

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



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

(10) 国际公布号
WO 2021/184962 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) **H04L 9/32** (2006.01)

(21) 国际申请号: PCT/CN2021/073820

(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:
202010190878.1 2020年3月18日 (18.03.2020) CN

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

(72) 发明人: 吴因金 (WU, Yinqian); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。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)。

(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,

(54) Title: METHOD AND APPARATUS FOR GENERATING SHARED CONTRACT KEY

(54) 发明名称: 生成共享合约密钥的方法及装置

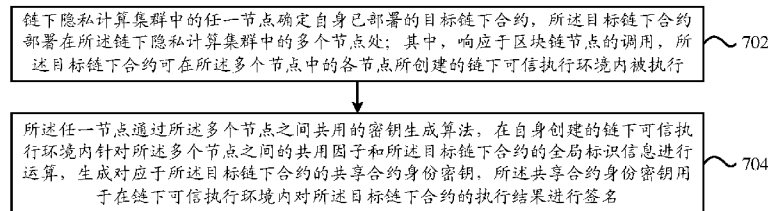


图 7

- 702 Any node in an off-chain privacy computation cluster determines a target off-chain contract that has been deployed by the node itself, wherein the target off-chain contract is deployed at a plurality of nodes in the off-chain privacy computation cluster, and in response to a call of a blockchain node, the target off-chain contract can be executed in an off-chain trusted execution environment created by each node of the plurality of nodes
- 704 By means of a key generation algorithm shared between the plurality of nodes, any node performs, in an off-chain trusted execution environment created thereby, an operation on shared factors between the plurality of nodes and global identification information of the target off-chain contract, and generates a shared contract identity key corresponding to the target off-chain contract, wherein the shared contract identity key is used for signing an execution result of the target off-chain contract in the off-chain trusted execution environment

(57) Abstract: Provided are a method and apparatus for generating a shared contract key. The method comprises: any node in an off-chain privacy computation cluster determining a target off-chain contract that has been deployed by the node itself, wherein the target off-chain contract is deployed at a plurality of nodes in the off-chain privacy computation cluster, and in response to a call of a blockchain node, the target off-chain contract can be executed in an off-chain trusted execution environment created by each node of the plurality of nodes; and by means of a key generation algorithm shared between the plurality of nodes, any node performing, in an off-chain trusted execution environment created thereby, an operation on shared factors between the plurality of nodes and global identification information of the target off-chain contract, and generating a shared contract identity key corresponding to the target

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(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))。

off-chain contract, wherein the shared contract identity key is used for signing an execution result of the target off-chain contract in the off-chain trusted execution environment. According to the scheme for generating a shared contract key, privacy protection can be realized.

(57) 摘要: 本说明书提供一种生成共享合约密钥的方法及装置, 该方法包括: 链下隐私计算集群中的任一节点确定自身已部署的目标链下合约, 目标链下合约部署在链下隐私计算集群中的多个节点处; 其中, 响应于区块链节点的调用, 目标链下合约可在多个节点中的各节点所创建的链下可信执行环境内被执行; 任一节点通过多个节点之间共用的密钥生成算法, 在自身创建的链下可信执行环境内针对多个节点之间的共用因子和目标链下合约的全局标识信息进行运算, 生成对应于目标链下合约的共享合约身份密钥, 共享合约身份密钥用于在链下可信执行环境内对目标链下合约的执行结果进行签名。上述生成共享合约密钥的方案可以实现隐私保护。

生成共享合约密钥的方法及装置

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，尤其涉及一种生成共享合约密钥的方法及装置。

背景技术

[02] 在相关技术中，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生成共享合约密钥的方法及装置，能够在链下环境内安全实现共享合约密钥的操作。

[04] 根据本说明书一个或多个实施例的第一方面，提出了一种生成共享合约密钥的方法，包括：链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于区块链节点的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行；所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

[05] 根据本说明书一个或多个实施例的第二方面，提出了一种生成共享合约密钥的方法，包括：链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于客户端的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行；

[06] 所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

[07] 根据本说明书一个或多个实施例的第三方面，提出了一种生成共享合约密钥的装置，包括：合约确定单元，使链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于区块链节点的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行；合约密钥生成单元，使所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

[08] 根据本说明书一个或多个实施例的第四方面，提出了一种生成共享合约密钥的装置，包括：合约确定单元，使隐私计算集群中的任一节点确定自身已部署的目标智能合约，所述目标智能合约部署在所述隐私计算集群中的多个节点处；其中，响应于客户端的调用，所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行；合约密钥生成单元，使所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约

的全局标识信息进行运算，生成对应于所述目标智能合约的共享合约身份密钥，所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名。

[09] 根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，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或第二方面所述的方法。

[10] 根据本说明书一个或多个实施例的第六方面，提出了一种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或第二方面所述方法的步骤。

[11] 综上所述，本说明书通过在链下隐私计算节点上实现链下可信执行环境，使得链下隐私计算节点可以提供安全可靠的运行环境，并且该链下可信执行环境的可靠性可以通过远程证明予以验证，从而能够安全可靠地生成共享合约身份密钥，并在集群内的节点之间传输，使得所有节点处部署的同一合约具有相同的共享合约身份密钥。

附图说明

[12] 图1是一示例性实施例提供的一种共享集群密钥的方法的流程图。

[13] 图2是一示例性实施例提供的一种链下隐私计算节点之间形成集群身份的示意图。

[14] 图3是一示例性实施例提供的一种实现远程证明的场景示意图。

[15] 图4是一示例性实施例提供的另一种实现远程证明的场景示意图。

[16] 图5是一示例性实施例提供的一种部署链下合约的场景示意图。

[17] 图6是一示例性实施例提供的另一种部署链下合约的场景示意图。

[18] 图7是一示例性实施例提供的一种生成共享合约密钥的方法的流程图。

[19] 图8是一示例性实施例提供的一种验证链下合约的示意图。

[20] 图9是一示例性实施例提供的另一种验证链下合约的示意图。

[21] 图10是一示例性实施例提供的一种调用链下合约的场景示意图。

[22] 图11是一示例性实施例提供的另一种生成共享合约密钥的方法的流程图。

[23] 图12是一示例性实施例提供的一种设备的结构示意图。

[24] 图13是一示例性实施例提供的一种生成共享合约密钥的装置的框图。

[25] 图14是一示例性实施例提供的另一种生成共享合约密钥的装置的框图。

具体实施方式

[26] 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。

[27] 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。

[28] 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。

[29] 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。

[30] 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。

[31] 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。

[32] 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。

[33] 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。

[34] 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。

[35] 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。

[36] 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。

[37] 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。

[38] 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。那么当用户向链下隐私计算节点发起一基于 WASM 程序的计算任务时，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。

[39] 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、动态扩展扩容等问题。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。下面对控制节点管理链下隐私计算节点请求加入集群的过程进行说明。

[40] 当任一链下隐私计算节点请求加入链下隐私计算集群时，控制节点可以向该节点发起挑战，并接收该节点返回的远程证明报告。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。

[41] 例如，以 Intel SGX 技术为例，链下 TEE 为链下隐私计算节点上创建的用于实现链

下隐私计算的 enclave，远程证明过程还涉及到链下隐私计算节点上另一个特殊的 enclave，即 quoting enclave（简称 QE），QE 是由英特尔提供并签名的架构型 enclave（Architectural Enclave）。上述 enclave 首先需要生成一用于本地认证的 REPORT（报告）结构，并由 QE 基于该 REPORT 结构验证该 enclave 是否与自身处于同一平台上，而后由 QE 将该 REPORT 结构封装为一结构体 QUOTE（即自荐信息），并使用 EPID(enhanced privacy identification) 密钥进行签名。EPID 密钥不仅代表链下隐私计算节点这一平台，还代表链下隐私计算节点的底层硬件的可信度，还可以绑定处理器固件的版本等信息，并且只有 QE 才能访问到 EPID 密钥，以用于对上述的结构体 QUOTE 进行签名。在 SGX 技术中，上述的认证服务器可以为英特尔公司提供的 IAS（Intel Attestation Service）服务器，链下隐私计算节点向 IAS 服务器发送经过签名的上述结构体 QUOTE，使得 IAS 服务器可以对签名进行验证，并向链下隐私计算节点返回相应的远程证明报告。

[42] 控制节点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 可信的情况下通过链下隐私计算节点加入链下隐私计算集群的请求，将该链下隐私计算节点作为该链下隐私计算集群的成员节点。

[43] 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。

[44] 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。

[45] 相应地，控制节点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。控制节点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控制节点时，还可以关联提供 IAS 的证书链，使得控制节点可以从该证书链中提取 IAS 服务器的公钥。然后，控制节点可以从远程证明报告中提取结构体 QUOTE 和签名验证结果。控制节点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，控制节点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，控制节点可以从结构体 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，控制节点预先获得了链下 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，控制节点可以将“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，控制节点就判定该链下隐私计

算节点的链下 TEE 不可信，而如果控制节点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，控制节点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。

[46] 除了 MREnclave 和 MRSigner 之外，控制节点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数据对，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数据对相关，比如该节点身份信息可以包含该数据对中的公钥（即节点身份公钥）。其中，代表身份信息的数据对可以存在一组或多组，比如一组数据对为用于签名与验签的数据对（即签名数据对），一组数据对为用于加密与解密的数据对（即加密数据对），则节点身份信息可以包括签名数据对中的签名公钥和加密数据对中的加密公钥。在一组数据对中，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。

[47] 相应的，控制节点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，控制节点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。假定控制节点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，控制节点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控制节点的同时，可以关联提供节点身份信息，当然控制节点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，控制节点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。如果第二待校验哈希值通过验证，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。

[48] 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，即针对第一待校验哈希值的验证、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校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，而对第一待校验哈希值可以不验证或者部分验证。例如，控制节点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校验哈希值，比如信任等级为 0 时，不需要验证第一待校验哈希值，信任等级为 1 时，验证第一待校验哈希值中的 MRSigner，信任等级为 2 时，验证第一待校验哈希值中的 MREnclave 等。

[49] 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，控制节点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，控制节点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。假定控制节点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，控制节点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，控制节点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。

[50] 需要说明的是，控制节点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。

[51] 基于上述验证链下隐私计算节点的方式，控制节点可将验证通过的节点加入链下隐私计算集群，从而建立一包含多个链下隐私计算节点的链下隐私计算集群。而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，上述的各个链下隐私计算节点均需在各自的链下 TEE 内维护集群加密私钥、集群签名私钥。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。

[52] 图 1 是一示例性实施例提供的一种共享集群密钥的方法的流程图。如图 1 所示，该方法可以包括步骤 102~步骤 106。

[53] 步骤 102，链下隐私计算集群中的任一节点获取所述链下隐私计算集群中其他节点发送的第一远程证明报告，所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成。

[54] 在本实施例中，针对所述其他节点的第一远程证明报告和产生的第一自荐信息，可参考前述内容中的解释，在此不再赘述。而在获取第一远程证明报告后，所述任一节点可根据第一远程证明报告确定所述其他节点创建的链下可信执行环境是否可信。具体而言，可根据认证服务器的公钥对第一远程证明报告进行签名验证，并在签名验证通过且第一远程证明报告包含的远程认证结果为通过认证的情况下，从第一远程证明报告携带的第一自荐信息内提取出第一待检验哈希值，该第一待检验哈希值为所述其他节点的链下可信执行环境中预设信息的哈希值。在提取出第一待检验哈希值后，将预先获得的针对所述其他节点的链下可信执行环境中预设信息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其他节点的链下可信执行环境可信的前提条件。类似的，确定链下可信执行环境是否可信的操作的具体过程，可参考上述控制节点确定待加入接点的链下可信执行环境是否可信的过程，在此不再赘述。

[55] 步骤 104，所述任一节点获取对应于所述链下隐私计算集群的集群身份密钥，所述集群身份密钥在所述任一节点创建的第二链下可信执行环境内生成，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/或签名验签。

[56] 在本实施例中，在需要生成集群身份时，控制节点可以将某一链下隐私计算节点

选取为主节点、其他的链下隐私计算节点为从节点，由主节点生成代表集群身份的密钥对（集群身份密钥），并进而将该密钥对分享至各个从节点，最终使得所有链下隐私计算节点都维护了统一的、代表集群身份的密钥对。例如，在链下隐私计算集群内的各个节点均已生成自身的节点身份信息之后，控制节点选取上述步骤 104 中的“任一节点”作为主节点，在自身创建的链下 TEE 内生成对应于链下隐私计算集群的集群身份密钥，进而在需要向其他节点共享集群身份密钥时，获取生成的集群身份密钥实施共享操作。

[57] 步骤 106，所述任一节点在根据所述第一远程证明报告确定所述第一链下可信执行环境可信的情况下，向所述其他节点发送所述集群身份密钥和第二远程证明报告，在所述第二远程证明报告表明所述第二链下可信执行环境可信的情况下，所述集群身份密钥被所述其他节点认可，所述第二远程证明报告由认证服务器对所述任一节点针对所述第二链下可信执行环境产生的第二自荐信息进行验证后生成。

[58] 在本实施例中，所述其他节点在确定出第二远程证明报告表明第二链下可信执行环境可信的情况下认可集群身份密钥，从而在自身的第一链下可信执行环境内维护集群身份密钥。

[59] 而所述任一节点在向所述其他节点发送所述集群身份密钥之前，可先对所述其他节点的第一节点身份信息进行验证。进一步的，由于第一节点身份信息中包含所述其他节点的节点身份公钥，可在验证通过的情况下获取第一节点身份信息中包含的节点身份公钥以对集群身份密钥进行加密，使得只有所述其他节点通过自身的节点身份私钥才可对集群身份密钥进行解密，从而保证了所述任一节点向所述其他节点共享集群身份密钥的安全性。具体而言，所述任一节点可获取所述其他节点提供的第一节点身份信息（比如，所述其他节点可将第一节点身份信息与第一远程证明报告关联发送至所述任一节点），并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，所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息。同时，所述任一节点获取所述其他节点提供的第二标准哈希值（比如，第二标准哈希值可包含在第一远程证明报告中），所述第二标准哈希值由所述其他节点在所述其他节点在所述其他节点的链下可信执行环境内生成自身的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。进一步的，所述任一节点将第二待校验哈希值与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其他节点的节点身份信息中包含的节点身份公钥，从而采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名，并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。所述任一节点在向所述其他节点共享加密后的集群身份密钥时，将自身的第二远程证明报告与加密后的集群身份密钥关联发送至所述其他节点以证明身份。那么，所述其他节点在根据第二远程证明报告确定所述任一节点创建的链下可信执行环境可信的情况下，采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密，以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名，并在签名验证通过的情况下在自身的链下可信执行环境内维护所述集群身份密钥。

[60] 而针对获取所述任一节点的节点身份公钥的方式，与所述任一节点获取所述其他节点的节点身份公钥的方式类似。具体而言，所述任一节点可向所述其他节点提供第二节点身份信息（比如，所述任一节点可将第二节点身份信息与第二远程证明报告关联发送至所述其他节点），第二节点身份信息包含所述任一节点的节点身份公钥和所述任一节点的其他身份信息。同时，所述任一节点向所述其他节点提供第三标准哈希值（比如，第三标准哈希值可包含在第二远程证明报告中），所述第三标准哈希值由所述任一节点在所述任一节点的链下可信执行环境内生成自身的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。那么，所述其他节点在对第二节点身份信息进行哈希计算得到的第三待校验哈希值与第三标准哈希值一致的情况下，采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密，以及采用所述任一节点的节点身份信息中包含的

节点身份公钥验证所述集群身份密钥的签名,并在签名验证通过的情况下在所述其他节点的链下可信执行环境内维护所述集群身份密钥。

[61] 类似的,控制节点可选取链下隐私计算集群中区别于“任一节点”的其他节点作为主节点,在自身创建的链下 TEE 内生成对应于链下隐私计算集群的集群身份密钥,进而向“任一节点”共享集群身份密钥。

[62] 在该情况下,所述任一节点获取所述集群身份密钥的过程包括:所述任一节点向所述链下隐私计算集群中其他节点提供第二远程证明报告(所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成),进一步的,所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的链下可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告,所述集群身份密钥在所述其他节点创建的链下可信执行环境内生成,所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成。那么,所述任一节点在确定出所述第一远程证明报告表明所述其他节点的链下可信执行环境可信的情况下认可所述集群身份密钥,进而在自身创建的链下可信执行环境内维护所述集群身份密钥。上述由任一节点获取其他节点共享的集群身份密钥的过程,与上述任一节点向其他节点共享集群身份密钥的过程的类似,在此不再赘述。

[63] 由此可见,所述任一节点在向所述其他节点共享集群身份密钥之前,需对所述其他节点进行验证,而所述其他节点在接收到所述任一节点共享的集群身份密钥之后,同样也需要对所述任一节点进行验证,从而保证共享集群身份密钥的安全性。

[64] 如图 2 所示,假定链下隐私计算集群中包括节点 20、节点 21、节点 22 等若干链下隐私计算节点,需要在这些节点之间建立统一的集群身份。首先,每个链下隐私计算节点分别创建链下 TEE,并分别在各自的链下 TEE 内创建节点身份,比如节点 20 创建了 TEE1,并在 TEE1 内创建了代表自身节点身份的密钥对 Key-0,节点 21 创建了 TEE2,并在 TEE1 内创建了代表自身节点身份的密钥对 Key-1,节点 22 创建了 TEE3,并在 TEE1 内创建了代表自身节点身份的密钥对 Key-2 等。各个链下隐私计算节点加入集群的时机往往不同,因而创建链下 TEE 和节点身份的时机也不同。通常,节点需要向链下隐私集群的控制节点发起申请,而控制节点会向发出申请的节点发起挑战,以验证该节点的硬件环境、链下 TEE 内运行的软件等,并在验证通过后将该节点加入链下隐私计算集群,使得该节点成为链下隐私计算节点。

[65] 在需要生成集群身份时,控制节点可以将某一链下隐私计算节点选取为主节点、其他的链下隐私计算节点为从节点,由主节点生成代表集群身份的密钥对,并进而将该密钥对分享至各个从节点,最终使得所有链下隐私计算节点都维护了统一的、代表集群身份的密钥对。如图 2 所示,假定节点 20 被选取为主节点、节点 21-22 等为从节点。首先,节点 20 在 TEE1 内生成代表集群身份的密钥对,即集群身份密钥对 C-Key。然后,节点 20 分别向各个从节点发起挑战,使得节点 21、节点 22 等从节点分别生成远程证明报告,该过程可以参考前文所述,此处不再赘述。在远程证明报告内可以包含 MREnclave、MRSigner、节点身份信息的哈希值等信息。节点 20 分别接收各个从节点返回的远程证明报告和节点身份信息,并通过如前文所述的方式进行验证,以确定各个从节点是否可信。

[66] 以节点 21 为例,假定节点 20 通过远程证明的方式确定该节点 21 可信。在上述代表节点 20 身份的密钥对 Key-0 中,譬如包含一组签名密钥对 Key-0-S 和一组加密密钥对 Key-0-T,节点 20 可以采用签名密钥对 Key-0-S 中的签名私钥对上述的集群身份密钥对 C-Key 进行签名。同时,在节点 21 向节点 20 提供的节点身份信息中,包含代表节点 21 身份的密钥对 Key-1 中的公钥,比如签名密钥对 Key-1-S 中的签名公钥、加密密钥对 Key-1-T 中的加密公钥。因此,节点 20 可以采用加密密钥对 Key-1-T 中的加密公钥,对

上述的集群身份密钥对 C-Key 及其签名数据进行加密, 得到加密后密钥对, 并发送至节点 21。

[67] 节点 20 也基于前文所述的方式, 触发获得针对自身创建的 TEE1 而生成的远程证明报告, 而节点 20 除了向节点 21 发送上述的加密后密钥对之外, 还将该远程证明报告以及节点 20 自身的节点身份信息发送至节点 21, 以供节点 21 对该节点 20 进行验证。而节点 21 在验证确定节点 20 可信的情况下, 通过自身维护的加密密钥对 Key-1-T 中的加密私钥对收到的加密后密钥对进行解密, 得到集群身份密钥对 C-Key 及其签名数据; 以及, 节点 21 从节点 20 的节点身份信息中提取出签名密钥对 Key-0-S 中的签名公钥, 并针对上述解密得到的签名数据进行验证, 如果签名验证成功, 则节点 21 认定解密得到的集群身份密钥对 C-Key 有效, 确定该密钥对 C-Key 可以代表链下隐私计算集群的集群身份。类似地, 通过上述方式, 主节点可以将集群身份密钥对 C-Key 共享至各个从节点, 最终使得链下隐私计算集群中的所有链下隐私计算节点均获得该集群身份密钥对 C-Key。

[68] 无论是针对单节点形式的链下隐私计算节点, 还是链下隐私计算集群的形式, 链下合约的部署方均可在链下隐私计算节点中部署链下合约, 以供后续调用执行计算任务。

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

[70] 以如图 3 所示的场景为例。一种情况下, 客户端 31 可以通过链下渠道直接向链下隐私计算节点 32 发起挑战, 即客户端 31 向链下隐私计算节点 32 发起链下挑战。另一种情况下, 客户端 31 可以通过区块链网络 33 向链下隐私计算节点 32 发起挑战, 即客户端 31 向链下隐私计算节点 33 发起链上挑战。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智能合约 (简称预言机合约), 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链下隐私计算节点 32。

[71] 客户端 31 通过链上渠道向链下隐私计算节点 32 发起挑战时, 涉及到区块链网络 33 与链下隐私计算节点 32 之间的数据交互, 即链上、链下的数据交互, 该数据交互过程可以由预言机合约与预言机服务器 34 通过上述的步骤②配合实现, 该预言机合约与预言机服务器 34 之间的配合机制即为预言机机制。其中, 客户端 31 向节点 33n 提交的交易应当直接或间接调用上述的预言机合约, 以触发预言机机制。其中, 如果将预言机合约的合约地址填入该交易的 to 字段, 表明该交易直接调用了预言机合约; 如果将某一链上合约的合约地址填入该交易的 to 字段, 且该链上合约调用了预言机合约, 表明该交易间接调用了预言机合约。链上合约调用预言机合约, 一种情况下可以是在链上合约的字节码中预先写入了预言机合约的合约地址, 另一种情况下可以是将预言机合约的合约地址作为调用该链上合约时的入参, 并将该入参填入上述交易的数据字段。除了将挑战信息或其他数据从链上传递至链下, 预言机机制还可以将数据从链下传递至链上, 具体可由预言机服务器 34 将链下数据传递至预言机合约, 然后由预言机合约将链下数据传递至数据需求方, 比如这里的链下数据可以包括远程证明报告或者调用链下合约所产生

的隐私计算结果等。在上述的预言机机制中，将数据从链上传递至链下可以视为“请求”过程，将数据从链下传递至链上可以视为“响应”过程，这两个过程通常成对出现。

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

[73] 客户端向链下隐私计算节点发起挑战的过程中，或者链下隐私计算节点向客户端反馈远程证明报告的过程中，涉及到设备之间的数据交互。以图 3 所示的场景为例，所涉及的数据交互可以包括：客户端 31 与链下隐私计算节点 32 之间的数据交互（客户端 31 向链下隐私计算节点 32 发起链下挑战，链下隐私计算节点 32 向客户端 31 返回远程证明报告）、客户端 31 与节点 33n 之间的数据交互（客户端 31 向节点 33n 发送挑战交易、节点 33n 向客户端 31 返回远程证明报告）、节点 33n 与预言机服务器 34 之间的数据交互（预言机服务器 34 从节点 33n 读取挑战信息、预言机服务器 34 向节点 33n 反馈远程证明报告）、预言机服务器 34 与链下隐私计算节点 32 之间的数据交互（预言机服务器 34 向链下隐私计算节点 32 发送挑战信息、链下隐私计算节点 32 向预言机服务器 34 返回远程证明报告）等。在实现上述任一数据交互的过程中，数据发送方与数据接收方之间传输的数据存在泄露的可能性，并且节点 33n 会将挑战交易上链导致该挑战交易被公开，因此可以通过对数据进行加密传输的方式，避免造成信息泄露。

[74] 以客户端 31 向节点 33n 提交挑战交易为例。通过挑战交易向链下隐私计算节点 32 发起链上挑战，使得节点 33n 可以将客户端 31 提交的挑战交易与其他节点进行共识后上链，对客户端 31 的挑战行为进行存证。但是，如果客户端 31 并不希望自己的挑战行为被其他用户随意获知，可以对挑战交易进行隐私保护。客户端 31 可以对挑战交易进行加密，而节点 33n 可以接收经过加密的挑战交易，这样可以确保传输过程中不会造成挑战交易的内容泄露。节点 33n 处可以部署链上 TEE，并且节点 33n 可以将经过加密的挑战交易读入该链上 TEE 后，在链上 TEE 内解密，可以确保解密得到的挑战交易仅存在于链上 TEE 内、不会外泄。节点 33n 直接将经过加密的挑战交易上链，并且通过对加密数据的查看权限进行管理，可以限制能够查看挑战交易的用户，而其他用户直接查看区块链数据时仅能够获得加密后的挑战交易。实际上，节点 33n 可以确保需要隐私保护的数据仅在链上 TEE 内能够被解密为明文形式，一旦离开链上 TEE 均采用密文形式。

[75] 针对挑战交易的加密传输，可以采用对称加密或非对称加密的形式。当采用对称加密时，客户端 31 和节点 33n 分别维护有相同的对称密钥，比如该对称密钥可由客户端 31 与节点 33n 通过诸如 DH(Diffie-Hellman) 或 ECDH(Elliptic Curve Diffie-Hellman) 等算法协商得到，或者由 KMS(Key Management Service, 密钥管理服务) 服务器分发至客户端 31 和节点 33n，本说明书并不限制密钥来源。当密钥由 KMS 服务器分发时，KMS 服务器可以通过远程证明的方式确定节点 33n 处的链上 TEE 可信，然后将密钥加密传输至该链上 TEE 内，远程证明的方式与客户端 31 对链下隐私计算节点 32 的远程证明过程类似，此处暂不赘述。那么，客户端 31 可以通过上述的对称密钥对挑战交易

进行加密, 而节点 33n 将对称密钥维护于链上 TEE 中, 因而将经过加密的挑战交易读入链上 TEE 内, 并通过该对称密钥执行解密操作得到上述的挑战交易。对称加密采用的加密算法, 例如可以包括 DES 算法, 3DES 算法, TDEA 算法, Blowfish 算法, RC5 算法, IDEA 算法等。

[76] 当采用非对称加密时, 节点 33n 维护有非对称密钥的私钥, 比如称之为节点私钥, 而客户端 31 可以获得该节点私钥对应的节点公钥。非对称密钥可由节点 33n 在链上 TEE 内生成, 或者由 KMS 服务器分发至该节点 33n, 本说明书并不限制密钥来源。类似地, 当密钥由 KMS 服务器分发时, KMS 服务器可以通过远程证明的方式确定节点 33n 处的链上 TEE 可信, 然后将密钥加密传输至该链上 TEE 内。那么, 客户端 31 可以通过节点公钥对挑战交易进行加密, 而节点 33n 将节点私钥维护于链上 TEE 中, 因而将经过加密的挑战交易读入链上 TEE 内, 并通过节点私钥执行解密操作得到上述的挑战交易。非对称加密采用的非对称加密算法, 例如可以包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC (椭圆曲线加密算法) 等。

[77] 针对挑战交易的加密传输, 还可以采用对称加密与非对称加密相结合的形式。客户端 31 可以维护一对称密钥, 比如该对称密钥可由客户端 31 随机生成, 且客户端 31 可以获得上述非对称密钥中的公钥。客户端 31 可以通过对称密钥对挑战交易进行加密, 得到加密后挑战交易, 并通过非对称密钥加密该对称密钥、得到加密后密钥, 然后客户端 31 同时将加密后挑战交易与加密后密钥传输至节点 33n。相应的, 节点 33n 将加密后挑战交易与加密后密钥读入链上 TEE 内, 首先通过节点私钥对加密后密钥进行解密, 得到对称密钥, 然后通过对称密钥对加密后挑战交易进行解密。相比较而言, 对称加密的加解密效率相对更高、但安全性相对较低, 而非对称加密的加解密效率相对较低、但安全性相对更高, 因此基于对称加密与非对称加密相结合的形式, 可以兼顾加解密效率与安全性。

[78] 类似地, 在其他数据交互的过程中, 通过使得数据发送方与数据接收方之间维护相同的对称密钥, 或者使得数据发送方维护有非对称密钥的公钥、数据接收方维护有非对称密钥的私钥, 或者结合对称加密与非对称加密的形式, 可以实现任意的数据发送方与数据接收方之间的数据加密传输, 此处不再赘述。

[79] 链下隐私计算节点可能属于链下隐私计算集群, 该链下隐私计算集群包含多个链下隐私计算节点。如果各个链下隐私计算节点之间完全独立, 那么客户端与单个链下隐私计算节点之间的交互过程可以参考上文所述的实施例。而另一种方式下, 链下隐私计算集群可以包含一控制节点, 并由该控制节点对集群内的所有链下隐私计算节点进行统一管理。比如, 客户端可以向控制节点发起挑战, 并接收控制节点返回的上述链下隐私计算节点的远程证明报告。与前述实施例相类似的, 客户端可以向控制节点发起链下挑战, 或者客户端可以向区块链节点提交挑战交易, 该挑战交易所含的挑战信息由区块链节点通过预言机机制传输至控制节点, 使得控制节点向客户端返回链下隐私计算节点的远程证明报告。

[80] 以如图 4 所示的场景为例。一种情况下, 客户端 41 可以通过链下渠道直接向控制节点 42 发起挑战, 即客户端 41 向控制节点 42 发起链下挑战。另一种情况下, 客户端 41 可以通过区块链网络 43 向控制节点 42 发起挑战, 即客户端 41 向控制节点 42 发起链上挑战。链上挑战的发起过程可以包括三个步骤: 步骤①, 客户端 41 向区块链网络 43 提交一笔用于发起挑战的交易, 比如称之为挑战交易, 该挑战交易可由区块链网络 43 内的某一节点 43n 接收和执行; 步骤②, 节点 43n 调用预先部署的预言机智能合约 (简称预言机合约), 该预言机合约可以将上述挑战交易所含的挑战信息传递至链下的预言机服务器 44, 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 44 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 44 将挑战信息通过链下渠道发送至控制节点 42。

[81] 客户端 41 向控制节点 42 发起挑战时, 可以将挑战目标设定为控制节点 42 所处集群内的某一链下隐私计算节点, 比如链下隐私计算节点 42n, 那么控制节点 42 会根据收到的挑战, 向客户端 41 返回链下隐私计算节点 42n 对应的远程证明报告。客户端 41 也可以不设定挑战目标, 那么控制节点 42 收到挑战后, 从链下隐私计算集群中进行选择, 比如在选取了链下隐私计算节点 42n 的情况下, 向客户端 41 返回该链下隐私计算节点 42n 对应的远程证明报告。

[82] 其中, 控制节点 42 在收到客户端 41 发起的挑战后, 可以将该挑战转发至链下隐私计算节点 42n, 使得链下隐私计算节点 42n 临时触发远程证明过程, 以产生相应的远程证明报告, 然后通过控制节点 42 反馈至客户端 41。或者, 控制节点 42 在收到客户端 41 发起的挑战后, 可以将该挑战转发至链下隐私计算节点 42n, 而如果链下隐私计算节点 42n 上已经存在预先生成的远程证明报告, 那么链下隐私计算节点 42n 将该远程证明报告返回控制节点 42, 由控制节点 42 提供至客户端 41, 而无需临时触发远程证明过程。或者, 控制节点 42 在收到客户端 41 发起的挑战后, 如果本地已经存在预先生成的对应于链下隐私计算节点 42n 的远程证明报告, 那么链下隐私计算节点 42n 将该远程证明报告提供至客户端 41, 而无需向链下隐私计算节点 42n 转发挑战, 也无需链下隐私计算节点 42n 因此临时触发远程证明过程。其中, 链下隐私计算节点 42n 本地存在的远程证明报告, 可以是该链下隐私计算节点 42n 响应于除客户端 41 之外的其他挑战者的挑战而触发产生, 比如该其他挑战者可以包括其他客户端、控制节点 42、KMS 服务器等, 本说明书并不对此进行限制。而链下隐私计算节点 42n 通过控制节点 42 将远程证明报告提供至上述的其他挑战者时, 控制节点 42 可以对收到的远程证明报告进行缓存。因此, 控制节点 42 在收到客户端 41 发起的挑战后, 可以首先查看查看本地是否存在先前获得的远程证明报告, 如果存在则将该远程证明报告反馈至客户端 41, 否则将挑战转发至链下隐私计算节点 42n; 以及, 链下隐私计算节点 42n 在收到挑战后, 可以首先查看查看本地是否存在先前获得的远程证明报告, 如果存在则将该远程证明报告反馈至控制节点 42, 否则临时触发远程证明过程。其中, 远程证明报告可以具有一定的时限性, 比如 40 分钟或其他时长, 超时的远程证明报告可以被客户端 41 认定为失效, 控制节点 42 或链下隐私计算节点 42n 也可以主动清除已失效的远程证明报告以避免反馈至客户端 41。

[83] 在图 4 所示的实施例中, 客户端 41 与控制节点 42 之间、控制节点 42 与链下隐私计算节点 42n 之间、客户端 41 与节点 43n 之间、节点 43n 与预言机服务器 44 之间、预言机服务器 44 与控制节点 42 之间等, 均可能产生数据交互。对于任意的数据交互过程, 均可以采用如前文所述的加密数据传输方案, 包括对称加密、非对称加密或两者结合的形式, 此处不再赘述。

[84] 或者, 针对链下隐私计算集群的情况, 基于各个链下隐私计算节点在各自的链下 TEE 内均维护有集群身份密钥, 可将链下隐私计算集群视为一个整体, 由控制节点在选取响应客户端的节点, 链下隐私计算集群中各节点在与外界设备 (比如区块链节点、客户端等) 进行交互的过程中, 并非采用自身的节点身份密钥, 而是采用集群身份密钥对交互数据进行加密与解密, 或者生成与验证签名。其中, 采用集群身份密钥进行加密与解密, 或者生成与验证签名的方式与上述采用节点身份密钥的过程类似, 在此不再赘述。

[85] 基于上述方案, 部署方通过客户端在确定链下隐私计算节点可信的情况下, 可以向链下隐私计算节点部署链下合约。链下合约与区块链节点所执行的链上合约类似, 均可以为运行于虚拟机中的字节码, 此处不再赘述。通过对链下合约的字节码进行加密传输, 可以避免在传输过程中发生数据泄露或修改等, 确保隐私性和安全性。

[86] 与前述的挑战过程相类似的, 客户端可以通过链下途径将链下合约的字节码加密传输至链下隐私计算节点, 即针对字节码的传输过程与区块链网络无关, 这样可以跳过区块链节点之间的共识过程、减少链上链下的交互操作, 使得字节码的传输效率更高。或者, 客户端可以通过链上途径将链下合约的字节码加密传输至链下隐私计算节点, 比

如客户端生成链下合约部署交易,该链下合约部署交易中包含对字节码进行加密得到的字节码密文,客户端将链下合约部署交易加密后提交至区块链节点,加密后的链下合约部署交易可在区块链节点处创建的链上 TEE 内被解密、得到字节码密文,然后由区块链节点通过预言机机制将该字节码密文传输至链下隐私计算节点。

[87] 以如图 5 所示的场景为例。一种情况下,客户端 51 可以通过链下渠道直接向链下隐私计算节点 52 加密传输字节码,即客户端 51 向链下隐私计算节点 52 链下传输加密后的字节码密文。另一种情况下,客户端 51 可以通过区块链网络 53 向链下隐私计算节点 52 加密传输字节码,即客户端 51 向链下隐私计算节点 52 链上传输加密后的字节码密文。链上加密传输的过程可以包括三个步骤:步骤①,客户端 51 向区块链网络 53 提交一笔用于部署链下合约的交易,即链下合约部署交易,该链下合约部署交易可由区块链网络 53 内的某一节点 53n 接收和执行;步骤②,节点 53n 调用预言机合约,该预言机合约可以将上述链下合约部署交易所含的字节码传递至链下的预言机服务器 55,比如预言机合约可以产生包含该字节码的事件,而预言机服务器 55 可以通过监听预言机合约产生的事件,从而获取上述的字节码;步骤③,预言机服务器 55 将字节码通过链下渠道发送至链下隐私计算节点 52。

[88] 在链下加密传输的过程中,仅涉及到客户端 51 与链下隐私计算节点 52 之间的数据交互,可以采用如前文所述的对称加密、非对称加密或两者结合的加密传输方案,此处不再赘述。在链上加密传输的过程中,涉及到多个对象之间的数据交互,需要确保字节码始终处于加密状态。例如,在客户端 51 向节点 53n 提交链下合约部署交易时,可以通过如前文所述的对称加密、非对称加密或两者结合的加密传输方案对该链下合约部署交易进行加密传输,使得链下合约部署交易所含的字节码处于加密保护状态。其中,链下合约部署交易所含的字节码可能处于明文状态或密文状态。如果处于密文状态,表明客户端 51 对字节码进行加密后,将字节码密文添加至链下合约部署交易的 data 字段,并且客户端 51 应当确保该字节码密文仅最终环节的链下隐私计算节点 52 能够解密,而其他的节点 53n、预言机服务器 55 等均无法解密,那么节点 53n 在自身创建的链上 TEE 内对链下合约部署交易进行解密后得到字节码密文后,预言机服务器 55 可以直接读取该字节码密文,然后由预言机服务器 55 将该字节码密文传输至链下隐私计算节点 52。如果处于明文状态,表明客户端 51 直接将明文的字节码添加至链下合约部署交易的 data 字段,而该链下合约部署交易可以调用一链上合约,那么节点 53n 在链上 TEE 内对链下合约部署交易进行解密后得到明文的字节码后,可以通过链上 TEE 内部署的虚拟机执行上述链上合约,从而在链上 TEE 内将字节码加密为相应的字节码密文,并确保该字节码密文仅能够由链下隐私计算节点 52 能够解密,然后由预言机服务器 55 读取该字节码密文,并进而将该字节码密文传输至链下隐私计算节点 52。

[89] 针对字节码进行加密时,可以采用对称加密、非对称加密或两者结合的方式,本说明书并不对此进行限制。当采用非对称加密或者对称加密与非对称加密结合的方式时,涉及到一组非对称密钥对,客户端 51 或节点 53n 需要获知该非对称密钥对的公钥,且该非对称密钥对的私钥需要由链下隐私计算节点 52 所维护,使得该链下隐私计算节点 52 可以基于该私钥对收到的字节码密文进行解密。例如,该非对称密钥对可以为前文所述的、链下隐私计算节点 52 在链下 TEE 中产生的加密密钥对;相应地,链下隐私计算节点 52 在收到字节码密文后,将该字节码密文读入链下 TEE 中,并基于加密私钥对该字节码密文进行解密,从而得到明文的字节码。

[90] 链下隐私计算节点 52 在链下 TEE 中解密得到明文的字节码后,可以在链下 TEE 中对字节码进行重新加密后,存储至链下 TEE 之外的存储空间,比如链下隐私计算节点 52 的硬盘中,从而完成对链下合约的部署。此处,链下隐私计算节点 52 通常采用一对称密钥,通过对称加密的方式对字节码进行加密并存储,这样在后续调用该字节码时,相比于采用非对称加密的形式而言,可以更快地完成解密操作。该对称密钥可由链下隐

私计算节点 52 在链下 TEE 中生成, 或者由其他对象通过加密传输的方式分发至链下隐私计算节点 52。例如, 可由 KMS 服务器对链下隐私计算节点 52 发起挑战, 并通过远程证明验证该链下隐私计算节点 52 可信的情况下, 向该链下隐私计算节点 52 分发上述的对称密钥。链下隐私计算节点 52 可以将 KMS 服务器分发的对称密钥作为根密钥, 并将基于该根密钥派生得到的衍生密钥应用于针对字节码的加密存储。再例如, 基于 Intel SGX 技术, 上述对称密钥可以为烧录于链下隐私计算节点 52 的 CPU 内 e-fuses 存储电路中的 RSK(Root Seal Key)密钥, 或者该 RSK 密钥派生得到的衍生密钥(即 Seal Key)。当然, 链下隐私计算节点 52 也可以采用非对称加密或者对称加密与非对称加密结合的方式, 对字节码进行加密存储, 本说明书并不对此进行限制。

[91] 除了在链下隐私计算节点 52 处安全存储链下合约的字节码之外, 客户端 51 还可以向链下隐私计算节点 52 指明用于执行该字节码的执行引擎。例如, 在链下隐私计算节点 52 处创建的链下 TEE 中, 可以部署有若干执行引擎, 比如 EVM、WASM 虚拟机等中的一个或多个, 尤其是在同时部署了多种执行引擎的情况下, 客户端 51 可以向链下隐私计算节点 52 发送与上述字节码相关联的执行引擎指定信息, 该执行引擎指定信息向链下隐私计算节点 52 指示用于执行上述字节码的执行引擎, 比如采用 EVM 还是 WSAM 虚拟机等。例如, 可以将字节码与执行引擎指定信息打包加密后, 一并传输至链下隐私计算节点 52; 也可以分别对字节码和执行引擎指定信息进行加密传输, 此时执行引擎指定信息应当包含相应的字节码或者链下合约的信息, 比如字节码的哈希值等, 以便于据此确定执行引擎指定信息对应于哪个链下合约。相应的, 链下隐私计算节点 52 在部署链下合约时, 除了对字节码进行加密存储之外, 还需标注出字节码所需采用的执行引擎的信息, 从而在后续的调用过程中据此选用恰当的虚拟机, 以作为处理相应字节码的执行引擎。

[92] 通过上述方式, 客户端 51 可以向链下隐私计算节点 52 部署更多的链下合约; 类似地, 其他客户端也可以向链下隐私计算节点 52 部署链下合约。为了便于管理, 以及便于后续对链下合约进行调用, 链下隐私计算节点 52 可以为部署的链下合约生成相应的合约 ID, 链下合约与合约 ID 之间一一对应。例如, 在完成针对链下合约的部署操作后, 链下隐私计算节点 52 可以对该链下合约的字节码进行哈希运算, 得到第一哈希值, 并将该第一哈希值作为该链下合约的合约 ID。当然, 链下隐私计算节点 52 也可以通过其他方式生成合约 ID, 本说明书并不对此进行限制。

[93] 如果将上述的第一哈希值作为链下合约的合约 ID, 那么该第一哈希值还可以具有其他作用。在完成部署后, 链下隐私计算节点 52 可以向客户端 51 反馈部署结果信息, 该部署结果信息包含上述的第一哈希值, 而客户端 51 还可以对自己发出的字节码进行哈希计算得到第二哈希值, 并将第一哈希值与第二哈希值进行比较: 如果两者一致, 表明链下隐私计算节点 52 部署的字节码正确无误, 没有在传输过程中被替换或者发生其他意外, 客户端 51 可以确认链下合约在链下隐私计算节点 52 处部署成功; 而如果两者不一致, 客户端 51 可以认为链下合约部署失败, 或者已部署的链下合约存在风险。客户端 51 可以将成功部署的链下合约标记为可信合约, 将未成功部署的链下合约标记为不可信合约或不维护, 从而在后续过程中仅针对可信合约进行调用。如果客户端 51 将字节码通过链下途径传输至链下隐私计算节点 52, 那么链下隐私计算节点 52 同样通过链下途径将部署结果信息返回至客户端 51; 如果客户端 51 将字节码通过链上途径传输至链下隐私计算节点 52, 那么链下隐私计算节点 52 同样通过链上途径将部署结果信息反馈至客户端 51。

[94] 当链下隐私计算节点属于链下隐私计算集群时, 由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, 那么客户端在部署链上合约的过程中, 首先将字节码加密传输至控制节点, 然后由控制节点转发至集群内的一个或多个链下隐私计算节点, 从而将链上合约的字节码部署至集群内的一个或多个链下隐私计算节点。如果部署至多个链

下隐私计算节点,那么这些链下隐私计算节点可以同时向外提供针对同一链下合约的调用能力,从而实现并行的链下隐私计算,还可以在多个链下隐私计算节点之间实现负载均衡。

[95] 以如图 6 所示的场景为例。一种情况下,客户端 61 可以通过链下渠道直接向控制节点 62 发送字节码密文,即客户端 61 向控制节点 62 链下加密传输字节码,进而由控制节点 62 转发至集群内的一个或多个链下隐私计算节点。另一种情况下,客户端 61 可以通过区块链网络 63 向控制节点 62 加密传输字节码,即客户端 61 向控制节点 62 链上传输加密后的字节码密文。链上加密传输的过程可以包括三个步骤:步骤①,客户端 61 向区块链网络 63 提交一笔用于部署链下合约的交易,即链下合约部署交易,该链下合约部署交易可由区块链网络 63 内的某一节点 63n 接收和执行;步骤②,节点 63n 调用预言机合约,该预言机合约可以将上述链下合约部署交易所含的字节码传递至链下的预言机服务器 64,比如预言机合约可以产生包含该字节码的事件,而预言机服务器 64 可以通过监听预言机合约产生的事件,从而获取上述的字节码;步骤③,预言机服务器 64 将字节码通过链下渠道发送至控制节点 62,并进而由控制节点 62 转发至集群内的一个或多个链下隐私计算节点。

[96] 如果仅需部署至一个链下隐私计算节点,比如图 6 所示的链下隐私计算节点 62n,那么与图 5 所示实施例相类似的,客户端 61 或节点 63n 在针对字节码进行加密时,只需要确保该链下隐私计算节点 62n 能够解密即可。例如,可以采用该链下隐私计算节点 62n 在链下 TEE 内生成的加密公钥对字节码进行加密,而链下隐私计算节点 62n 在收到字节码密文后,可以在链下 TEE 内通过加密私钥对该字节码密文进行解密,从而获得明文的字节码。同时,客户端 61 可以携带部署目标指示信息,控制节点 62 可以根据该部署目标指示信息确定相应的部署目标为链下隐私计算节点 62n,从而将字节码密文准确转发至该链下隐私计算节点 62n,而无需转发至集群内其他的链下隐私计算节点。如果客户端 61 并未携带部署目标指示信息,控制节点 62 可以将字节码密文转发至集群内的所有链下隐私计算节点,但只有链下隐私计算节点 62n 能够成功解密并完成部署。

[97] 如果需要部署至集群内的多个链下隐私计算节点,除了独立部署的方式之外,本说明书中还可以将链下合约同时向多个链下隐私计算节点进行安全部署。如前所述,每个链下隐私计算节点都存在各自的节点身份信息,且节点身份信息涉及到每个链下隐私计算节点在各自的链下 TEE 内创建的密钥对,比如加密密钥对和签名密钥对,或者兼顾加密与签名功能的密钥对。下面以加密密钥对和签名密钥对为例进行说明。基于各个链下隐私计算节点在各自的链下 TEE 内均维护有集群身份密钥,可将链下隐私计算集群视为一个整体,利用上述在各个节点共享的集群身份密钥将链下合约同时向多个链下隐私计算节点进行安全部署,从而确保多个链下隐私计算节点都能够顺利解密收到的字节码密文。其中,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,经上述共享集群身份密钥的过程,各个链下隐私计算节点在各自的链下 TEE 内均维护有集群加密私钥、集群签名私钥,那么客户端 61 或节点 63n 只要使用集群加密公钥对字节码进行加密,即可确保上述的各个链下隐私计算节点均能够在各自的链下 TEE 内通过集群加密私钥进行解密,从而获得字节码并完成部署。当然,即便仅部署至单个链下隐私计算节点,也可以采用上述的集群加密公钥对字节码进行加密,只要相应的链下隐私计算节点能够顺利解密即可。实际上,基于集群身份,客户端 61 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。

[98] 以图 1 实施例中的所述任一节点为例,部署方在向所述任一节点部署目标链下合约之前,可向所述任一节点发起挑战,那么所述任一节点可响应于部署方发起的挑战,向部署方提供自身的远程证明报告,即第二远程证明报告。其中,部署方可在根据第二远程证明报告确定所述任一节点创建的链下可信执行环境可信的情况下发送加密后的

目标链下合约。比如,可采用集群身份密钥中的集群身份公钥对目标链下合约的字节码进行加密,再将加密后的字节码发送至所述任一节点。所述任一节点在接收到被加密的目标链下合约后,在所述任一节点的链下可信执行环境内通过集群身份密钥中的集群身份私钥解密目标链下合约并进行部署。而在完成对目标链下合约的部署之后,在区块链节点通过预言机机制对所述目标链下合约发起调用的情况下,所述任一节点可在所述任一节点的链下可信执行环境内执行目标链下合约,并通过预言机机制将执行结果反馈至区块链节点。

[99] 此外,在前文所述的挑战过程中,如果需要将挑战发送至链下隐私计算节点,而非由控制节点直接反馈远程证明报告,那么也可以采用集群加密公钥对挑战信息进行加密,只要相应的链下隐私计算节点能够顺利解密即可。但是,如果希望控制节点直接反馈远程证明报告(预先获得的远程证明报告,或者由控制节点向链下隐私计算节点发起挑战而得到),则应当采用控制节点的身份公钥对挑战信息进行加密,确保控制节点能够在自身创建的 TEE 内通过身份私钥实现解密。

[100] 在如图 6 所示的实施例中,客户端 61 可以发送执行引擎指定信息,使得部署了链下合约的链下隐私计算节点可以据此获知用于执行上述字节码的执行引擎,此处不再赘述,可以参考图 5 所示的实施例。另外,客户端 61 可以收到部署结果信息,该部署结果信息包含链下合约的哈希值,比如第一哈希值,使得客户端 61 可以将该第一哈希值与自己发出的字节码对应的第二哈希值进行比较,从而确定链下隐私计算节点是否成功部署了上述的链上合约,此处不再赘述,可以参考图 5 所示的实施例。如果链上合约被部署至多个链下隐私计算节点,控制节点 62 只需要确保所有链下隐私计算节点反馈的部署结果信息都一致,并将任意一个链下隐私计算节点反馈的部署结果信息传输至客户端 61 即可。

[101] 基于上述实施例,本说明书可以基于远程证明的方式对链下隐私计算节点的硬件安全性、链下 TEE 的软件正确性等方面进行有效验证,从而在验证链下隐私计算节点可信的情况下,将链下合约通过加密传输的方式安全部署至链下隐私计算节点,并且该链下合约仅在链下隐私计算节点创建的链下 TEE 内执行,具有极高的安全性,可以承担区块链节点分配的链下隐私计算任务,并确保该链下隐私技术任务安全、可靠、高效地执行。同时,由于计算任务在链下隐私计算节点上执行时,并不涉及到节点之间的共识机制,因而只需要在单个链下隐私计算节点上执行该计算任务即可,相比于受共识机制的限制而使得所有区块链节点都需要执行的链上合约而言,能够极大地节省执行计算任务所带来的资源消耗。

[102] 在本说明书的技术方案中,除了链下隐私计算节点可以存在统一的集群身份之外,可以为链下隐私计算节点上部署的链下合约生成合约身份。当集群内存在多个链下隐私计算节点时,每个链下隐私计算节点可以为自身已部署的链下合约建立合约身份,且不同链下隐私计算节点针对同一链下合约生成的合约身份相同。因此,该相同的合约身份可理解为链下隐私计算集群中多个节点的共享合约身份。其中,合约身份可由合约身份密钥所定义,下面对生成共享合约密钥的过程进行说明。

[103] 请参见图 7,图 7 是一示例性实施例提供的一种生成共享合约密钥的方法的流程图。如图 7 所示,该方法可以包括步骤 702~步骤 704。

[104] 步骤 702,链下隐私计算集群中的任一节点确定自身已部署的目标链下合约,所述目标链下合约部署在所述链下隐私计算集群中的多个节点处;其中,响应于区块链节点的调用,所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行。

[105] 步骤 704,所述任一节点通过所述多个节点之间共用的密钥生成算法,在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算,生成对应于所述目标链下合约的共享合约身份密钥,所述共享合约

身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

[106] 以上述在各个节点处部署目标链下合约为例，当在链下隐私计算集群中的任一节点中部署目标链下合约时，该任一节点可针对目标链下合约生成共享合约身份密钥。作为一示例性实施例，该任一节点在创建的链下可信执行环境内采用链下隐私计算集群内各节点之间共用的密钥生成算法，基于链下隐私计算集群内各节点的共用因子和目标链下合约的全局标识信息（隐私计算集群中各节点部署的链下合约相同，且各节点部署的同一链下合约的全局标识信息相同），生成对应于目标链下合约的共享合约身份密钥。其中，目标链下合约在区块链节点通过预言机机制对部署于该任一节点的目标链下合约发起调用的情况下在该任一节点的链下可信执行环境内执行，且执行结果在该任一节点的链下可信执行环境内被采用共享合约身份密钥进行签名，经签名后的执行结果可通过预言机机制反馈至区块链节点。可见，各个链下隐私计算节点通过上述方式来为自身已部署的链下合约生成共享合约身份密钥，可以保证各个节点针对同一链下合约生成的共享合约身份密钥也相同。同时，相比于由任一节点来统一生成共享合约身份密钥再向其他节点共享的方式，共享合约身份密钥由各个节点自身生成的效率更高。需要说明的是，密钥生成算法可根据实际情况灵活选取，比如 bcrypt 算法、scrypt 算法、PBKDF2 等。

[107] 在一种情况下，共用因子可由控制节点生成，并由控制节点在各个节点加入集群时统一下发，那么加入集群的每个节点均可维护该共用因子。在另一种情况下，共用因子包括对应于隐私计算集群的集群身份密钥，该集群身份密钥用于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，对交互数据进行加密解密和/或签名验签。

[108] 举例而言，共享合约身份密钥可以包括合约加密密钥对和合约签名密钥对；其中，合约身份公钥包含合约加密密钥对中的公钥和合约签名密钥对中的公钥，合约身份私钥包含合约加密密钥对中的私钥和合约签名密钥对中的私钥。那么，客户端或区块链节点除了采用集群身份公钥对调用请求进行加密之外，还可以采用合约加密公钥对调用请求内所含的入参数据的信息进行加密。链下隐私计算节点在收到针对某一链下合约的调用请求后，采用该链下合约对应的合约加密私钥对调用请求内加密后的入参数据的信息进行解密，从而确保入参数据的信息只能由被调用的链下合约所获得，而不会被其他链下合约获得。以及，在得到目标链下合约的执行结果后，链下隐私计算节点在通过预言机机制将执行结果反馈至区块链节点之前，在自身的链下可信执行环境内采用目标链下合约的合约身份私钥对执行结果进行签名，那么，签名后的执行结果在采用目标链下合约的合约身份公钥对执行结果进行签名验证且通过签名验证的情况下，被判定由目标链下合约生成。换言之，链下隐私计算节点可以通过被调用的链下合约的合约签名私钥对执行结果进行签名，而客户端或节点可以通过合约签名公钥进行验签，从而确定该执行结果确实是由被调用的链下合约所产生。

[109] 链下隐私计算节点可以选取统一的集群身份密钥和链下合约的合约 ID，并采用密钥衍生算法对集群身份密钥和合约 ID 进行衍生以得到相应的共享合约身份密钥，由于集群身份密钥相同、而不同链下合约的合约 ID 必然不同，因而可以确保：同一链下隐私计算节点上部署的不同链下合约存在不同的合约身份，而不同链下隐私计算节点上部署的同一链下合约存在相同的合约身份。相应地，控制节点在分配收到的调用请求时，只需要关注于集群内的各个链下隐私计算节点的空闲程度，并基于空闲程度进行任务分配，而无需关注其他信息。其中，密钥衍生算法可根据实际情况灵活选取，比如可以采用 PBKDF2 密钥衍生算法，当然本说明书并不对此进行限制。

[110] 基于上述实施例，本说明书可以基于远程证明的方式对链下隐私计算节点的硬件安全性、链下 TEE 的软件正确性等方面进行有效验证，从而在验证链下隐私计算节点可信的情况下，将链下合约通过加密传输的方式安全部署至链下隐私计算节点，并且该链下合约仅在链下隐私计算节点创建的链下 TEE 内执行，具有极高的安全性，可以承

担区块链节点分配的链下隐私计算任务，并确保该链下隐私技术任务安全、可靠、高效地执行。同时，由于计算任务在链下隐私计算节点上执行时，并不涉及到节点之间的共识机制，因而只需要在单个链下隐私计算节点上执行该计算任务即可，相比于受共识机制的限制而使得所有区块链节点都需要执行的链上合约而言，能够极大地节省执行计算任务所带来的资源消耗。

[111] 基于本说明书的链下合约部署方案，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验验证。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。

[112] 用户通过客户端调用目标链下合约之前，可对链下隐私计算节点中部署的目标链下合约发起挑战，以确保链下隐私计算节点中部署的目标链下合约可信，进而按照用户预期执行计算任务。下面结合图 8-9 分别针对单节点形式和集群形式的挑战过程进行说明。

[113] 如图 8 所示，针对单节点的形式，与图 3 所示实施例类似，客户端 81 可向链下隐私计算节点 82 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 81 向区块链网络 83 提交一笔用于向目标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 83 内的某一节点 83n 接收和执行；步骤②，节点 83n 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 84，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 84 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 84 将挑战信息通过链下渠道发送至控制节点 82。

[114] 通过对链下隐私计算节点 82 部署的目标链下合约发起挑战，客户端 81 可获取针对链下隐私计算节点 82 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 82 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 81 向链下隐私计算节点 82 发起挑战，挑战目标为链下隐私计算节点 82 部署的目标链下合约，进而接收链下隐私计算节点 82 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 82 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 81。在另一种情况下，由客户端 81 向链下隐私计算节点 82 发起挑战，挑战目标为链下隐私计算节点 82 创建的链下 TEE，进而接收链下隐私计算节点 82 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 82 发送针对部署于链下隐私计算节点 82 处的目标链下合约的合约信息的获取请求，接收链下隐私计算节点 82 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 82 请求获取目标链下合约的合约信息（即待验证合约信息）。

[115] 其中，客户端 81 可通过链上挑战向挑战目标发起挑战。比如，向区块链节点 83n 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 83n 通过预言机机制传输至链下隐私计算节点 82，所述挑战信息用于向挑战目标发起挑战。或者，客户端 81 直接向链下隐私计算节点 82 中的挑战目标发起链下挑战。

[116] 在本实施例中，客户端 81 根据远程证明报告对链下隐私计算节点 82 的链下 TEE 进行验证的操作可以包括：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，从远程证明报告携带的自荐信息内提取出第一待检验哈希值，第一待检验哈希值为链下 TEE 的预设信息的哈希值，再将预先获得的针对该链下 TEE 的第一标准哈希值与第一待检验哈希值进行比较。其中，将比较结果一致作为确认该链下 TEE 可信的前提条件。需要说明的是，此部分内容可参考前述控制节点验证待加入节点的过程，在此不再赘述。

[117] 如图 8 所示，在一实施例中，链下隐私计算节点 82 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 82 的节点身份公钥和链下隐私计算节点 82 的其他身份信息。那么，客户端 81 可利用第二标准哈希值验证链下隐私计算节点 82 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 82 的节点身份公钥和链下隐私计算节点 82 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 82 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目标链下合约的验证。比如，客户端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 82 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 82 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 82 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 82 实际的节点身份公钥，而隐私计算节点 82 实际的节点身份公钥可用于验证隐私计算节点 82 的签名。其中，链下隐私计算节点 82 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 81。需要说明的是，此部分内容可参考前述控制节点验证待加入节点的过程，在此不再赘述。

[118] 如图 8 所示，在另一实施例中，链下隐私计算节点 82 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 82 的节点身份公钥、链下隐私计算节点 82 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 82 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 82 可向客户端 81 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 82 的节点身份公钥、链下隐私计算节点 82 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 82 的真实节点身份信息。那么，客户端 81 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。当比较结果为一一致时，说明隐私计算节点 82 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校验哈希值进行比较，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 82 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 82 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 81。需要说明的是，此部分内容可参考前述控制节点验证待加入节点的过程，在此不再赘述。

[119] 客户端 81 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 82 处的目标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 82 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 82 在链下 TEE 内生成。比如，链下隐私计算节点 82 可将部署的目标链下合约读入链下 TEE 内并采用自身的节点身份私钥进行签名。

[120] 客户端 81 采用链下隐私计算节点 82 的节点身份公钥对待验证合约信息进行签名验证，以及根据目标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 82 向外公开发布节点身份公钥以由客户端 81 获取。或者，客户端 81 通过上述验证链下隐私计算节点 82 的节点身份信息的方式获取。同时，目标链下合约的合约信息也可处于公开状态，比如目标链下合约的部署方向外公开发布合约信息以由客户端 81 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。

[121] 在签名验证和合约信息验证通过的情况下，客户端 81 可确定客户端 81 在通过区块链节点的预言机机制对目标链下合约发起调用时，该目标链下合约由链下隐私计算节点 82 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 82 的链下 TEE 可信，那么在验证链下隐私计算节点 82 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 82 提供的待验证合约信息确实由链下隐私计算节点 82 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 82 的链下 TEE 内的目标链下合约，即确保链下隐私计算节点 82 中部署的目标链下合约可信，可按照用户预期执行计算任务。

[122] 如图 9 所示，针对链下隐私计算集群的形式，与图 4 所示实施例类似，客户端 91 可向控制节点 92 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 91 向区块链网络 93 提交一笔用于向目标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 93 内的某一节点 93n 接收和执行；步骤②，节点 93n 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 94，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 94 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 94 将挑战信息通过链下渠道发送至控制节点 92。

[123] 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。

[124] 如图 9 所示，用户在通过客户端 91 调用集群中的目标链下合约之前，可通过客户端 91 对集群中部署的目标链下合约发起挑战（在链下隐私计算集群中的每个节点均部署目标链下合约后发起挑战）。控制节点 92 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 92n 响应挑战为例进行说明。控制节点 92 选取节点 92n 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 92n 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 92n 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 92n 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 92n 的链下 TEE。

[125] 如图 9 所示，在一实施例中，节点 92n 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 92n 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 92n 来代表集群，节点 92n 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 91 可利用第二标准哈希值验证节点 92n 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 92n 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目标链下合约的验证。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 92n 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 92n 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 92 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 92 实际维护的对应于集群的集群身份公钥，而隐私计算节点 92 实际维护的集群身份公钥可用于验证隐私计算节点 92 的签名。其中，节点 92n 可通过控制节点 92 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 91。需要说明的是，此部分内容可参考前述控制节点验证待加入节点的过程，在此不再赘述。

[126] 如图 9 所示，在另一实施例中，节点 92n 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 92n 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 92n 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 92n 可向客户端 91 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 92n 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 92n 提供的真实集群身份信息。那么，客户端 91 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。当比较结果为一一致时，说明隐私计算节点 92 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 92 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 92n 可通过控制节点 92 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 91。需要说明的是，此部分内容可参考前述控制节点验证待加入节点的过程，在此不再赘述。

[127] 与上述图 8 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 92n 发送至控制节点 92，再由控制节点 92 转发至客户端 91。控制节点 92 可一并向客户端 91 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 91 根据集群远程证明报告验证通过后再向节点 92n 获取待验证合约信息以向客户端 91 提供待验证合约信息。其中，待验证合约信息为部署在节点 92n 处的目标链下合约的合约信息，并由节点 92n 在节点 92n 的链下 TEE 内采用集群身份私钥（维护在节点 92n 的链下 TEE 内）进行签名。比如，节点 92n 将部署在节点 92n 处的目标链下合约读入链下 TEE 内，并采用集群身份私钥进行签名。

[128] 客户端 91 在根据集群远程证明报告确定链下 TEE 可信（即节点 92n 的链下 TEE，由节点 92n 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，以及根据目标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 91 向外公开发布集群身份公钥以由客户端 91 获取。或者，客户端 91 通过上述验证集群身份信息的方式获取。同时，目标链下合约的合约信息也可处于公开状态，比如目标链下合约的部署方向外公开发布合约信息以由客户端 91 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。

[129] 与上述单节点形式中验证目标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 91 可确定客户端 91 在通过区块链节点的预言机机制对目标链下合约发起调用时，该目标链下合约由节点 92n 在链下 TEE 可信执行环境中执行，即确保节点 92n 中部署的目标链下合约可信，可按照用户预期执行计算任务。

[130] 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。

[131] 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数据字段，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。

[132] 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。

[133] 如图 10 所示，假定客户端 1001 希望对已部署的链下合约进行调用（比如在验证目标链下合约通过之后）。客户端 1001 可以通过链下渠道向控制节点 1002 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 1002 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 1002n，由该节点 1002n 对调用请求进行响应。节点 1002n 在自身创建的链下 TEE 中通过集群身份私钥解密调用请求，获得调用请求中包含的合约 ID、函数名和入参数据的信息。合约 ID 譬如可以为链下合约的字节码的哈希值，使得节点 1002n 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客户端 1001 希望调用的函数；如果链下合约仅包含一个函数，或者客户端 1001 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。入参数据的信息可以为入参数据本身，

或者入参数据的描述信息，比如该描述信息可以为存储地址等，使得节点 1002n 可以据此获取入参数据，尤其是当客户端 1001 本身并非数据拥有者的情况下，可以省去客户端 1001 与数据拥有者之间的交互，还可以降低调用请求的数据量、加快其传输速度。然后，节点 1002n 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。节点 1002n 可以在链下 TEE 中对该调用结果进行加密后，经由控制节点 1002 反馈至客户端 1001。

[134] 客户端 1001 可以通过链上渠道向控制节点 1002 发送调用请求。客户端 1001 可以向区块链网络 1003 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 1001 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 1004 监听到之后，由预言机服务器 1004 获取调用请求并传输至控制节点 1002。然后，控制节点 1002 将调用请求分配至诸如链下隐私计算节点 1002n 进行响应。以及，控制节点 1002 可以通过预言机机制将调用结果反馈至链上，而节点 1003n 可以主动发起一笔交易，将该调用结果上链，或者节点 1003n 可以将调用结果反馈至客户端 1001，由客户端 1001 重新发起一笔交易将该调用结果上链。

[135] 如果入参数据为区块链数据，客户端 1001 可以向区块链网络 1003 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合约 ID、函数名和入参数据的信息，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 1003n 收到加密后的链下合约调用交易后，在节点 1003n 创建的链上 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，以获取被作为入参数据的区块链数据，该区块链数据通常处于加密状态，节点 1003n 可以在链上 TEE 内解密为明文，然后将该明文的区块链数据与链下合约调用交易所含的合约 ID、函数名打包为调用请求，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 1002，由控制节点 1002 将调用请求分配至诸如链下隐私计算节点 1002n 进行响应。以及，控制节点 1002 可以通过预言机机制将调用结果反馈至链上，而节点 1003n 可以将该调用结果上链。

[136] 客户端 1001 或节点 1003n 除了采用集群身份公钥对调用请求进行加密之外，还可以采用合约加密公钥对调用请求内所含的入参数据的信息进行加密。链下隐私计算节点 1002n 在收到针对某一链下合约的调用请求后，采用该链下合约对应的合约加密私钥对调用请求内加密后的入参数据的信息进行解密，从而确保入参数据的信息只能由被调用的链下合约所获得，而不会被其他链下合约获得。以及，在得到调用结果（即执行链下合约得到的执行结果）后，链下隐私计算节点 1002n 可以通过被调用的链下合约的合约签名私钥对调用结果进行签名，而客户端 1001 或节点 1003n 可以通过合约签名公钥进行验签，从而确定该调用结果确实是由被调用的链下合约所产生。

[137] 在图 10 所示实施例，以链下隐私计算集群为例进行描述。实际上，客户端 1001 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。

[138] 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，集群身份密钥和共享合约身份密钥与此类似。

[139] 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。

[140] 在本说明书的技术方案中,还可由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“链下隐私计算集群”称为“隐私计算集群”,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。

[141] 相应地,图 11 是一示例性实施例提供的另一种生成共享合约密钥的方法的流程图。如图 11 所示,该方法可以包括步骤 1102~1104。

[142] 步骤 1102, 隐私计算集群中的任一节点确定自身已部署的目标智能合约,所述目标智能合约部署在所述隐私计算集群中的多个节点处;其中,响应于客户端的调用,所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行。

[143] 步骤 1104, 所述任一节点通过所述多个节点之间共用的密钥生成算法,在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约的全局标识信息进行运算,生成对应于所述目标智能合约的共享合约身份密钥,所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名。

[144] 如前所述,所述共用因子包括对应于所述多个节点的集群身份密钥,在所述客户端与所述多个节点进行交互以部署或调用智能合约的过程中,所述集群身份密钥用于对交互数据进行加密解密和/或签名验签。

[145] 如前所述,所述集群身份密钥在所述任一节点创建的可信执行环境内生成;所述任一节点向所述隐私计算集群中的其他节点共享所述集群身份密钥,包括:所述任一节点获取所述其他节点发送的第一远程证明报告,所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成;所述任一节点在根据所述第一远程证明报告确定所述其他节点的可信执行环境可信的情况下,向所述其他节点发送所述集群身份密钥和第二远程证明报告,在所述第二远程证明报告表明所述任一节点的可信执行环境可信的情况下,所述集群身份密钥被所述其他节点认可,所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成。

[146] 如前所述,所述任一节点根据所述第一远程证明报告确定所述其他节点的可信执行环境可信,包括:根据所述认证服务器的公钥对所述第一远程证明报告进行签名验证;在签名验证通过且所述第一远程证明报告包含的远程认证结果为通过认证的情况下,从所述第一远程证明报告携带的所述第一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其他节点的可信执行环境中预设信息的哈希值;将预先获得的针对所述其他节点的可信执行环境中预设信息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其他节点的可信执行环境可信的前提条件。

[147] 如前所述,在向所述其他节点发送所述集群身份密钥之前,所述任一节点获取所述其他节点提供的第一节点身份信息,并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,所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息;获取所述其他节点提供的第二标准哈希值,所述第二标准哈希值由所述其他节点在所述其他节点的可信执行环境内生成自身的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;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其他节点的节点身份信息中包含的

节点身份公钥；采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名，并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。

[148] 如前所述，所述任一节点向所述其他节点提供第二节点身份信息，所述第二节点身份信息包含所述任一节点的节点身份公钥和所述任一节点的其他身份信息；所述任一节点向所述其他节点提供第三标准哈希值，所述第三标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成自身的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；其中，在对所述第二节点身份信息进行哈希计算得到的第三待校验哈希值与所述第三标准哈希值一致的情况下，所述其他节点采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密，以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名，并在签名验证通过的情况下在所述其他节点的可信执行环境内维护所述集群身份密钥。

[149] 如前所述，所述任一节点获取所述集群身份密钥，包括：所述任一节点向所述隐私计算集群中其他节点提供第二远程证明报告，所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成；所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告，所述集群身份密钥在所述其他节点创建的可信执行环境内生成，所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成；所述任一节点在确定出所述第一远程证明报告表明所述其他节点的可信执行环境可信的情况下认可所述集群身份密钥。

[150] 如前所述，所述任一节点在接收到被采用所述集群身份密钥中的集群身份公钥加密后的所述目标智能合约的情况下，在所述任一节点的可信执行环境内通过所述集群身份密钥中的集群身份私钥解密所述目标智能合约并进行部署。

[151] 如前所述，在接收到加密后的所述目标智能合约之前，所述任一节点响应于所述目标智能合约的部署方发起的挑战，向所述部署方提供第二远程证明报告，所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成，加密后的所述目标智能合约由所述部署方在根据所述第二证明报告确定任一节点的可信执行环境可信的情况下发送。

[152] 如前所述，在所述客户端对部署于所述任一节点的所述目标智能合约发起调用之前，所述任一节点向所述客户端提供所述集群远程证明报告，所述集群远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成；向所述客户端提供部署于所述任一节点处的所述目标智能合约的待验证合约信息，所述待验证合约信息被所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥进行签名，所述集群身份密钥中的集群身份私钥由所述任一节点维护在所述任一节点的可信执行环境内；在所述客户端根据所述集群远程证明报告确定所述任一节点的可信执行环境可信的情况下，由所述客户端采用所述集群身份密钥中的集群身份公钥对所述待验证合约信息进行签名验证，以及根据所述目标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，确定所述目标智能合约由所述任一节点在所述任一节点的可信执行环境内执行。

[153] 如前所述，所述集群远程证明报告携带的所述任一节点针对创建的可信执行环境产生的第二自荐信息内包含第四待检验哈希值，所述第四待检验哈希值为所述任一节点的可信执行环境的预设信息的哈希值，所述第四待检验哈希值用于所述客户端在根据所述认证服务器的公钥对所述集群远程证明报告进行签名验证并签名验证通过，且所述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，与预先获得的针对所述任一节点的可信执行环境中预设信息的第四标准哈希值进行比较，且比较结果一致被作为所

述客户端确认所述任一节点的可信执行环境可信的前提条件。

[154] 如前所述, 所述任一节点向所述客户端提供集群身份信息, 所述集群身份信息中包含集群身份密钥中的集群身份公钥和所述任一节点的节点身份信息中除所述任一节点的节点身份公钥以外的其他身份信息, 所述集群身份信息被所述客户端进行哈希计算以得到第五待校验哈希值; 所述任一节点向所述客户端提供第五标准哈希值, 所述第五标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成所述集群身份信息后对所述集群身份信息进行哈希计算得到; 所述第五标准哈希值用于与所述第五待校验哈希值进行比较, 且所述客户端在比较结果一致的情况下获取所述集群身份信息中包含的所述集群身份公钥。

[155] 如前所述, 所述任一节点接收所述客户端对所述目标智能合约发起的调用交易, 所述调用交易被采用所述集群身份密钥中的集群身份公钥进行加密, 所述调用交易由所述隐私计算集群的控制节点接收, 并根据所述隐私计算集群的负载情况转发至所述任一节点; 所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥对所述调用交易进行解密, 以响应于解密后的调用交易执行所述目标智能合约。

[156] 如前所述, 所述共享合约身份密钥中的合约身份私钥用于对执行所述目标智能合约得到的执行结果进行签名, 所述共享合约身份密钥中的合约身份公钥用于对调用所述目标智能合约时所采用的入参数数据进行加密。

[157] 需要说明的是, 上述生成共享合约密钥的具体过程可参考上述图 7 所示的实施例, 在此不再赘述。

[158] 与上述方法实施例相对应, 本说明书还提供了一种生成共享合约密钥的装置的实施例。

[159] 本说明书的生成共享合约密钥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。

[160] 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, 在逻辑层面上形成生成共享合约密钥的装置。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于各个逻辑单元, 也可以是硬件或逻辑器件。

[161] 在一实施例中, 请参考图 13, 在软件实施方式中, 该生成共享合约密钥的装置可以包括: 合约确定单元 1301, 使链下隐私计算集群中的任一节点确定自身已部署的目标链下合约, 所述目标链下合约部署在所述链下隐私计算集群中的多个节点处; 其中, 响应于区块链节点的调用, 所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行; 合约密钥生成单元 1302, 使所述任一节点通过所述多个节点之间共用的密钥生成算法, 在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算, 生成对应于所述目标链下合约的共享合约身份密钥, 所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

[162] 可选的, 所述共用因子包括对应于所述多个节点的集群身份密钥, 在区块链节点与所述多个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/或签名验签。

[163] 可选的, 所述集群身份密钥在所述任一节点创建的链下可信执行环境内生成; 所述装置还包括: 获取单元 1303, 使所述任一节点获取所述链下隐私计算集群中的其他节

点发送的第一远程证明报告,所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成;发送单元 1304,使所述任一节点在根据所述第一远程证明报告确定所述其他节点的链下可信执行环境可信的情况下,向所述其他节点发送所述集群身份密钥和第二远程证明报告,在所述第二远程证明报告表明所述任一节点的链下可信执行环境可信的情况下,所述集群身份密钥被所述其他节点认可,所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成。

[164]可选的,发送单元 1304 还用于:根据所述认证服务器的公钥对所述第一远程证明报告进行签名验证;在签名验证通过且所述第一远程证明报告包含的远程认证结果为通过认证的情况下,从所述第一远程证明报告携带的所述第一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其他节点的链下可信执行环境中预设信息的哈希值;将预先获得的针对所述其他节点的链下可信执行环境中预设信息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其他节点的链下可信执行环境可信的前提条件。

[165]可选的,发送单元 1304 还用于:获取所述其他节点提供的第一节点身份信息,并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,所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息;获取所述其他节点提供的第二标准哈希值,所述第二标准哈希值由所述其他节点在所述其他节点的链下可信执行环境内生成自身的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;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其他节点的节点身份信息中包含的节点身份公钥;采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名,并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。

[166]可选的,发送单元 1304 还用于:使所述任一节点向所述其他节点提供第二节点身份信息,所述第二节点身份信息包含所述任一节点的节点身份公钥和所述任一节点的其他身份信息;使所述任一节点向所述其他节点提供第三标准哈希值,所述第三标准哈希值由所述任一节点在所述任一节点的链下可信执行环境内生成自身的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;其中,在对所述第二节点身份信息进行哈希计算得到的第三待校验哈希值与所述第三标准哈希值一致的情况下,所述其他节点采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密,以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名,并在签名验证通过的情况下在所述其他节点的链下可信执行环境内维护所述集群身份密钥。

[167]可选的,发送单元 1304 还用于:使所述任一节点向所述链下隐私计算集群中其他节点提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成;使所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的链下可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告,所述集群身份密钥在所述其他节点创建的链下可信执行环境内生成,所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成;使所述任一节点在确定出所述第一远程证明报告表明所述其他节点的链下可信执行环境可信的情况下认可所述集群身份密钥。

[168]可选的,还包括:部署单元 1305,使所述任一节点在接收到被采用所述集群身份密钥中的集群身份公钥加密后的所述目标链下合约的情况下,在所述任一节点的链下可信执行环境内通过所述集群身份密钥中的集群身份私钥解密所述目标链下合约并进行部署。

[169]可选的,在接收到加密后的所述目标链下合约之前,部署单元 1305 还用于:使所

述任一节点响应于所述目标链下合约的部署方发起的挑战,向所述部署方提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成,加密后的所述目标链下合约由所述部署方在根据所述第二证明报告确定任一节点的链下可信执行环境可信的情况下发送。

[170]可选的,加密后的所述目标链下合约由所述目标链下合约的部署方上传至所述链下隐私计算集群的控制节点,并由所述控制节点转发至所述任一节点。

[171]可选的,所述区块链节点基于客户端发起的交易,对所述目标链下合约发起调用;在区块链节点通过预言机机制对部署于所述任一节点的所述目标链下合约发起调用之前,发送单元 1304 还用于:使所述任一节点向所述客户端提供所述集群远程证明报告,所述集群远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成;使所述任一节点向所述客户端提供部署于所述任一节点处的所述目标链下合约的待验证合约信息,所述待验证合约信息被所述任一节点在所述任一节点的链下可信执行环境内采用所述集群身份密钥中的集群身份私钥进行签名,所述集群身份密钥中的集群身份私钥由所述任一节点维护在所述任一节点的链下可信执行环境内;在所述客户端根据所述集群远程证明报告确定所述任一节点的链下可信执行环境可信的情况下,由所述客户端采用所述集群身份密钥中的集群身份公钥对所述待验证合约信息进行签名验证,以及根据所述目标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,确定所述目标链下合约由所述任一节点在所述任一节点的链下可信执行环境内执行。

[172]可选的,所述集群远程证明报告携带的所述任一节点针对创建的链下可信执行环境产生的第二自荐信息内包含第四待检验哈希值,所述第四待检验哈希值为所述任一节点的链下可信执行环境的预设信息的哈希值,所述第四待检验哈希值用于所述客户端在根据所述认证服务器的公钥对所述集群远程证明报告进行签名验证并签名验证通过,且所述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,与预先获得的针对所述任一节点的链下可信执行环境中预设信息的第四标准哈希值进行比较,且比较结果一致被作为所述客户端确认所述任一节点的链下可信执行环境可信的前提条件。

[173]可选的,发送单元 1304 还用于:使所述任一节点向所述客户端提供集群身份信息,所述集群身份信息中包含集群身份密钥中的集群身份公钥和所述任一节点的节点身份信息中除所述任一节点的节点身份公钥以外的其他身份信息,所述集群身份信息被所述客户端进行哈希计算以得到第五待校验哈希值;使所述任一节点向所述客户端提供第五标准哈希值,所述第五标准哈希值由所述任一节点在所述任一节点的链下可信执行环境内生成所述集群身份信息后对所述集群身份信息进行哈希计算得到;所述第五标准哈希值用于与所述第五待校验哈希值进行比较,且所述客户端在比较结果一致的情况下获取所述集群身份信息中包含的所述集群身份公钥。

[174]可选的,所述客户端在所述链下隐私计算集群中的每个节点均部署所述目标链下合约后发起挑战,且所发起的挑战由所述链下隐私计算集群的控制节点接收,以及转发至所述任一节点。

[175]可选的,部署单元 1305 还用于:使所述任一节点接收区块链节点通过预言机机制对所述目标链下合约发起的调用交易,所述调用交易被采用所述集群身份密钥中的集群身份公钥进行加密,所述调用交易由所述链下隐私计算集群的控制节点接收,并根据所述链下隐私计算集群的负载情况转发至所述任一节点;使所述任一节点在所述任一节点的链下可信执行环境内采用所述集群身份密钥中的集群身份私钥对所述调用交易进行解密,以响应于解密后的调用交易执行所述目标链下合约。

[176]可选的,所述共享合约身份密钥中的合约身份私钥用于对执行所述目标链下合约得到的执行结果进行签名,所述共享合约身份密钥中的合约身份公钥用于对调用所述目标链下合约时所采用的入参数据进行加密。

[177] 在另一实施例中，请参考图 14，在软件实施方式中，该生成共享合约密钥的装置可以包括：合约确定单元 1401，使隐私计算集群中的任一节点确定自身已部署的目标智能合约，所述目标智能合约部署在所述隐私计算集群中的多个节点处；其中，响应于客户端的调用，所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行；合约密钥生成单元 1402，使所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约的全局标识信息进行运算，生成对应于所述目标智能合约的共享合约身份密钥，所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名。

[178] 可选的，所述共用因子包括对应于所述多个节点的集群身份密钥，在所述客户端与所述多个节点进行交互以部署或调用智能合约的过程中，所述集群身份密钥用于对交互数据进行加密解密和/或签名验签。

[179] 可选的，所述集群身份密钥在所述任一节点创建的可信执行环境内生成；所述装置还包括：获取单元 1403，使所述任一节点获取所述其他节点发送的第一远程证明报告，所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成；发送单元 1404，使所述任一节点在根据所述第一远程证明报告确定所述其他节点的可信执行环境可信的情况下，向所述其他节点发送所述集群身份密钥和第二远程证明报告，在所述第二远程证明报告表明所述任一节点的可信执行环境可信的情况下，所述集群身份密钥被所述其他节点认可，所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成。

[180] 可选的，发送单元 1404 还用于：根据所述认证服务器的公钥对所述第一远程证明报告进行签名验证；在签名验证通过且所述第一远程证明报告包含的远程认证结果为通过认证的情况下，从所述第一远程证明报告携带的所述第一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其他节点的可信执行环境中预设信息的哈希值；将预先获得的针对所述其他节点的可信执行环境中预设信息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其他节点的可信执行环境可信的前提条件。

[181] 可选的，发送单元 1404 还用于：获取所述其他节点提供的第一节点身份信息，并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，所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息；获取所述其他节点提供的第二标准哈希值，所述第二标准哈希值由所述其他节点在所述其他节点的可信执行环境内生成自身的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；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其他节点的节点身份信息中包含的节点身份公钥；采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名，并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。

[182] 可选的，发送单元 1404 还用于：所述任一节点向所述其他节点提供第二节点身份信息，所述第二节点身份信息包含所述任一节点的节点身份公钥和所述任一节点的其他身份信息；所述任一节点向所述其他节点提供第三标准哈希值，所述第三标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成自身的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；其中，在对所述第二节点身份信息进行哈希计算得到的第三待校验哈希值与所述第三标准哈希值一致的情况下，所述其他节点采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密，以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名，并在签名验证通过的情况下在所述其他节点的可信执行环境内维护所述集群身份密钥。

[183]可选的,发送单元 1404 还用于:所述任一节点向所述隐私计算集群中其他节点提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成;所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告,所述集群身份密钥在所述其他节点创建的可信执行环境内生成,所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成;所述任一节点在确定出所述第一远程证明报告表明所述其他节点的可信执行环境可信的情况下认可所述集群身份密钥。

[184]可选的,还包括:部署单元 1405,所述任一节点在接收到被采用所述集群身份密钥中的集群身份公钥加密后的所述目标智能合约的情况下,在所述任一节点的可信执行环境内通过所述集群身份密钥中的集群身份私钥解密所述目标智能合约并进行部署。

[185]可选的,在接收到加密后的所述目标智能合约之前,部署单元 1405 还用于:使所述任一节点响应于所述目标智能合约的部署方发起的挑战,向所述部署方提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成,加密后的所述目标智能合约由所述部署方在根据所述第二证明报告确定任一节点的可信执行环境可信的情况下发送。

[186]可选的,在所述客户端对部署于所述任一节点的所述目标智能合约发起调用之前,发送单元 1404 还用于:所述任一节点向所述客户端提供所述集群远程证明报告,所述集群远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成;向所述客户端提供部署于所述任一节点处的所述目标智能合约的待验证合约信息,所述待验证合约信息被所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥进行签名,所述集群身份密钥中的集群身份私钥由所述任一节点维护在所述任一节点的可信执行环境内;在所述客户端根据所述集群远程证明报告确定所述任一节点的可信执行环境可信的情况下,由所述客户端采用所述集群身份密钥中的集群身份公钥对所述待验证合约信息进行签名验证,以及根据所述目标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,确定所述目标智能合约由所述任一节点在所述任一节点的可信执行环境内执行。

[187]可选的,所述集群远程证明报告携带的所述任一节点针对创建的可信执行环境产生的第二自荐信息内包含第四待检验哈希值,所述第四待检验哈希值为所述任一节点的可信执行环境的预设信息的哈希值,所述第四待检验哈希值用于所述客户端在根据所述认证服务器的公钥对所述集群远程证明报告进行签名验证并签名验证通过,且所述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,与预先获得的针对所述任一节点的可信执行环境中预设信息的第四标准哈希值进行比较,且比较结果一致被作为所述客户端确认所述任一节点的可信执行环境可信的前提条件。

[188]可选的,发送单元 1404 还用于:所述任一节点向所述客户端提供集群身份信息,所述集群身份信息中包含集群身份密钥中的集群身份公钥和所述任一节点的节点身份信息中除所述任一节点的节点身份公钥以外的其他身份信息,所述集群身份信息被所述客户端进行哈希计算以得到第五待校验哈希值;所述任一节点向所述客户端提供第五标准哈希值,所述第五标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成所述集群身份信息后对所述集群身份信息进行哈希计算得到;所述第五标准哈希值用于与所述第五待校验哈希值进行比较,且所述客户端在比较结果一致的情况下获取所述集群身份信息中包含的所述集群身份公钥。

[189]可选的,部署单元 1405 还用于:所述任一节点接收所述客户端对所述目标智能合约发起的调用交易,所述调用交易被采用所述集群身份密钥中的集群身份公钥进行加密,所述调用交易由所述隐私计算集群的控制节点接收,并根据所述隐私计算集群的负载情

况转发至所述任一节点；所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥对所述调用交易进行解密，以响应于解密后的调用交易执行所述目标智能合约。

[190] 可选的，所述共享合约身份密钥中的合约身份私钥用于对执行所述目标智能合约得到的执行结果进行签名，所述共享合约身份密钥中的合约身份公钥用于对调用所述目标智能合约时所采用的入参数数据进行加密。

[191] 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。

[192] 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。

[193] 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。

[194] 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。

[195] 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。

[196] 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。

[197] 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。

[198] 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。

[199] 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。

[200] 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。

[201] 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。

[202] 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。

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

[204] 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、一种生成共享合约密钥的方法，包括：

链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于区块链节点的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行；

所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

2、根据权利要求1所述的方法，所述共用因子包括对应于所述多个节点的集群身份密钥，在区块链节点与所述多个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/或签名验签。

3、根据权利要求2所述的方法，所述集群身份密钥在所述任一节点创建的链下可信执行环境内生成；所述任一节点向所述链下隐私计算集群中的其他节点共享所述集群身份密钥，包括：

所述任一节点获取所述其他节点发送的第一远程证明报告，所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成；

所述任一节点在根据所述第一远程证明报告确定所述其他节点的链下可信执行环境可信的情况下，向所述其他节点发送所述集群身份密钥和第二远程证明报告，在所述第二远程证明报告表明所述任一节点的链下可信执行环境可信的情况下，所述集群身份密钥被所述其他节点认可，所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成。

4、根据权利要求3所述的方法，所述任一节点根据所述第一远程证明报告确定所述其他节点的链下可信执行环境可信，包括：

根据所述认证服务器的公钥对所述第一远程证明报告进行签名验证；

在签名验证通过且所述第一远程证明报告包含的远程认证结果为通过认证的情况下，从所述第一远程证明报告携带的所述第一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其他节点的链下可信执行环境中预设信息的哈希值；

将预先获得的针对所述其他节点的链下可信执行环境中预设信息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其他节点的链下可信执行环境可信的前提条件。

5、根据权利要求3所述的方法，所述任一节点在向所述其他节点发送所述集群身份密钥之前，还包括：

获取所述其他节点提供的第一节点身份信息，并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，所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息；

获取所述其他节点提供的第二标准哈希值，所述第二标准哈希值由所述其他节点在所述其他节点的链下可信执行环境内生成自身的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；

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其他节点的节点身份信息中包含的节点身份公钥；

采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名，并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。

6、根据权利要求3所述的方法，还包括：

所述任一节点向所述其他节点提供第二节点身份信息，所述第二节点身份信息包含

所述任一节点的节点身份公钥和所述任一节点的其他身份信息;

所述任一节点向所述其他节点提供第三标准哈希值,所述第三标准哈希值由所述任一节点在所述任一节点的链下可信执行环境内生成自身的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;

其中,在对所述第二节点身份信息进行哈希计算得到的第三待校验哈希值与所述第三标准哈希值一致的情况下,所述其他节点采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密,以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名,并在签名验证通过的情况下在所述其他节点的链下可信执行环境内维护所述集群身份密钥。

7、根据权利要求2所述的方法,所述任一节点获取所述集群身份密钥,包括:

所述任一节点向所述链下隐私计算集群中其他节点提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成;

所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的链下可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告,所述集群身份密钥在所述其他节点创建的链下可信执行环境内生成,所述第一远程证明报告由认证服务器对所述其他节点针对创建的链下可信执行环境产生的第一自荐信息进行验证后生成;

所述任一节点在确定出所述第一远程证明报告表明所述其他节点的链下可信执行环境可信的情况下认可所述集群身份密钥。

8、根据权利要求2所述的方法,还包括:

所述任一节点在接收到被采用所述集群身份密钥中的集群身份公钥加密后的所述目标链下合约的情况下,在所述任一节点的链下可信执行环境内通过所述集群身份密钥中的集群身份私钥解密所述目标链下合约并进行部署。

9、根据权利要求8所述的方法,所述任一节点在接收到加密后的所述目标链下合约之前,还包括:

响应于所述目标链下合约的部署方发起的挑战,向所述部署方提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成,加密后的所述目标链下合约由所述部署方在根据所述第二远程证明报告确定任一节点的链下可信执行环境可信的情况下发送。

10、根据权利要求8所述的方法,加密后的所述目标链下合约由所述目标链下合约的部署方上传至所述链下隐私计算集群的控制节点,并由所述控制节点转发至所述任一节点。

11、根据权利要求2所述的方法,所述区块链节点基于客户端发起的交易,对所述目标链下合约发起调用;在区块链节点通过预言机机制对部署于所述任一节点的所述目标链下合约发起调用之前,所述方法还包括:

所述任一节点向所述客户端提供所述集群远程证明报告,所述集群远程证明报告由认证服务器对所述任一节点针对创建的链下可信执行环境产生的第二自荐信息进行验证后生成;

向所述客户端提供部署于所述任一节点处的所述目标链下合约的待验证合约信息,所述待验证合约信息被所述任一节点在所述任一节点的链下可信执行环境内采用所述集群身份密钥中的集群身份私钥进行签名,所述集群身份密钥中的集群身份私钥由所述任一节点维护在所述任一节点的链下可信执行环境内;

在所述客户端根据所述集群远程证明报告确定所述任一节点的链下可信执行环境可信的情况下,由所述客户端采用所述集群身份密钥中的集群身份公钥对所述待验证合约信息进行签名验证,以及根据所述目标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,确定所述目标链下合约由所述任一节点在所述任一节点的链下可信执行环境内执行。

12、根据权利要求 11 所述的方法,所述集群远程证明报告携带的所述任一节点针对创建的链下可信执行环境产生的第二自荐信息内包含第四待检验哈希值,所述第四待检验哈希值为所述任一节点的链下可信执行环境的预设信息的哈希值,所述第四待检验哈希值用于所述客户端在根据所述认证服务器的公钥对所述集群远程证明报告进行签名验证并签名验证通过,且所述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,与预先获得的针对所述任一节点的链下可信执行环境中预设信息的第四标准哈希值进行比较,且比较结果一致被作为所述客户端确认所述任一节点的链下可信执行环境可信的前提条件。

13、根据权利要求 11 所述的方法,还包括:

所述任一节点向所述客户端提供集群身份信息,所述集群身份信息中包含集群身份密钥中的集群身份公钥和所述任一节点的节点身份信息中除所述任一节点的节点身份公钥以外的其他身份信息,所述集群身份信息被所述客户端进行哈希计算以得到第五待校验哈希值;

所述任一节点向所述客户端提供第五标准哈希值,所述第五标准哈希值由所述任一节点在所述任一节点的链下可信执行环境内生成所述集群身份信息后对所述集群身份信息进行哈希计算得到;

所述第五标准哈希值用于与所述第五待校验哈希值进行比较,且所述客户端在比较结果一致的情况下获取所述集群身份信息中包含的所述集群身份公钥。

14、根据权利要求 11 所述的方法,所述客户端在所述链下隐私计算集群中的每个节点均部署所述目标链下合约后发起挑战,且所发起的挑战由所述链下隐私计算集群的控制节点接收,以及转发至所述任一节点。

15、根据权利要求 2 所述的方法,还包括:

所述任一节点接收区块链节点通过预言机机制对所述目标链下合约发起的调用交易,所述调用交易被采用所述集群身份密钥中的集群身份公钥进行加密,所述调用交易由所述链下隐私计算集群的控制节点接收,并根据所述链下隐私计算集群的负载情况转发至所述任一节点;

所述任一节点在所述任一节点的链下可信执行环境内采用所述集群身份密钥中的集群身份私钥对所述调用交易进行解密,以响应于解密后的调用交易执行所述目标链下合约。

16、根据权利要求 1 所述的方法,所述共享合约身份密钥中的合约身份私钥用于对执行所述目标链下合约得到的执行结果进行签名,所述共享合约身份密钥中的合约身份公钥用于对调用所述目标链下合约时所采用的入参数据进行加密。

17、一种生成共享合约密钥的方法,包括:

隐私计算集群中的任一节点确定自身已部署的目标智能合约,所述目标智能合约部署在所述隐私计算集群中的多个节点处;其中,响应于客户端的调用,所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行;

所述任一节点通过所述多个节点之间共用的密钥生成算法,在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约的全局标识信息进行运算,生成对应于所述目标智能合约的共享合约身份密钥,所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名。

18、根据权利要求 17 所述的方法,所述共用因子包括对应于所述多个节点的集群身份密钥,在所述客户端与所述多个节点进行交互以部署或调用智能合约的过程中,所述集群身份密钥用于对交互数据进行加密解密和/或签名验签。

19、根据权利要求 18 所述的方法,所述集群身份密钥在所述任一节点创建的可信

执行环境内生成；所述任一节点向所述隐私计算集群中的其他节点共享所述集群身份密钥，包括：

所述任一节点获取所述其他节点发送的第一远程证明报告，所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成；

所述任一节点在根据所述第一远程证明报告确定所述其他节点的可信执行环境可信的情况下，向所述其他节点发送所述集群身份密钥和第二远程证明报告，在所述第二远程证明报告表明所述任一节点的可信执行环境可信的情况下，所述集群身份密钥被所述其他节点认可，所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成。

20、根据权利要求 19 所述的方法，所述任一节点根据所述第一远程证明报告确定所述其他节点的可信执行环境可信，包括：

根据所述认证服务器的公钥对所述第一远程证明报告进行签名验证；

在签名验证通过且所述第一远程证明报告包含的远程认证结果为通过认证的情况下，从所述第一远程证明报告携带的所述第一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其他节点的可信执行环境中预设信息的哈希值；

将预先获得的针对所述其他节点的可信执行环境中预设信息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其他节点的可信执行环境可信的前提条件。

21、根据权利要求 19 所述的方法，所述任一节点在向所述其他节点发送所述集群身份密钥之前，还包括：

获取所述其他节点提供的第一节点身份信息，并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，所述第一节点身份信息包含所述其他节点的节点身份公钥和所述其他节点的其他身份信息；

获取所述其他节点提供的第二标准哈希值，所述第二标准哈希值由所述其他节点在所述其他节点的可信执行环境内生成自身的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；

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其他节点的节点身份信息中包含的节点身份公钥；

采用所述任一节点的节点身份私钥对所述集群身份密钥进行签名，并采用所述其他节点的节点身份公钥对签名后的集群身份密钥进行加密。

22、根据权利要求 19 所述的方法，还包括：

所述任一节点向所述其他节点提供第二节点身份信息，所述第二节点身份信息包含所述任一节点的节点身份公钥和所述任一节点的其他身份信息；

所述任一节点向所述其他节点提供第三标准哈希值，所述第三标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成自身的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；

其中，在对所述第二节点身份信息进行哈希计算得到的第三待校验哈希值与所述第三标准哈希值一致的情况下，所述其他节点采用所述其他节点的节点身份私钥对接收到的集群身份密钥进行解密，以及采用所述任一节点的节点身份信息中包含的节点身份公钥验证所述集群身份密钥的签名，并在签名验证通过的情况下在所述其他节点的可信执行环境内维护所述集群身份密钥。

23、根据权利要求 18 所述的方法，所述任一节点获取所述集群身份密钥，包括：

所述任一节点向所述隐私计算集群中其他节点提供第二远程证明报告，所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成；

所述任一节点接收所述其他节点在根据所述第二远程证明报告确定所述任一节点的可信执行环境可信的情况下发送的所述集群身份密钥和第一远程证明报告,所述集群身份密钥在所述其他节点创建的可信执行环境内生成,所述第一远程证明报告由认证服务器对所述其他节点针对创建的可信执行环境产生的第一自荐信息进行验证后生成;

所述任一节点在确定出所述第一远程证明报告表明所述其他节点的可信执行环境可信的情况下认可所述集群身份密钥。

24、根据权利要求 18 所述的方法,还包括:

所述任一节点在接收到被采用所述集群身份密钥中的集群身份公钥加密后的所述目标智能合约的情况下,在所述任一节点的可信执行环境内通过所述集群身份密钥中的集群身份私钥解密所述目标智能合约并进行部署。

25、根据权利要求 24 所述的方法,所述任一节点在接收到加密后的所述目标智能合约之前,还包括:

响应于所述目标智能合约的部署方发起的挑战,向所述部署方提供第二远程证明报告,所述第二远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成,加密后的所述目标智能合约由所述部署方在根据所述第二远程证明报告确定任一节点的可信执行环境可信的情况下发送。

26、根据权利要求 18 所述的方法,在所述客户端对部署于所述任一节点的所述目标智能合约发起调用之前,所述方法还包括:

所述任一节点向所述客户端提供所述集群远程证明报告,所述集群远程证明报告由认证服务器对所述任一节点针对创建的可信执行环境产生的第二自荐信息进行验证后生成;

向所述客户端提供部署于所述任一节点处的所述目标智能合约的待验证合约信息,所述待验证合约信息被所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥进行签名,所述集群身份密钥中的集群身份私钥由所述任一节点维护在所述任一节点的可信执行环境内;

在所述客户端根据所述集群远程证明报告确定所述任一节点的可信执行环境可信的情况下,由所述客户端采用所述集群身份密钥中的集群身份公钥对所述待验证合约信息进行签名验证,以及根据所述目标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,确定所述目标智能合约由所述任一节点在所述任一节点的可信执行环境内执行。

27、根据权利要求 26 所述的方法,所述集群远程证明报告携带的所述任一节点针对创建的可信执行环境产生的第二自荐信息内包含第四待检验哈希值,所述第四待检验哈希值为所述任一节点的可信执行环境的预设信息的哈希值,所述第四待检验哈希值用于所述客户端在根据所述认证服务器的公钥对所述集群远程证明报告进行签名验证并签名验证通过,且所述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,与预先获得的针对所述任一节点的可信执行环境中预设信息的第四标准哈希值进行比较,且比较结果一致被作为所述客户端确认所述任一节点的可信执行环境可信的前提条件。

28、根据权利要求 26 所述的方法,还包括:

所述任一节点向所述客户端提供集群身份信息,所述集群身份信息中包含集群身份密钥中的集群身份公钥和所述任一节点的节点身份信息中除所述任一节点的节点身份公钥以外的其他身份信息,所述集群身份信息被所述客户端进行哈希计算以得到第五待校验哈希值;

所述任一节点向所述客户端提供第五标准哈希值,所述第五标准哈希值由所述任一节点在所述任一节点的可信执行环境内生成所述集群身份信息后对所述集群身份信息进行哈希计算得到;

所述第五标准哈希值用于与所述第五待校验哈希值进行比较,且所述客户端在比较

结果一致的情况下获取所述集群身份信息中包含的所述集群身份公钥。

29、根据权利要求 18 所述的方法，还包括：

所述任一节点接收所述客户端对所述目标智能合约发起的调用交易，所述调用交易被采用所述集群身份密钥中的集群身份公钥进行加密，所述调用交易由所述隐私计算集群的控制节点接收，并根据所述隐私计算集群的负载情况转发至所述任一节点；

所述任一节点在所述任一节点的可信执行环境内采用所述集群身份密钥中的集群身份私钥对所述调用交易进行解密，以响应于解密后的调用交易执行所述目标智能合约。

30、根据权利要求 17 所述的方法，所述共享合约身份密钥中的合约身份私钥用于对执行所述目标智能合约得到的执行结果进行签名，所述共享合约身份密钥中的合约身份公钥用于对调用所述目标智能合约时所采用的入参数据进行加密。

31、一种生成共享合约密钥的装置，包括：

合约确定单元，使链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于区块链节点的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行；

合约密钥生成单元，使所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名。

32、一种生成共享合约密钥的装置，包括：

合约确定单元，使隐私计算集群中的任一节点确定自身已部署的目标智能合约，所述目标智能合约部署在所述隐私计算集群中的多个节点处；其中，响应于客户端的调用，所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行；

合约密钥生成单元，使所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约的全局标识信息进行运算，生成对应于所述目标智能合约的共享合约身份密钥，所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名。

33、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 1-30 中任一项所述的方法。

34、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 1-30 中任一项所述方法的步骤。

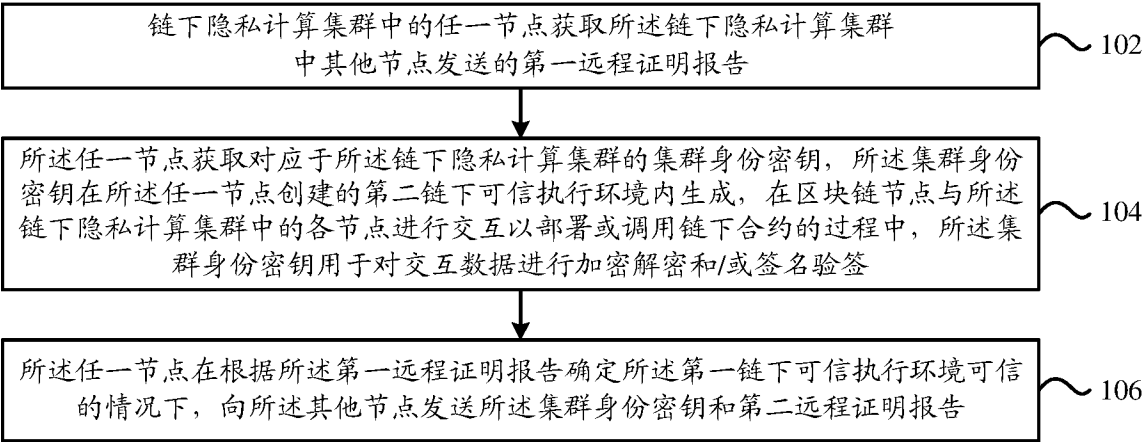


图 1

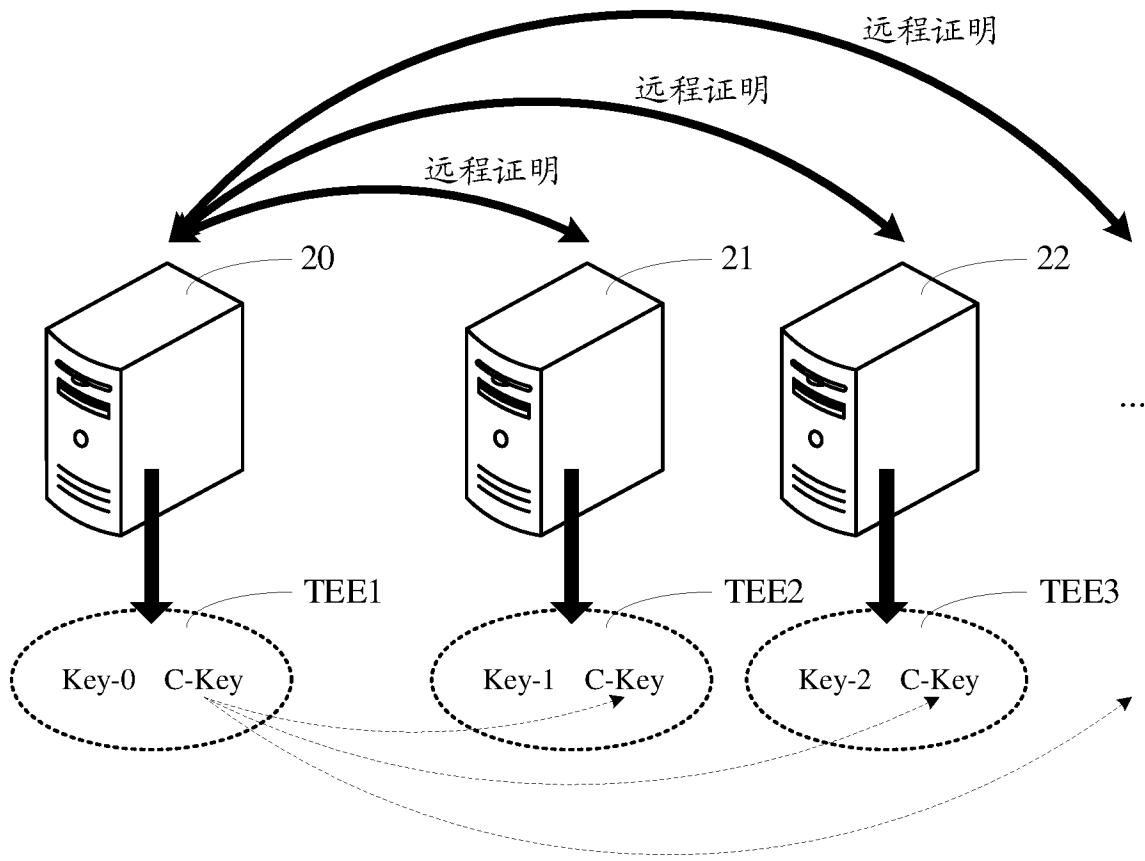


图 2

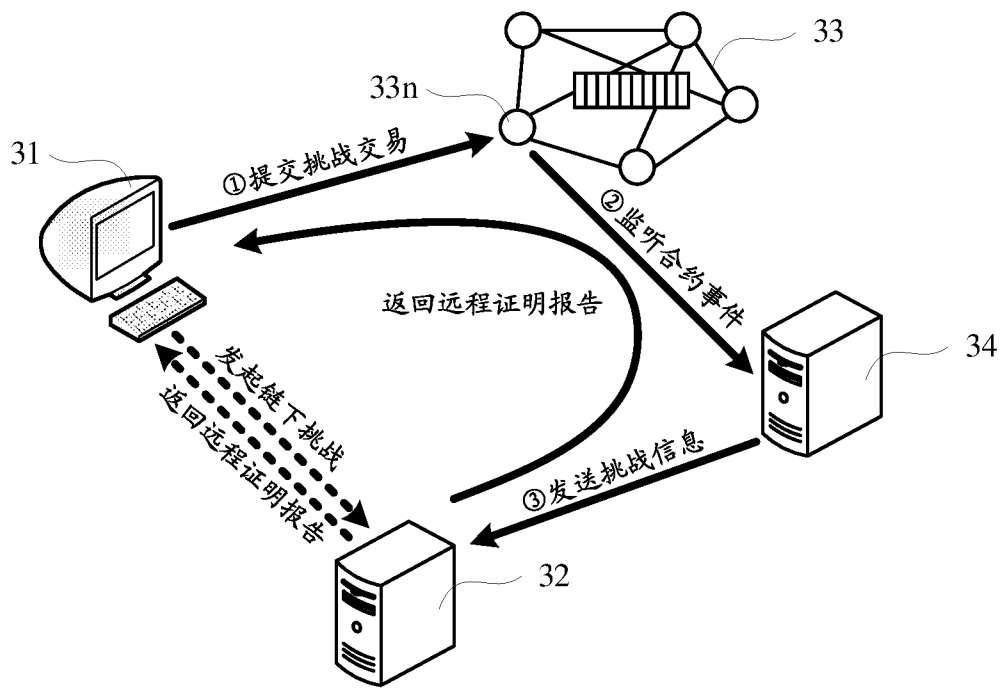


图 3

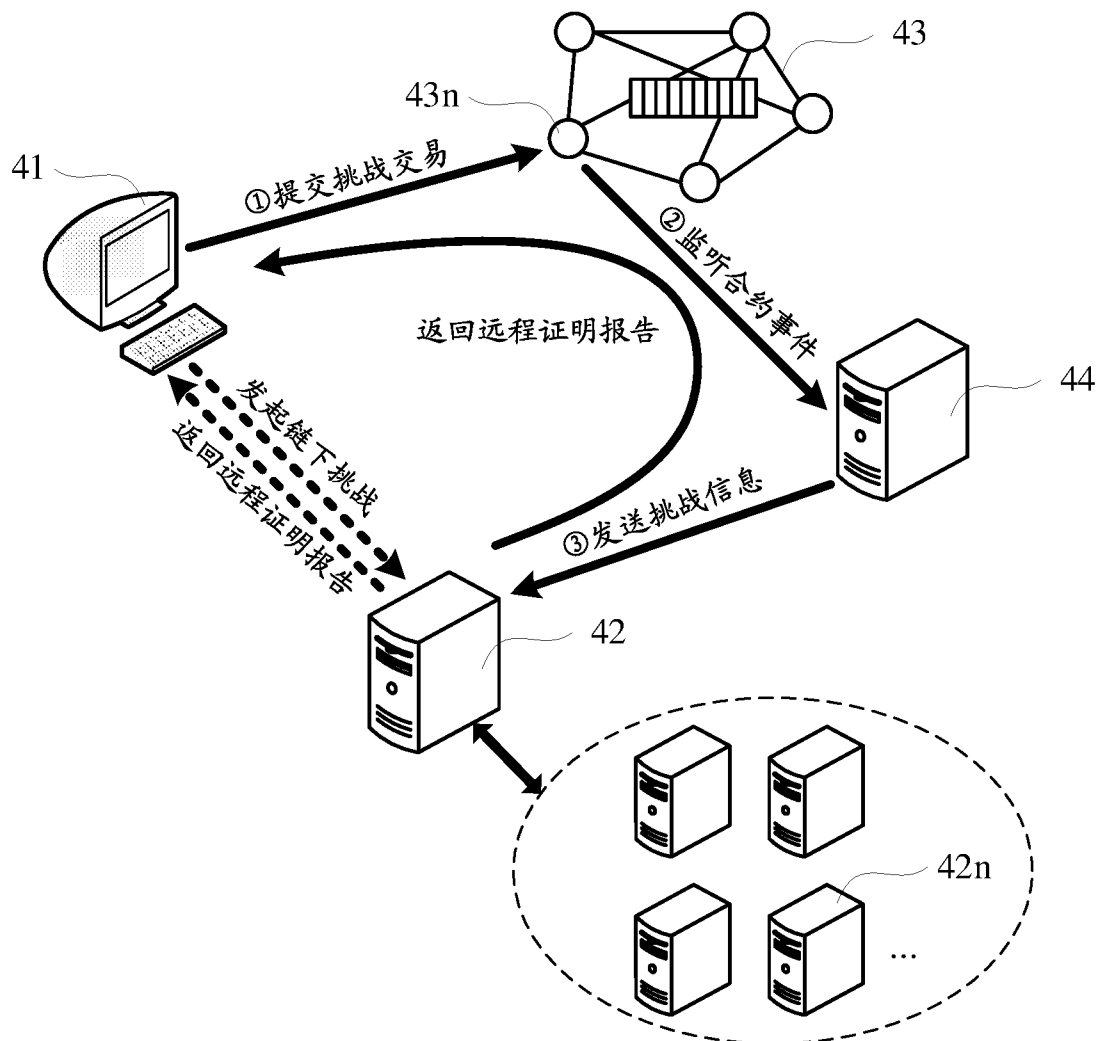


图 4

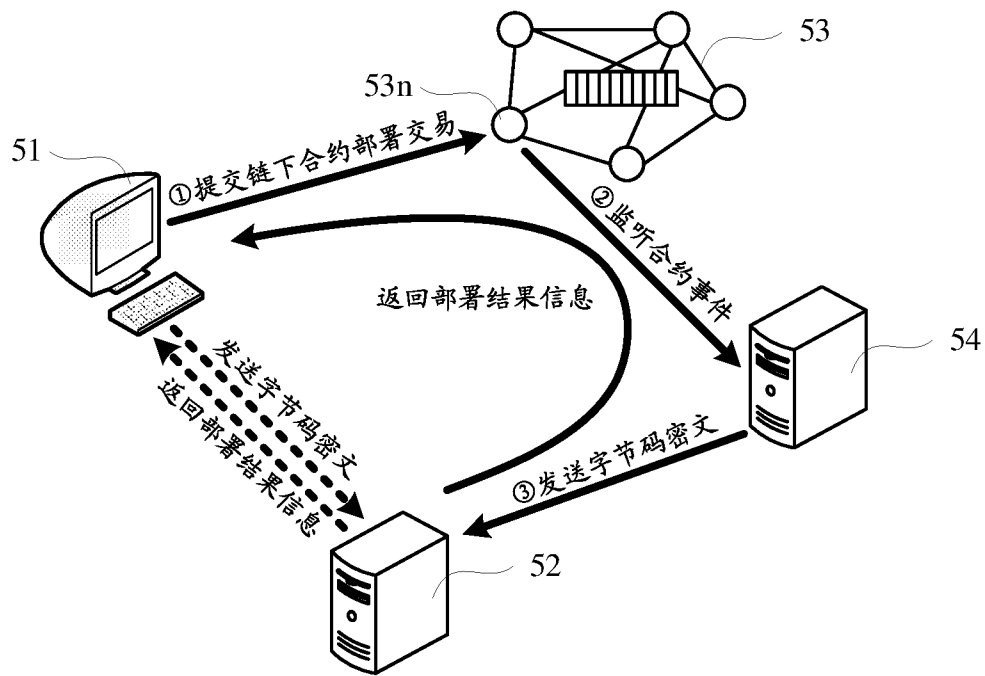


图 5

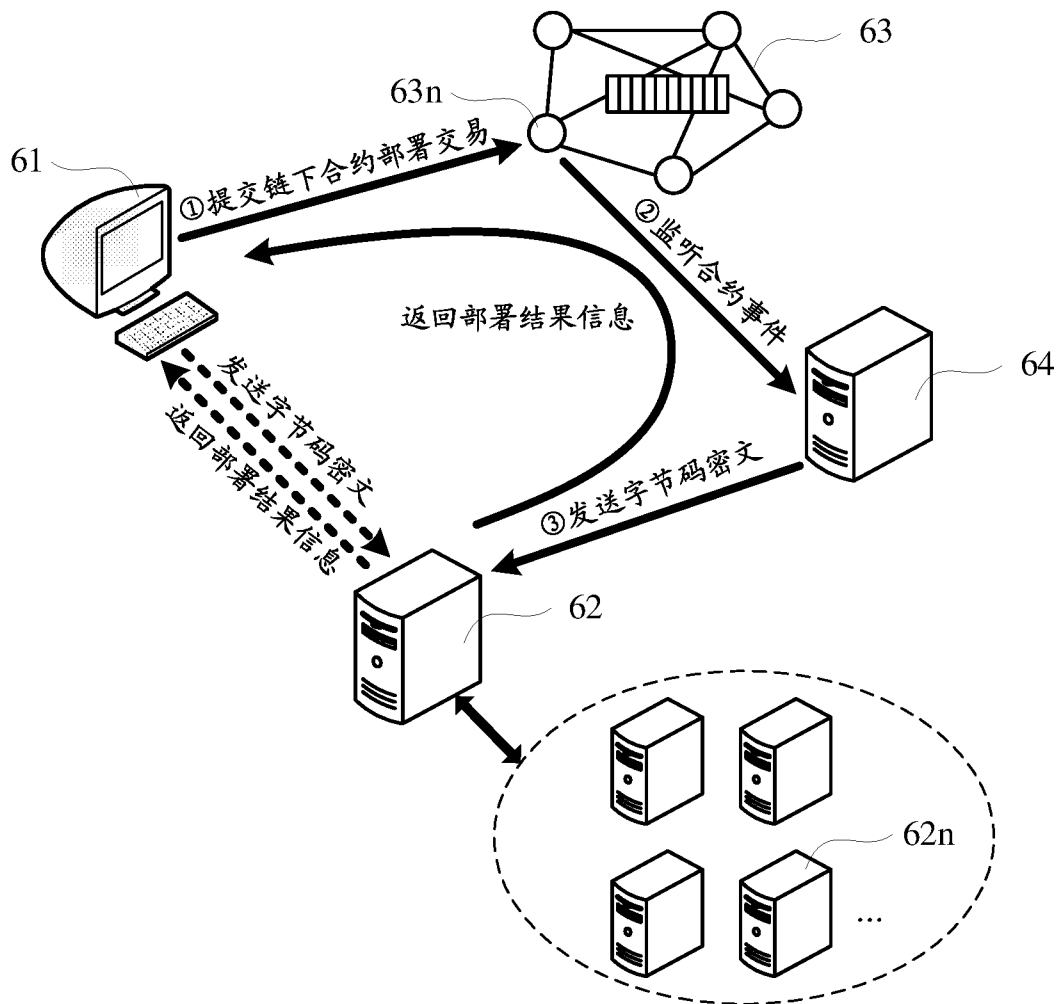


图 6

链下隐私计算集群中的任一节点确定自身已部署的目标链下合约，所述目标链下合约部署在所述链下隐私计算集群中的多个节点处；其中，响应于区块链节点的调用，所述目标链下合约可在所述多个节点中的各节点所创建的链下可信执行环境内被执行

702

所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的链下可信执行环境内针对所述多个节点之间的共用因子和所述目标链下合约的全局标识信息进行运算，生成对应于所述目标链下合约的共享合约身份密钥，所述共享合约身份密钥用于在链下可信执行环境内对所述目标链下合约的执行结果进行签名

704

图 7

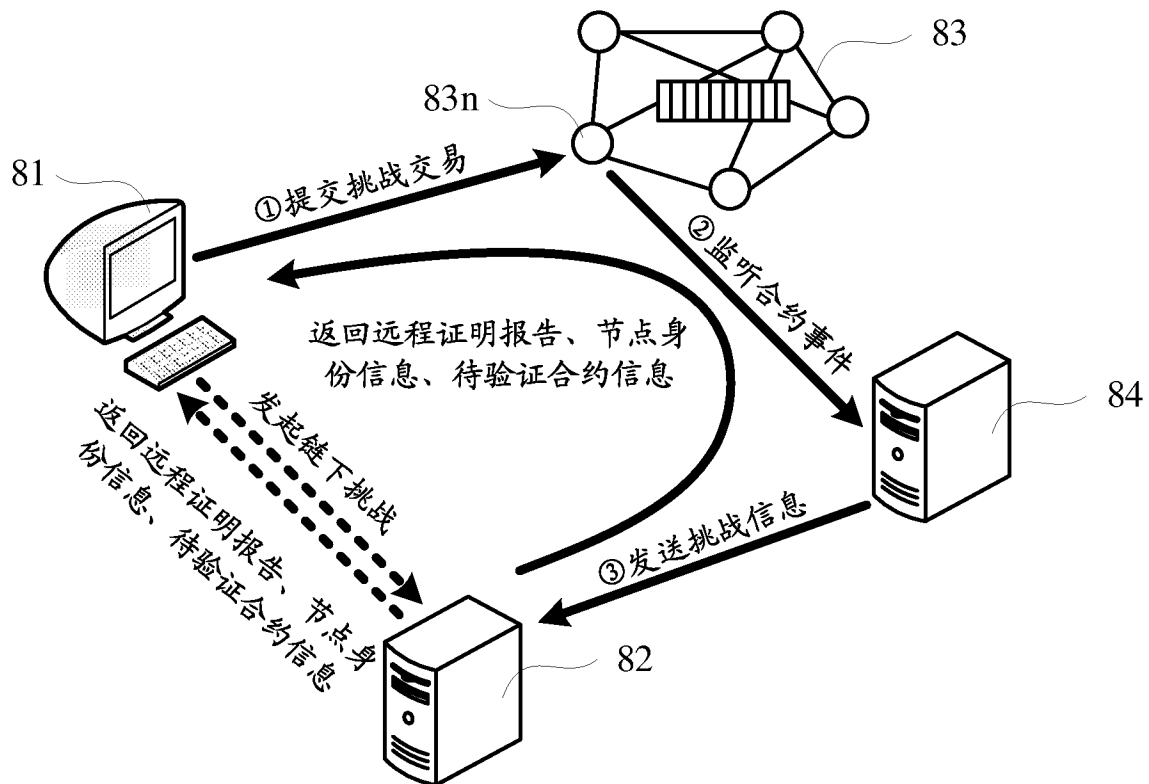


图 8

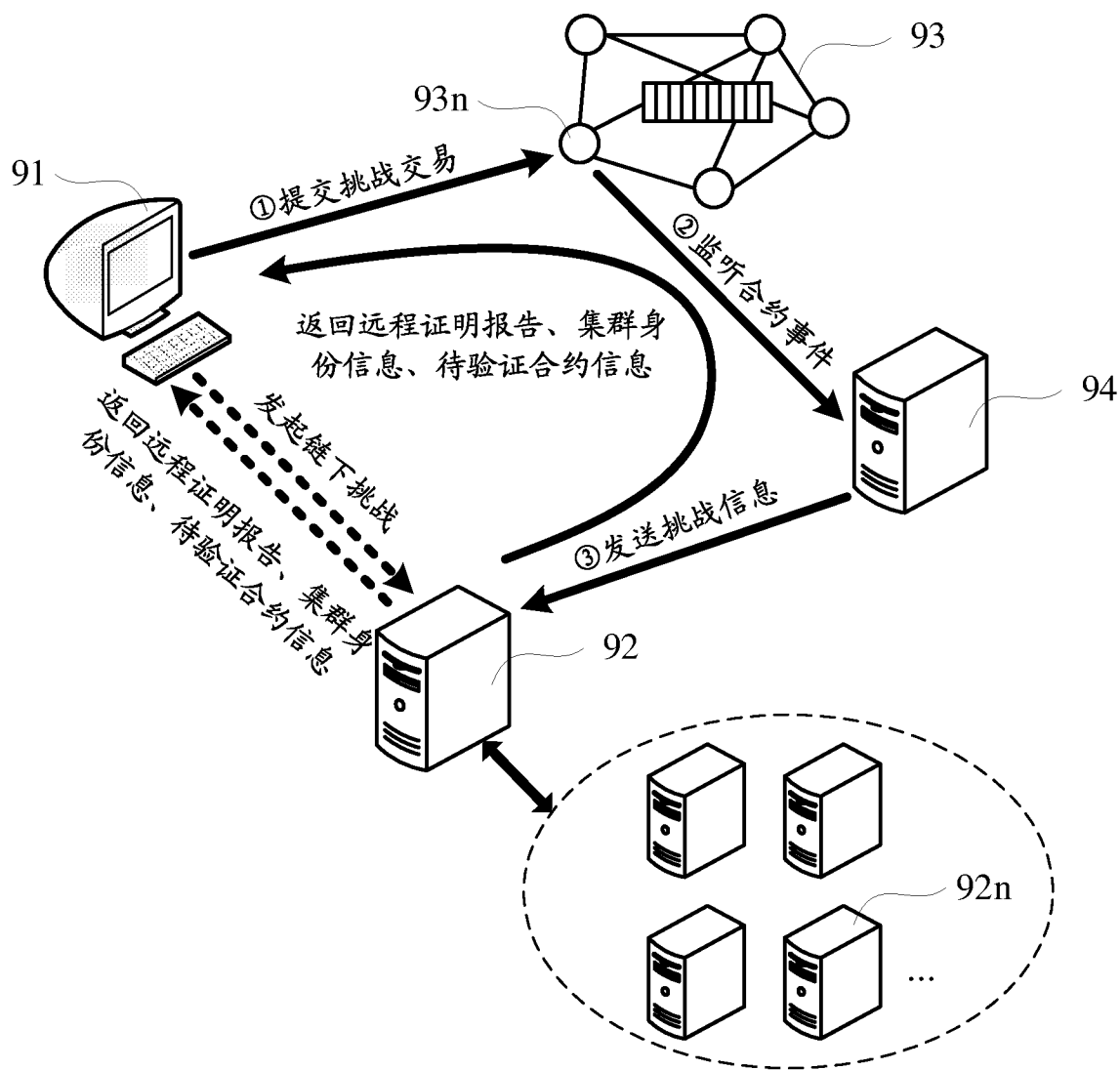


图 9

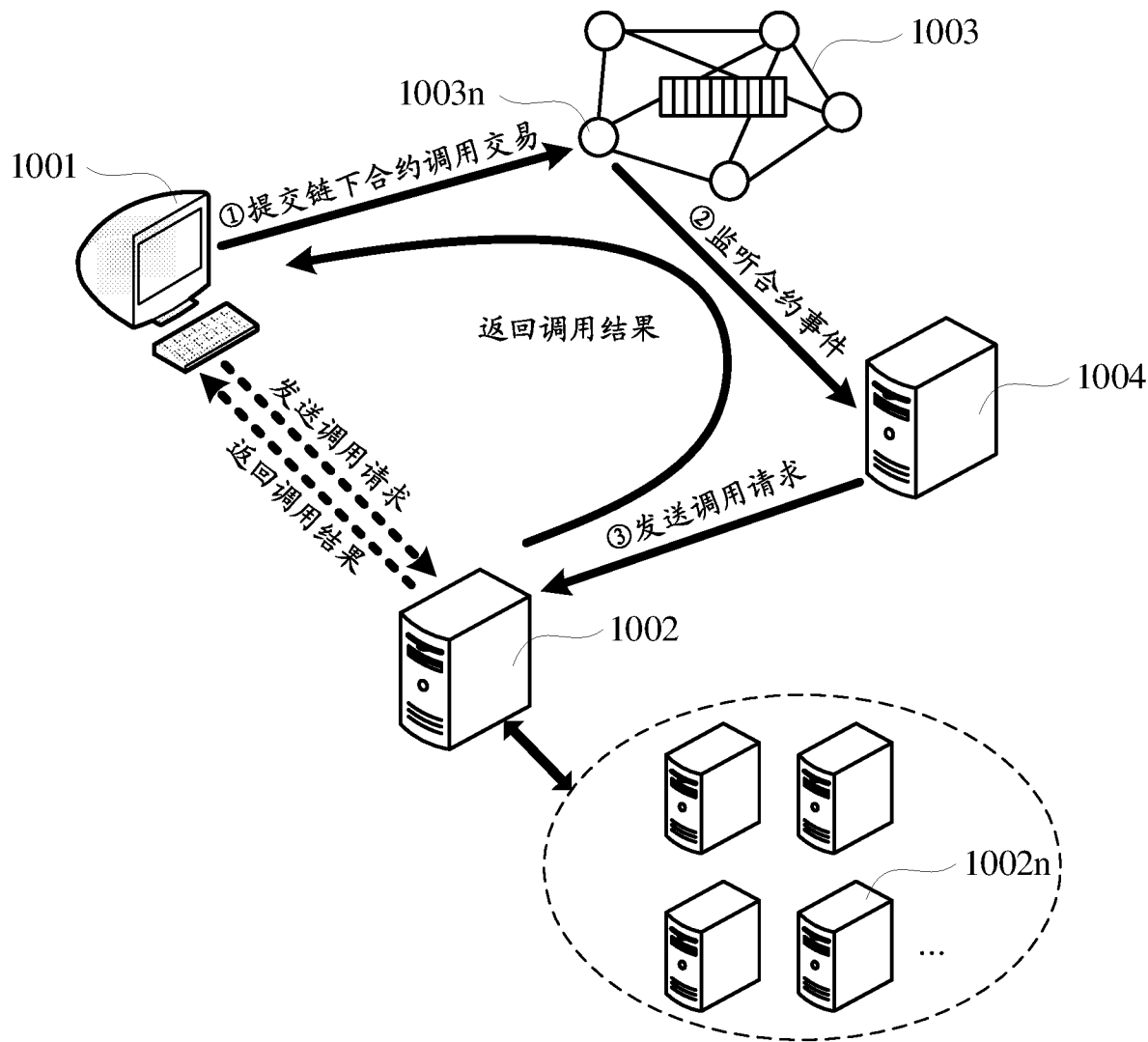


图 10

隐私计算集群中的任一节点确定自身已部署的目标智能合约，所述目标智能合约部署在所述隐私计算集群中的多个节点处；其中，响应于客户端的调用，所述目标智能合约可在所述多个节点中的各节点所创建的可信执行环境内被执行

1102

所述任一节点通过所述多个节点之间共用的密钥生成算法，在自身创建的可信执行环境内针对所述多个节点之间的共用因子和所述目标智能合约的全局标识信息进行运算，生成对应于所述目标智能合约的共享合约身份密钥，所述共享合约身份密钥用于在可信执行环境内对所述目标智能合约的执行结果进行签名

1104

图 11

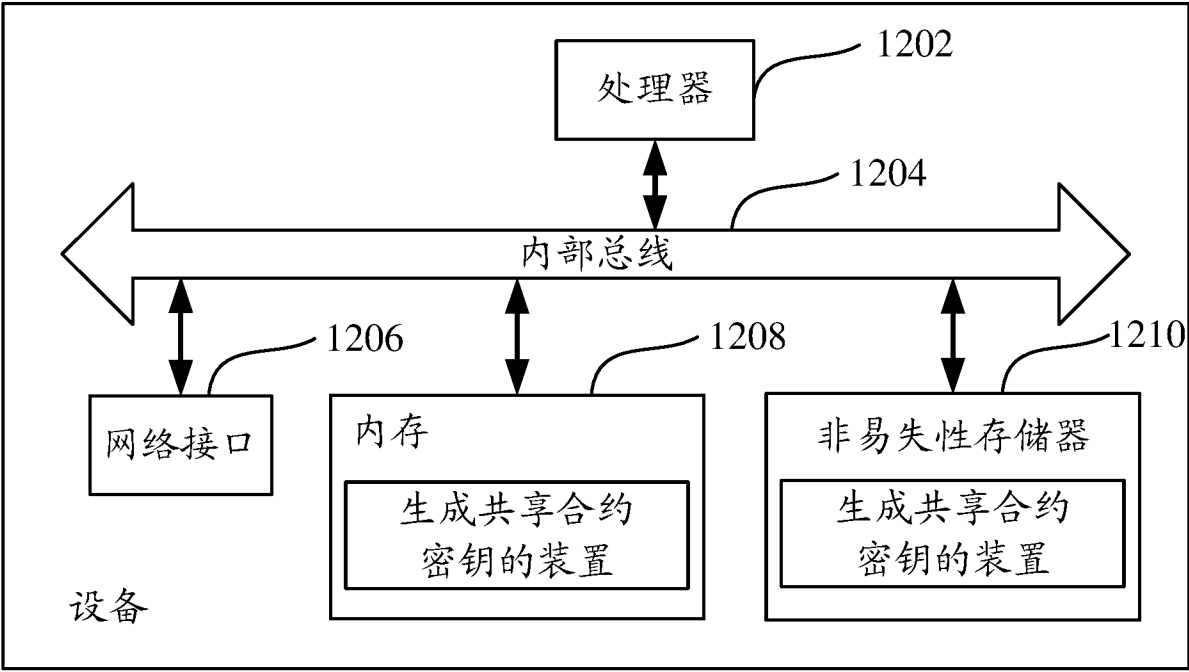


图 12

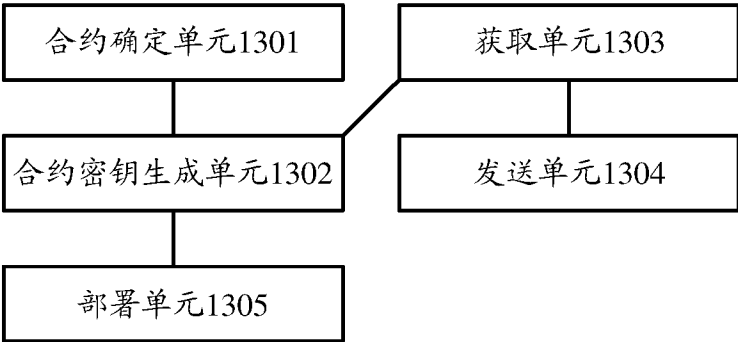


图 13

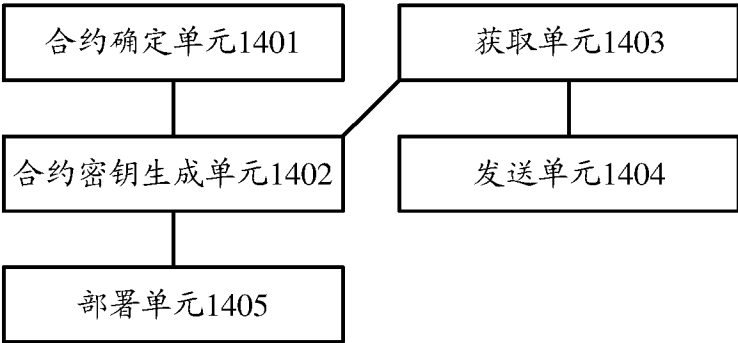


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/073820

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04L 9/32(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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; USTXT; EPTXT; WOTXT; GOOGLE: 吴因金, 邱鸿霖, 支付宝, 吴行行, 链下, 链外, 区块链, 合约, 密钥, 可信环境, 隐私计算集群, 共用因子, 远程证明, 共享, 公共, 统一, 哈希, 标识信息, 预言机, TEE, block chain, off, out, under, key, share, common, contract, signature, SGX, identification, factor, parameter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111092726 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 01 May 2020 (2020-05-01) claims 1-34, description, paragraphs 0051-0194	1-34
A	CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019 (2019-11-29) description, paragraphs 0056-0058, 0090-0092	1-34
A	CN 110750803 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 04 February 2020 (2020-02-04) description paragraphs 0080-0085	1-34
A	CN 109831298 A (ALIBABA GROUP HOLDING LIMITED) 31 May 2019 (2019-05-31) description, paragraphs 0053-0065	1-34
A	CN 109003078 A (ALIBABA GROUP HOLDING LIMITED) 14 December 2018 (2018-12-14) entire document	1-34
A	US 2017372300 A1 (POKITDOK INC.) 28 December 2017 (2017-12-28) entire document	1-34



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

29 March 2021

Date of mailing of the international search report

26 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/CN2021/073820

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111092726	A	01 May 2020	CN	111092726	B	28 July 2020
				CN	112152800	A	29 December 2020
CN	110520884	A	29 November 2019	US	2019279206	A1	12 September 2019
				WO	2019072297	A2	18 April 2019
				EP	3563329	A2	06 November 2019
				MX	2019008597	A	09 September 2019
				EP	3563329	A4	11 December 2019
				CA	3049924	A1	18 April 2019
				BR	112019014847	A2	14 April 2020
				KR	20200074910	A	25 June 2020
				PH	12019501714	A1	09 March 2020
				AU	2018347199	A1	02 July 2020
				JP	2020516104	A	28 May 2020
				RU	2729700	C1	11 August 2020
				WO	2019072297	A3	18 July 2019
				SG	11201906754	A1	27 August 2019
				HK	40017317	A0	18 September 2020
				KR	2212817	B1	08 February 2021
				IN	201947029881	A	19 June 2020
CN	110750803	A	04 February 2020	None			
CN	109831298	A	31 May 2019	CN	109831298	B	15 May 2020
				CN	111614464	A	01 September 2020
CN	109003078	A	14 December 2018	US	2020004737	A1	02 January 2020
				AU	2019294726	A1	18 June 2020
				US	10776348	B2	15 September 2020
				US	2020349148	A1	05 November 2020
				SG	CN 11202005051 U	A	29 June 2020
				WO	2020006164	A1	02 January 2020
				EP	3701673	A1	02 September 2020
				KR	20200088827	A	23 July 2020
				TW	202001608	A	01 January 2020
				CA	3084084	A1	02 January 2020
				HK	40001517	A0	01 January 2021
				IN	202047022757	A	01 January 2021
US	2017372300	A1	28 December 2017	WO	2017223540	A1	28 December 2017
				US	10108954	B2	23 October 2018

国际检索报告

国际申请号

PCT/CN2021/073820

A. 主题的分类 H04L 9/08(2006.01)i; H04L 9/32(2006.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类																							
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) H04L 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;USTXT;EPTXT;WOTXT;GOOGLE:吴因金, 邱鸿霖, 支付宝, 吴行行, 链下, 链外, 区块链, 合约, 密钥, 可信环境, 隐私计算集群, 共用因子, 远程证明, 共享, 公共, 统一, 哈希, 标识信息, 预言机, TEE, block chain, off, out, under, key, share, common, contract, signature, SGX, identification, factor, parameter																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 111092726 A (支付宝杭州信息技术有限公司) 2020年 5月 1日 (2020 - 05 - 01) 权利要求第1-34项, 说明书第0051-0194段</td> <td>1-34</td> </tr> <tr> <td>A</td> <td>CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29) 说明书第0056-0058、0090-0092段</td> <td>1-34</td> </tr> <tr> <td>A</td> <td>CN 110750803 A (支付宝杭州信息技术有限公司) 2020年 2月 4日 (2020 - 02 - 04) 说明书第0080-0085段</td> <td>1-34</td> </tr> <tr> <td>A</td> <td>CN 109831298 A (阿里巴巴集团控股有限公司) 2019年 5月 31日 (2019 - 05 - 31) 说明书第0053-0065段</td> <td>1-34</td> </tr> <tr> <td>A</td> <td>CN 109003078 A (阿里巴巴集团控股有限公司) 2018年 12月 14日 (2018 - 12 - 14) 全文</td> <td>1-34</td> </tr> <tr> <td>A</td> <td>US 2017372300 A1 (POKITDOK INC) 2017年 12月 28日 (2017 - 12 - 28) 全文</td> <td>1-34</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 111092726 A (支付宝杭州信息技术有限公司) 2020年 5月 1日 (2020 - 05 - 01) 权利要求第1-34项, 说明书第0051-0194段	1-34	A	CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29) 说明书第0056-0058、0090-0092段	1-34	A	CN 110750803 A (支付宝杭州信息技术有限公司) 2020年 2月 4日 (2020 - 02 - 04) 说明书第0080-0085段	1-34	A	CN 109831298 A (阿里巴巴集团控股有限公司) 2019年 5月 31日 (2019 - 05 - 31) 说明书第0053-0065段	1-34	A	CN 109003078 A (阿里巴巴集团控股有限公司) 2018年 12月 14日 (2018 - 12 - 14) 全文	1-34	A	US 2017372300 A1 (POKITDOK INC) 2017年 12月 28日 (2017 - 12 - 28) 全文	1-34
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
PX	CN 111092726 A (支付宝杭州信息技术有限公司) 2020年 5月 1日 (2020 - 05 - 01) 权利要求第1-34项, 说明书第0051-0194段	1-34																					
A	CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29) 说明书第0056-0058、0090-0092段	1-34																					
A	CN 110750803 A (支付宝杭州信息技术有限公司) 2020年 2月 4日 (2020 - 02 - 04) 说明书第0080-0085段	1-34																					
A	CN 109831298 A (阿里巴巴集团控股有限公司) 2019年 5月 31日 (2019 - 05 - 31) 说明书第0053-0065段	1-34																					
A	CN 109003078 A (阿里巴巴集团控股有限公司) 2018年 12月 14日 (2018 - 12 - 14) 全文	1-34																					
A	US 2017372300 A1 (POKITDOK INC) 2017年 12月 28日 (2017 - 12 - 28) 全文	1-34																					
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td> * 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																			
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																						
国际检索实际完成的日期		国际检索报告邮寄日期																					
2021年 3月 29日		2021年 4月 26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 传真号 (86-10)62019451		白生斌 电话号码 (86-20)28950890																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/073820

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	111092726	A	2020年 5月 1日	CN	111092726	B	2020年 7月 28日
				CN	112152800	A	2020年 12月 29日
CN	110520884	A	2019年 11月 29日	US	2019279206	A1	2019年 9月 12日
				WO	2019072297	A2	2019年 4月 18日
				EP	3563329	A2	2019年 11月 6日
				MX	2019008597	A	2019年 9月 9日
				EP	3563329	A4	2019年 12月 11日
				CA	3049924	A1	2019年 4月 18日
				BR	112019014847	A2	2020年 4月 14日
				KR	20200074910	A	2020年 6月 25日
				PH	12019501714	A1	2020年 3月 9日
				AU	2018347199	A1	2020年 7月 2日
				JP	2020516104	A	2020年 5月 28日
				RU	2729700	C1	2020年 8月 11日
				WO	2019072297	A3	2019年 7月 18日
				SG	11201906754	A1	2019年 8月 27日
				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
CN	110750803	A	2020年 2月 4日	无			
CN	109831298	A	2019年 5月 31日	CN	109831298	B	2020年 5月 15日
				CN	111614464	A	2020年 9月 1日
CN	109003078	A	2018年 12月 14日	US	2020004737	A1	2020年 1月 2日
				AU	2019294726	A1	2020年 6月 18日
				US	10776348	B2	2020年 9月 15日
				US	2020349148	A1	2020年 11月 5日
				SG	11202005051U	A	2020年 6月 29日
				WO	2020006164	A1	2020年 1月 2日
				EP	3701673	A1	2020年 9月 2日
				KR	20200088827	A	2020年 7月 23日
				TW	202001608	A	2020年 1月 1日
				CA	3084084	A1	2020年 1月 2日
				HK	40001517	A0	2021年 1月 1日
				IN	202047022757	A	2021年 1月 1日
US	2017372300	A1	2017年 12月 28日	WO	2017223540	A1	2017年 12月 28日
				US	10108954	B2	2018年 10月 23日