(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 2021/184963 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/CN2021/073846

(22) 国际申请日: 2021 年 1 月 26 日 (26.01.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010191197.7 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,

(54) **Title:** CONTRACT CALLING METHOD AND APPARATUS

(54) **发明名称**: 调用合约的方法及装置

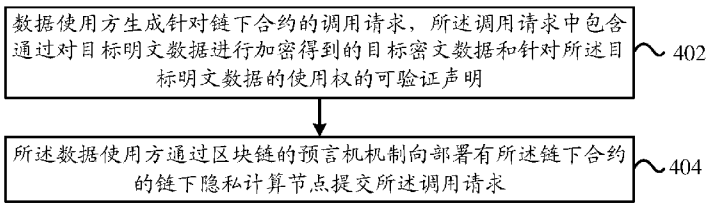


图 4

402 A data usage party generates a calling request for an off-chain contract, the calling request containing target ciphertext data obtained by encrypting target plaintext data and a verifiable statement for the right to use the target plaintext data

404 The data usage party submits, by means of an oracle mechanism of a block chain, the calling request to off-chain private computing nodes on which the off-chain contract is deployed

(57) **Abstract:** The present description provides a contract calling method and apparatus. Said method can comprise: a data usage party generating a calling request for an off-chain contract, the calling request containing target ciphertext data obtained by encrypting target plaintext data and a verifiable statement for the right to use the target plaintext data; and the data usage party submitting, by means of an oracle mechanism of a block chain, the calling request to off-chain private computing nodes on which the off-chain contract is deployed, the calling request being used for instructing the off-chain private computing nodes to execute, if a calling condition is satisfied, the off-chain contract within an off-chain trusted execution environment created by the off-chain private computing nodes, so as to process the target plaintext data, the calling condition including determining, according to the verifiable statement, that a data owning party of the target plaintext data has granted to the data usage party the right to use. The described process of calling a contract can ensure data security and privacy protection.

WO 2021/184963 A1

[见续页]

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))。

(57) 摘要：本说明书提供一种调用合约的方法及装置，该方法可以包括：数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。上述调用合约的过程可确保数据安全和隐私保护。

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。

[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：数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[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：链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[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：数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[07] 根据本说明书一个或多个实施例的第四方面，提出了一种调用合约的方法，包括：隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[08] 根据本说明书一个或多个实施例的第五方面，提出了一种调用合约的装置，包括：生成单元，使数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目

标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；提交单元，使所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[09] 根据本说明书一个或多个实施例的第六方面，提出了一种调用合约的装置，包括：接收单元，使链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；执行单元，使所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[10] 根据本说明书一个或多个实施例的第七方面，提出了一种调用合约的装置，包括：生成单元，使数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；提交单元，使所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[11] 根据本说明书一个或多个实施例的第八方面，提出了一种调用合约的装置，包括：接收单元，使隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；执行单元，使所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[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、第三方面或第四方面所述的方法。

[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、第三方面或第四方面所述方法的步骤。

附图说明

[14] 图 1 是一示例性实施例提供的一种验证链下合约的方法的流程图。

[15] 图 2 是一示例性实施例提供的验证链下合约的方法的场景示意图。

[16] 图 3 是一示例性实施例提供的验证链下合约的方法的场景示意图。

[17] 图 4 是一示例性实施例提供的一种数据使用方侧的调用合约的方法的流程图。

[18] 图 5 是一示例性实施例提供的一种调用合约的方法的场景示意图。

[19] 图 6 是一示例性实施例提供的创建 DID 的流程图。

[20] 图 7 是一示例性实施例提供的数据授权过程的流程图。

[21] 图 8 是一示例性实施例提供的另一种调用合约的方法的流程图。

[22] 图 9 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方法的流程图。

[23] 图 10 是一示例性实施例提供的另一种数据使用方侧的调用合约的方法的流程图。
[24] 图 11 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方法的流程图。
[25] 图 12 是一示例性实施例提供的一种设备的示意结构图。
[26] 图 13 是一示例性实施例提供的一种数据使用方侧的调用合约的装置的框图。
[27] 图 14 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。
[28] 图 15 是一示例性实施例提供的另一种数据使用方侧的调用合约的装置的框图。
[29] 图 16 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。

具体实施方式

[30] 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。

[31] 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。应当理解，尽管在本说明书可能采用术语第一、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”。

[32] 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。

[33] 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。

[34] 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。

[35] 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。

[36] 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。

[37] 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。

[38] 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。

[39] 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。

[40] 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。

[41] 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。可配置单节点形式的链下隐私计算节点来执行计算任务；或者，可通过链下隐私计算集群的形式向用户提供高并发和高可用的隐私计算服务，从而解决节点的负载均衡、故障转移、动态扩展缩容等问题。其中，该链下隐私计算集群可以包含一控制节点和多个链下隐私计算节点，各节点用于部署相同的链下合约（至少一个）以执行计算任务，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。

[42] 与上述区块链节点类似，可在链下隐私计算节点上创建链下 TEE（即链下可信执行环境），该链下 TEE 基于 CPU 硬件实现的与外部完全隔离的可信执行环境。链下隐私计算节点通过创建链下 TEE，可以通过该链下 TEE 实现对链下合约的部署操作以及部署后的调用执行操作，并确保操作过程中的数据安全和隐私保护。举例而言，可在链下隐私计算节点上部署链下合约，并在该链下隐私计算节点创建的链下 TEE 内部署 WASM 虚拟机。用户作为目标数据的数据使用方，可向链下隐私计算节点发起一基于 WASM 程序的计算任务，用于调用链下合约对目标数据进行计算（即目标数据为链下合约的入参数据），那么链下隐私计算节点可将链下合约读入链下 TEE 内并编译成 WASM 字节码，以 WASM 虚拟机作为执行引擎，将编译得到的 WASM 字节码在 WASM 虚拟机中执行，以对目标数据进行计算。需要说明的是，本说明书中的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。

[43] 数据使用方通过客户端调用链下合约之前，可对链下隐私计算节点中部署的链下合约发起挑战，以确保链下隐私计算节点中部署的链下合约可信，进而按照用户预期执行计算任务。

[44] 图 1 是一示例性实施例提供的一种验证链下合约的方法的流程图。如图 1 所示，该方法可以包括步骤 102~106。

[45] 步骤 102，所述数据使用方获取针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成。

[46] 在本实施例中，链下隐私计算节点包含单节点和链下隐私计算集群两种形式。针对单节点形式，数据使用方直接向链下隐私计算节点发起挑战，从而接收链下隐私计算节点返回的远程证明报告。在该情况下，链下隐私计算节点的身份信息为该链下隐私计算节点的节点身份信息，链下隐私计算节点的身份私钥为该链下隐私计算节点的节点身份私钥，链下隐私计算节点的身份公钥为该链下隐私计算节点的节点身份公钥。针对链下隐私计算集群的形式，在链下隐私计算节点属于链下隐私计算集群的情况下，数据使用方向链下隐私计算集群的控制节点发起挑战，由控制节点来选取链下隐私计算集群中的节点来响应挑战，从而获取选取出的节点的远程证明报告，并向数据使用方返回该远程证明报告。在该情况下，链下隐私计算节点代表链下隐私计算集群与外部对象交互。因此，链下隐私计算节点的身份信息为该链下隐私计算集群的集群身份信息，链下隐私计算节点的身份公钥为该链下隐私计算集群的集群身份密钥中的集群身份公钥，链下隐私计算节点的身份私钥为集群身份密钥中的集群身份私钥。其中，在区块链节点与链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，集群身份密钥用于

对交互数据进行加密解密和/或签名签名验证。而针对集群身份密钥的生成，可由链下隐私计算集群的控制节点选取集群中的任一节点作为主节点来生成集群身份密钥，并向集群内的其他节点共享集群身份密钥。

[47] 步骤 104，所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，获取部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护。

[48] 在本实施例中，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。换言之，远程证明报告由认证服务器对链下隐私计算节点针对自身的链下 TEE 产生的自荐信息进行验证后生成。

[49] 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。

[50] 数据使用方在获得链下隐私计算节点的远程证明报告之后，可以根据该远程证明报告来验证相应的链下隐私计算节点是否可信，具体指验证该链下隐私计算节点上部署的链下 TEE 是否可信，并在确定链下 TEE 可信的情况下进一步对部署于该链下隐私计算节点处的链下合约（在该可信的链下 TEE 内执行）进行校验。

[51] 具体而言，链下隐私计算节点在创建链下 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 中预设信息的哈希值，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。

[52] 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。

[53] 相应地，数据使用方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。数据使用方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数据使用方时，还可以关联提供IAS的证书链，使得数据使用方可以从该证书链中提取IAS服务器的公钥。然后，数据使用方可以从远程证明报告中提取结构体QUOTE和签名验证结果。数据使用方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，数据使用方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，数据使用方可以从结构体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，数据使用方预先获得了链下TEE的上述预设信息的第一标准哈希值，比如为MREnclave和MRSigner的可信值（以下称之为可信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，数据使用方可以将“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TEE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，数据使用方就判定该链下隐私计算节点的链下TEE不可信，而如果数据使用方设定的所有前提条件都被满足，就可以确认该链下隐私计算节点的链下TEE可信。此外，数据使用方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。

[54] 除了MREnclave和MRSigner之外，数据使用方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（即节点身份公钥）。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签名验证的密钥对（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（即其他身份信息），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自身的链下TEE内生成节点身份信息（比如在链下TEE初始化时生成）后，可对生成的节点身份信息进行哈希计算得到第二标准哈希值。而链下隐私计算节点在生成结构体QUOTE时，可以将该第二标准哈希值添加至结构体QUOTE中。

[55] 相应的，数据使用方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，数据使用方可以提取远程证明报告所含的签名验证结果和第二标准哈希值，并验证签名验证结果，以及利用第二标准哈希值验证链下隐私计算节点的节点身份信息是否正确，且两验证步骤之间并不存在必然的先后顺序，两者之间可以完全独立。假定数据使用方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，继续利用第二标准哈希值对链下隐私计算节点的节点身份信息进行验证。为了对链下隐私计算节点的节点身份信息进行验证，数据使用方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数据使用方的同时，可以关联提供节点身份信息，当然数据使用方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，数据使用方可以对获得的节点身份信息进行哈希计算得到第二待校验哈希值，将计算得到的第二待校验哈希值与上述的第二标准哈希值进行比较，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，可以证明获

得的节点身份信息正是链下隐私计算节点在自身的链下 TEE 内生成的节点身份信息。那么，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。

[56] 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、针对节点身份信息的验证。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节点身份信息进行验证；或者，在一些情况下，可以仅验证节点身份信息，而对第一待检验哈希值可以不验证或者部分验证。例如，数据使用方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。

[57] 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，比如代表节点身份的节点身份公钥等。节点身份信息还可以包含与链下 TEE 相关的信息，那么链下隐私计算节点在自身的链下 TEE 内生成节点身份信息后，对生成的节点身份信息进行哈希计算得到哈希值，并将该哈希值添加至结构体 QUOTE 时，该哈希值相当于同时实现了上述第一待检验哈希值和第二标准哈希值的作用。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，数据使用方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，数据使用方可以提取远程证明报告所含的签名验证结果和该哈希值，并验证签名验证结果，以及利用该哈希值验证链下隐私计算节点的节点身份信息是否正确，且两验证步骤之间并不存在必然的先后顺序，两者之间可以完全独立。假定数据使用方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，继续利用该哈希值对链下隐私计算节点的节点身份信息进行验证。为了对链下隐私计算节点的节点身份信息进行验证，数据使用方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，数据使用方可以对获得的节点身份信息进行哈希计算得到待校验哈希值，将计算得到的待校验哈希值与上述远程证明报告所含的哈希值进行比较，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。

[58] 需要说明的是，数据使用方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。

[59] 步骤 106，所述数据使用方采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行验签，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过所述预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

[60] 在本实施例中，针对集群的形式，在完成对链下隐私计算集群的建立后，需要为这些链下隐私计算节点生成统一的身份信息，比如称为集群身份密钥。集群身份密钥可以包括集群加密密钥对和集群签名密钥对，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。通过为链下隐私计算集群中的各个节点生成统一的身份信息，与链下隐私计算集群对接的外部对象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。以链下隐私计算节点的第一身份信息为例，针对单节点形式，链下隐私计算节点提供的第一身份信息为该链下隐私计算节点的节点身份

信息（不包含节点身份私钥），身份公钥为该链下隐私计算节点的节点身份公钥，其他身份信息（身份信息中除身份公钥以外的其他身份信息）为链下隐私计算节点的其他节点身份信息，即节点身份信息中除节点身份公钥以外的其他节点身份信息。针对链下隐私计算集群的形式，链下隐私计算节点提供的第一身份信息为链下隐私计算集群的集群身份信息，身份公钥为链下隐私计算集群的集群身份公钥，其他身份信息（身份信息中除身份公钥以外的其他身份信息）为上述其他节点身份信息。而针对链下隐私计算节点的第二身份信息，在第一身份信息的基础上，还包含链下可信执行环境的预设信息的哈希值，包含的其他内容相同，在此不再赘述。下面结合图 2-3 分别对单节点形式和集群形式的挑战过程进行详细说明。

[61] 如图 2 所示，针对单节点的形式，数据使用方的客户端 21 可向链下隐私计算节点 22 发起链下挑战或者链上挑战。链上挑战的发起过程可以包括三个步骤：步骤①，客户端 21 向区块链网络 23 提交一笔用于向链下合约发起挑战的交易，比如称之为挑战交易，该挑战交易可由区块链网络 23 内的某一节点 23n 接收和执行；步骤②，节点 23n 调用预先部署的预言机合约，该预言机合约可以将上述挑战交易所含的挑战信息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挑战信息的事件，而预言机服务器 24 可以通过监听预言机合约产生的事件，从而获取上述的挑战信息；步骤③，预言机服务器 24 将挑战信息通过链下渠道发送至控制节点 22。

[62] 通过对链下隐私计算节点 22 部署的链下合约发起挑战，客户端 21 可获取针对链下隐私计算节点 22 创建的链下 TEE 的远程证明报告，该远程证明报告由认证服务器对链下隐私计算节点 22 针对链下 TEE 产生的自荐信息进行验证后生成。在一种情况下，由客户端 21 向链下隐私计算节点 22 发起挑战，挑战目标为链下隐私计算节点 22 部署的链下合约，进而接收链下隐私计算节点 22 响应于该挑战返回的所述远程证明报告和所述待验证合约信息，即链下隐私计算节点 22 响应于该挑战，将所述远程证明报告和所述待验证合约信息一次性返回至客户端 21。在另一种情况下，由客户端 21 向链下隐私计算节点 22 发起挑战，挑战目标为链下隐私计算节点 22 创建的链下 TEE，进而接收链下隐私计算节点 22 返回的远程证明报告，并在根据所述远程证明报告确定所述链下 TEE 可信的情况下，向链下隐私计算节点 22 发送针对部署于链下隐私计算节点 22 处的链下合约的合约信息的获取请求，接收链下隐私计算节点 22 响应于所述获取请求返回的待验证合约信息。而在根据所述远程证明报告确定所述链下 TEE 不可信的情况下，则无需再向链下隐私计算节点 22 请求获取链下合约的合约信息（即待验证合约信息）。

[63] 其中，客户端 21 可通过链上挑战向挑战目标发起挑战。比如，向区块链节点 23n 提交针对挑战目标的挑战交易，该挑战交易包含的挑战信息由区块链节点 23n 通过预言机机制传输至链下隐私计算节点 22，所述挑战信息用于向挑战目标发起挑战。或者，客户端 21 直接向链下隐私计算节点 22 中的挑战目标发起链下挑战。

[64] 如图 2 所示，在一实施例中，链下隐私计算节点 22 在链下 TEE 内生成自身的节点身份信息后，可对生成的节点身份信息进行哈希计算得到第二标准哈希值；其中，所生成的节点身份信息中包含链下隐私计算节点 22 的节点身份公钥和链下隐私计算节点 22 的其他身份信息。那么，客户端 21 可利用第二标准哈希值验证链下隐私计算节点 22 提供的第一节点身份信息（即声明的节点身份信息，包含链下隐私计算节点 22 的节点身份公钥和链下隐私计算节点 22 的其他身份信息，不一定为真实数据，此时可理解为待验证身份信息），并在验证通过的情况下获取可验证链下隐私计算节点 22 的节点身份信息中包含的节点身份公钥，从而利用该节点身份公钥完成后续对链下合约的验证。比如，客户端 21 对获取到的第一节点身份信息进行哈希计算以得到第二待校验哈希值，并将第二待校验哈希值与链下隐私计算节点 22 提供的第二标准哈希值进行比较，从而在比较结果一致的情况下判定节点身份信息验证通过。由于节点身份信息由链下隐私计算节点 22 在链下 TEE 内生成并计算得到第二标准哈希值，那么在根据远程证明报告判

定链下 TEE 可信后，若第二待校验哈希值与第二标准哈希值相同，则说明隐私计算节点 22 提供的第一节点身份信息为在链下 TEE 内生成的节点身份信息，从而其中包含的节点身份公钥为隐私计算节点 22 实际的节点身份公钥，而链下隐私计算节点 22 实际的节点身份公钥可用于验证隐私计算节点 22 的签名。其中，链下隐私计算节点 22 可将第二标准哈希值、远程证明报告、第一节点身份信息一同发送至客户端 21。需要说明的是，此部分内容可参考前述步骤 104 中针对链下隐私计算节点进行验证的过程，在此不再赘述。

[65] 如图 2 所示，在另一实施例中，链下隐私计算节点 22 在链下 TEE 内生成自身的节点身份信息包含链下隐私计算节点 22 的节点身份公钥、链下隐私计算节点 22 的其他身份信息和链下 TEE 的预设信息的哈希值，那么链下隐私计算节点 22 在自身的链下 TEE 内生成节点身份信息后，对生成的节点身份信息进行哈希计算得到第三标准哈希值，那么第三标准哈希值相当于同时实现了上述第一待检验哈希值和第二标准哈希值的作用。具体而言，链下隐私计算节点 22 可向客户端 21 提供远程证明报告、第三标准哈希值和第二节点身份信息（此时可理解为待验证身份信息）。其中，第二节点身份信息包含链下隐私计算节点 22 的节点身份公钥、链下隐私计算节点 22 的其他身份信息和第四待校验哈希值，第四待校验哈希值为链下 TEE 的预设信息的哈希值；同时，第二节点身份信息为声明的节点身份信息，并不一定为链下隐私计算节点 22 的真实节点身份信息。那么，客户端 21 在根据认证服务器的公钥对远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，对获取到的第二节点身份信息进行哈希计算以得到第三待校验哈希值，并将第三待校验哈希值与第三标准哈希值进行比较。当比较结果为一致时，说明隐私计算节点 22 提供的第二节点身份信息为在链下 TEE 内生成的节点身份信息，也即其中包含的第四待校验哈希值为链下 TEE 的实际预设信息的哈希值。因此，进一步将预先获得的针对所述链下 TEE 预设信息的第四标准哈希值与第四待检验哈希值进行比较，并将比较结果一致作为确认所述链下 TEE 可信的前提条件。同时，第二节点身份信息包含的节点身份公钥可判定为隐私计算节点 22 实际的节点身份公钥，可用于对待验证合约信息进行签名验证。其中，链下隐私计算节点 22 可将第三标准哈希值、远程证明报告、第二节点身份信息一同发送至客户端 21。需要说明的是，此部分内容可参考前述步骤 104 中针对链下隐私计算节点进行验证的过程，在此不再赘述。

[66] 客户端 21 在根据远程证明报告确定链下 TEE 可信的情况下，获取部署于链下隐私计算节点 22 处的链下合约的待验证合约信息，待验证合约信息被链下隐私计算节点 22 在链下 TEE 内采用自身的节点身份私钥进行签名，节点身份私钥由链下隐私计算节点 22 在链下 TEE 内生成。比如，链下隐私计算节点 22 可将部署的链下合约读入链下 TEE 内并采用自身的节点身份私钥进行签名。

[67] 客户端 21 采用链下隐私计算节点 22 的节点身份公钥对待验证合约信息进行签名验证，以及根据链下合约的合约信息对待验证合约信息进行合约信息验证。其中，节点身份公钥处于公开状态，比如链下隐私计算节点 22 向外公开发布节点身份公钥以由客户端 21 获取。或者，客户端 21 通过上述验证链下隐私计算节点 22 的节点身份信息的方式获取。同时，链下合约的合约信息也可处于公开状态，比如链下合约的部署方向外公开发布合约信息以由客户端 21 获取。其中，合约信息可以包括链下合约的名称、描述、版本号、字节码哈希值、合约身份公钥等信息，本说明书并不对此进行限制。

[68] 在签名验证和合约信息验证通过的情况下，客户端 21 可确定客户端 21 在通过区块链节点的预言机机制对链下合约发起调用时，该链下合约由链下隐私计算节点 22 在链下 TEE 可信执行环境中执行。本说明书中验证链下合约的过程为先验证链下隐私计算节点 22 的链下 TEE 可信，那么在验证链下隐私计算节点 22 的链下 TEE 可信的情况下，若验证签名得到链下隐私计算节点 22 提供的待验证合约信息确实由链下隐私计算

节点 22 的节点身份私钥（维护在链下 TEE 内）签名，则可确定出当前挑战的链下合约为运行在链下隐私计算节点 22 的链下 TEE 内的链下合约，即确保链下隐私计算节点 22 中部署的链下合约可信，可按照用户预期执行计算任务。

[69] 下面结合图 3 针对集群形式的挑战过程进行说明。如图 3 所示，客户端 31 可向控制节点 32 发起链下挑战或者链上挑战。链上挑战的发起过程可以包括三个步骤：步骤①，客户端 31 向区块链网络 33 提交一笔用于向链下合约发起挑战的交易，比如称之为挑战交易，该挑战交易可由区块链网络 33 内的某一节点 33n 接收和执行；步骤②，节点 33n 调用预先部署的预言机合约，该预言机合约可以将上述挑战交易所含的挑战信息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挑战信息的事件，而预言机服务器 34 可以通过监听预言机合约产生的事件，从而获取上述的挑战信息；步骤③，预言机服务器 34 将挑战信息通过链下渠道发送至控制节点 32。

[70] 链下隐私计算集群作为一个整体向外提供执行计算任务的功能。其中，集群内各个节点均部署有相同的链下合约，那么各个节点均可以代表集群来执行计算任务，比如，计算任务可由控制节点来分配。因此，各个节点在代表集群与外部进行数据交互时，使用代表集群身份的集群身份密钥来对与外部交互的数据进行解密或签名，而非使用节点自身的节点身份密钥。相应的，外部对象在通过客户端与集群进行交互时，将集群视为一个整体而无需关心集群内部的结构，因此采用集群身份密钥进行加密或验证签名。

[71] 如图 3 所示，用户在通过客户端 31 调用集群中的链下合约之前，可通过客户端 31 对集群中部署的链下合约发起挑战。控制节点 32 在接收到挑战后，可选取集群中的任意节点来响应该挑战。比如，可选取上述用于生成集群身份密钥的主节点，或者选取集群中的从节点，本说明书并不对选取响应挑战的节点的方式进行限制。以节点 32n 响应挑战为例进行说明。控制节点 32 选取节点 32n 来代表集群响应挑战，向挑战方提供代表集群的集群远程证明报告。其中，集群远程证明报告由认证服务器对节点 32n 针对自身的链下 TEE 产生的自荐信息进行验证后生成，即集群远程证明报告为对应于节点 32n 的链下 TEE 的远程证明报告。具体而言，集群远程证明报告携带的自荐信息内包含第一待检验哈希值，该第一待检验哈希值为节点 32n 的链下 TEE 的预设信息的哈希值，该第一待检验哈希值用于挑战方在根据认证服务器的公钥对集群远程证明报告进行签名验证并签名验证通过，且集群远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对链下 TEE 的第一标准哈希值（比如，为链下 TEE 的上述预设信息的可信哈希值）进行比较，且比较结果一致被作为挑战方确认链下 TEE 可信的前提条件。其中，挑战方根据集群远程证明报告验证链下 TEE 的过程可参考前述控制节点验证待加入节点的链下 TEE 的内容，在此不再赘述。实际上，挑战方根据集群远程证明报告验证的链下 TEE 为节点 32n 的链下 TEE。

[72] 如图 3 所示，在一实施例中，节点 32n 在链下 TEE 内生成自身的节点身份信息时，还可在链下 TEE 内生成代表集群的集群身份信息，并对生成的集群身份信息进行哈希计算得到第二标准哈希值；其中，所生成的集群身份信息中包含集群身份公钥和节点 32n 的节点身份信息中除节点身份公钥以外的其他身份信息。换言之，基于通过节点 32n 来代表集群，节点 32n 的节点身份信息与集群身份信息之间的差异在于：节点身份信息中记录的公钥为节点身份公钥，集群身份信息中记录的公钥为集群身份公钥；持此之外，其他身份信息相同。那么，客户端 31 可利用第二标准哈希值验证节点 32n 提供的第一集群身份信息（即声明的集群身份信息，包含集群身份公钥和节点 32n 的其他身份信息，不一定为真实数据，此时可理解为待验证身份信息），并在验证通过的情况下获取集群身份信息中包含的集群身份公钥，从而利用该集群身份公钥完成后续对链下合约的验证。比如，客户端对获取到的第一集群身份信息进行哈希计算以得到第二待校验哈希值，并将第二待校验哈希值与节点 32n 提供的第二标准哈希值进行比较，从而在比较结果一致的情况下判定集群身份验证通过。由于集群身份信息由节点 32n 在链下 TEE 内生成并

计算得到第二标准哈希值，那么在根据远程证明报告判定链下 TEE 可信后，若第二待校验哈希值与第二标准哈希值相同，则说明隐私计算节点 32 提供的第一集群身份信息为在链下 TEE 内生成的集群身份信息，从而其中包含的集群身份公钥为隐私计算节点 32 实际维护的对应于集群的集群身份公钥，而隐私计算节点 32 实际维护的集群身份公钥可用于验证隐私计算节点 32 的签名。其中，节点 32n 可通过控制节点 32 将第二标准哈希值、远程证明报告、第一集群身份信息一同发送至客户端 31。需要说明的是，此部分内容可参考前述步骤 104 中针对链下隐私计算节点进行验证的过程，在此不再赘述

[73] 如图 3 所示，在另一实施例中，节点 32n 在链下 TEE 内生成的集群身份信息可包含集群身份公钥、节点 32n 的节点身份信息中除节点身份公钥以外的其他身份信息和链下 TEE 的预设信息的哈希值，那么节点 32n 在自身的链下 TEE 内生成集群身份信息后，对生成的集群身份信息进行哈希计算得到第三标准哈希值，那么第三标准哈希值相当于同时实现了上述第一待检验哈希值和第二标准哈希值的作用。具体而言，节点 32n 可向客户端 31 提供远程证明报告、第三标准哈希值和第二集群身份信息（此时可理解为待验证身份信息）。其中，第二集群身份信息包含集群身份公钥、节点 32n 的其他身份信息和第四待校验哈希值，第四待校验哈希值为链下 TEE 的预设信息的哈希值；同时，第二集群身份信息为声明的集群身份信息，并不一定为节点 32n 提供的真实集群身份信息。那么，客户端 31 在根据认证服务器的公钥对远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，对获取到的第二集群身份信息进行哈希计算以得到第三待校验哈希值，并将第三待校验哈希值与第三标准哈希值进行比较。当比较结果为一致时，说明隐私计算节点 32 提供的第二集群身份信息为在链下 TEE 内生成的集群身份信息，也即其中包含的第四待校验哈希值为链下 TEE 的实际预设信息的哈希值。因此，进一步将预先获得的针对所述链下 TEE 预设信息的第四标准哈希值与第四待检验哈希值进行比较，并将比较结果一致作为确认所述链下 TEE 可信的前提条件。同时，第二集群身份信息包含的集群身份公钥可判定为隐私计算节点 32 实际维护的集群身份公钥，可用于对待验证合约信息进行签名验证。其中，节点 32n 可通过控制节点 32 将第三标准哈希值、远程证明报告、第二集群身份信息一同发送至客户端 31。需要说明的是，此部分内容可参考前述步骤 104 中针对链下隐私计算节点进行验证的过程，在此不再赘述。

[74] 与上述图 2 所示的实施例类似，集群远程证明报告和待验证合约信息由节点 32n 发送至控制节点 32，再由控制节点 32 转发至客户端 31。控制节点 32 可一并向客户端 31 提供集群远程证明报告和待验证合约信息，也可先提供集群远程证明报告，并在客户端 31 根据集群远程证明报告验证通过后再向节点 32n 获取待验证合约信息以向客户端 31 提供待验证合约信息。其中，待验证合约信息为部署在节点 32n 处的链下合约的合约信息，并由节点 32n 在节点 32n 的链下 TEE 内采用集群身份私钥（维护在节点 32n 的链下 TEE 内）进行签名。比如，节点 32n 将部署在节点 32n 处的链下合约读入链下 TEE 内，并采用集群身份私钥进行签名。

[75] 客户端 31 在根据集群远程证明报告确定链下 TEE 可信（即节点 32n 的链下 TEE，由节点 32n 代表集群，用户感知不到集群内的其他节点）的情况下，采用集群身份公钥对待验证合约信息进行签名验证，以及根据链下合约的合约信息对待验证合约信息进行合约信息验证。其中，集群身份公钥处于公开状态，比如控制节点 31 向外公开发布集群身份公钥以由客户端 31 获取。或者，客户端 31 通过上述验证集群身份信息的方式获取。同时，链下合约的合约信息也可处于公开状态，比如链下合约的部署方向外公开发布合约信息以由客户端 31 获取。其中，合约信息可以包括链下合约的名称、描述、版本号、字节码哈希值、合约身份公钥等信息，本说明书并不对此进行限制。

[76] 与上述单节点形式中验证链下合约的原理类似，在签名验证和合约信息验证通过的情况下，客户端 31 可确定客户端 31 在通过区块链节点的预言机机制对链下合约发起

调用时，该链下合约由节点 32n 在链下 TEE 可信执行环境中执行，即确保节点 32n 中部署的链下合约可信，可按照用户预期执行计算任务。

[77] 需要说明的是，在链下隐私计算集群的形式中，各类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被判定为失效。比如，共享集群身份密钥过程中涉及的远程证明报告均由节点实时向认证服务器控制节点获取，而集群远程证明报告可由控制节点在本地缓存并设定老化时长。

[78] 在本说明书的链下合约调用方案中，区块链节点可以将计算任务分配至链下隐私计算节点，并调用链下隐私计算节点上部署的链下合约，通过在链下隐私计算节点创建的链下 TEE 内执行该链下合约，以完成上述的计算任务。通过远程证明、加密传输、基于签名的身份验证等技术，可以确保链下隐私计算节点得到的计算结果可靠，并且在计算过程中不会造成数据泄露，具有极高的安全性。在计算完成后，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。

[79] 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。

[80] 进一步的，目标数据作为链下合约的入参数据的同时，也属于目标数据的数据拥有方的隐私数据。因此，出于隐私保护，对于需要调用链下合约对目标数据进行处理的用户（以下称为数据使用方），数据拥有方可对这些用户针对目标数据的使用权进行权限控制。同时，明文形式的目标数据仅由数据拥有方持有，数据拥有方可对明文形式的目标数据进行加密（以下称为目标明文数据）得到密文形式的目标数据（以下称为目标密文数据），并且仅在链下隐私计算节点的链下 TEE 内可对目标密文数据进行解密。那么，数据拥有方可对已授予使用权的用户提供目标密文数据，以供该用户后续调用链下隐私计算节点在链下 TEE 内对目标密文数据进行解密并执行链下合约对解密得到的目标明文数据进行处理。下面结合图 4-7 对基于数据权限控制的链下合约调用方法进行说明。

[81] 图 4 是一示例性实施例提供的一种数据使用方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。

[82] 步骤 402，数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明。

[83] 在本实施例中，数据使用方在调用执行链下合约对目标明文数据进行处理（即理解为使用目标明文数据）的前提条件包括：目标明文数据的数据拥有方向该数据使用方授予了针对目标明文数据的使用权。比如，数据拥有方可对自身持有的目标明文数据进行加密得到目标密文数据，并声明该目标密文数据需要经该数据拥有方的授权才可使用。那么，数据使用方在调用链下合约之前，需向数据拥有方发起针对目标明文数据的授权请求，由数据拥有方对该数据使用方进行审核，并在审核通过后向该数据使用方颁发针对目标明文数据的使用权的 VC（Verifiable Claim，可验证声明），以及提供目标密文数据。数据使用方在获得可验证声明后，便可在后续调用链下合约对目标明文数据进行

处理时，向链下隐私计算节点出示该可验证声明，由链下隐私计算节点根据该可验证声明校验数据使用方针对目标明文数据的使用权，并在校验通过的情况下执行链下合约以完成对目标明文数据的处理。

[84] 在本实施例中，类似的，针对单节点形式和集群形式，数据使用方向链下隐私计算节点提交调用请求的方式也不同。在链下隐私计算节点为单节点形式的情况下，数据使用方向区块链节点提交调用请求，由该区块链节点通过预言机机制向链下隐私计算节点转发调用请求。在链下隐私计算节点属于链下隐私计算集群的情况下，数据使用方向区块链节点提交调用请求，由该区块链节点通过预言机机制向链下隐私计算集群的控制节点转发调用请求，再由控制节点将调用请求转发至集群中的链下隐私计算节点。下面结合图 5 对集群形式的情况进行详细说明，单节点形式的情况与此类似。

[85] 如图 5 所示，假定数据使用方的客户端 51 希望对已部署的链下合约进行调用（比如在验证链下合约通过之后）。客户端 51 可以通过链下渠道向控制节点 52 发送调用请求，该调用请求采用集群身份公钥进行加密，控制节点 52 可以基于负载均衡算法将该调用请求分配至集群内的某个链下隐私计算节点，比如节点 52n，由该节点 52n 对调用请求进行响应。节点 52n 在自身创建的链下 TEE 中通过集群身份私钥解密调用请求，从而获得调用请求中包含的入参数据。然后，节点 52n 可以在链下 TEE 中执行链下合约的字节码，以针对入参数据进行处理，从而得到相应的调用结果。进一步的，节点 52n 可以在链下 TEE 中对该调用结果进行加密后，经由控制节点 52 反馈至客户端 51。

[86] 客户端 51 可以通过链上渠道向控制节点 52 发送调用请求。客户端 51 可以向区块链网络 53 提交链下合约调用交易，该链下合约调用交易中包含调用请求，该调用请求由客户端 51 采用集群身份公钥进行加密。当然，链下合约调用交易本身也可以是加密传输的，比如采用集群身份公钥对调用交易进行加密，或者其他加密方式，这可以参考前文所述的数据加密传输的内容，此处不再赘述。链下合约调用交易可以调用预言机合约，使得预言机合约针对该交易所含的调用请求产生相应的合约事件，该合约事件被预言机服务器 54 监听到之后，由预言机服务器 54 获取调用请求并传输至控制节点 52。然后，控制节点 52 将调用请求分配至诸如链下隐私计算节点 52n 进行响应。以及，控制节点 52 可以通过预言机机制将调用结果反馈至链上，而节点 53n 可以主动发起一笔交易，将该调用结果上链，或者节点 53n 可以将调用结果反馈至客户端 51，由客户端 51 重新发起一笔交易将该调用结果上链。

[87] 如果入参数据为区块链数据，即数据拥有方向数据使用方提供的目标密文数据存证在区块链上，可由数据使用方从区块链上获取。客户端 51 可以向区块链网络 53 提交加密后的链下合约调用交易，该链下合约调用交易中包含入参数据的信息，并且该链下合约调用交易调用了用于获取入参数据的链上合约。节点 53n 收到加密后的链下合约调用交易后，在链上 TEE 中进行解密，然后通过链上 TEE 内部署的虚拟机执行被调用的链上合约，以获取被作为入参数据的区块链数据，节点 53n 可以在链上 TEE 内解密为明文，然后将该明文的区块链数据打包至调用请求中，并在链上 TEE 内采用集群身份公钥对该调用请求进行加密，而后基于预言机机制传输至控制节点 52，由控制节点 52 将调用请求分配至诸如链下隐私计算节点 52n 进行响应。以及，控制节点 52 可以通过预言机机制将调用结果反馈至链上，而节点 53n 可以将该调用结果上链。

[88] 在图 5 所示实施例中，以链下隐私计算集群为例进行描述。实际上，客户端 51 也可以直接与单个链下隐私计算节点进行交互，以调用该链下隐私计算节点上部署的链下合约，此处不再赘述。

[89] 步骤 404，所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出

所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[90] 在本实施例中，调用请求中记录有数据拥有方的身份、数据使用方的身份和可验证声明，这些信息均由数据使用方写入该调用请求中。换言之，调用请求中包含的上述信息均由数据使用方提供，用于声明可验证声明为目标明文数据的数据拥有方向该数据使用方颁发的可验证声明，而调用请求中的上述信息存在伪造的可能。具体而言，伪造的情况包含以下至少之一：调用请求中记录的数据拥有方的身份并非实际的数据拥有方的身份、调用请求中记录的数据使用方的身份并非实际的数据使用方的身份、调用请求中包含的可验证声明并非由实际的数据拥有方颁发、调用请求中包含的可验证声明并非颁发给实际的数据使用方。因此，链下隐私计算节点在接收到调用请求后，应先执行针对上述情况的校验操作以发现伪造的问题，从而提高数据的安全性。作为一示例性实施例，在以下校验操作均通过的情况下，链下隐私计算节点可校验出调用请求中的可验证声明为目标明文数据的数据拥有方（实际的数据拥有方）向数据使用方（即提交调用请求的实际数据使用方）颁发的可验证声明，也即确定出数据拥有方向数据使用方授予了针对目标明文数据的使用权：针对调用请求中记录的数据拥有方的身份的第一真实性校验操作、针对调用请求中记录的数据使用方的身份的第二真实性校验操作、针对可验证声明的实际颁发方为数据拥有方的第三真实性校验操作，以及针对可验证声明的实际颁发对象为数据使用方的第四真实性校验操作。其中，对于颁发方和颁发对象的理解为：由颁发方向颁发对象颁发可验证声明。需要说明的是，上述第一真实性校验操作~第四真实性校验操作之间并不存在执行顺序上的限制。

[91] 可通过 DIS（Decentralized Identifier Service，去中心化的身份服务）来为各个用户创建身份。DIS 可为用户提供不受任何单一注册中心、身份服务商或者认证中心限制的，完全由用户自身控制的 DID（Decentralized Identifier，去中心化身份标识符）。

[92] 基于通过 DID 来表示数据使用方和数据拥有方的身份标识，数据拥有方除了向数据使用者颁发可验证声明和提供目标密文数据以外，还提供采用与该数据拥有方的 DID 对应的私钥对目标明文数据进行签名得到的第一签名信息，从而可用于证明该数据拥有方的身份。比如，可直接对目标明文数据本身进行签名得到第一签名信息，或者先对目标明文数据进行哈希计算得到哈希值，再对该哈希值进行签名得到第一签名信息。同时，数据使用方生成调用请求时，为了证明该数据使用方的身份，采用与该数据使用方的 DID 对应的私钥对调用请求进行签名以得到相应的第二签名信息，并将该第二签名信息添加到调用请求中。综上，调用请求中至少包含目标密文数据、可验证声明、数据使用方的 DID、对应于目标明文数据的第一签名信息、数据拥有方的 DID 和对应于调用请求的第二签名信息。

[93] 基于上述生成调用请求的过程，链下隐私计算节点可通过第一用户公钥对调用请求中对应于目标明文数据的第一签名信息进行签名验证；其中，第一用户公钥与调用请求中记录的数据拥有方（不一定为实际的数据拥有方）的第一 DID 相对应。由于只有实际的数据拥有方才持有目标明文数据（向其他用户提供的是对目标明文数据加密得到的目标密文数据），那么在签名验证通过的情况（说明第一签名信息由实际的数据拥有方采用自身的私钥对目标明文数据进行签名得到）下，说明调用请求中记录的数据拥有方的第一 DID，为实际的数据拥有方的 DID，那么可判定第一真实性校验操作通过。

[94] 类似的，链下隐私计算节点在通过第二用户公钥对调用请求中对应于该调用请求的第二签名信息进行签名验证且签名验证通过的情况下，可判定第二真实性校验操作通过；其中，第二用户公钥与调用请求中记录的数据使用方的第二 DID 相对应。

[95] 在此基础上，在可验证声明的实际颁发方的 DID 与上述第一 DID 相匹配的情况下，说明调用请求中的可验证声明由实际的数据拥有方颁发，因此可判定第三真实性校验操作通过。以及，在可验证声明的实际颁发对象的 DID 与上述第二 DID 相匹配的情况下，说明调用请求中的可验证声明由实际的数据使用方接收（即是颁发给实际的数据使用方

的），因此可判定第四真实性校验操作通过。

[96] 在本实施例中，可验证声明的颁发方在颁发该可验证声明时，会在该可验证声明中记录自身的 DID 以及颁发对象的 DID；同时，采用与自身 DID 对应的私钥对该可验证声明进行签名，并将签名记录在该可验证声明中，以用于证明自身的身份。因此，可通过以下方式确定出可验证声明的实际颁发方的 DID 和可验证声明的实际颁发对象的 DID：读取调用请求中可验证声明记录的颁发方的 DID，并获取与读取到的 DID 对应的第三用户公钥，采用第三用户公钥对调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将调用请求中可验证声明记录的颁发方的 DID 作为实际颁发方的 DID；以及，将调用请求中可验证声明记录的颁发对象的 DID 作为实际颁发对象的 DID。

[97] 在本实施例中，可验证声明中包含数据拥有方定义的针对目标明文数据的调用规则，也即规定可验证声明的颁发对象如何使用目标明文数据。调用规则可针对目标明文数据的使用权进行细化控制；比如，链下合约中允许处理目标明文数据的合约函数、目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处理的频率。因此，步骤 404 中链下隐私计算节点在根据可验证声明确定出目标明文数据的数据拥有方向数据使用方授予了使用权后，还需进一步校验调用请求指示的调用操作是否符合可验证声明定义的调用规则，也即调用条件还包括调用请求指示的调用操作符合可验证声明定义的调用规则。

[98] 在本实施例中，数据拥有方可采用链下合约的合约身份公钥对目标明文数据进行加密得到目标密文数据，从而确保目标明文数据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。链下隐私计算节点的链下 TEE 内维护有对应于合约身份公钥的合约身份私钥，那么链下隐私计算节点在收到针对链下合约的调用请求后，可在链下 TEE 内采用该合约身份私钥对调用请求中的目标密文数据进行解密。

[99] 类似的，链下隐私计算节点在得到调用结果（即执行链下合约得到的执行结果）后，可在链下 TEE 内采用被调用的链下合约的合约身份私钥对调用结果进行签名，而数据使用方的客户端在获取链下隐私计算节点通过预言机机制反馈至区块链节点的执行结果后，可采用被调用的链下合约的合约身份公钥对执行结果进行签名验证，以及在签名验证通过的情况下，判定执行结果由被调用的链下合约生成。

[100] 需要说明的是，本说明书中加密与解密，生成签名与验证签名，可采用同一组密钥对，或者分别配置一组加密密钥对和一组签名密钥对。其中，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和相应的私钥。下面以节点身份密钥为例进行说明，集群身份密钥和合约身份密钥与此类似。

[101] 在一种情况下，节点身份密钥为一组密钥对，包含节点身份公钥和节点身份私钥。其中，节点身份公钥可用于对数据进行加密，那么可采用节点身份私钥对该数据进行解密；节点身份私钥可用于对数据进行签名，那么可采用节点身份公钥对该数据进行签名验证。在另一种情况下，可配置两组密钥对，分别为节点加密密钥对和节点签名密钥对。其中，节点加密密钥对用于对数据进行加密与解密，节点签名密钥对用于对数据进行签名与验证签名。

[102] 由以上实施例可见，数据拥有方可对自身拥有的目标明文数据进行加密得到目标密文数据，并向数据使用方提供目标密文数据，以及向数据使用方颁发针对该目标明文数据的使用权的可验证声明，可实现对目标明文数据使用权的权限控制，即控制目标明文数据允许被哪些用户调用链下合约进行处理。通过上述针对目标明文数据的授权机制，目标明文数据的使用权由数据拥有方把控，可有效提高数据拥有方的隐私安全性。进一步的，在进行授权时引入 DID 来表示各个用户的身份，可以使得用户的身份真正为用户所拥有并支配，用户可对自身的身份进行自主创建，以及完全去中心化的身份管理。

[103] 为了便于理解，下面结合图 6-8 对数据拥有方向数据使用方颁发针对目标明文数据使用权的可验证声明，以及数据使用方通过可验证声明调用链下合约对目标明文数据进行处理的过程进行详细说明。

[104] 图 6 是一示例性实施例提供的创建 DID 的流程图。如图 6 所示，该方法可以包括步骤 602~步骤 608。

[105] 步骤 602，数据使用方通过使用方客户端创建 DID、对应于 DID 的公钥和私钥，以及相应的 DID 文档。

[106] 在本实施例中，与数据使用方 DID 对应的公钥需发布至区块链进行存证，而与数据使用方 DID 对应的私钥则由数据使用方保管，比如保存在使用方客户端中。

[107] 在 DIS 系统中，一个 DID（Decentralized Identifier，去中心化身份标识符)对应一个实体（比如，数据使用方、数据拥有方等用户），而针对该 DID 的具体使用方式，则由与该 DID 对应的 DID 文档（DID Document）描述。DID 文档用于描述如何使用相应的 DID，至少包含相应 DID 的公钥；除此之外，还可记录加密方式、证明目的、验证方法和服务端点等信息。其中，证明目的与验证方法相结合，以提供证明事物的机制。例如，DID 文档可以指定特定的验证方法，例如密码公钥或化名生物特征协议，可以用于验证为目的而创建的方法。服务端点支持与 DID 控制器的可信交互。DID 和 DID 文档可直接登记在区块链或其他分布式网络上，而无需向中心化注册机构申请，通过利用区块链等分布式网络技术的不可篡改、哈希加密等特性，可实现让数字身份真正为用户所拥有并支配，而不再有任何中间人（即使是 DID 技术供应商）接触拥有控制用户的身份和数据。

[108] 步骤 604，使用方客户端创建一笔用于存证 DID 和 DID 文档的交易。

[109] 步骤 606，使用方客户端向区块链节点发起该用于存证 DID 和 DID 文档的交易。

[110] 步骤 608，区块链节点在区块链上存证 DID 和 DID 文档。

[111] 需要说明的是，存证 DID 和 DID 文档的区块链，与上述利用预言机机制调用链下合约的区块链可以是同一区块链，也可以是不同的区块链。

[112] 步骤 610，使用方客户端向区块链节点获取创建 DID 成功的回执。

[113] 在本实施例中，区块链节点在存证 DID 和 DID 文档之后，可生成用于记存证 DID 和 DID 文档成功的事件，并存储到区块链日志中。那么，使用方客户端可通过区块链的回调机制来获取该事件，从而确定出在区块链上已存证 DID 和 DID 文档，也即数据使用方创建 DID 成功。同时，还可生成相应的提示消息以供数据使用方查看，以告知数据使用方链上创建 DID 成功。

[114] 图 7 是一示例性实施例提供的数据授权过程的流程图。如图 7 所示，该过程可以包括步骤 702~步骤 722。

[115] 步骤 702，数据使用方通过使用方客户端创建针对目标明文数据的授权请求（包含使用方 DID、使用方信息和签名）。

[116] 在本实施例中，在创建授权请求时，在授权请求中记录使用方信息以供数据拥有方审核该数据使用方是否具备目标明文数据使用权的资格，也即由数据拥有方根据使用方信息来决定是否向数据使用方授权目标明文数据使用权。同时，使用方客户端采用与使用方 DID 对应的私钥对授权请求进行签名，并将得到的签名记录在授权请求中，以用于表明数据使用方的身份。

[117] 步骤 704，使用方客户端向数据拥有方的拥有方客户端发送授权请求。

[118] 步骤 706，拥有方客户端读取授权请求中包含的数据使用方 DID。

[119] 步骤 708，拥有方客户端向区块链节点发起针对使用方 DID 的查询交易。

[120] 步骤 710，区块链节点查询与使用方 DID 对应的 DID 文档。

[121] 步骤 712，拥有方客户端获取查询到的 DID 文档。

[122] 步骤 714，拥有方客户端采用 DID 文档中的公钥对授权请求中的签名进行签名验

证。

[123] 在本实施例中，由上述图 6 创建 DID 的过程可知，使用方 DID 的 DID 文档中记录有与使用方 DID 对应的公钥，那么可利用该公钥来验证授权请求中的使用方 DID 是否为数据使用方实际的 DID，也即验证数据使用方是否为授权请求中使用方 DID 的合法拥有者。

[124] 在本实施例中，除上述通过在授权请求中添加签名的方式以外，还可由拥有方客户端向使用方客户端发起针对 DID 的认证挑战，以完成对使用 DID 的验证。具体而言，使用方客户端创建的 DID 授权请求中无需添加签名，而是由拥有方客户端在获取到与使用方 DID 对应的 DID 文档中记录的公钥后，向使用方客户端发起 DID 认证挑战（DID auth challenge）消息，该消息中包含一段随机的字符串，用于要求使用方客户端采用使用方 DID 的私钥来该字符串进行签名。使用方客户端在收到 DID 认证挑战消息后，采用使用方 DID 的私钥对字符串进行签名，并将字符串和签名发送给拥有方客户端。那么，拥有方客户端可采用 DID 文档中的公钥对签名进行签名验证，进而在签名验证通过的情况下，确认数据使用方为授权请求中记录的使用方 DID 的合法拥有者。

[125] 步骤 716，在签名验证通过的情况下拥有方客户端对授权请求中的使用方信息进行审核，以确定出是否向数据使用方授予针对目标明文数据的使用权。

[126] 在本实施例中，除上述线上审核的方式以外，还可由数据使用方线下向数据拥有方提供使用方信息以供数据拥有方进行审核。而具体的审核方式，可根据实际情况灵活设定；当然，本说明书并不对此进行限制。

[127] 步骤 718，在审核通过的情况下，拥有方客户端创建使用方针对目标明文数据的使用权的可验证声明。

[128] 在本实施例中， DID 是一个实体的标识，而该实体拥有哪些权限、能力、行为和资产等具体信息，则通过可验证声明来表达。需要注意的是，一个 DID 可以拥有一个或多个可验证声明。举例而言，可验证声明中可包含以下字段：

[129] issuer: 声明颁发者（颁发方）；

[130] didsubject: 声明接收者（颁发对象）的 DID;

[131] expire: 声明过期时间;

[132] issuance date: 声明颁发时间;

[133] claim: 声明内容，可以是明文，也可以是密文，哈希等;

[134] proof: 有效性证明。

[135] 假设数据拥有方预先也采用上述图 6 的方式创建了自身的 DID。那么，数据拥有方可在 issuer 中记录自身的 DID，在 didsubject 中记录通过审核的数据使用方的 DID，在 expire 中记录目标明文数据的使用权的有效期，在 issuance date 中记录颁发该可验证声明的时刻，在 claim 中记录链下合约中允许处理目标明文数据的合约函数、允许调用链下合约对目标明文数据进行处理的次数（也即使用目标明文数据的次数）和允许调用链下合约对目标明文数据进行处理的频率（也即使用目标明文数据的频率）。而为了证明该可验证声明是由数据拥有方颁发的，数据拥有方需要采用自身的私钥对该可验证声明进行签名，并将签名记录在 proof 中。当然，上述针对可验证声明中包含的字段以及调用规则的描述，仅仅为一举例，在实际应用中可根据实际情况灵活调整。

[136] 步骤 720，拥有方客户端向使用方客户端返回可验证声明和数据拥有方的签名体。

[137] 在本实施例中，数据拥有方的签名体中至少包含第一签名信息，第一签名信息由拥有方客户端采用与自身 DID 对应的私钥对目标明文数据进行签名得到。

[138] 步骤 722，使用方客户端保存可验证声明和签名体。

[139] 图 8 是一示例性实施例提供的另一种调用合约的方法的流程图。如图 8 所示，该调用过程可以包括步骤 802~步骤 830。

[140] 步骤 802，使用方客户端创建调用请求。

[141] 在本实施例中，使用方客户端可获取数据拥有方采用链下合约的合约身份公钥对目标明文数据进行加密得到的目标密文数据，进而在需要调用链下合约对目标明文数据进行处理时，创建调用请求，该调用请求中包含目标密文数据、从数据拥有方获取到的可验证声明、数据使用方 DID、数据使用方的签名和数据拥有方的签名体。其中，对于数据使用方的签名，可由使用方客户端采用与数据使用方的 DID 对应的私钥对调用请求进行签名得到。当然，调用请求还可包含与调用操作相关的信息，比如链下合约的合约 ID、被调用函数的函数名等。合约 ID 譬如可以为链下合约的字节码的哈希值，使得链下隐私计算节点（可能部署有多个链下合约）可以据此找到相应的已部署的链下合约的字节码。链下合约可能包含多个函数，因而函数名可以指明数据使用方希望调用的函数；如果链下合约仅包含一个函数，或者数据使用方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名的信息。

[142] 当然，目标密文数据作为入参数据，可能为区块链数据，那么调用请求中可不必包含目标密文数据本身，而是包含入参数据的描述信息（比如为入参数据在区块链上的索引或存储地址等）。使用方客户端可以通过链上渠道向链下隐私计算节点发送调用请求，比如使用方客户端可以向区块链网络提交链下合约调用交易，该链下合约调用交易中包含调用请求，并且该链下合约调用交易用于调用获取区块链上存证的入参数据的链上合约。当然，链下合约调用交易本身也可以是加密传输的，这可以参考前文所述的数据加密传输的内容，此处不再赘述。那么，区块链节点收到加密后的链下合约调用交易后，在自身的链上 TEE 中进行解密，然后通过链上 TEE 内部署的虚拟机执行被调用的链上合约，从而根据调用请求中记录的描述信息获取被作为入参数据的区块链数据（即目标密文数据）。然后，区块链节点可通过预言机机制将该区块链数据与调用请求一并发送至链下隐私计算节点。比如，区块链节点可将该区块链数据写入调用请求中，或者将该区块链数据与调用请求打包发送至链下隐私计算节点，或者读取调用请求中包含的可验证声明、签名体、DID 等数据，并根据这些数据与该区块链数据重新生成一调用请求，将重新生成的调用请求发送至链下隐私计算节点。

[143] 步骤 804，使用方客户端向链下隐私计算节点提交调用请求。

[144] 步骤 806，链下隐私计算节点在链下 TEE 内解密目标密文数据。

[145] 步骤 808，链下隐私计算节点向区块链节点发起针对数据使用方 DID 和数据拥有方 DID 的查询交易。

[146] 在本实施例中，在一种情况下，调用请求中可直接记录数据拥有方 DID 和数据使用方 DID。其中，数据拥有方的签名体中可包含数据拥有方 DID。在该情况下，将数据拥有方 DID 作为调用请求中记录的数据拥有方的第一 DID，将该数据使用方 DID 作为调用请求中记录的数据使用方的第二 DID。在另一种情况下，调用请求中可无需直接记录数据拥有方 DID 和数据使用方 DID，而是将调用请求中可验证声明中记录的颁发方作为上述第一 DID，以及将调用请求中可验证声明中记录的颁发对象作为上述第二 DID。

[147] 在本实施例中，查询交易中包含数据使用方 DID 和数据拥有方 DID，从而从区块链（用于存证 DID 和 DID 文档的区块链）上查询相应的 DID 文档。当然，链下隐私计算节点向区块链查询数据使用方的 DID 文档，与查询数据拥有方的 DID 文档之间可相互独立，不存在优先级。比如，链下隐私计算节点还可以先向区块链查询数据使用方的 DID 文档，再查询数据拥有方的 DID 文档；或者，先向区块链查询数据拥有方的 DID 文档，再查询数据使用方的 DID 文档。

[148] 步骤 810，区块链节点查询数据使用方的 DID 文档和数据拥有方的 DID 文档。

[149] 步骤 812，链下隐私计算节点获取区块链节点查询到的 DID 文档。

[150] 步骤 814，链下隐私计算节点验证数据拥有方的签名。

[151] 步骤 816，链下隐私计算节点验证数据使用方的签名。

[152] 在本实施例中，调用请求中记录有数据拥有方 DID、数据使用方 DID 和可验证声

明，这些信息均由数据使用方提供，用于声明可验证声明为目标明文数据的数据拥有方向该数据使用方颁发的可验证声明，而调用请求中的上述信息存在伪造的可能。具体而言，伪造的情况包含以下至少之一：调用请求中记录的数据拥有方 DID 并非实际的数据拥有方 DID（实际的数据拥有方 DID 为目标明文数据实际拥有方的 DID）、调用请求中记录的数据使用方 DID 并非实际的数据使用方 DID（比如，发起调用请求的数据使用方填写了其他用户的 DID 来假冒该用户）、调用请求中包含的可验证声明并非由实际的数据拥有方颁发、调用请求中包含的可验证声明并非颁发给实际的数据使用方。

[153] 因此，链下隐私计算节点可通过数据拥有方的 DID 文档中记录的公钥（即第一用户公钥）对签名体中记录的签名（即第一签名信息）进行签名验证。由于只有实际的数据拥有方才持有目标明文数据（向其他用户提供的是目标密文数据），才能够对目标明文数据进行签名，其他用户无法对目标明文数据进行签名，那么在签名验证通过的情况（说明签名体中的签名由实际的数据拥有方采用自身 DID 对应的私钥对目标明文数据进行签名得到）下，说明调用请求中记录的数据拥有方 DID（即第一 DID）为实际的数据拥有方 DID。以数字签名的方式为例，数据拥有方在提供签名体时，对目标明文数据进行哈希计算得到第一哈希值，再采用与自身 DID 对应的私钥对第一哈希值进行签名得到第一签名信息，并将第一签名信息添加到签名体中。链下隐私计算节点通过步骤 806 解密目标密文数据得到了目标明文数据，对该目标明文数据进行哈希计算得到第二哈希值，基于第二哈希值和数据拥有方的 DID 文档中记录的公钥对第一签名信息进行签名验证，从而在签名验证通过的情况下，判定调用请求中记录的数据拥有方 DID 为实际的数据拥有方 DID，进而排除伪造数据拥有方 DID 的可能。

[154] 需要说明的是，数据拥有方可能存在多对用于签名的非对称密钥，那么数据拥有方在提供签名体时，可在签名体中添加公钥 ID，该公钥 ID 对应的公钥，与对目标明文数据签名所采用的私钥为一对非对称密钥对。

[155] 类似的，调用请求中记录的第二签名信息，由数据使用方采用与数据使用方 DID 对应的私钥对调用请求进行签名得到。因此，链下隐私计算节点可通过数据使用方的 DID 文档中记录的公钥（即第二用户公钥）对第二签名信息进行签名验证，并在签名验证通过的情况下，判定调用请求中记录的数据使用方的第二 DID 为实际的数据使用方 DID。

[156] 步骤 818，链下隐私计算节点校验可验证声明的实际颁发方是否为数据拥有方。

[157] 步骤 820，链下隐私计算节点校验可验证声明的实际颁发对象是否为数据使用方。

[158] 承接于上述步骤 814-816 的验证，还需进一步验证调用请求中的可验证声明是否为数据拥有方向数据使用方颁发的可验证声明。比如，在调用请求中记录的数据拥有方 DID 和数据使用方 DID 通过验证的情况下，若可验证声明的实际颁发方的 DID 与数据拥有方 DID 相匹配，则说明调用请求中的可验证声明由实际的数据拥有方颁发。以及，若可验证声明的实际颁发对象的 DID 与数据使用方 DID 相匹配，则说明调用请求中的可验证声明由实际的数据使用方接收（即是颁发给实际的数据使用方的）。需要说明的是，步骤 814-820 之间不存在时间先后顺序上的限制，本实施例中的顺序仅为举例说明。

[159] 由上述图 7 颁发可验证声明的过程可知，可验证声明的颁发方在颁发该可验证声明时，会在该可验证声明中记录自身的 DID 以及颁发对象的 DID，同时采用与自身 DID 对应的私钥对该可验证声明进行签名，并将签名记录在该可验证声明的 proof 中以用于证明自身的身份。

[160] 以验证了调用请求中记录的数据拥有方 DID 和数据使用方 DID 且验证均通过为例进行说明。若可验证声明中记录的颁发方 DID 与数据拥有方 DID 不同，或者可验证声明中记录的颁发对象 DID 与数据使用方 DID 不同，则说明可验证声明不正确，判定禁止使用目标明文数据。否则，进一步读取可验证声明的 issuer 记录的颁发方 DID，并获取与读取到的颁发方 DID 对应的第三用户公钥（即数据拥有方的 DID 文档中记录的公

钥），采用第三用户公钥对 proof 中记录的签名进行签名验证，并在签名验证通过的情况下确认可验证声明验证通过，也即确认可验证声明记录的颁发方 DID 为实际颁发方的 DID（也为实际的数据拥有方 DID）；以及，可验证声明记录的颁发对象 DID 为实际颁发对象的 DID（也为实际的数据使用方 DID）。

[161] 步骤 822，链下隐私计算节点校验调用操作是否符合可验证声明中定义的调用规则。

[162] 在本实施例中，在确认出调用请求中的可验证声明为目标明文数据的数据拥有方（实际的数据拥有方）向数据使用方（即提交调用请求的实际数据使用方）颁发的可验证声明后，链下隐私计算节点可以认可该可验证声明中定义的调用规则，即该可验证声明中定义的调用规则可信。那么，可进一步根据调用规则对数据使用方针对目标明文数据的使用权进行控制。

[163] 可校验调用请求指示的调用操作是否符合可验证声明中定义的调用规则。若符合，在转入步骤 824；否则，判定数据使用方禁止执行链下合约对目标明文数据进行处理。比如，当根据可验证声明中的 expire 判断出数据使用方针对目标明文数据的使用权到期时，禁止执行链下合约对目标明文数据进行处理。又如，当数据使用方所需调用的合约函数不符合调用规则中定义的允许处理目标明文数据的合约函数时，禁止执行链下合约对目标明文数据进行处理。当然，调用规则的具体内容可根据实际需求灵活设定，本说明书并不对此进行限制。

[164] 步骤 824，链下隐私计算节点在 TEE 内执行链下合约。

[165] 步骤 826，链下隐私计算节点在 TEE 内采用链下合约的合约身份私钥对执行结果签名。

[166] 步骤 828，链下隐私计算节点向使用方客户端反馈执行结果。

[167] 步骤 830，使用方客户端采用链下合约的合约身份公钥验证执行结果。

[168] 由以上实施例可见，数据拥有方可对自身拥有的目标明文数据进行加密得到目标密文数据，并向数据使用方提供目标密文数据，以及向数据使用方颁发针对该目标明文数据的使用权的可验证声明，可实现对目标明文数据使用权的权限控制，即控制目标明文数据允许被哪些用户调用链下合约进行处理。通过上述针对目标明文数据的授权机制，目标明文数据的使用权由数据拥有方把控，可有效提高数据拥有方的隐私安全性。进一步的，在进行授权时引入 DID 来表示各个用户的身份，可以使得用户的身份真正为用户所拥有并支配，用户可对自身的身份进行自主创建，以及完全去中心化的身份管理。

[169] 对应于上述数据使用方侧的实施例，本说明书还提出了链下隐私计算节点侧的实施例，在数据使用方侧实施例中所涉及的描述同样可以适用于链下隐私计算节点侧的实施例，下文中不再对此进行赘述。

[170] 相应地，图 9 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方法的流程图。如图 9 所示，该方法可以包括步骤 902~步骤 904。

[171] 步骤 902，链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明。

[172] 如前所述，所述链下隐私计算节点接收所述区块链节点通过所述预言机机制转发的所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点；或者，

[173] 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所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点，并由所述区块链节点通过所述预言机机制转发至所述控制节点。

[174] 步骤 904 所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数

据使用方授予了所述使用权。

[175] 如前所述，所述链下隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[176] 如前所述，所述链下隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；所述链下隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；所述链下隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；所述链下隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

[177] 如前所述，所述链下隐私计算节点可读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

[178] 如前所述，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[179] 如前所述，所述调用规则包括以下至少之一：所述链下合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处理的频率。

[180] 如前所述，所述目标密文数据由所述数据拥有方采用所述链下合约的合约身份公钥对所述目标明文数据进行加密得到，所述链下可信执行环境内维护有对应于所述合约身份公钥的合约身份私钥，所述目标密文数据由所述链下隐私计算节点在所述链下可信执行环境内采用所述合约身份私钥进行解密。

[181] 如前所述，所述链下隐私计算节点在所述链下可信执行环境内采用所述链下合约的合约身份私钥对执行所述链下合约得到的执行结果进行签名；所述链下隐私计算节点通过所述预言机机制将所述执行结果反馈至区块链节点以由所述数据使用方获取，所述数据使用方在采用所述链下合约的合约身份公钥对所述执行结果进行签名验证且签名验证通过的情况下，判定所述执行结果由所述链下合约生成。

[182] 如前所述，在接收所述调用请求之前，链下隐私计算节点向数据使用方提供针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成；所述链下隐私计算节点向所述数据使用方提供部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护；所述待验证合约信息由所述数据使用方在根据所

述远程证明报告确定所述链下可信执行环境可信的情况下，采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过区块链节点的预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

[183] 如前所述，所述链下隐私计算节点接收所述数据使用方向所述链下隐私计算节点发起的挑战，向所述数据使用方返回所述远程证明报告；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，在所述链下隐私计算集群的控制节点接收到所述数据使用方发起的挑战后，向所述控制节点发送所述远程证明报告，所述远程证明报告由所述控制节点返回至所述数据使用方。

[184] 如前所述，所述远程证明报告携带的所述自荐信息内包含第一待检验哈希值，所述第一待检验哈希值为所述链下可信执行环境的预设信息的哈希值，所述第一待检验哈希值用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述链下可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述链下可信执行环境可信的前提条件。

[185] 如前所述，所述链下隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述链下隐私计算节点的身份公钥和所述链下隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；所述链下隐私计算节点向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[186] 如前所述，所述链下隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述链下隐私计算节点的身份公钥、所述链下隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述链下可信执行环境的预设信息的哈希值；所述链下隐私计算节点向所述数据使用方提供第三标准哈希值，所述第三标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认所述链下可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述链下可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[187] 如前所述，所述链下可信执行环境内维护有对应于所述身份公钥的身份私钥；所述链下隐私计算节点在所述链下可信执行环境内采用所述身份私钥对所述调用请求进行解密，所述调用请求由所述数据使用方采用所述链下隐私计算节点的身份公钥进行加密。

[188] 如前所述，所述链下隐私计算节点的身份私钥为所述链下隐私计算节点的节点身份密钥中的节点身份私钥，所述链下隐私计算节点的身份公钥为所述节点身份密钥中的节点身份公钥；其中，在区块链节点与所述链下隐私计算节点进行交互以部署或调用链下合约的过程中，所述节点身份密钥用于对交互数据进行加密解密和/或签名签名验证；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的身份公钥为所述链下隐私计算集群的集群身份密钥中的集群身份公钥，所述链下隐

私计算节点的身份私钥为所述集群身份密钥中的集群身份私钥；其中，在区块链节点与所述链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名签名验证。
[189] 在本说明书的技术方案中，还可由数据使用方通过使用方客户端直接与隐私计算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“目标链下合约”称为“目标智能合约”。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。
[190] 图 10 是一示例性实施例提供的另一种数据使用方侧的调用合约的方法的流程图。如图 10 所示，该方法可以包括步骤 1002~步骤 1004。
[191] 步骤 1002，数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明。
[192] 步骤 1004，所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。
[193] 如前所述，在以下校验操作均通过的情况下，所述隐私计算节点确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。
[194] 如前所述，在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。
[195] 如前所述，通过以下方式确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符：读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。
[196] 如前所述，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[197] 如前所述，所述调用规则包括以下至少之一：所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。

[198] 如前所述，在提交所述调用请求之前，所述数据使用方获取针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成；所述数据使用方在根据所述远程证明报告确定所述可信执行环境可信的情况下，获取部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护；所述数据使用方采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。

[199] 如前所述，所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证；在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，从所述远程证明报告携带的所述自荐信息内提取出第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值；将预先获得的针对所述可信执行环境的第一标准哈希值与所述第一待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件。

[200] 如前所述，所述数据使用方获取所述隐私计算节点提供的第一身份信息，并对获取到的第一身份信息进行哈希计算以得到第二待校验哈希值，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息；所述数据使用方获取所述隐私计算节点提供的第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述数据使用方将所述第二待校验哈希值与所述第二标准哈希值进行比较，并在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[201] 如前所述，所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，获取所述隐私计算节点提供的第二身份信息，并对获取到的第二身份信息进行哈希计算以得到第三待校验哈希值，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值；获取所述隐私计算节点提供的第三标准哈希值，并将所述第三待校验哈希值与第三标准哈希值进行比较，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，将预先获得的针对所述可信执行环境的第四标准哈希值与所述第四待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件；其中，所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[202] 相应的，图 11 是一示例性实施例提供的一种隐私计算节点侧的调用合约的方法的流程图。如图 11 所示，该方法可以包括步骤 1102~步骤 1104。

[203] 步骤 1102，隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明。

[204] 步骤 1104，所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件

包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[205] 如前所述，所述隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[206] 如前所述，所述隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；所述隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；所述隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；所述隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

[207] 如前所述，所述隐私计算节点确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符，包括：读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

[208] 如前所述，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[209] 如前所述，所述调用规则包括以下至少之一：所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。

[210] 如前所述，在接收所述调用请求之前，隐私计算节点向数据使用方提供针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成；所述隐私计算节点向所述数据使用方提供部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护；所述待验证合约信息由所述数据使用方在根据所述远程证明报告确定所述可信执行环境可信的情况下，采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。

[211] 如前所述，所述远程证明报告携带的所述自荐信息内包含第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值，所述第一待检验哈希值

用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述可信执行环境可信的前提条件。

[212] 如前所述，所述隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；所述隐私计算节点向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[213] 如前所述，所述隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值；所述隐私计算节点向所述数据使用方提供第三标准哈希值，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认所述可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[214] 与上述方法实施例相对应，本说明书还提供了调用合约的装置的实施例。

[215] 本说明书的调用合约的装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。

[216] 从硬件层面而言，请参考图 12，图 12 是一示例性实施例提供的一种设备的示意结构图。如图 12 所示，在硬件层面，该设备包括处理器 1202、内部总线 1204、网络接口 1206、内存 1208 以及非易失性存储器 1210，当然还可能包括其他业务所需要的硬件。处理器 1202 从非易失性存储器 1210 中读取对应的计算机程序到内存 1208 中然后运行，在逻辑层面上形成调用合约的装置。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。

[217] 请参考图 13，在一种软件实施方式中，数据使用方侧的调用合约的装置可以包括：生成单元 1301，使数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；提交单元 1302，使所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[218] 可选的，所述提交单元 1302 具体用于：使所述数据使用方向区块链节点提交所述调用请求，由所述区块链节点通过所述预言机机制向所述链下隐私计算节点转发所述调用请求；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，所述数据使

用方向区块链节点提交所述调用请求，由所述区块链节点通过所述预言机机制向所述链下隐私计算集群的控制节点转发所述调用请求，所述调用请求由所述控制节点转发至所述链下隐私计算节点。

[219] 可选的，在以下校验操作均通过的情况下，所述链下隐私计算节点确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[220] 可选的，在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

[221] 可选的，通过以下方式确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符：读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

[222] 可选的，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[223] 可选的，所述调用规则包括以下至少之一：所述链下合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处理的频率。

[224] 可选的，所述目标密文数据由所述数据拥有方采用所述链下合约的合约身份公钥对所述目标明文数据进行加密得到，所述链下可信执行环境内维护有对应于所述合约身份公钥的合约身份私钥，所述目标密文数据由所述链下隐私计算节点在所述链下可信执行环境内采用所述合约身份私钥进行解密。

[225] 可选的，所述提交单元 1302 具体用于：使所述数据使用方获取所述链下隐私计算节点通过所述预言机机制反馈至区块链节点的执行结果，所述执行结果由所述链下隐私计算节点执行所述链下合约得到，并在所述链下可信执行环境内被采用所述链下合约的合约身份私钥进行签名；所述数据使用方在采用所述链下合约的合约身份公钥对所述执行结果进行签名验证且签名验证通过的情况下，判定所述执行结果由所述链下合约生成。

[226] 可选的，在提交所述调用请求之前，所述装置还包括：报告获取单元 1303，使所述数据使用方获取针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成；信息获取单元 1304，使所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，获取部署于所述链下隐私计算节点处的所述链下合约的

待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护；验证单元 1305，使所述数据使用方采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过所述预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

[227] 可选的，所述报告获取单元 1303 具体用于：使所述数据使用方向所述链下隐私计算节点发起挑战，并接收所述链下隐私计算节点返回的远程证明报告；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，所述数据使用方向所述链下隐私计算集群的控制节点发起挑战，并接收所述控制节点返回的远程证明报告。

[228] 可选的，所述信息获取单元 1304 具体用于：使所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证；在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，从所述远程证明报告携带的所述自荐信息内提取出第一待检验哈希值，所述第一待检验哈希值为所述链下可信执行环境的预设信息的哈希值；将预先获得的针对所述链下可信执行环境的第一标准哈希值与所述第一待检验哈希值进行比较，并将比较结果一致作为确认所述链下可信执行环境可信的前提条件。

[229] 可选的，所述验证单元 1305 具体用于：使所述数据使用方获取所述链下隐私计算节点提供的第一身份信息，并对获取到的第一身份信息进行哈希计算以得到第二待校验哈希值，所述第一身份信息包含所述链下隐私计算节点的身份公钥和所述链下隐私计算节点的其他身份信息；所述数据使用方获取所述链下隐私计算节点提供的第二标准哈希值，所述第二标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述数据使用方将所述第二待校验哈希值与所述第二标准哈希值进行比较，并在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[230] 可选的，所述信息获取单元 1304 具体用于：使所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，获取所述链下隐私计算节点提供的第二身份信息，并对获取到的第二身份信息进行哈希计算以得到第三待校验哈希值，所述第二身份信息包含所述链下隐私计算节点的身份公钥、所述链下隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述链下可信执行环境的预设信息的哈希值；获取所述链下隐私计算节点提供的第三标准哈希值，并将所述第三待校验哈希值与第三标准哈希值进行比较，所述第三标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，将预先获得的针对所述链下可信执行环境的第四标准哈希值与所述第四待检验哈希值进行比较，并将比较结果一致作为确认所述链下可信执行环境可信的前提条件；其中，所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[231] 可选的，所述调用请求由所述数据使用方采用所述链下隐私计算节点的身份公钥进行加密，所述链下可信执行环境内维护有对应于所述身份公钥的身份私钥，所述调用请求由所述链下隐私计算节点在所述链下可信执行环境内采用所述身份私钥进行解密。

[232] 可选的，所述链下隐私计算节点的身份私钥为所述链下隐私计算节点的节点身份密钥中的节点身份私钥，所述链下隐私计算节点的身份公钥为所述节点身份密钥中的节点身份公钥；其中，在区块链节点与所述链下隐私计算节点进行交互以部署或调用链下合约的过程中，所述节点身份密钥用于对交互数据进行加密解密和/或签名签名验证；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

的身份公钥为所述链下隐私计算集群的集群身份密钥中的集群身份公钥，所述链下隐私计算节点的身份私钥为所述集群身份密钥中的集群身份私钥；其中，在区块链节点与所述链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名签名验证。

[233] 请参考图 14，在另一种软件实施方式中，链下隐私计算节点侧的调用合约的装置可以包括：接收单元 1401，使链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；执行单元 1402，使所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[234] 可选的，所述链下隐私计算节点接收所述区块链节点通过所述预言机机制转发的所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点；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所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点，并由所述区块链节点通过所述预言机机制转发至所述控制节点。

[235] 可选的，所述链下隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[236] 可选的，所述链下隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；所述链下隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；所述链下隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；所述链下隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

[237] 可选的，所述执行单元 1402 具体用于：使所述链下隐私计算节点读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

[238] 可选的，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[239] 可选的，所述调用规则包括以下至少之一：所述链下合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处

理的频率。

[240] 可选的，所述目标密文数据由所述数据拥有方采用所述链下合约的合约身份公钥对所述目标明文数据进行加密得到，所述链下可信执行环境内维护有对应于所述合约身份公钥的合约身份私钥，所述目标密文数据由所述链下隐私计算节点在所述链下可信执行环境内采用所述合约身份私钥进行解密。

[241] 可选的，所述执行单元 1402 具体用于：所述链下隐私计算节点在所述链下可信执行环境内采用所述链下合约的合约身份私钥对执行所述链下合约得到的执行结果进行签名；所述链下隐私计算节点通过所述预言机机制将所述执行结果反馈至区块链节点以由所述数据使用方获取，所述数据使用方在采用所述链下合约的合约身份公钥对所述执行结果进行签名验证且签名验证通过的情况下，判定所述执行结果由所述链下合约生成。

[242] 可选的，在接收所述调用请求之前，所述装置还包括：报告提供单元 1403，使链下隐私计算节点向数据使用方提供针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成；信息提供单元 1404，使所述链下隐私计算节点向所述数据使用方提供部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护；所述待验证合约信息由所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过区块链节点的预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

[243] 可选的，所述报告提供单元 1403 具体用于：使所述链下隐私计算节点接收所述数据使用方向所述链下隐私计算节点发起的挑战，向所述数据使用方返回所述远程证明报告；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，在所述链下隐私计算集群的控制节点接收到所述数据使用方发起的挑战后，向所述控制节点发送所述远程证明报告，所述远程证明报告由所述控制节点返回至所述数据使用方。

[244] 可选的，所述远程证明报告携带的所述自荐信息内包含第一待检验哈希值，所述第一待检验哈希值为所述链下可信执行环境的预设信息的哈希值，所述第一待检验哈希值用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述链下可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述链下可信执行环境可信的前提条件。

[245] 可选的，所述信息提供单元 1404 具体用于：使所述链下隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述链下隐私计算节点的身份公钥和所述链下隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[246] 可选的，所述信息提供单元 1404 具体用于：使所述链下隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述链下隐私计算节点的身份公钥、所述链下隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述链下可信执行环境的预设信息的哈希值；向所述数据使用方提供第三标准哈

希值，所述第三标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认所述链下可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述链下可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[247] 可选的，所述链下可信执行环境内维护有对应于所述身份公钥的身份私钥；所述接收单元 1401 具体用于：

[248] 所述链下隐私计算节点在所述链下可信执行环境内采用所述身份私钥对所述调用请求进行解密，所述调用请求由所述数据使用方采用所述链下隐私计算节点的身份公钥进行加密。

[249] 可选的，所述链下隐私计算节点的身份私钥为所述链下隐私计算节点的节点身份密钥中的节点身份私钥，所述链下隐私计算节点的身份公钥为所述节点身份密钥中的节点身份公钥；其中，在区块链节点与所述链下隐私计算节点进行交互以部署或调用链下合约的过程中，所述节点身份密钥用于对交互数据进行加密解密和/或签名签名验证；或者，

[250] 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的身份公钥为所述链下隐私计算集群的集群身份密钥中的集群身份公钥，所述链下隐私计算节点的身份私钥为所述集群身份密钥中的集群身份私钥；其中，在区块链节点与所述链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名签名验证。

[251] 请参考图 15，在另一种软件实施方式中，数据使用方侧的调用合约的装置可以包括：生成单元 1501，使数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；提交单元 1502，使所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[252] 可选的，在以下校验操作均通过的情况下，所述隐私计算节点确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[253] 可选的，在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述

第四真实性校验操作通过。
[254] 可选的，通过以下方式确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符：读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。
[255] 可选的，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。
[256] 可选的，所述调用规则包括以下至少之一：所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。
[257] 可选的，在提交所述调用请求之前，所述装置还包括：报告获取单元 1503，使所述数据使用方获取针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成；信息获取单元 1504，使所述数据使用方在根据所述远程证明报告确定所述可信执行环境可信的情况下，获取部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护；验证单元 1505，使所述数据使用方采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。
[258] 可选的，报告获取单元 1503 具体用于：根据所述认证服务器的公钥对所述远程证明报告进行签名验证；在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，从所述远程证明报告携带的所述自荐信息内提取出第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值；将预先获得的针对所述可信执行环境的第一标准哈希值与所述第一待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件。
[259] 可选的，信息获取单元 1504 具体用于：所述数据使用方获取所述隐私计算节点提供的第一身份信息，并对获取到的第一身份信息进行哈希计算以得到第二待校验哈希值，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息；所述数据使用方获取所述隐私计算节点提供的第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述数据使用方将所述第二待校验哈希值与所述第二标准哈希值进行比较，并在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。
[260] 可选的，信息获取单元 1504 具体用于：根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，获取所述隐私计算节点提供的第二身份信息，并对获取到的第二身份信息进行哈希计算以得到第三待校验哈希值，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值；获取所述隐私计算节点提供的第三标准哈希值，并将所述第三待校验哈希值与第三标准哈希值进行比较，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，

将预先获得的针对所述可信执行环境的第四标准哈希值与所述第四待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件；其中，所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[261] 请参考图 16，在另一种软件实施方式中，隐私计算节点侧的调用合约的装置可以包括：接收单元 1601，使隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；执行单元 1602，使所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

[262] 可选的，所述隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权：针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

[263] 可选的，所述隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；所述隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应；所述隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；所述隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

[264] 可选的，所述隐私计算节点确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符，包括：读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

[265] 可选的，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

[266] 可选的，所述调用规则包括以下至少之一：所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。

[267] 可选的，在接收所述调用请求之前，所述装置还包括：报告提供单元 1603，使隐私计算节点向数据使用方提供针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成；信息提供单元 1604，使所述隐私计算节点向所述数据使用方提供部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护；所述待验证合约信息由所述数据使用

方在根据所述远程证明报告确定所述可信执行环境可信的情况下，采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。

[268] 可选的，所述远程证明报告携带的所述自荐信息内包含第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值，所述第一待检验哈希值用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述可信执行环境可信的前提条件。

[269] 可选的，信息提供单元 1604 具体用于：所述隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；所述隐私计算节点向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

[270] 可选的，信息提供单元 1604 具体用于：所述隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值；所述隐私计算节点向所述数据使用方提供第三标准哈希值，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认所述可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

[271] 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。具体的，计算机例如可以为个人计算机、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何设备的组合。

[272] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[273] 本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[274] 本说明书是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器

执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。
[275] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。
[276] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。
[277] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。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。
[278] 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。
[279] 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。
[280] 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。
[281] 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。
[282] 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。
[283] 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:

数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明;

所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

2、根据权利要求 1 所述的方法，所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，包括:

所述数据使用方向区块链节点提交所述调用请求，由所述区块链节点通过所述预言机机制向所述链下隐私计算节点转发所述调用请求；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，所述数据使用方向区块链节点提交所述调用请求，由所述区块链节点通过所述预言机机制向所述链下隐私计算集群的控制节点转发所述调用请求，所述调用请求由所述控制节点转发至所述链下隐私计算节点。

3、根据权利要求 1 所述的方法，在以下校验操作均通过的情况下，所述链下隐私计算节点确定出所述数据拥有方向所述数据使用方授予了所述使用权:

针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

4、根据权利要求 3 所述的方法，

在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应;

在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应;

在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过;

在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

5、根据权利要求 4 所述的方法，通过以下方式确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符:

读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥;

采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，

将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

6、根据权利要求 1 所述的方法，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

7、根据权利要求 6 所述的方法，所述调用规则包括以下至少之一:

所述链下合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处理的频率。

8、根据权利要求 1 所述的方法，所述目标密文数据由所述数据拥有方采用所述链下合约的合约身份公钥对所述目标明文数据进行加密得到，所述链下可信执行环境内维

护有对应于所述合约身份公钥的合约身份私钥，所述目标密文数据由所述链下隐私计算节点在所述链下可信执行环境内采用所述合约身份私钥进行解密。

9、根据权利要求 1 所述的方法，还包括：

所述数据使用方获取所述链下隐私计算节点通过所述预言机机制反馈至区块链节点的执行结果，所述执行结果由所述链下隐私计算节点执行所述链下合约得到，并在所述链下可信执行环境内被采用所述链下合约的合约身份私钥进行签名；

所述数据使用方在采用所述链下合约的合约身份公钥对所述执行结果进行签名验证且签名验证通过的情况下，判定所述执行结果由所述链下合约生成。

10、根据权利要求 1 所述的方法，在提交所述调用请求之前，所述方法还包括：

所述数据使用方获取针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成；

所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，获取部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护；

所述数据使用方采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过所述预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

11、根据权利要求 10 所述的方法，所述数据使用方获取针对所述链下可信执行环境的远程证明报告，包括：

所述数据使用方向所述链下隐私计算节点发起挑战，并接收所述链下隐私计算节点返回的远程证明报告；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，所述数据使用方向所述链下隐私计算集群的控制节点发起挑战，并接收所述控制节点返回的远程证明报告。

12、根据权利要求 10 所述的方法，所述数据使用方根据所述远程证明报告对所述链下可信执行环境进行验证，包括：

根据所述认证服务器的公钥对所述远程证明报告进行签名验证；

在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，从所述远程证明报告携带的所述自荐信息内提取出第一待检验哈希值，所述第一待检验哈希值为所述链下可信执行环境的预设信息的哈希值；

将预先获得的针对所述链下可信执行环境的第一标准哈希值与所述第一待检验哈希值进行比较，并将比较结果一致作为确认所述链下可信执行环境可信的前提条件。

13、根据权利要求 10 所述的方法，还包括：

所述数据使用方获取所述链下隐私计算节点提供的第一身份信息，并对获取到的第一身份信息进行哈希计算以得到第二待校验哈希值，所述第一身份信息包含所述链下隐私计算节点的身份公钥和所述链下隐私计算节点的其他身份信息；

所述数据使用方获取所述链下隐私计算节点提供的第二标准哈希值，所述第二标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

所述数据使用方将所述第二待校验哈希值与所述第二标准哈希值进行比较，并在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

14、根据权利要求 10 所述的方法，所述数据使用方根据所述远程证明报告对所述链下可信执行环境进行验证，包括：

根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，获取所述链下隐私计算节点提供的第二身份信息，并对获取到的第二身份信息进行哈希计算以得到第三待校验哈希值，所述第二身份信息包含所述链下隐私计算节点的身份公钥、所述链下隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述链下可信执行

环境的预设信息的哈希值；

获取所述链下隐私计算节点提供的第三标准哈希值，并将所述第三待校验哈希值与第三标准哈希值进行比较，所述第三标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，将预先获得的针对所述链下可信执行环境的第四标准哈希值与所述第四待检验哈希值进行比较，并将比较结果一致作为确认所述链下可信执行环境可信的前提条件；其中，所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

15、根据权利要求 1 所述的方法，所述调用请求由所述数据使用方采用所述链下隐私计算节点的身份公钥进行加密，所述链下可信执行环境内维护有对应于所述身份公钥的身份私钥，所述调用请求由所述链下隐私计算节点在所述链下可信执行环境内采用所述身份私钥进行解密。

16、根据权利要求 13-15 中任一所述的方法，所述链下隐私计算节点的身份私钥为所述链下隐私计算节点的节点身份密钥中的节点身份私钥，所述链下隐私计算节点的身份公钥为所述节点身份密钥中的节点身份公钥；其中，在区块链节点与所述链下隐私计算节点进行交互以部署或调用链下合约的过程中，所述节点身份密钥用于对交互数据进行加密解密和/或签名签名验证；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的身份公钥为所述链下隐私计算集群的集群身份密钥中的集群身份公钥，所述链下隐私计算节点的身份私钥为所述集群身份密钥中的集群身份私钥；其中，在区块链节点与所述链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名签名验证。

17、一种调用合约的方法，包括：

链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

18、根据权利要求 17 所述的方法，所述链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，包括：

所述链下隐私计算节点接收所述区块链节点通过所述预言机机制转发的所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点；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所述调用请求，所述调用请求由所述数据使用方提交至所述区块链节点，并由所述区块链节点通过所述预言机机制转发至所述控制节点。

19、根据权利要求 17 所述的方法，所述链下隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权：

针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

20、根据权利要求 19 所述的方法，

所述链下隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应；

所述链下隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身

份标识符相对应；

所述链下隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过；

所述链下隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

21、根据权利要求 20 所述的方法，所述链下隐私计算节点确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符，包括：

读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；

采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，

将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

22、根据权利要求 17 所述的方法，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

23、根据权利要求 22 所述的方法，所述调用规则包括以下至少之一：

所述链下合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述链下合约对所述目标明文数据进行处理的次数和允许调用所述链下合约对所述目标明文数据进行处理的频率。

24、根据权利要求 18 所述的方法，所述目标密文数据由所述数据拥有方采用所述链下合约的合约身份公钥对所述目标明文数据进行加密得到，所述链下可信执行环境内维护有对应于所述合约身份公钥的合约身份私钥，所述目标密文数据由所述链下隐私计算节点在所述链下可信执行环境内采用所述合约身份私钥进行解密。

25、根据权利要求 18 所述的方法，还包括：

所述链下隐私计算节点在所述链下可信执行环境内采用所述链下合约的合约身份私钥对执行所述链下合约得到的执行结果进行签名；

所述链下隐私计算节点通过所述预言机机制将所述执行结果反馈至区块链节点以由所述数据使用方获取，所述数据使用方在采用所述链下合约的合约身份公钥对所述执行结果进行签名验证且签名验证通过的情况下，判定所述执行结果由所述链下合约生成。

26、根据权利要求 18 所述的方法，在接收所述调用请求之前，所述方法还包括：

链下隐私计算节点向数据使用方提供针对所述链下可信执行环境的远程证明报告，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针对所述链下可信执行环境产生的自荐信息进行验证后生成；

所述链下隐私计算节点向所述数据使用方提供部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息，所述待验证合约信息被所述链下隐私计算节点在所述链下可信执行环境内采用所述链下隐私计算节点的身份私钥进行签名，所述身份私钥由所述链下隐私计算节点在所述链下可信执行环境内维护；

所述待验证合约信息由所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在通过区块链节点的预言机机制对所述链下合约发起调用时，所述链下合约由所述链下隐私计算节点在所述链下可信执行环境中执行。

27、根据权利要求 26 所述的方法，所述链下隐私计算节点向数据使用方提供针对所述链下可信执行环境的远程证明报告，包括：

接收所述数据使用方向所述链下隐私计算节点发起的挑战，向所述数据使用方返回所述远程证明报告；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，在所述链下隐私计算集群的控制节点接收到所述数据使用方发起的挑战后，向所述控制节点发送所述远程证明报告，所述远程证明报告由所述控制节点返回至所述数据使用方。

28、根据权利要求 26 所述的方法，所述远程证明报告携带的所述自荐信息内包含

第一待检验哈希值，所述第一待检验哈希值为所述链下可信执行环境的预设信息的哈希值，所述第一待检验哈希值用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述链下可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述链下可信执行环境可信的前提条件。

29、根据权利要求 26 所述的方法，还包括：

所述链下隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述链下隐私计算节点的身份公钥和所述链下隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；

所述链下隐私计算节点向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

30、根据权利要求 26 所述的方法，还包括：

所述链下隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述链下隐私计算节点的身份公钥、所述链下隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述链下可信执行环境的预设信息的哈希值；

所述链下隐私计算节点向所述数据使用方提供第三标准哈希值，所述第三标准哈希值由所述链下隐私计算节点在所述链下可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认所述链下可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述链下可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

31、根据权利要求 17 所述的方法，所述链下可信执行环境内维护有对应于所述身份公钥的身份私钥；所述方法还包括：

所述链下隐私计算节点在所述链下可信执行环境内采用所述身份私钥对所述调用请求进行解密，所述调用请求由所述数据使用方采用所述链下隐私计算节点的身份公钥进行加密。

32、根据权利要求 29-31 中任一所述的方法，所述链下隐私计算节点的身份私钥为所述链下隐私计算节点的节点身份密钥中的节点身份私钥，所述链下隐私计算节点的身份公钥为所述节点身份密钥中的节点身份公钥；其中，在区块链节点与所述链下隐私计算节点进行交互以部署或调用链下合约的过程中，所述节点身份密钥用于对交互数据进行加密解密和/或签名签名验证；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的身份公钥为所述链下隐私计算集群的集群身份密钥中的集群身份公钥，所述链下隐私计算节点的身份私钥为所述集群身份密钥中的集群身份私钥；其中，在区块链节点与所述链下隐私计算集群中的各节点进行交互以部署或调用链下合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名签名验证。

33、一种调用合约的方法，包括：

数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

34、根据权利要求 33 所述的方法，在以下校验操作均通过的情况下，所述隐私计算节点确定出所述数据拥有方向所述数据使用方授予了所述使用权:

针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

35、根据权利要求 34 所述的方法，

在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应;

在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应;

在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过;

在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

36、根据权利要求 35 所述的方法，通过以下方式确定出所述实际颁发方的去中心化身份标识符和所述实际颁发对象的去中心化身份标识符:

读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥;

采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符; 以及，

将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

37、根据权利要求 33 所述的方法，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

38、根据权利要求 37 所述的方法，所述调用规则包括以下至少之一:

所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。

39、根据权利要求 33 所述的方法，在提交所述调用请求之前，所述方法还包括:

所述数据使用方获取针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成;

所述数据使用方在根据所述远程证明报告确定所述可信执行环境可信的情况下，获取部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护;

所述数据使用方采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。

40、根据权利要求 39 所述的方法，所述数据使用方根据所述远程证明报告对所述可信执行环境进行验证，包括:

根据所述认证服务器的公钥对所述远程证明报告进行签名验证;

在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，从所述远程证明报告携带的所述自荐信息内提取出第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值;

将预先获得的针对所述可信执行环境的第一标准哈希值与所述第一待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件。

41、根据权利要求 39 所述的方法，还包括:

所述数据使用方获取所述隐私计算节点提供的第一身份信息，并对获取到的第一身份信息进行哈希计算以得到第二待校验哈希值，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息;

所述数据使用方获取所述隐私计算节点提供的第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到;

所述数据使用方将所述第二待校验哈希值与所述第二标准哈希值进行比较，并在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

42、根据权利要求 39 所述的方法，所述数据使用方根据所述远程证明报告对所述可信执行环境进行验证，包括:

根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，获取所述隐私计算节点提供的第二身份信息，并对获取到的第二身份信息进行哈希计算以得到第三待校验哈希值，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值;

获取所述隐私计算节点提供的第三标准哈希值，并将所述第三待校验哈希值与第三标准哈希值进行比较，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到;

在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，将预先获得的针对所述可信执行环境的第四标准哈希值与所述第四待检验哈希值进行比较，并将比较结果一致作为确认所述可信执行环境可信的前提条件；其中，所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

43、一种调用合约的方法，包括:

隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明;

所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

44、根据权利要求 43 所述的方法，所述隐私计算节点在以下校验操作均通过的情况下确定出所述数据拥有方向所述数据使用方授予了所述使用权:

针对所述调用请求中记录的所述数据拥有方的身份的第一真实性校验操作、针对所述调用请求中记录的所述数据使用方的身份的第二真实性校验操作、针对所述可验证声明的实际颁发方为所述数据拥有方的第三真实性校验操作，以及针对所述可验证声明的实际颁发对象为所述数据使用方的第四真实性校验操作。

45、根据权利要求 44 所述的方法，

所述隐私计算节点在通过第一用户公钥对所述调用请求中对应于所述目标明文数据的第一签名信息进行签名验证且签名验证通过的情况下，判定所述第一真实性校验操作通过，所述第一用户公钥与所述调用请求中记录的所述数据拥有方的第一去中心化身份标识符相对应;

所述隐私计算节点在通过第二用户公钥对所述调用请求中对应于所述调用请求的第二签名信息进行签名验证且签名验证通过的情况下，判定所述第二真实性校验操作通过，所述第二用户公钥与所述调用请求中记录的所述数据使用方的第二去中心化身份标识符相对应;

所述隐私计算节点在所述可验证声明的实际颁发方的去中心化身份标识符与所述第一去中心化身份标识符相匹配的情况下，判定所述第三真实性校验操作通过;

所述隐私计算节点在所述可验证声明的实际颁发对象的去中心化身份标识符与所述第二去中心化身份标识符相匹配的情况下，判定所述第四真实性校验操作通过。

46、根据权利要求 45 所述的方法，所述隐私计算节点确定出所述实际颁发方的去

中心化身份标识符和所述实际颁发对象的去中心化身份标识符，包括：

读取所述调用请求中可验证声明记录的颁发方的去中心化身份标识符，并获取与读取到的去中心化身份标识符对应的第三用户公钥；

采用所述第三用户公钥对所述调用请求中可验证声明记录的签名进行签名验证，并在签名验证通过的情况下将所述调用请求中可验证声明记录的颁发方的去中心化身份标识符作为所述实际颁发方的去中心化身份标识符；以及，

将所述调用请求中可验证声明记录的颁发对象的去中心化身份标识符作为所述实际颁发对象的去中心化身份标识符。

47、根据权利要求 43 所述的方法，所述调用条件还包括所述调用请求指示的调用操作符合所述可验证声明定义的调用规则。

48、根据权利要求 47 所述的方法，所述调用规则包括以下至少之一：

所述智能合约中允许处理所述目标明文数据的合约函数、所述目标明文数据的使用权的有效期、允许调用所述智能合约对所述目标明文数据进行处理的次数和允许调用所述智能合约对所述目标明文数据进行处理的频率。

49、根据权利要求 43 所述的方法，在接收所述调用请求之前，所述方法还包括：

隐私计算节点向数据使用方提供针对所述可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述隐私计算节点针对所述可信执行环境产生的自荐信息进行验证后生成；

所述隐私计算节点向所述数据使用方提供部署于所述隐私计算节点处的所述智能合约的待验证合约信息，所述待验证合约信息被所述隐私计算节点在所述可信执行环境内采用所述隐私计算节点的身份私钥进行签名，所述身份私钥由所述隐私计算节点在所述可信执行环境内维护；

所述待验证合约信息由所述数据使用方在根据所述远程证明报告确定所述可信执行环境可信的情况下，采用所述隐私计算节点的身份公钥对所述待验证合约信息进行签名验证，以及根据所述智能合约的合约信息对所述待验证合约信息进行合约信息验证，并在签名验证和合约信息验证通过的情况下，确定所述数据使用方在对所述智能合约发起调用时，所述智能合约由所述隐私计算节点在所述可信执行环境中执行。

50、根据权利要求 49 所述的方法，所述远程证明报告携带的所述自荐信息内包含第一待检验哈希值，所述第一待检验哈希值为所述可信执行环境的预设信息的哈希值，所述第一待检验哈希值用于所述数据使用方在根据所述认证服务器的公钥对所述远程证明报告进行签名验证并签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，与预先获得的针对所述可信执行环境的第一标准哈希值进行比较，且比较结果一致被作为所述数据使用方确认所述可信执行环境可信的前提条件。

51、根据权利要求 49 所述的方法，还包括：

所述隐私计算节点向所述数据使用方提供第一身份信息，所述第一身份信息包含所述隐私计算节点的身份公钥和所述隐私计算节点的其他身份信息，所述第一身份信息被所述数据使用方进行哈希计算以得到第二待校验哈希值；

所述隐私计算节点向所述数据使用方提供第二标准哈希值，所述第二标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

所述第二标准哈希值用于与所述第二待校验哈希值进行比较，且所述数据使用方在比较结果一致的情况下获取所述隐私计算节点的第一身份信息中包含的所述身份公钥。

52、根据权利要求 49 所述的方法，还包括：

所述隐私计算节点向所述数据使用方提供自身的第二身份信息，所述第二身份信息包含所述隐私计算节点的身份公钥、所述隐私计算节点的其他身份信息和第四待校验哈希值，所述第四待校验哈希值为所述可信执行环境的预设信息的哈希值；

所述隐私计算节点向所述数据使用方提供第三标准哈希值，所述第三标准哈希值由所述隐私计算节点在所述可信执行环境内生成自身的身份信息后对生成的身份信息进行哈希计算得到；

所述第二身份信息在所述数据使用方根据所述认证服务器的公钥对所述远程证明报告进行签名验证并在签名验证通过且所述远程证明报告包含的远程认证结果为通过认证的情况下，被所述数据使用方进行哈希计算以得到第三待校验哈希值；其中，确认

所述可信执行环境可信的前提条件包含在所述第三待校验哈希值与所述第三标准哈希值一致的情况下，所述第四待校验哈希值与所述数据使用方预先获得的针对所述可信执行环境的第四标准哈希值一致；所述第二身份信息包含的所述身份公钥用于对所述待验证合约信息进行签名验证。

53、一种调用合约的装置，包括：

生成单元，使数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

提交单元，使所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求，所述调用请求用于指示所述链下隐私计算节点在调用条件被满足的情况下，在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

54、一种调用合约的装置，包括：

接收单元，使链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

执行单元，使所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

55、一种调用合约的装置，包括：

生成单元，使数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

提交单元，使所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

56、一种调用合约的装置，包括：

接收单元，使隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明；

执行单元，使所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权。

57、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 1-52 中任一项所述的方法。

58、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 1-52 中任一项所述方法的步骤。

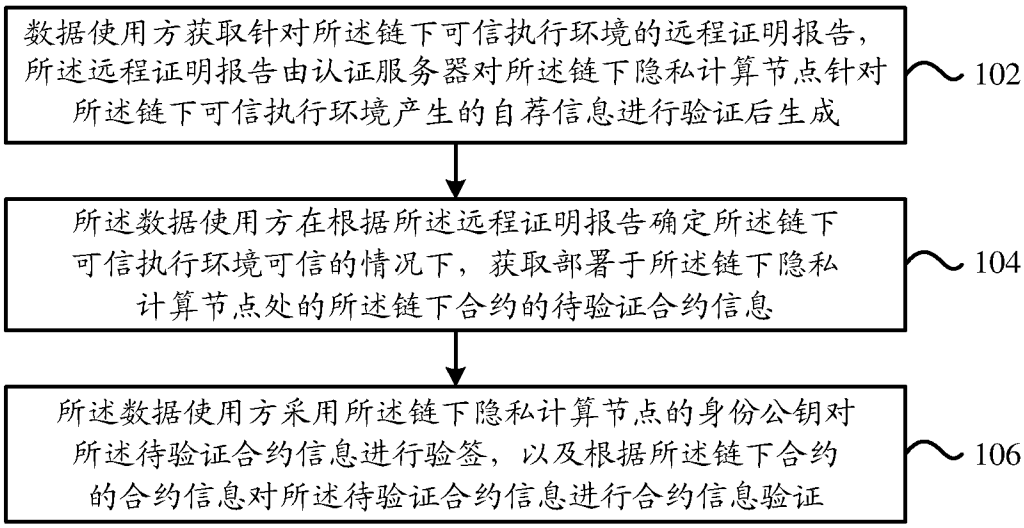

数据使用方获取针对所述链下可信执行环境的远程证明报告，所述远程证明报告由认证服务器对所述链下隐私计算节点针对所述链下可信执行环境产生的自荐信息进行验证后生成
102
所述数据使用方在根据所述远程证明报告确定所述链下可信执行环境可信的情况下，获取部署于所述链下隐私计算节点处的所述链下合约的待验证合约信息
104
所述数据使用方采用所述链下隐私计算节点的身份公钥对所述待验证合约信息进行验签，以及根据所述链下合约的合约信息对所述待验证合约信息进行合约信息验证
106

图 1

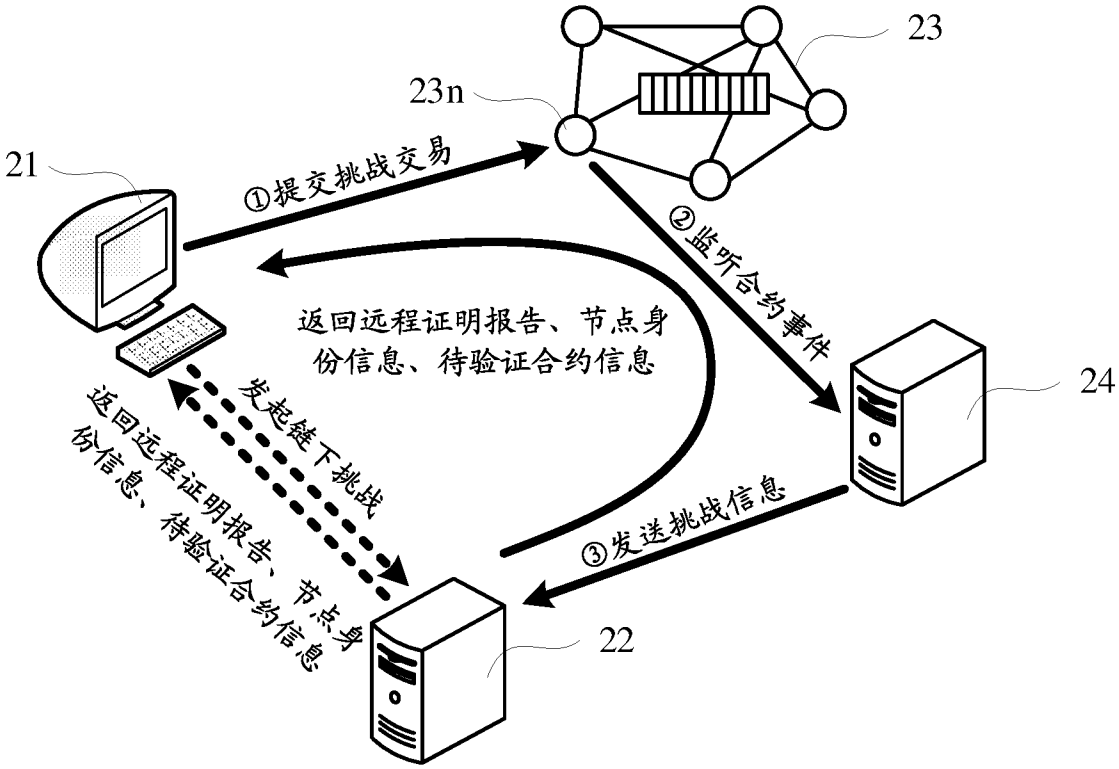

23
23n
21
①提交挑战交易
②监听合约事件
返回远程证明报告、节点身份信息、待验证合约信息
发起链下挑战
返回远程证明报告、节点身份信息、待验证合约信息
③发送挑战信息
24
22

图 2

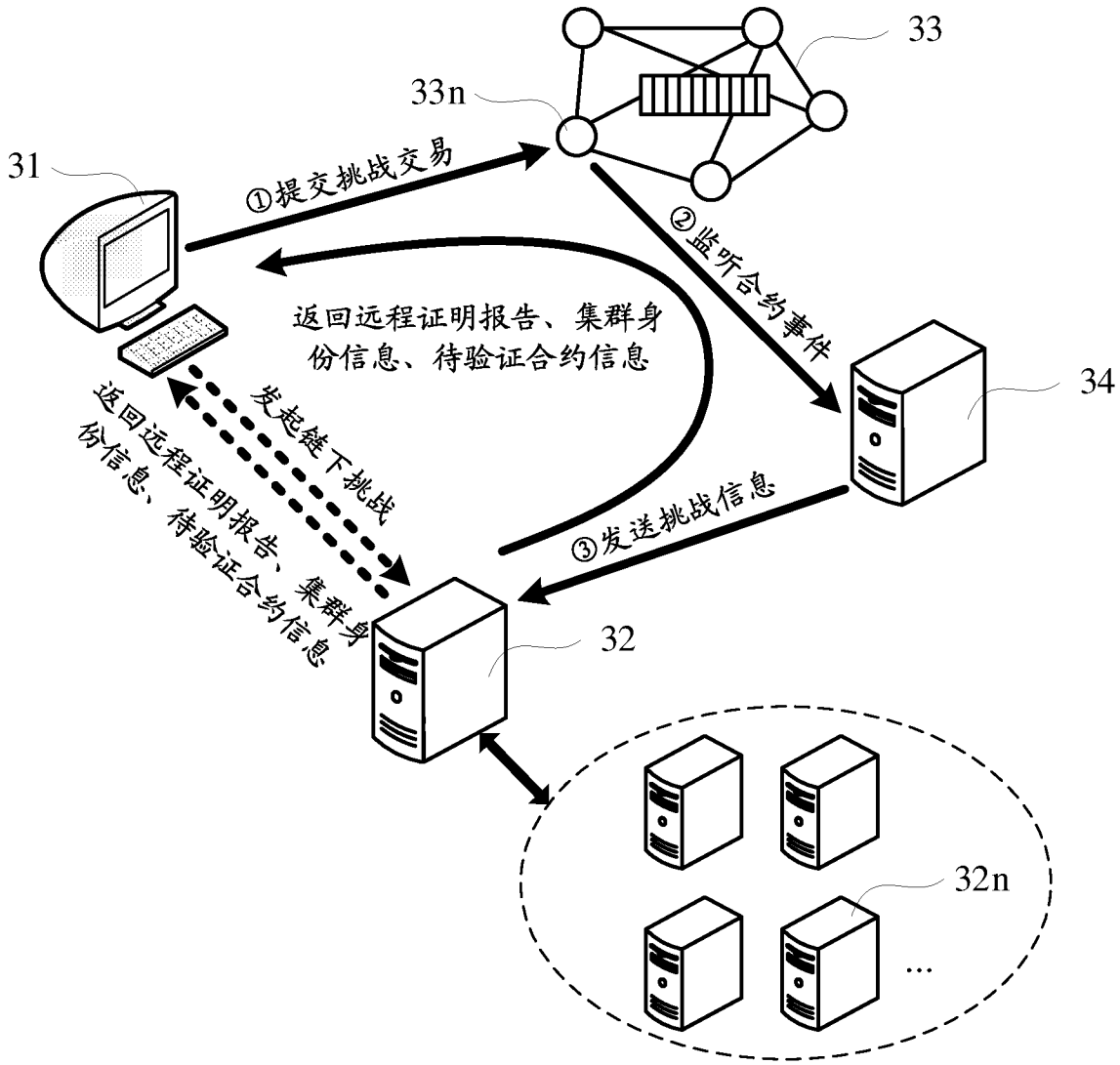

33
33n
31
①提交挑战交易
②监听合约事件
返回远程证明报告、集群身份信息、待验证合约信息
发起链下挑战
返回远程证明报告、集群身份信息、待验证合约信息
③发送挑战信息
34
32
32n
...

图 3

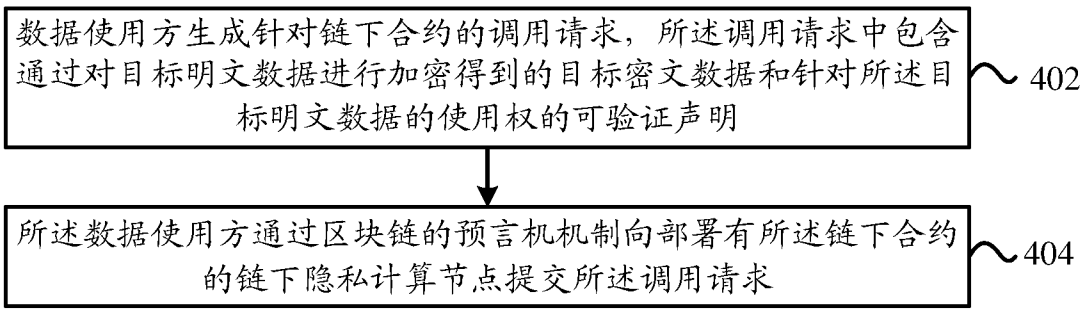

数据使用方生成针对链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明
402
所述数据使用方通过区块链的预言机机制向部署有所述链下合约的链下隐私计算节点提交所述调用请求
404

图 4

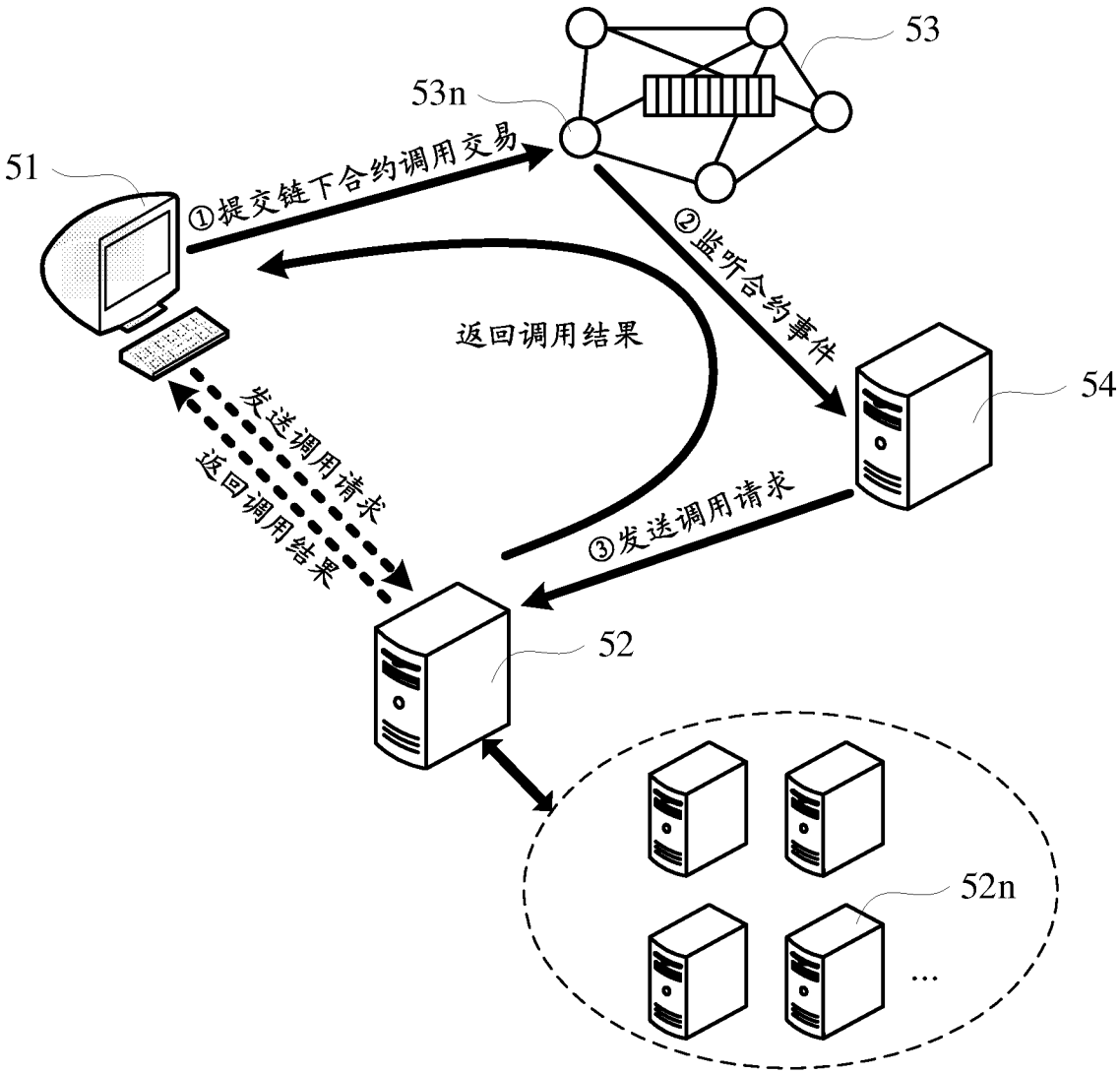

53
53n
51
①提交链下合约调用交易
②监听合约事件
返回调用结果
54
发送调用请求
返回调用结果
③发送调用请求
52
52n
...

图 5

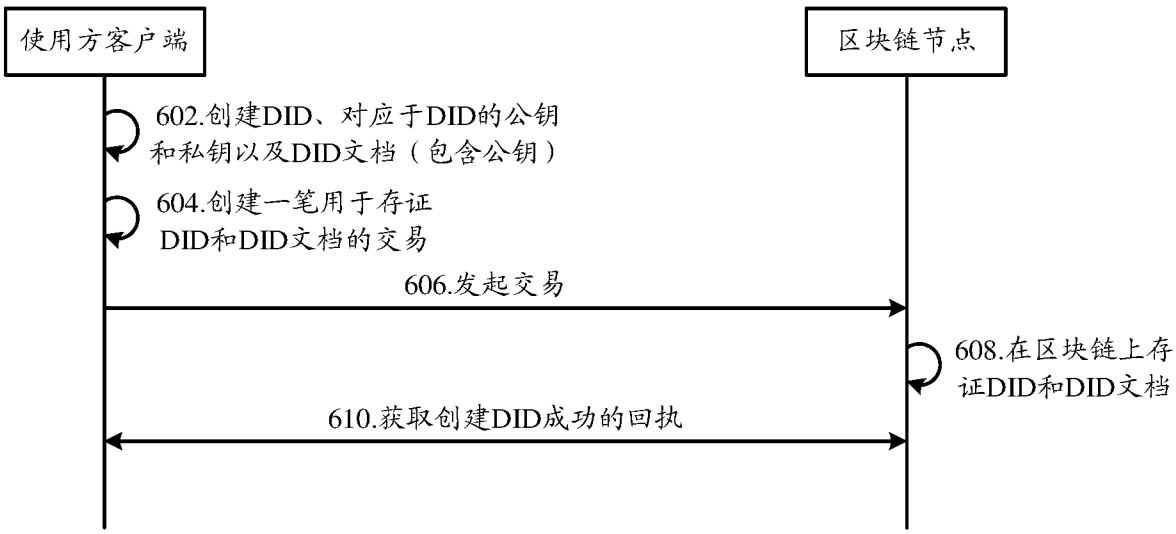

使用方客户端
区块链节点
602.创建DID、对应于DID的公钥和私钥以及DID文档（包含公钥）
604.创建一笔用于存证DID和DID文档的交易
606.发起交易
608.在区块链上存证DID和DID文档
610.获取创建DID成功的回执

图 6

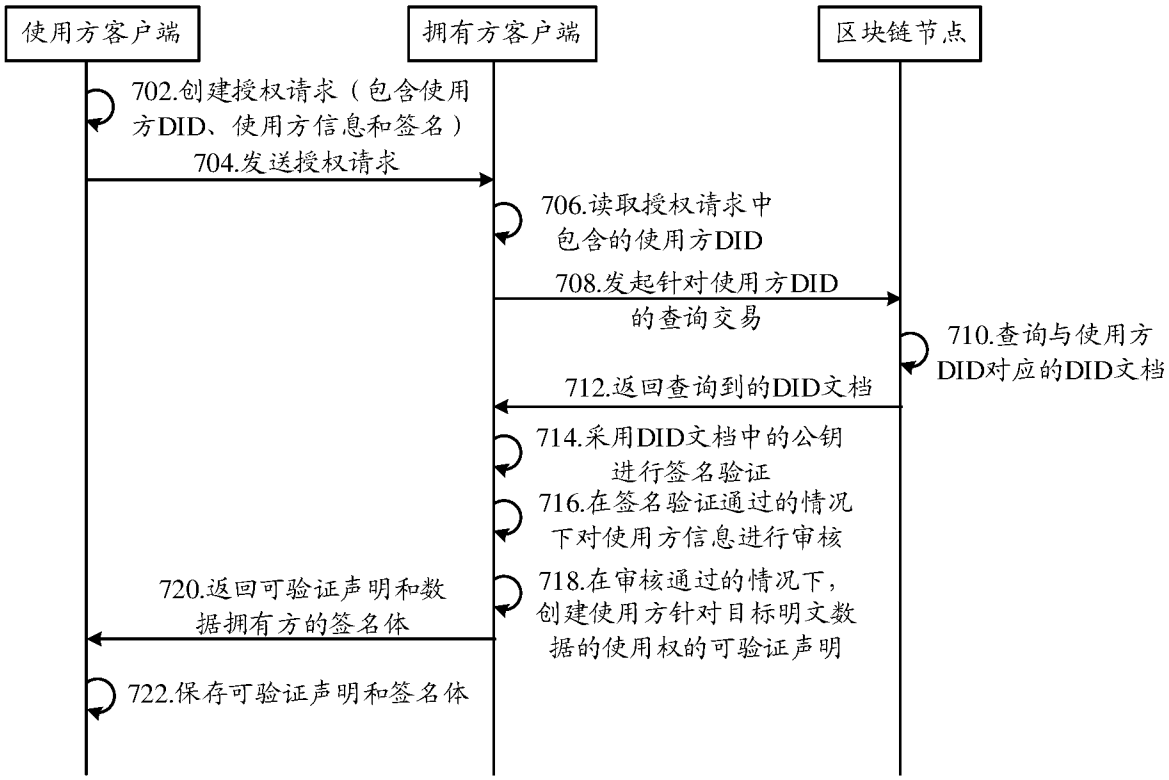

使用方客户端
拥有方客户端
区块链节点
702.创建授权请求（包含使用方DID、使用方信息和签名）
704.发送授权请求
706.读取授权请求中包含的使用方DID
708.发起针对使用方DID的查询交易
710.查询与使用方DID对应的DID文档
712.返回查询到的DID文档
714.采用DID文档中的公钥进行签名验证
716.在签名验证通过的情况下对使用方信息进行审核
718.在审核通过的情况下，创建使用方针对目标明文数据的使用权的可验证声明
720.返回可验证声明和数据拥有方的签名体
722.保存可验证声明和签名体

图 7

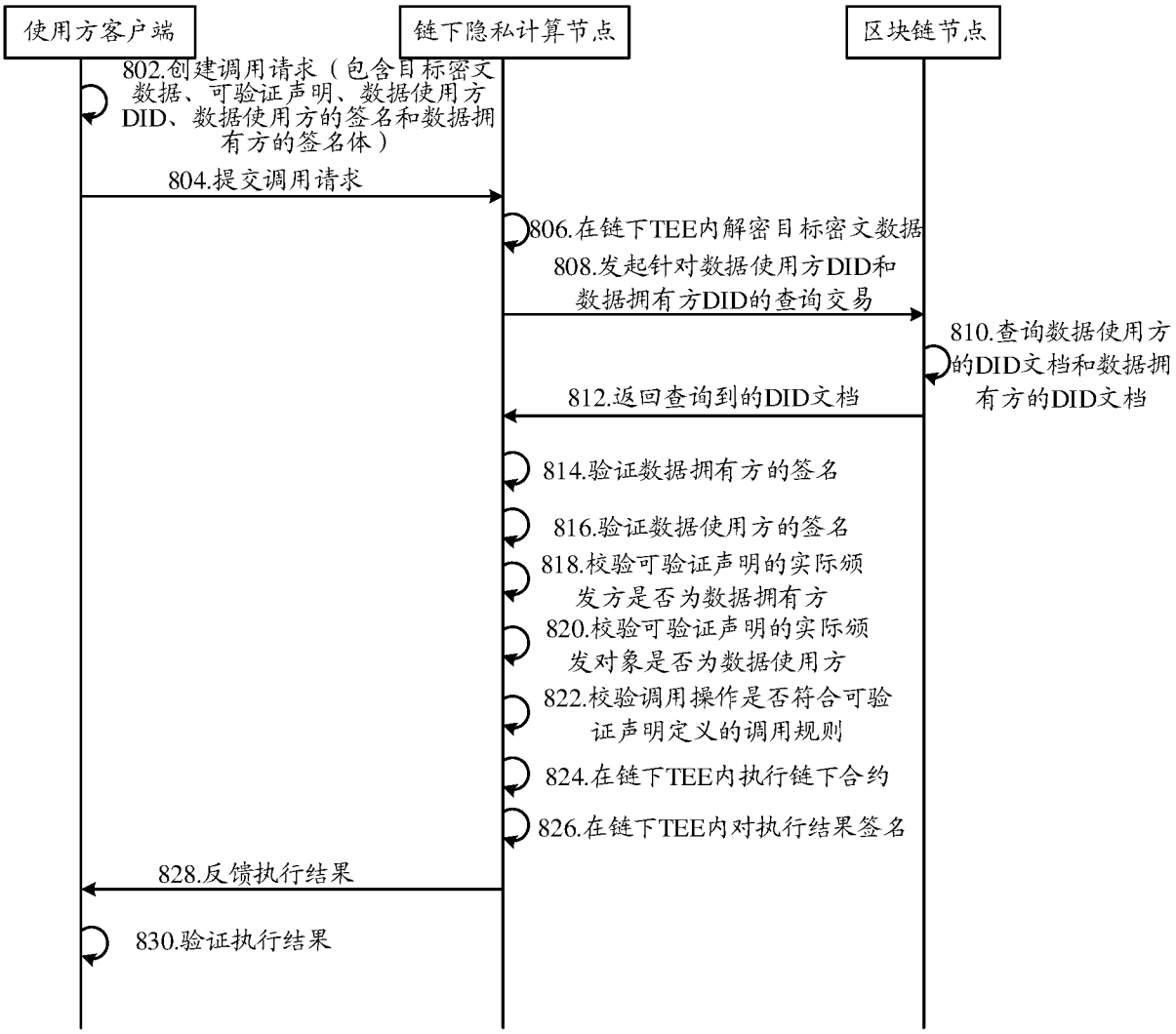

使用方客户端
链下隐私计算节点
区块链节点
802.创建调用请求（包含目标密文数据、可验证声明、数据使用方DID、数据使用方的签名和数据拥有方的签名体）
804.提交调用请求
806.在链下TEE内解密目标密文数据
808.发起针对数据使用方DID和数据拥有方DID的查询交易
810.查询数据使用方的DID文档和数据拥有方的DID文档
812.返回查询到的DID文档
814.验证数据拥有方的签名
816.验证数据使用方的签名
818.校验可验证声明的实际颁发方是否为数据拥有方
820.校验可验证声明的实际颁发对象是否为数据使用方
822.校验调用操作是否符合可验证声明定义的调用规则
824.在链下TEE内执行链下合约
826.在链下TEE内对执行结果签名
828.反馈执行结果
830.验证执行结果

图 8

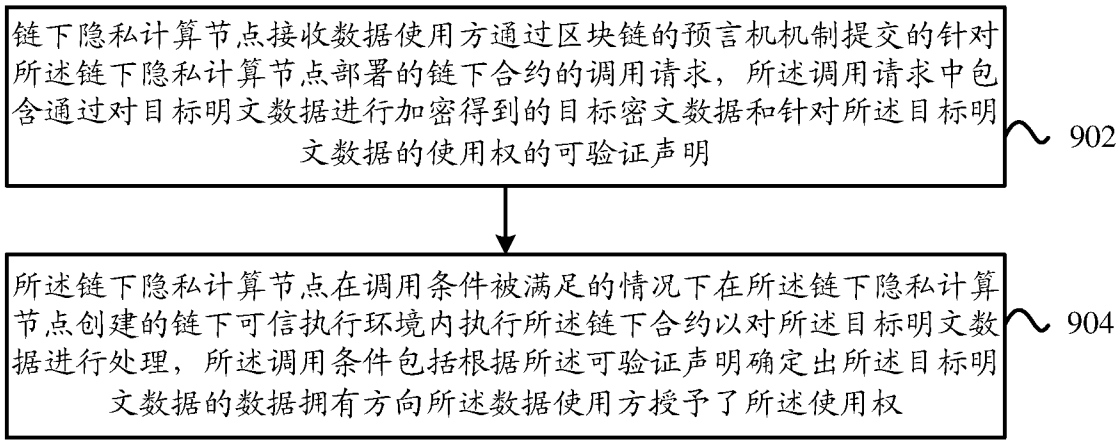

链下隐私计算节点接收数据使用方通过区块链的预言机机制提交的针对所述链下隐私计算节点部署的链下合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明
902
所述链下隐私计算节点在调用条件被满足的情况下在所述链下隐私计算节点创建的链下可信执行环境内执行所述链下合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权
904

图 9

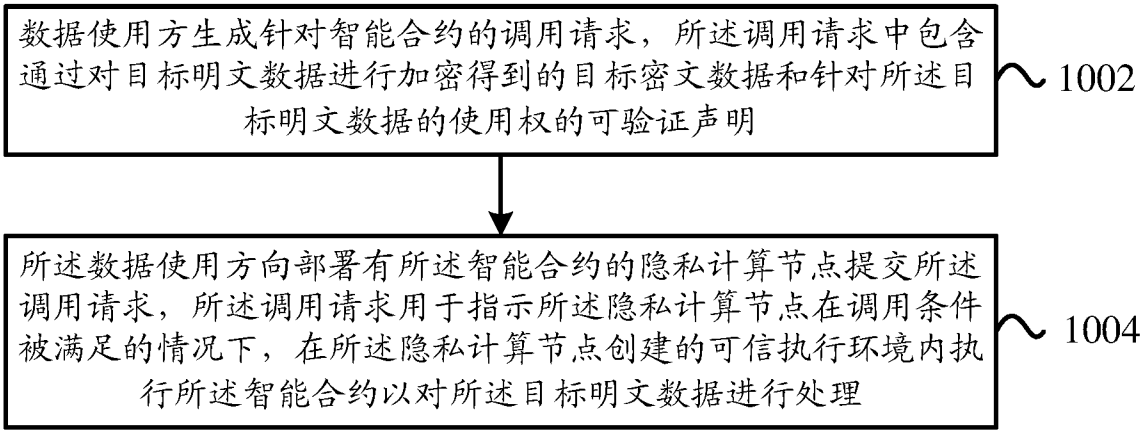

数据使用方生成针对智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明
1002
所述数据使用方向部署有所述智能合约的隐私计算节点提交所述调用请求，所述调用请求用于指示所述隐私计算节点在调用条件被满足的情况下，在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理
1004

图 10

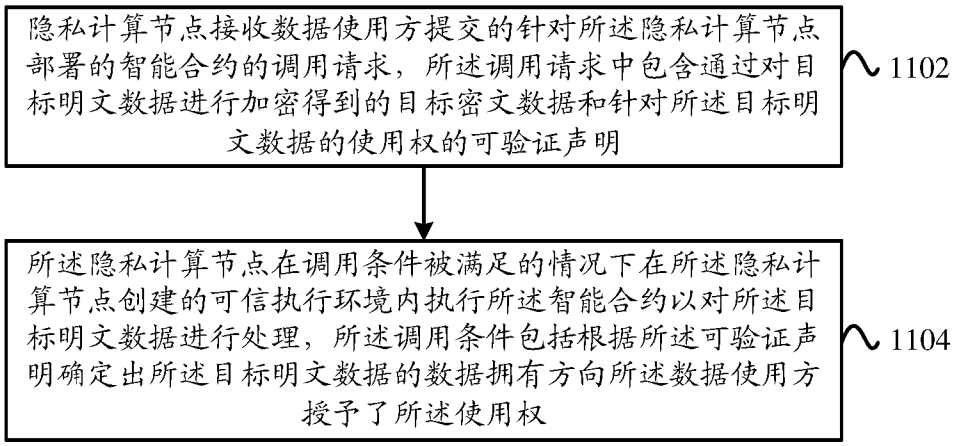

隐私计算节点接收数据使用方提交的针对所述隐私计算节点部署的智能合约的调用请求，所述调用请求中包含通过对目标明文数据进行加密得到的目标密文数据和针对所述目标明文数据的使用权的可验证声明
1102
所述隐私计算节点在调用条件被满足的情况下在所述隐私计算节点创建的可信执行环境内执行所述智能合约以对所述目标明文数据进行处理，所述调用条件包括根据所述可验证声明确定出所述目标明文数据的数据拥有方向所述数据使用方授予了所述使用权
1104

图 11

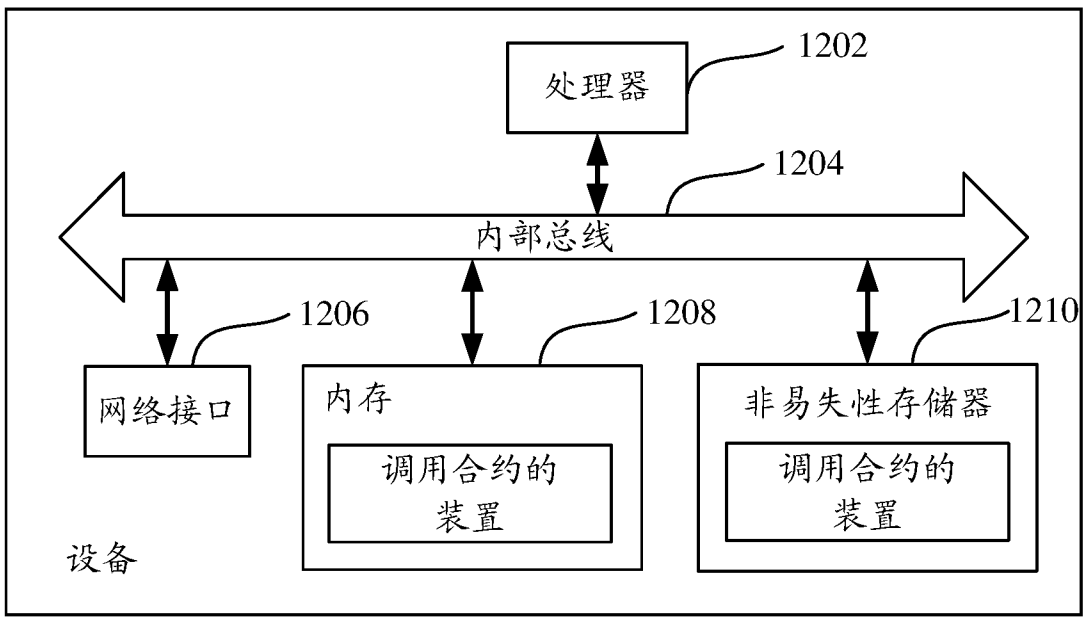

处理器
1202
1204
内部总线
1206
1208
1210
网络接口
内存
调用合约的装置
非易失性存储器
调用合约的装置
设备

图 12

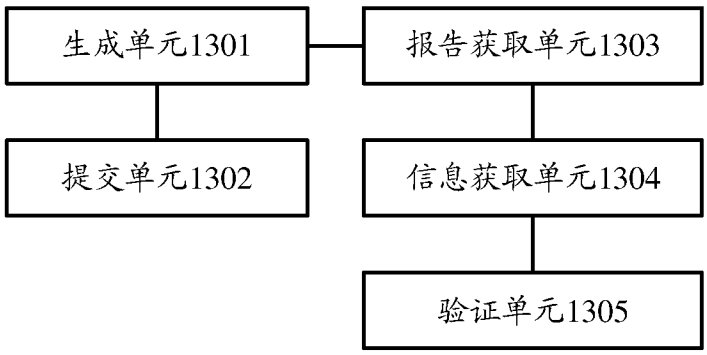


图 13

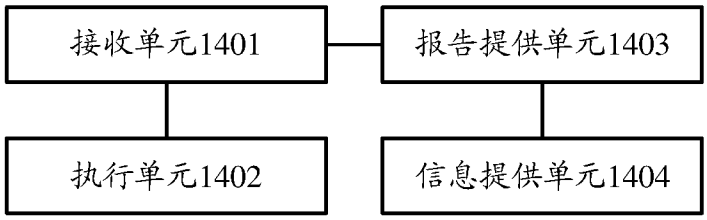


图 14

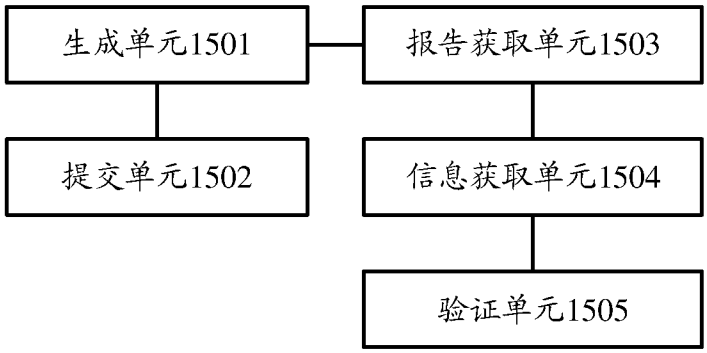


图 15

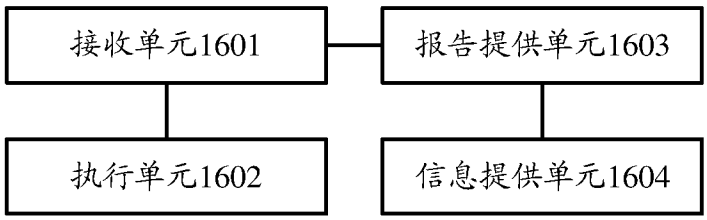


图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/073846

A. CLASSIFICATION OF SUBJECT MATTER

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

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)

CNABS; CNTXT; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 链下, 隐私, 计算, 可信, 环境, 区块链, 预言, 黑箱, 明文, 验证, 自荐, TEE, enclave, privacy, trust, environment, block, chain, prophecy, black box, plaintext, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111090876 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 01 May 2020 (2020-05-01) description, paragraphs [0004]-[0077], and figures 1-8	1-58
Y	CN 110457875 A (ALIBABA GROUP HOLDING LIMITED) 15 November 2019 (2019-11-15) description, paragraphs [0003]-[0081], and figures 1-12	1-3, 6-19, 22-34, 37-44, 47-58
A	CN 110457875 A (ALIBABA GROUP HOLDING LIMITED) 15 November 2019 (2019-11-15) description, paragraphs [0003]-[0081], and figures 1-12	4, 5, 20, 21, 35, 36, 45, 46
Y	CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019 (2019-11-29) description, paragraphs [0002]-[0090], and figures 1-6	1-3, 6-19, 22-34, 37-44, 47-58
Y	CN 110096551 A (ZHEJIANG TRCHAIN TECHNOLOGY CO., LTD.) 06 August 2019 (2019-08-06) description, paragraphs [0054]-[0062], and figures 1-8	1-3, 6-19, 22-32, 53, 54
A	CN 109886687 A (JUZIX TECHNOLOGY CO., LTD.) 14 June 2019 (2019-06-14) entire document	1-58

☐ 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
29 March 2021	**14 April 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/CN2021/073846

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111090876	A	01 May 2020	CN	111898153	A	06 November 2020
				CN	111090876	B	17 July 2020
CN	110457875	A	15 November 2019	HK	40018124	A0	30 September 2020
				WO	2021017441	A1	04 February 2021
				US	2020177604	A1	04 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
				HK	40017317	A0	18 September 2020
				KR	2212817	B1	08 February 2021
				IN	201947029881	A	19 June 2020
				SG	11201906754	A1	27 August 2019
CN	110096551	A	06 August 2019	None			
CN	109886687	A	14 June 2019	None			

国际检索报告

国际申请号
PCT/CN2021/073846

A. 主题的分类

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

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））

CNABS;CNTXT;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT：链下，隐私，计算，可信，环境，区块链，预言，黑箱，明文，验证，自荐，TEE，enclave，privacy，trust，environment，block，chain，prophecy，black box，plaintext，verify

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 111090876 A (支付宝杭州信息技术有限公司) 2020年 5月 1日 (2020-05-01) 说明书第[0004]-[0077]段，图1-8	1-58
Y	CN 110457875 A (阿里巴巴集团控股有限公司) 2019年 11月 15日 (2019-11-15) 说明书第[0003]-[0081]段，图1-12	1-3、6-19、22-34、37-44、47-58
A	CN 110457875 A (阿里巴巴集团控股有限公司) 2019年 11月 15日 (2019-11-15) 说明书第[0003]-[0081]段，图1-12	4、5、20、21、35、36、45、46
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[0002]-[0090]段，图1-6	1-3、6-19、22-34、37-44、47-58
Y	CN 110096551 A (浙江泰链科技有限公司) 2019年 8月 6日 (2019-08-06) 说明书第[0054]-[0062]段，图1-8	1-3、6-19、22-32、53、54
A	CN 109886687 A (矩阵元技术深圳有限公司) 2019年 6月 14日 (2019-06-14) 全文	1-58

☐ 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 29日	2021年 4月 14日

ISA/CN的名称和邮寄地址	受权官员
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	任洪潮
传真号 (86-10)62019451	电话号码 （86-512）88995644

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/073846

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	111090876	A	2020年 5月 1日	CN	111898153	A	2020年 11月 6日
				CN	111090876	B	2020年 7月 17日
CN	110457875	A	2019年 11月 15日	HK	40018124	A0	2020年 9月 30日
				WO	2021017441	A1	2021年 2月 4日
				US	2020177604	A1	2020年 6月 4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
				HK	40017317	A0	2020年 9月 18日
				KR	2212817	B1	2021年 2月 8日
				IN	201947029881	A	2020年 6月 19日
				SG	11201906754	A1	2019年 8月 27日
CN	110096551	A	2019年 8月 6日		无		
CN	109886687	A	2019年 6月 14日		无		