机节点确定为可信节点; 所述可信节点的公钥信息被所述链下隐私计算节点保存在本地。

[266] 可选的, 还包括: 报告接收单元 1705, 使所述控制节点接收所述预言机集群中的预言机节点的远程证明报告, 并基于所述远程报告证明验证所述预言机节点是否为可信节点; 所述控制节点在接收到所述链下隐私计算节点发送的外部数据访问请求的情况下, 基于负载均衡分配一可信节点用于处理该外部数据访问请求。

[267] 请参考图 18, 在隐私计算节点侧的软件实施方式中, 该访问外部数据的装置可以包括: 请求单元 1801, 使隐私计算节点在节点可信执行环境中执行智能合约的过程中, 在所述节点可信执行环境中生成外部数据访问请求, 并将所述外部数据访问请求加密传输至预言机; 响应单元 1802, 使所述隐私计算节点接收所述预言机加密返回的外部数据请求响应, 所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密; 反馈单元 1803, 使所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请求响应, 根据所述外部数据请求响应完成对所述智能合约的执行操作。

[268] 可选的, 所述请求单元 1801 进一步用于: 使所述隐私计算节点在节点可信执行环境内基于预言机加密公钥对所述外部数据访问请求进行加密, 并将加密后的外部数据访问请求发送至所述预言机; 其中, 所述预言机包括维护有预言机加密私钥的预言机节点; 或者, 在所述预言机为预言机集群的情况下, 所述预言机加密私钥由所述预言机集群的控制节点维护, 加密后的外部数据访问请求被所述控制节点解密后转发至所述预言机集群内的预言机节点进行处理。

[269] 可选的, 所述外部数据请求响应由预言机签名私钥进行签名; 还包括: 验签单元 1804, 使所述隐私计算节点基于预先获取的预言机签名公钥对所述外部数据请求响应进行验签; 其中, 所述隐私计算节点在确认验签成功的情况下, 根据所述外部数据请求响应完成对所述智能合约的执行操作。

[270] 可选的, 所述外部数据请求响应由预言机在预言机可信执行环境内采用节点公钥进行加密; 所述响应单元 1802 进一步用于: 所述隐私计算节点接收所述预言机加密返回的外部数据请求响应, 并在节点可信执行环境中通过节点私钥对接收到的外部数据请求响应进行解密。

[271] 可选的, 在所述隐私计算节点属于隐私计算集群的情况下, 节点私钥仅被所述隐私计算节点所维护, 或者节点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。

[272] 请参考图 19, 在另一种预言机侧的软件实施方式中, 该访问外部数据的装置可以包括: 接收单元 1901, 使预言机接收隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起; 访问单元 1902, 使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求, 并根据所述外部数据访问请求访问远程服务器; 返回单元 1903, 使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密, 将加密后的外部数据请求响应返回所述隐私计算节点; 所述外部数据请求响应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

[273] 可选的, 所述接收单元 1901 进一步用于: 在所述预言机为预言机节点的情况下, 所述预言机接收所述隐私计算节点在节点可信执行环境内基于预言机加密公钥加密的外部数据访问请求, 并基于预言机加密私钥对接收到的外部数据访问请求进行解密; 或者, 在所述预言机为预言机集群的情况下, 所述预言机集群中的控制节点接收所述隐私计算节点在节点可信执行环境内基于预言机加密公钥加密的外部数据访问请求, 并基于该控制节点维护的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理。

[274] 可选的, 还包括: 签名单元 1904, 使所述预言机基于预言机签名私钥对所述外部数据请求响应进行签名。

[275] 可选的, 所述返回单元 1903 进一步用于: 使所述预言机采用节点公钥对创建的外部数据请求响应进行加密, 并将加密的外部数据请求响应返回给所述隐私计算节点; 所述加密的外部数据请求响应由所述隐私计算节点在接收后基于节点私钥进行解密。

[276] 可选的, 在所述隐私计算节点属于隐私计算集群的情况下, 节点私钥仅被所述隐私计算节点所维护, 或者节点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。

[277] 请参考图 20, 在另一种预言机控制节点侧的软件实施方式中, 该访问外部数据的装置可以包括: 请求接收单元 2001, 使预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求, 所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起; 请求转发单元 2002, 使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求, 并向集群内被选取的预言机节点转发所述外部数据访问请求, 所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问; 结果返回单元 2003, 使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应, 并在控制节点可信执行环境内对所述外部数据请求响

应进行加密后，将经过加密的外部数据请求响应返回所述隐私计算节点。

[278] 可选的，所述外部数据请求响应由所述被选取的预言机节点在预言机可信执行环境内创建，并由所述被选取的预言机通过预言机私钥进行签名；所述签名后的外部数据请求响应在所述隐私计算节点基于预先获取的预言机公钥验签后，用于完成对所述智能合约的执行操作。

[279] 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。

[280] 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。

[281] 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。

[282] 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。

[283] 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。

[284] 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。

[285] 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。

[286] 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”。

[287] 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

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、一种访问外部数据的方法，包括：

链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求，在所述链下可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；

所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密；

所述链下隐私计算节点在所述链下可信执行环境内解密获得所述外部数据请求响应，根据所述外部数据请求响应完成对所述链下合约的执行操作。

2、根据权利要求 1 所述的方法，将所述外部数据访问请求加密传输至预言机，包括：

所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥对所述外部数据访问请求进行加密，并将加密后的外部数据访问请求发送至所述预言机；

其中，所述预言机包括维护有预言机加密私钥的预言机节点；或者，在所述预言机为预言机集群的情况下，所述预言机加密私钥由所述预言机集群的控制节点维护，加密后的外部数据访问请求被所述控制节点解密后转发至所述预言机集群内的预言机节点进行处理。

3、根据权利要求 1 所述的方法，所述外部数据请求响应由预言机签名私钥进行签名；所述方法还包括：

所述链下隐私计算节点基于预先获取的预言机签名公钥对所述外部数据请求响应进行验签；

其中，所述链下隐私计算节点在确认验签成功的情况下，根据所述外部数据请求响应完成对所述链下合约的执行操作。

4、根据权利要求 3 所述的方法，

在所述预言机为预言机节点的情况下，预言机签名私钥由所述预言机节点维护；所述方法还包括：所述链下隐私计算节点获取针对所述预言机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预言机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预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定所述预言机节点可信的情况下，所述链下隐私计算节点将预言机签名公钥在本地保存；

在所述预言机为预言机集群的情况下，预言机签名私钥由集群中响应于所述外部数据访问请求的预言机节点维护；所述方法还包括：所述链下隐私计算节点分别获取针对集群中各个预言机节点的远程证明报告，每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成，所述自荐信息与相应预言机节点上创建的可信执行环境相关；所述链下隐私计算节点根据所述远程证明报告确定出可信的预言机节点，并将相应的预言机签名公钥在本地保存。

5、根据权利要求 1 所述的方法，所述外部数据请求响应由预言机在预言机可信执行环境内采用链下节点公钥进行加密；所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，包括：

所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应，并在链下可信执行环境中通过链下节点私钥对接收到的外部数据请求响应进行解密。

6、根据权利要求 5 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，链下节点私钥仅被所述链下隐私计算节点所维护，或者链下节点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。

7、根据权利要求 1 所述的方法，

所述链下隐私计算节点在所述链下可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；包括：所述链下隐私计算节点获取执行所述链下合约产生的第一格式的外部数据访问请求，并将获取到的外部数据访问请求转换为第二格式；所述链下隐私计算节点将转换为第二格式的外部数据访问请求加密传输至预言机；

所述根据所述外部数据请求响应完成对所述链下合约的执行操作，包括：所述链下隐私计算节点将获取到的第二格式的外部数据请求响应转换为第一格式的外部数据请求响应；所述链下隐私计算节点基于所述第一格式的外部数据请求响应完成对所述链下合约的执行操作。

8、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外部数据访问请求中的字段进行检查；

在检测到所述外部数据访问请求中存在不符合访问要求的字段或请求内容，或者目的IP地址未处于预设白名单的情况下，所述链下隐私计算节点禁止执行访问外部数据的操作。

9、一种访问外部数据的方法，包括：

预言机接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起；所述链下合约在被区块链节点调用的情况下，由所述链下隐私计算节点在链下可信执行环境内执行；

所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；

所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述链下隐私计算节点；所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

10、根据权利要求9所述的方法，所述预言机接收链下隐私计算节点加密传输的外部数据访问请求，包括：

在所述预言机为预言机节点的情况下，所述预言机接收所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥加密的外部数据访问请求，并基于预言机加密私钥对接收到的外部数据访问请求进行解密；或者，

在所述预言机为预言机集群的情况下，所述预言机集群中的控制节点接收所述链下隐私计算节点在链下可信执行环境内基于预言机加密公钥加密的外部数据访问请求，并基于该控制节点维护的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理。

11、根据权利要求9所述的方法，还包括：

所述预言机基于预言机签名私钥对所述外部数据请求响应进行签名。

12、根据权利要求11所述的方法，

在所述预言机为预言机节点的情况下，预言机签名私钥由该预言机节点维护；所述方法还包括：所述预言机向所述链下隐私计算节点返回远程证明报告；所述远程证明报告由认证服务器对该预言机节点产生的自荐信息进行验证后生成，所述自荐信息与该预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定预言机节点可信的情况下，预言机签名公钥被所述链下隐私计算节点保存在本地；

在所述预言机为预言机集群的情况下，预言机签名私钥由集群中响应于所述外部数据访问请求的预言机节点维护；所述方法还包括：所述预言机集群中的控制节点向所述链下隐私计算节点返回集群中各个预言机节点的远程报告证明，每一远程证明报告由认证服务器对相应预言机节点产生的自荐信息进行验证后生成，所述自荐信息与相应预言机节点上创建的可信执行环境相关；在根据所述远程证明报告确定出可信预言机节点的情况下，所述可信预言机节点的预言机签名公钥被所述链下隐私计算节点保存在本地。

13、根据权利要求9所述的方法，所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，包括：

所述预言机采用链下节点公钥对创建的外部数据请求响应进行加密，并将加密的外部数据请求响应返回给所述链下隐私计算节点；所述加密的外部数据请求响应由所述链下隐私计算节点在接收后基于链下节点私钥进行解密。

14、根据权利要求13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，链下节点私钥仅被所述链下隐私计算节点所维护，或者链下节点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。

15、根据权利要求9所述的方法，

所述预言机接收链下隐私计算节点加密传输的外部数据访问请求，包括：所述预言机接收所述链下隐私计算节点发送的第二格式的外部数据访问请求；所述第二格式的外部数据访问请求由所述链下隐私计算节点在执行所述链下合约的情况下产生的第一格式的外部数据访问请求转换得到；

所述将加密后的外部数据请求响应返回所述链下隐私计算节点，包括：所述预言机将第二格式的外部数据请求响应返回所述链下隐私计算节点；所述第二格式的外部数据请求响应由所述链下隐私计算节点转换为第一格式的外部数据请求响应；所述链下隐私计算节点基于所述第一格式的外部数据请求响应完成对所述链下合约的执行操作。

16、一种访问外部数据的方法，包括：

预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中，响应于所述链下合约的外部数据访问需求而发起；

所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问；

所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述链下隐私计算节点。

17、根据权利要求16所述的方法，所述外部数据请求响应由所述被选取的预言机节点在预言机可信执行环境内创建，并由所述被选取的预言机通过预言机私钥进行签名；所述签名后的外部数据请求响应在所述链下隐私计算节点基于预先获取的预言机公钥验签后，用于完成对所述链下合约的执行操作。

18、根据权利要求16所述的方法，还包括：

所述控制节点向所述链下隐私计算节点发送远程证明报告；所述远程证明报告由所述链下隐私计算节点验证通过后，将所述远程证明对应的预言机节点确定为可信节点；所述可信节点的公钥信息被所述链下隐私计算节点保存在本地。

19、根据权利要求16所述的方法，还包括：

所述控制节点接收所述预言机集群中的预言机节点的远程证明报告，并基于所述远程证明报告验证所述预言机节点是否为可信节点；

所述控制节点在接收到所述链下隐私计算节点发送的外部数据访问请求的情况下，基于负载均衡分配一可信节点用于处理该外部数据访问请求。

20、一种访问外部数据的方法，包括：

隐私计算节点在节点可信执行环境中执行智能合约的过程中，在所述节点可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；

所述隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加

密;

所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请求响应,根据所述外部数据请求响应完成对所述智能合约的执行操作。

21、根据权利要求 20 所述的方法,将所述外部数据访问请求加密传输至预言机,包括:

所述隐私计算节点在节点可信执行环境内基于预言机加密公钥对所述外部数据访问请求进行加密,并将加密后的外部数据访问请求发送至所述预言机;

其中,所述预言机包括维护有预言机加密私钥的预言机节点;或者,在所述预言机为预言机集群的情况下,所述预言机加密私钥由所述预言机集群的控制节点维护,加密后的外部数据访问请求被所述控制节点解密后转发至所述预言机集群内的预言机节点进行处理。

22、根据权利要求 20 所述的方法,所述外部数据请求响应由预言机签名私钥进行签名;所述方法还包括:

所述隐私计算节点基于预先获取的预言机签名公钥对所述外部数据请求响应进行验签;

其中,所述隐私计算节点在确认验签成功的情况下,根据所述外部数据请求响应完成对所述智能合约的执行操作。

23、根据权利要求 20 所述的方法,所述外部数据请求响应由预言机在预言机可信执行环境内采用节点公钥进行加密;所述隐私计算节点接收所述预言机加密返回的外部数据请求响应,包括:

所述隐私计算节点接收所述预言机加密返回的外部数据请求响应,并在节点可信执行环境中通过节点私钥对接收到的外部数据请求响应进行解密。

24、根据权利要求 23 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,节点私钥仅被所述隐私计算节点所维护,或者节点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。

25、一种访问外部数据的方法,包括:

预言机接收隐私计算节点加密传输的外部数据访问请求,所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起;

所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求,并根据所述外部数据访问请求访问远程服务器;

所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密,将加密后的外部数据请求响应返回所述隐私计算节点;所述外部数据请求响应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

26、根据权利要求 25 所述的方法,所述预言机接收隐私计算节点加密传输的外部数据访问请求,包括:

在所述预言机为预言机节点的情况下,所述预言机接收所述隐私计算节点在节点可信执行环境内基于预言机加密公钥加密的外部数据访问请求,并基于预言机加密私钥对接收到的外部数据访问请求进行解密;或者,

在所述预言机为预言机集群的情况下,所述预言机集群中的控制节点接收所述隐私计算节点在节点可信执行环境内基于预言机加密公钥加密的外部数据访问请求,并基于该控制节点维护的预言机加密私钥对所述加密后的外部数据访问请求解密后转发至所述预言机集群内的预言机节点进行处理。

27、根据权利要求 25 所述的方法,还包括:

所述预言机基于预言机签名私钥对所述外部数据请求响应进行签名。

28、根据权利要求 25 所述的方法,所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密,包括:

所述预言机采用节点公钥对创建的外部数据请求响应进行加密,并将加密的外部数据请求响应返回给所述隐私计算节点;所述加密的外部数据请求响应由所述隐私计算节点在接收后基于节点私钥进行解密。

29、根据权利要求 28 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,节点私钥仅被所述隐私计算节点所维护,或者节点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。

30、一种访问外部数据的方法,包括:

预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求,所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起;

所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求,并向集群内被选取的预言机节点转发所述外部数据访问请求,所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问;

所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应,并在控制节点可信执行环境内对所述外部数据请求响应进行加密后,将经过加密的外部数据请求响应返回所述隐私计算节点。

31、根据权利要求 30 所述的方法,所述外部数据请求响应由所述被选取的预言机节点在预言机可信执行环境内创建,并由所述被选取的预言机通过预言机私钥进行签名;所述签名后的外部数据请求响应在所述隐私计算节点基于预先获取的预言机公钥验签后,用于完成对所述智能合约的执行操作。

32、一种访问外部数据的装置,包括:

请求单元,使链下隐私计算节点在链下可信执行环境中执行被区块链节点调用的链下合约的过程中,响应于所述链下合约的外部数据访问需求,在所述链下可信执行环境中生成外部数据访问请求,并将所述外部数据访问请求加密传输至预言机;

响应单元,使所述链下隐私计算节点接收所述预言机加密返回的外部数据请求响应,所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密;

反馈单元,使所述链下隐私计算节点在链下可信执行环境内解密获得所述外部数据请求响应,根据所述外部数据请求响应完成对所述链下合约的执行操作。

33、一种访问外部数据的装置,包括:

接收单元,使预言机接收链下隐私计算节点加密传输的外部数据访问请求,所述外部数据访问请求由所述链下隐私计算节点响应于链下合约的外部数据访问需求而发起;所述链下合约在被区块链节点调用的情况下,由所述链下隐私计算节点在链下可信执行环境内执行;

访问单元,使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求,并根据所述外部数据访问请求访问远程服务器;

返回单元,使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密,将加密后的外部数据请求响应返回所述链下隐私计算节点;所述外部数据请求响应用于在所述链下可信执行环境内解密后参与所述链下合约的执行操作。

34、一种访问外部数据的装置,包括:

请求接收单元,使预言机集群中的控制节点接收链下隐私计算节点加密传输的外部数据访问请求,所述外部数据访问请求由所述链下隐私计算节点在链下可信执行环境内执行被区块链节点调用的链下合约的过程中,响应于所述链下合约的外部数据访问需求而发起;

请求转发单元,使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求,并向集群内被选取的预言机节点转发所述外部数据访问请求,所述外部数据

访问请求用于指示被选取的预言机节点对远程服务器进行访问；

结果返回单元，使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述链下隐私计算节点。

35、一种访问外部数据的装置，包括：

请求单元，使隐私计算节点在节点可信执行环境中执行智能合约的过程中，在所述节点可信执行环境中生成外部数据访问请求，并将所述外部数据访问请求加密传输至预言机；

响应单元，使所述隐私计算节点接收所述预言机加密返回的外部数据请求响应，所述外部数据请求响应由所述预言机根据对远程服务器的访问结果在预言机可信执行环境内生成并加密；

反馈单元，使所述隐私计算节点在所述节点可信执行环境内解密获得所述外部数据请求响应，根据所述外部数据请求响应完成对所述智能合约的执行操作。

36、一种访问外部数据的装置，包括：

接收单元，使预言机接收隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起；

访问单元，使所述预言机在预言机可信执行环境内解密得到所述外部数据访问请求，并根据所述外部数据访问请求访问远程服务器；

返回单元，使所述预言机根据访问结果在预言机可信执行环境内创建外部数据请求响应并加密，将加密后的外部数据请求响应返回所述隐私计算节点；所述外部数据请求响应用于在所述节点可信执行环境内解密后参与所述智能合约的执行操作。

37、一种访问外部数据的装置，包括：

请求接收单元，使预言机集群中的控制节点接收隐私计算节点加密传输的外部数据访问请求，所述外部数据访问请求由所述隐私计算节点在节点可信执行环境内执行智能合约的过程中发起；

请求转发单元，使所述控制节点在控制节点可信执行环境内解密得到所述外部数据访问请求，并向集群内被选取的预言机节点转发所述外部数据访问请求，所述外部数据访问请求用于指示被选取的预言机节点对远程服务器进行访问；

结果返回单元，使所述控制节点接收所述被选取的预言机节点根据访问结果返回的外部数据请求响应，并在控制节点可信执行环境内对所述外部数据请求响应进行加密后，将经过加密的外部数据请求响应返回所述隐私计算节点。

38、一种电子设备，包括：

处理器；

用于存储处理器可执行任务的存储器；

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 1-31 中任一项所述的方法。

39、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 1-31 中任一项所述方法的步骤。

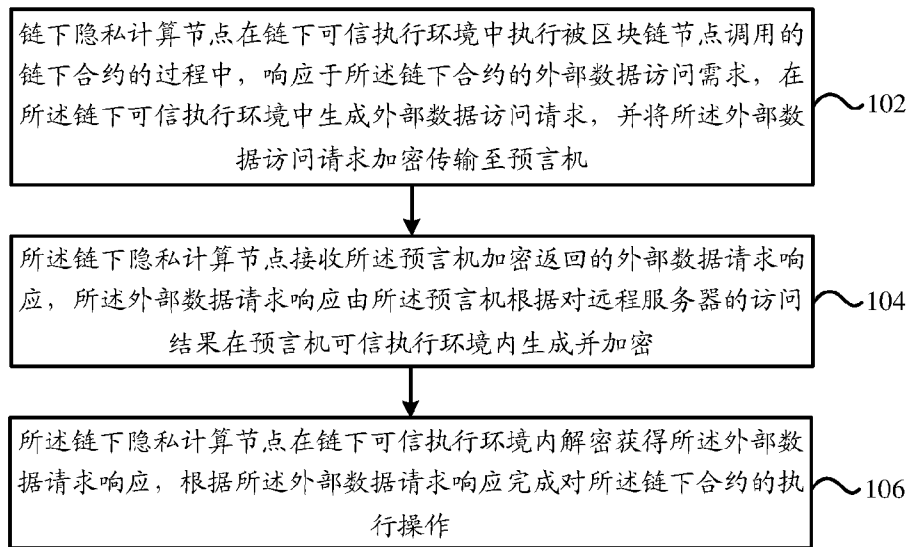


图 1

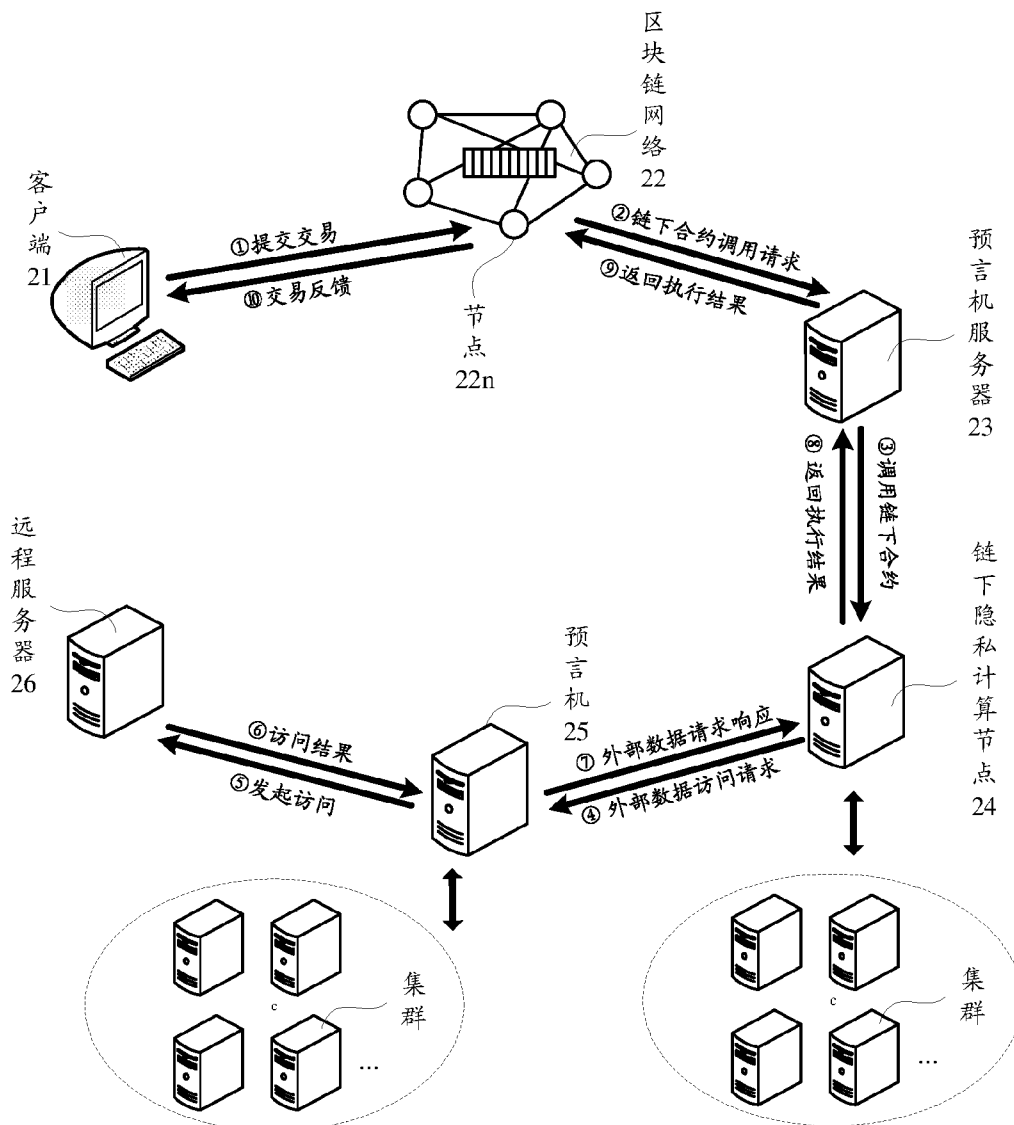


图 2

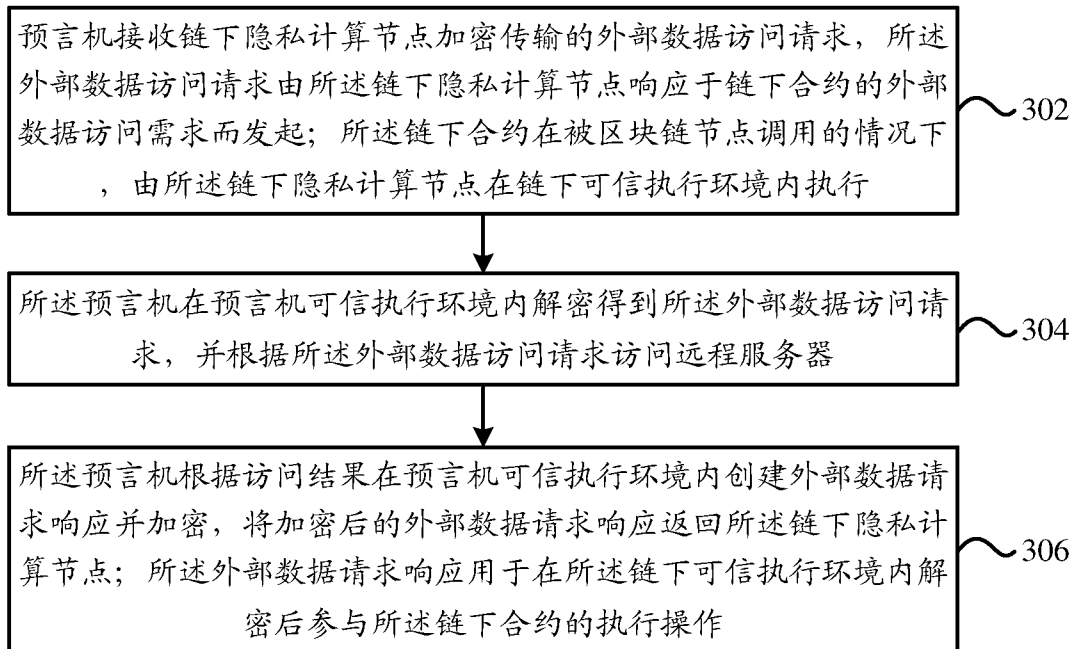


图 3

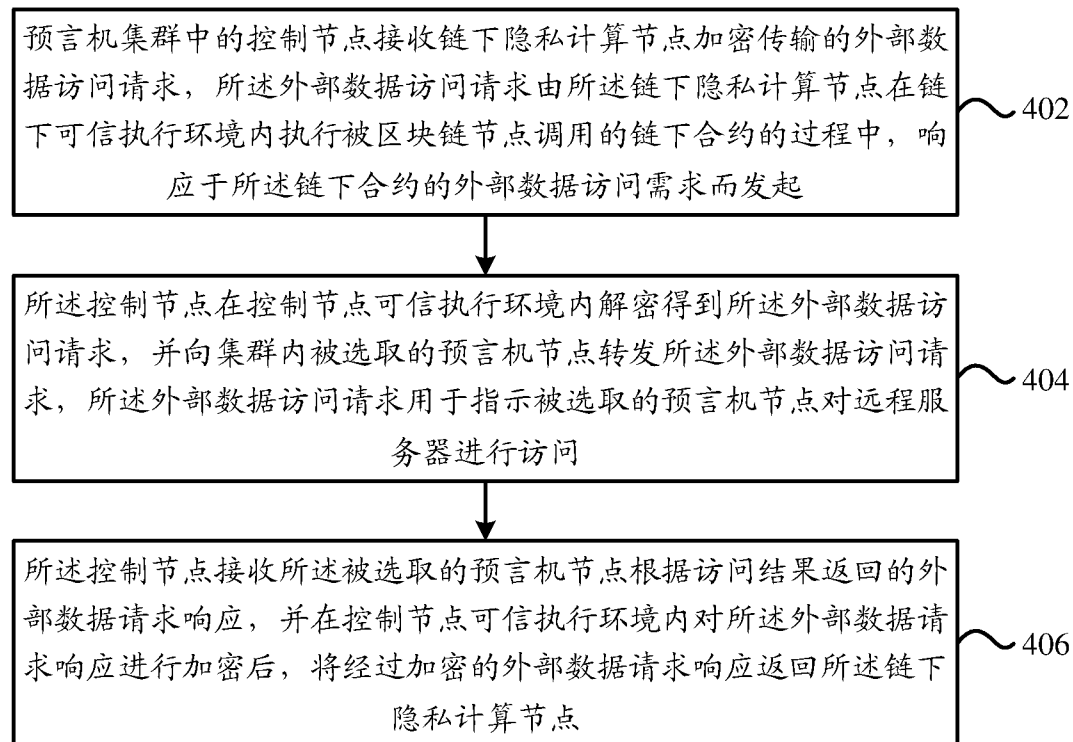


图 4

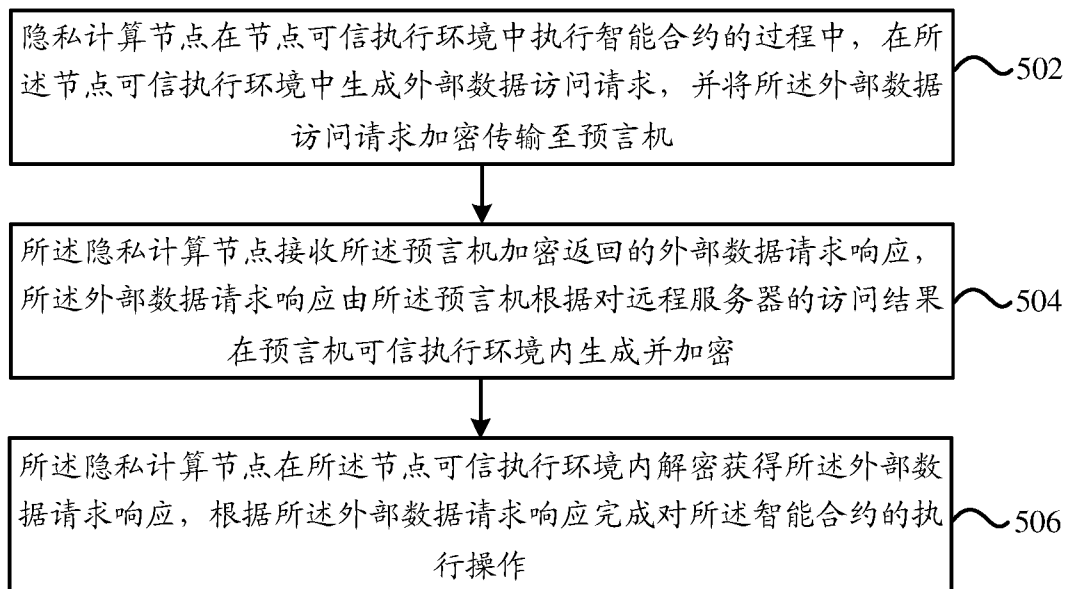


图 5

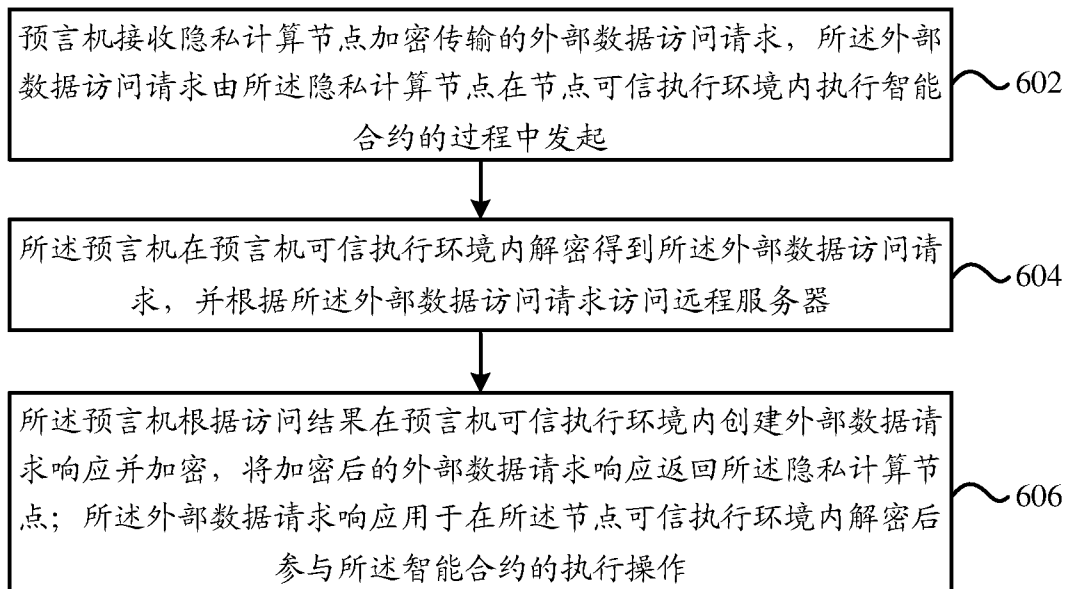


图 6

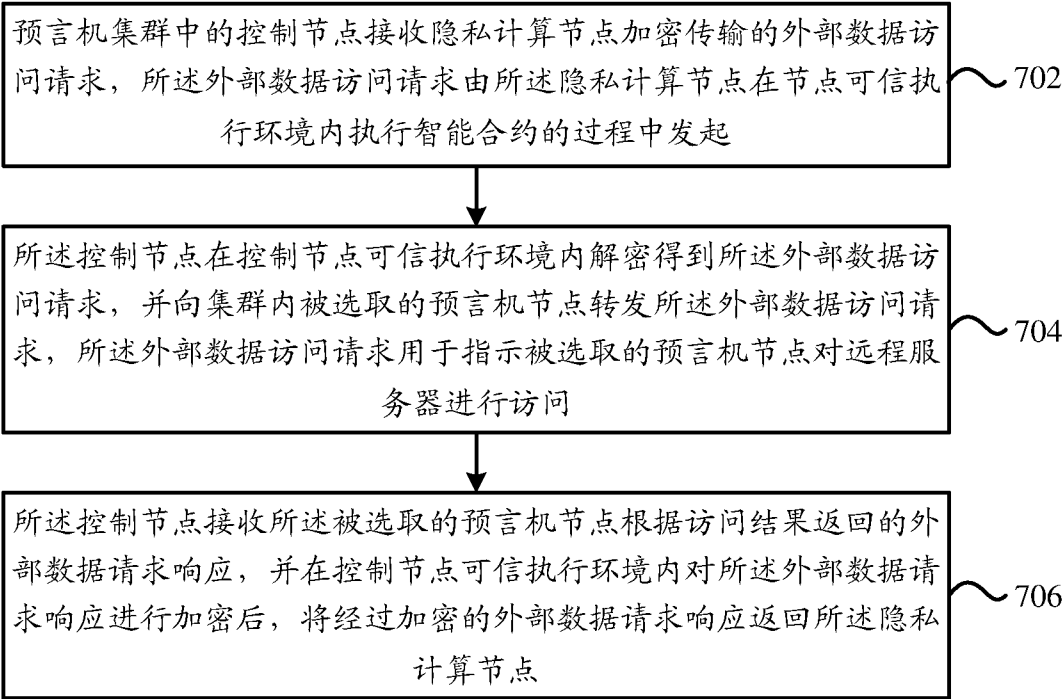


图 7

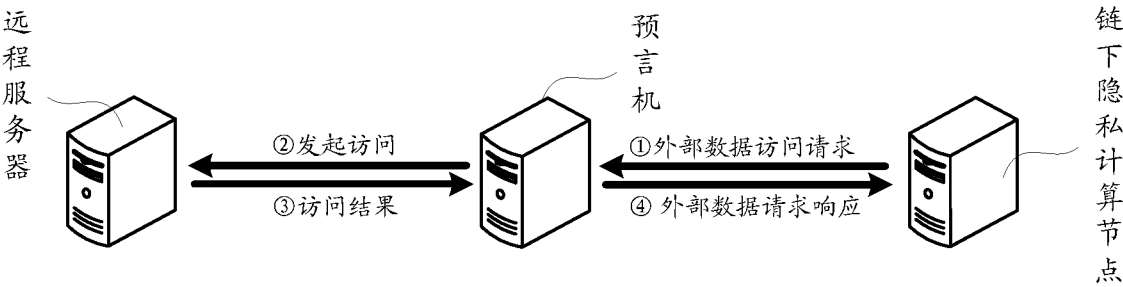


图 8

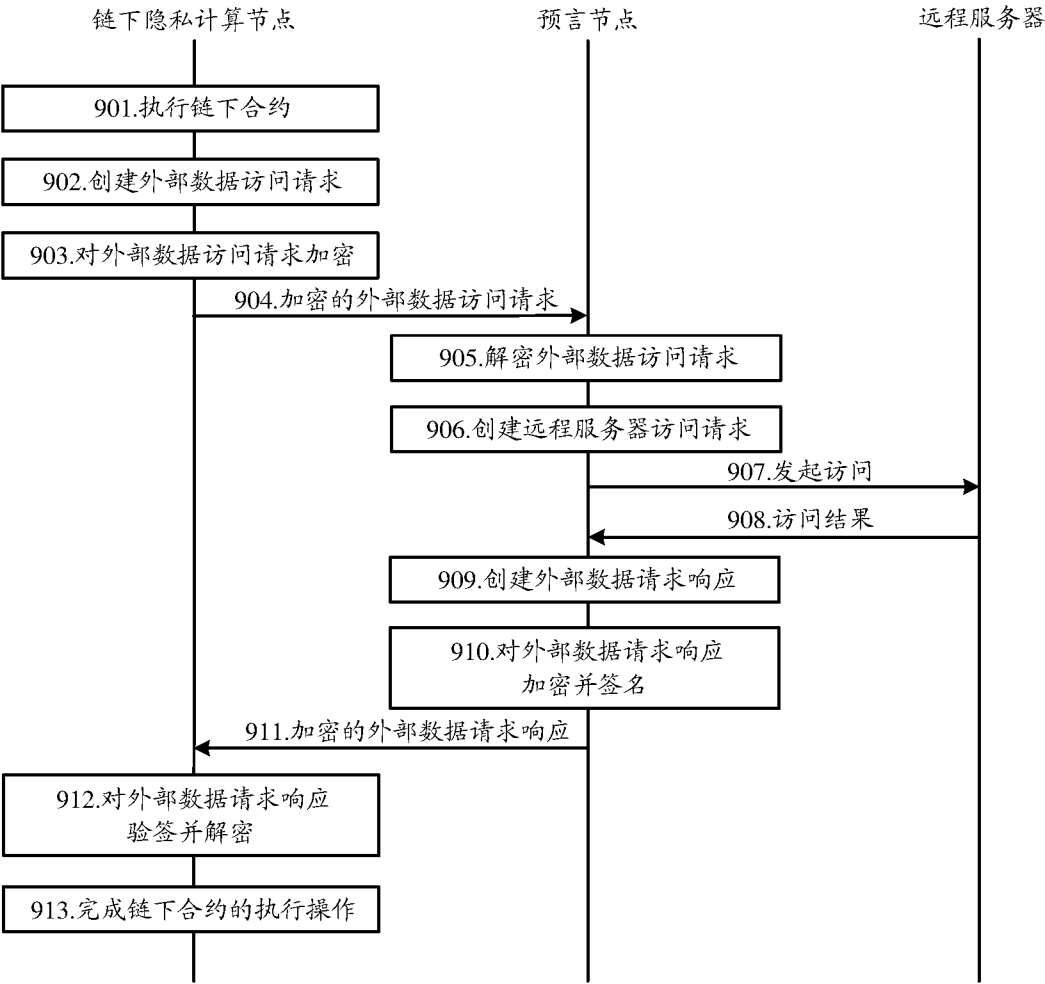


图 9

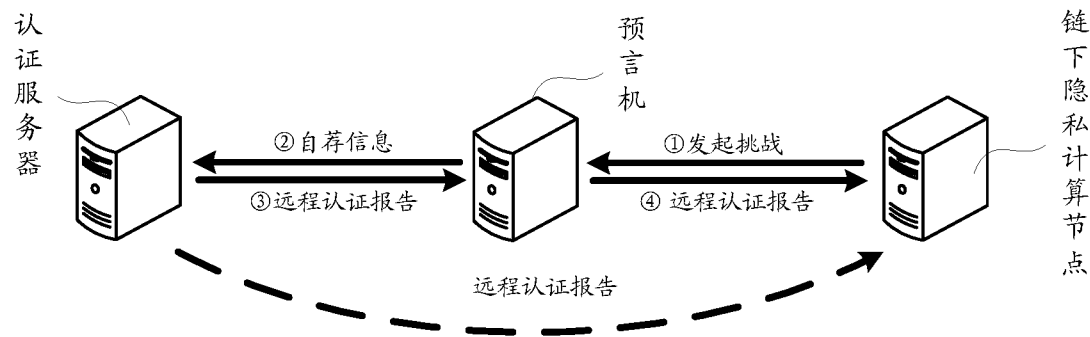


图 10

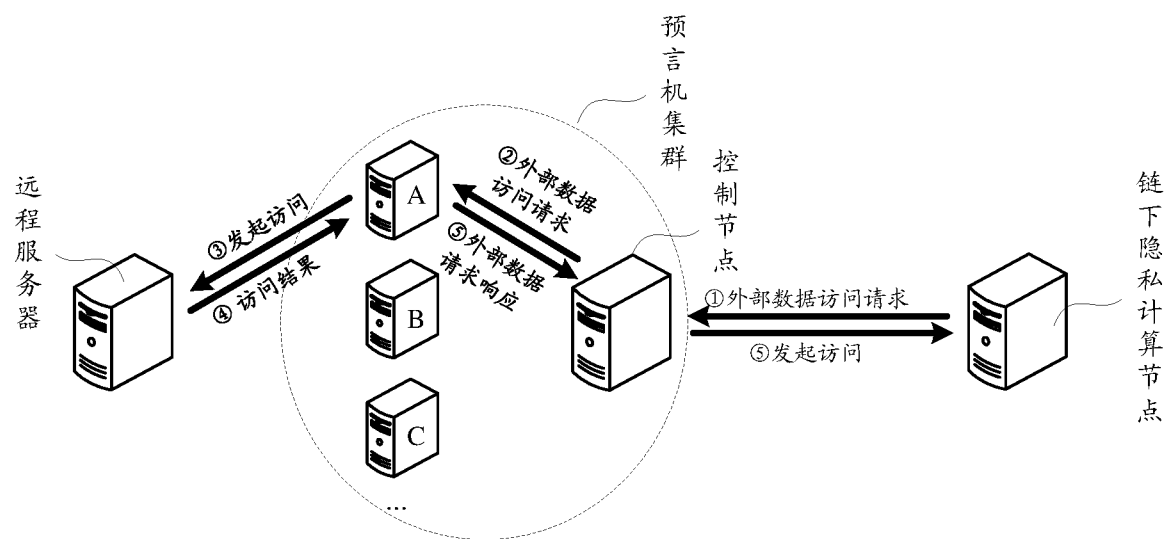


图 11

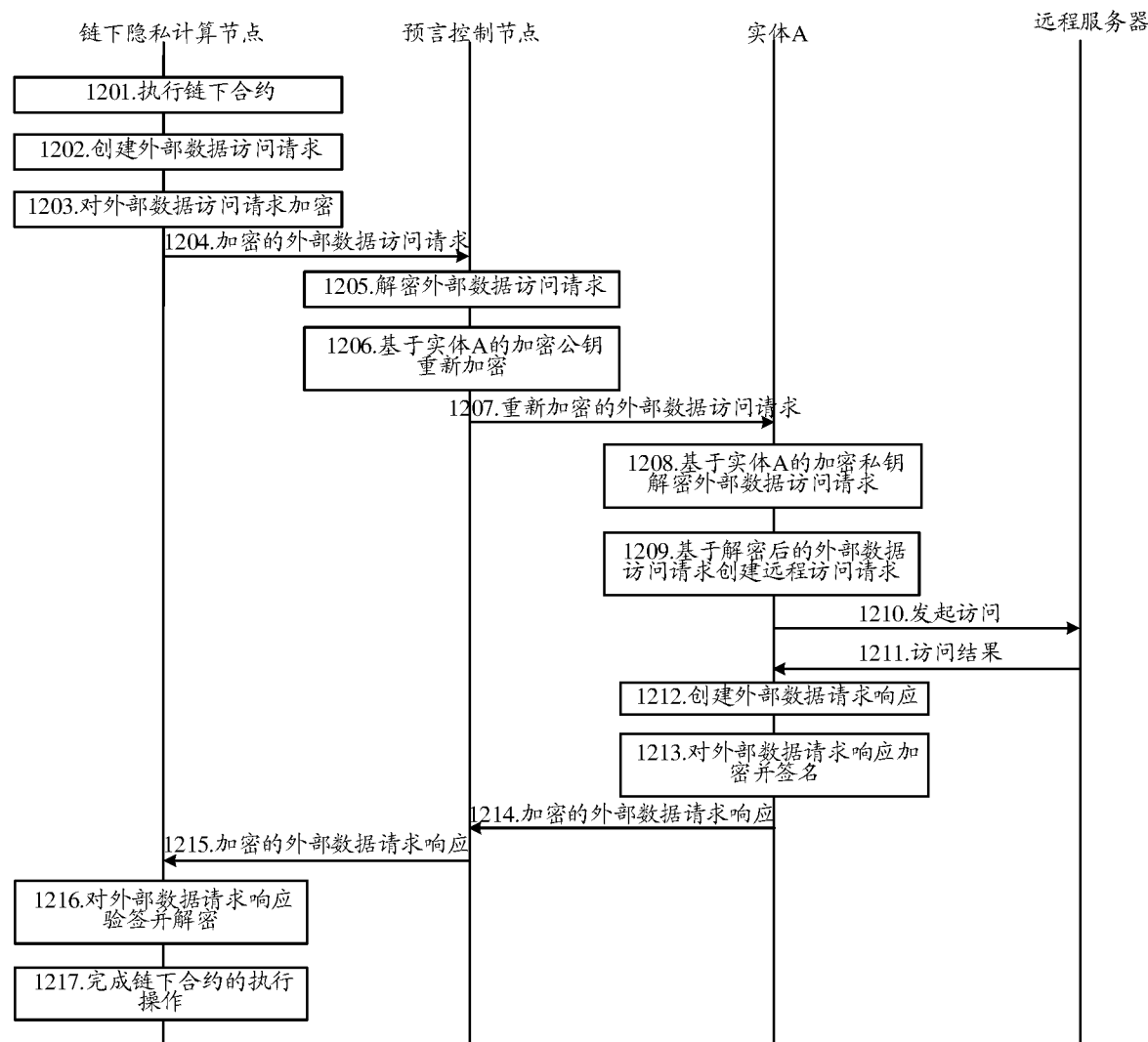


图 12

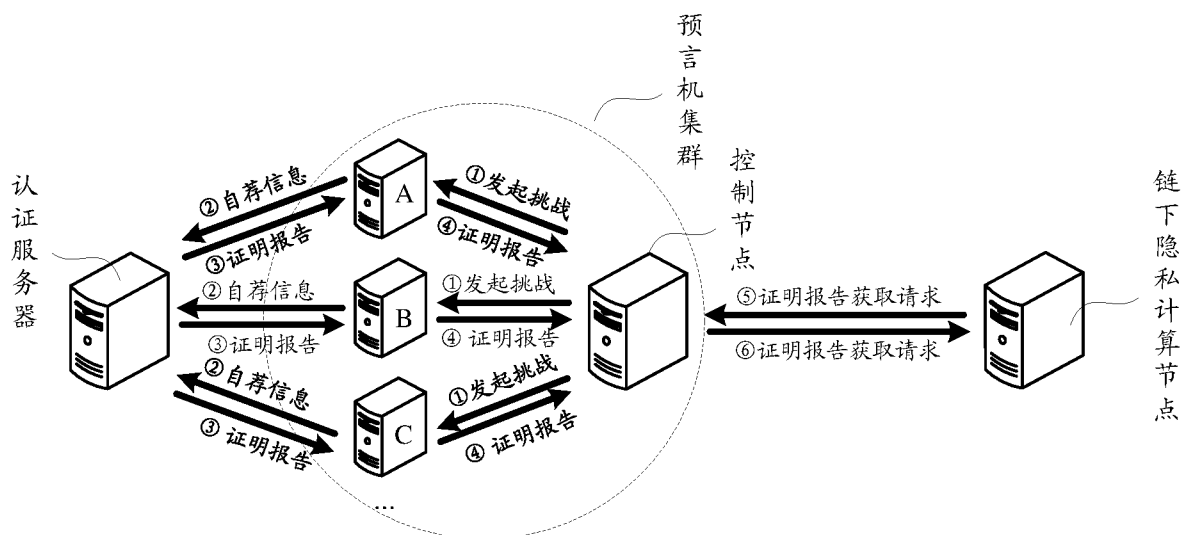


图 13

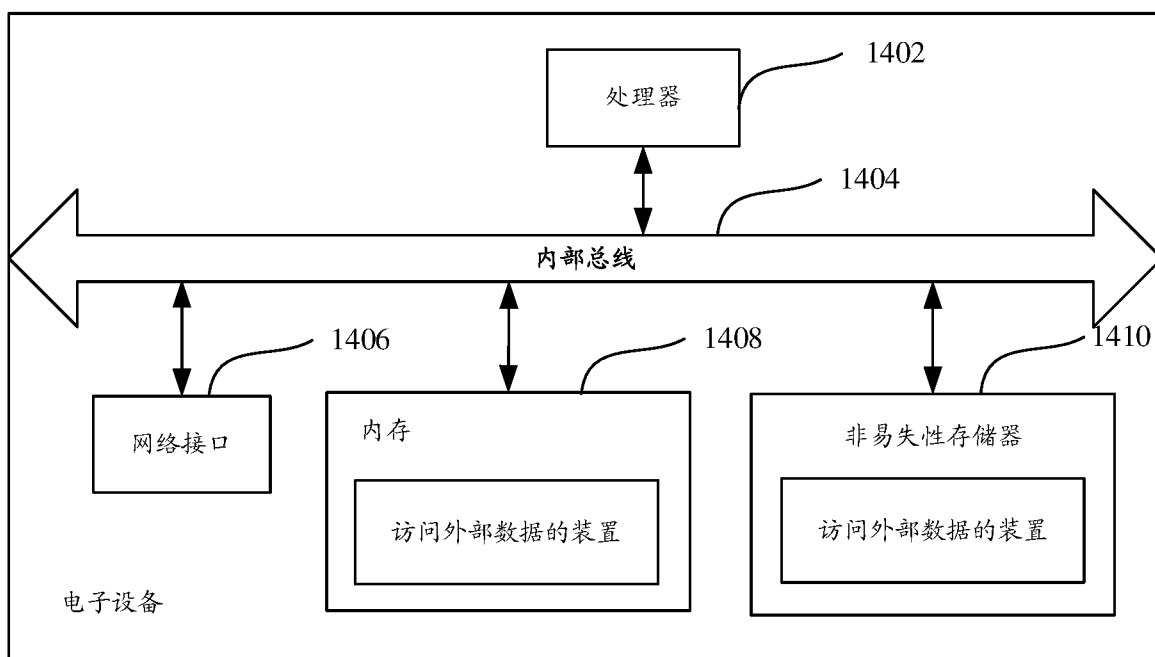


图 14

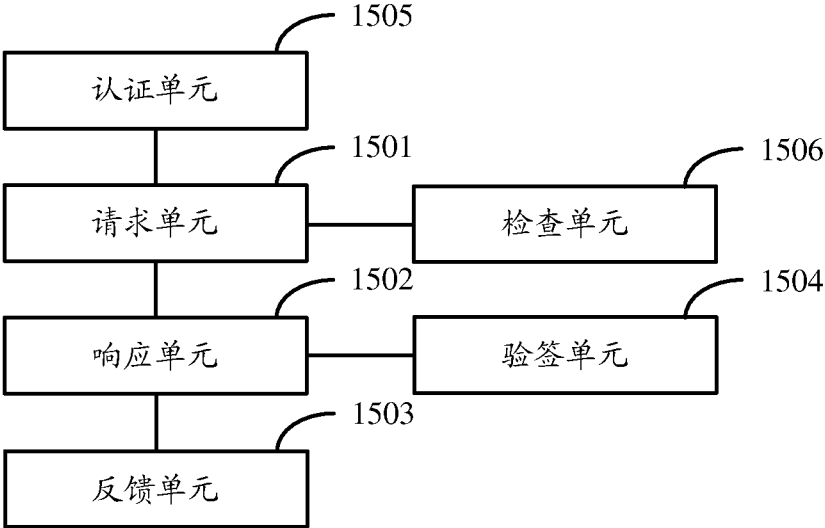


图 15

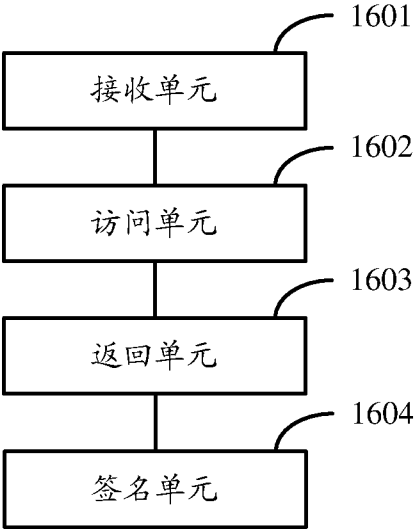


图 16

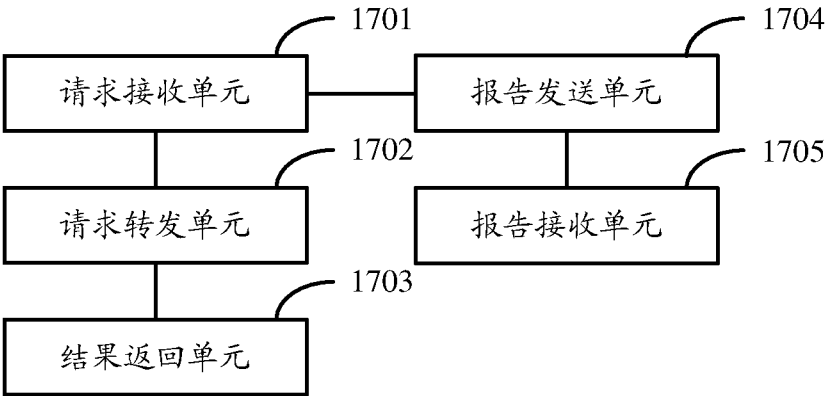


图 17

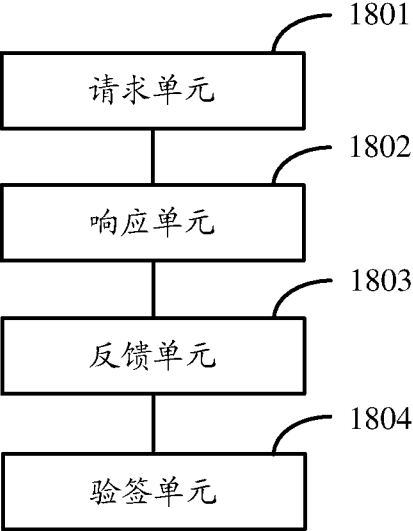


图 18

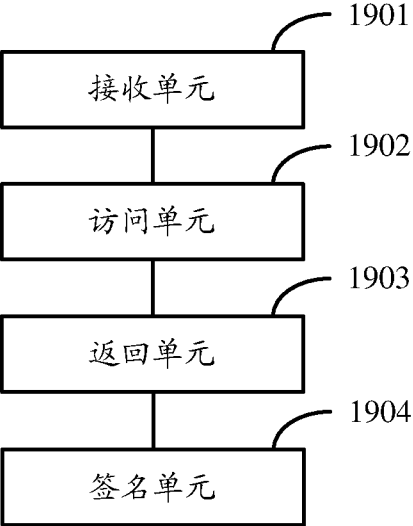


图 19

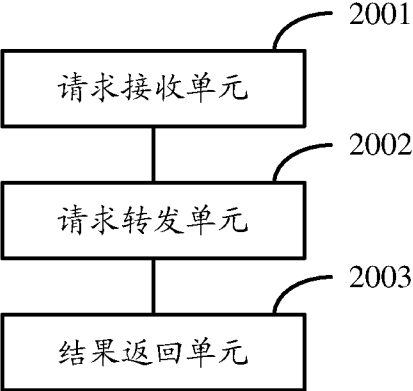


图 20

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/074240

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)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)

H04L; 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)

CNABS; CNTXT; VEN; USTXT; EPTXT; WOTXT; CNKI: 链下, 链外, 部署, 可信执行环境, 可信赖平台, 合约, 预言机, 访问, 请求, 响应, 加密, 解密, off 1w chain, under 1w chain, deploy, TEE, enclave, trustzone, SGX, contract, oracle, access, request, reply, response, encrypt+, decrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111092914 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 01 May 2020 (2020-05-01) claims 1-39	1-39
X	CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019 (2019-11-29) description, paragraphs [0062]-[0164], and figures 3-6	1-39
X	CN 109670335 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.) 23 April 2019 (2019-04-23) description, paragraphs [0027]-[0048], and figures 2-5	20-31, 35-39
A	CN 110473096 A (ALIBABA GROUP HOLDING LIMITED) 19 November 2019 (2019-11-19) entire document	1-39
A	US 9875368 B1 (GOOGLE INC. et al.) 23 January 2018 (2018-01-23) entire document	1-39
A	WO 2019180702 A1 (VALID NETWORK LTD) 26 September 2019 (2019-09-26) entire document	1-39



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

08 March 2021

Date of mailing of the international search report

31 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/CN2021/074240

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111092914	A	01 May 2020	CN	111092914	B	26 June 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
				EP	3563329	A4	11 December 2019
				CA	3049924	A1	18 April 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
				WO	2019072297	A3	18 July 2019
				SG	11201906754	A1	27 August 2019
				IN	201947029881	A	19 June 2020
				HK	40017317	A0	18 September 2020
CN	109670335	A	23 April 2019	None			
CN	110473096	A	19 November 2019	None			
US	9875368	B1	23 January 2018	US	9697371	B1	04 July 2017
WO	2019180702	A1	26 September 2019	SG	11202008741	A1	29 October 2020
				US	20200410460	A1	31 December 2020
				EP	3769243	A1	27 January 2021

国际检索报告

国际申请号

PCT/CN2021/074240

A. 主题的分类 H04L 29/06 (2006.01) 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) H04L; 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)) CNABS; CNTXT; VEN; USTXT; EPTXT; WOTXT; CNKI: 链下, 链外, 部署, 可信执行环境, 可信平台, 合约, 预言机, 访问, 请求, 响应, 加密, 解密, off 1w chain, under 1w chain, deploy, TEE, enclave, trustzone, SGX, contract, oracle, access, request, reply, response, encrypt+, decrypt+																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 111092914 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1-39</td> <td>1-39</td> </tr> <tr> <td>X</td> <td>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[0062]-[0164]段, 图3-6</td> <td>1-39</td> </tr> <tr> <td>X</td> <td>CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23) 说明书第[0027]-[0048]段, 图2-5</td> <td>20-31, 35-39</td> </tr> <tr> <td>A</td> <td>CN 110473096 A (阿里巴巴集团控股有限公司) 2019年 11月 19日 (2019 - 11 - 19) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>US 9875368 B1 (GOOGLE INC等) 2018年 1月 23日 (2018 - 01 - 23) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>WO 2019180702 A1 (VALID NETWORK LTD) 2019年 9月 26日 (2019 - 09 - 26) 全文</td> <td>1-39</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 111092914 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1-39	1-39	X	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[0062]-[0164]段, 图3-6	1-39	X	CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23) 说明书第[0027]-[0048]段, 图2-5	20-31, 35-39	A	CN 110473096 A (阿里巴巴集团控股有限公司) 2019年 11月 19日 (2019 - 11 - 19) 全文	1-39	A	US 9875368 B1 (GOOGLE INC等) 2018年 1月 23日 (2018 - 01 - 23) 全文	1-39	A	WO 2019180702 A1 (VALID NETWORK LTD) 2019年 9月 26日 (2019 - 09 - 26) 全文	1-39
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
PX	CN 111092914 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1-39	1-39																					
X	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[0062]-[0164]段, 图3-6	1-39																					
X	CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23) 说明书第[0027]-[0048]段, 图2-5	20-31, 35-39																					
A	CN 110473096 A (阿里巴巴集团控股有限公司) 2019年 11月 19日 (2019 - 11 - 19) 全文	1-39																					
A	US 9875368 B1 (GOOGLE INC等) 2018年 1月 23日 (2018 - 01 - 23) 全文	1-39																					
A	WO 2019180702 A1 (VALID NETWORK LTD) 2019年 9月 26日 (2019 - 09 - 26) 全文	1-39																					
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																			
* 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 2021年 3月 8日		国际检索报告邮寄日期 2021年 3月 31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 彭云 电话号码 (86-27)59371629																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/074240

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	111092914	A	2020年 5月 1日	CN	111092914	B	2020年 6月 26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
				EP	3563329	A4	2019年 12月 11日
				CA	3049924	A1	2019年 4月 18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
				WO	2019072297	A3	2019年 7月 18日
				SG	11201906754	A1	2019年 8月 27日
				IN	201947029881	A	2020年 6月 19日
				HK	40017317	A0	2020年 9月 18日
CN	109670335	A	2019年 4月 23日	无			
CN	110473096	A	2019年 11月 19日	无			
US	9875368	B1	2018年 1月 23日	US	9697371	B1	2017年 7月 4日
WO	2019180702	A1	2019年 9月 26日	SG	11202008741	A1	2020年 10月 29日
				US	20200410460	A1	2020年 12月 31日
				EP	3769243	A1	2021年 1月 27日