

# (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 2021/184975 A1**

(51) 国际专利分类号:  
**G06Q 40/04** (2012.01)

(21) 国际申请号: PCT/CN2021/074245

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

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
202010190874.3 2020 年 3 月 18 日 (18.03.2020) CN

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

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

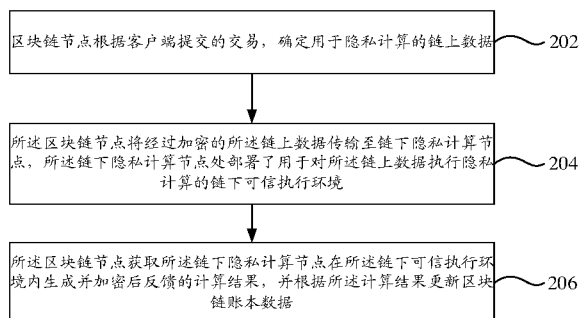
省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。吴因金 (WU, Yinqian); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

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

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

(54) Title: OFF-CHAIN PRIVACY CALCULATION METHOD AND APPARATUS FOR ON-CHAIN DATA

(54) 发明名称: 链上数据的链下隐私计算方法及装置



202 A blockchain node determines, according to a transaction submitted by a client, on-chain data for privacy calculation

204 The blockchain node transmits the encrypted on-chain data to an off-chain privacy calculation node, in which an off-chain trusted execution environment used for performing privacy calculation on the on-chain data is deployed

206 The blockchain node obtains the calculation result generated by the off-chain privacy calculation node in the off-chain trusted execution environment, encrypted, and then fed back by same, and updates blockchain ledger data according to the calculation result

图 2

(57) Abstract: An off-chain privacy calculation method and apparatus for on-chain data. The method comprises: a blockchain node determines, according to a transaction submitted by a client, on-chain data for privacy calculation (202); the blockchain node transmits the encrypted on-chain data to an off-chain privacy calculation node, in which an off-chain trusted execution environment used for performing privacy calculation on the on-chain data is deployed (204); the blockchain node obtains the calculation result generated by the off-chain privacy calculation node in the off-chain trusted execution environment, encrypted, and then fed back by same, and updates blockchain ledger data according to the calculation result (206). The method can realize privacy protection during the off-chain privacy calculation process.

(57) 摘要: 一种链上数据的链下隐私计算方法及装置, 该方法包括: 区块链节点根据客户端提交的交易, 确定用于隐私计算的链上数据 (202); 上述区块链节点将经过加密的链上数据传输至链下隐私计算节点, 该链下隐私计算节点处部署了用于对上述链上数据执行隐私计算的链下可信执行环境 (204); 上述区块链节点获取上述链下隐私计算节点在链下可信执行环境内生成并加密后反馈的计算结果, 并根据该计算结果更新区块链账本数据 (206)。该方法可以在链下隐私计算的过程中实现隐私保护。

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))。

## 链上数据的链下隐私计算方法及装置

### 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，尤其涉及一种链上数据的链下隐私计算方法及装置。

### 背景技术

[02] 区块链技术（也被称为，分布式账本技术）是一种去中心化的分布式数据库技术。由于采用去中心化的网络结构、共识机制和链式区块结构，使得区块链技术具有去中心化、公开透明、不可篡改、可信任等多种特点，适用于诸多对数据可靠性具有高需求的应用场景中。

[03] 针对区块链场景下的隐私需求，在相关技术中，通过同态加密（Homomorphic encryption）和零知识证明（Zero-knowledge proof）等加密技术实现该场景下的隐私保护，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。因此，通过在区块链节点上创建TEE环境，可以在性能损失相对较小的前提下很大程度上满足区块链场景下的隐私需求。

[04] 因此，通过在区块链节点上预先创建的TEE环境内调用并执行代码，可以在减少单个区块链节点的资源消耗的前提下加快代码的执行效率。

### 发明内容

[05] 有鉴于此，本说明书一个或多个实施例提供一种链上数据的链下隐私计算方法、装置及电子设备，能够在链下环境内协助区块链节点安全地完成计算任务。

[06] 根据本说明书一个或多个实施例的第一方面，提出了一种链上数据的链下隐私计算方法，包括：区块链节点根据客户端提交的交易，确定用于隐私计算的链上数据；所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，并根据所述计算结果更新区块链账本数据。

[07] 根据本说明书一个或多个实施例的第二方面，提出了一种链上数据的链下隐私计算方法，包括：链下隐私计算节点接收区块链节点传输的经过加密的链上数据，所述链下隐私计算节点处部署了链下可信执行环境，所述链上数据由所述区块链节点根据客户端提交的交易确定；所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果；所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果，所述计算结果用于更新区块链账本数据。

[08] 根据本说明书一个或多个实施例的第三方面，提出了一种链上数据的链下隐私计算方法，包括：客户端向区块链节点提交交易，以由所述区块链节点根据所述交易确定用于隐私计算的链上数据；所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下，将所述链上数据加密传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下，将所述计算结果发送给所述区块链节点用于更新区块链账本数据。

[09] 根据本说明书一个或多个实施例的第四方面，提出了一种链上数据的链下隐私计算装置，包括：链上数据确定单元，使区块链节点根据客户端提交的交易，确定用于隐私计算的链上数据；链上数据传输单元，使所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；计算结果获取单元，使所述区块链节点获取所述链下隐私

计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，并根据所述计算结果更新区块链账本数据。

[10] 根据本说明书一个或多个实施例的第五方面，提出了一种链上数据的链下隐私计算装置，包括：链上数据接收单元，使链下隐私计算节点接收区块链节点传输的经过加密的链上数据，所述链下隐私计算节点处部署了链下可信执行环境，所述链上数据由所述区块链节点根据客户端提交的交易确定；隐私计算执行单元，使所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果；计算结果反馈单元，使所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果，所述计算结果用于更新区块链账本数据。

[11] 根据本说明书一个或多个实施例的第六方面，提出了一种链上数据的链下隐私计算装置，包括：交易提交单元，使客户端向区块链节点提交交易，以由所述区块链节点根据所述交易确定用于隐私计算的链上数据；链上数据转发单元，使所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下，将所述链上数据加密传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；计算结果转发单元，使所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下，将所述计算结果发送给所述区块链节点，用于更新区块链账本数据。

[12] 根据本说明书一个或多个实施例的第七方面，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、第二方面或第三方面所述的方法。

[13] 根据本说明书一个或多个实施例的第八方面，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、第二方面或第三方面所述方法的步骤。

[14] 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，因而区块链节点可以将链上数据交由链下隐私计算节点进行安全计算。

#### 附图说明

[15] 图 1 是链上数据的链下隐私计算方法所对应网络架构的示意图。

[16] 图 2 是一示例性实施例提供的一种区块链节点侧的链上数据的链下隐私计算方法的流程图。

[17] 图 3 是一示例性实施例提供的一种链下隐私计算节点侧的链上数据的链下隐私计算方法的流程图。

[18] 图 4 是一示例性实施例提供的一种客户端侧的链上数据的链下隐私计算方法的流程图。

[19] 图 5 是一示例性实施例提供的一种链上数据的链下隐私计算方法对应的各设备之间的交互流程图。

[20] 图 6 是一示例性实施例提供的另一种链上数据的链下隐私计算方法对应的各设备之间的交互流程图。

[21] 图 7 是一示例性实施例示出的一种电子设备的结构示意图。

[22] 图 8 是一示例性实施例示出的一种区块链节点侧的链上数据的链下隐私计算装置的框图。

[23] 图 9 是一示例性实施例示出的一种链下隐私计算节点侧链上数据的链下隐私计算装置的框图。

[24] 图 10 是一示例性实施例示出的一种客户端侧链上数据的链下隐私计算装置的框图。

#### 具体实施方式

[25] 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述的实施方式并不代表与本发明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、本发明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。

[26] 需要说明的是：在其他实施例中并不一定按照本发明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发明说明书所描述的更多或更少。此外，本发明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；而本发明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。

[27] 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。

[28] 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链上 TEE，并将链上 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。

[29] 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。

[30] 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。

[31] 在链下隐私计算节点上创建的链下 TEE，与前文所述的区块链节点上创建的链上 TEE 相似，都是基于 CPU 硬件实现的与外部完全隔离的可信执行环境。链下隐私计算节点通过创建链下 TEE，可以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。

[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，以下简称“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，而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消耗量的成倍增长，从而整体上降低了区块链网络的交易执行效率。

[36] 为此，本说明书提出了基于在链下部署的隐私计算节点（即链下隐私计算节点，该链下隐私计算节点中预部署的链下合约在被调用时可以在链下隐私计算节点的链下 TEE 中执行），区块链节点将链上数据加密传输至链下隐私计算节点，由链下隐私计算节点使用链上数据在链下 TEE 中进行隐私计算，并将所得计算结果反馈至区块链节点。本方法将原本需要在所有区块链节点上执行的计算操作转移至某一链下隐私计算节点处执行，使得区块链节点只需要将链上数据传输至链下隐私计算节点并获取后者反馈的计算结果，然后基于该计算结果更新区块链账本数据即可，降低了区块链节点的计算资源消耗，从而有利于提高区块链网络的交易执行效率。并且在本方法中，链下隐私计算节点可以基于可验证计算（Verifiable Computation）技术证明其所获取链上数据的真实可信；同样的，区块链节点也可以基于可验证计算技术证明其所获取的计算结果确实是在链下 TEE 中使用链上数据执行预期计算得到的，从而实现了链上数据下链过程和链下计算结果反馈过程的可信认证。

[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] 图 1 是链上数据的链下隐私计算方法所对应网络架构的示意图。如图 1 所示,区块链节点通过客户端或预言机服务器两种可能的方式与链下隐私计算节点形成网络连接。其中,图中客户端可视为常规业务系统中的手机、平板电脑、PC 机、掌上电脑(PDAs, Personal Digital Assistants)、可穿戴式终端等电子设备上运行的应用程序;图中预言机服务器可视为区块链节点连接的 Oracle Services 等预言机服务器。图中链下隐私计算节点可以为独立的链下隐私计算节点,也可以为包含多个链下隐私计算节点的链下隐私计算集群(如图 1 右侧虚线框所示)中的某一链下隐私计算节点。在链下隐私计算节点归属于链下隐私计算集群的情况下,链下隐私计算集群中的控制节点分别与客户端及预言机服务器直接连接,负责将接收到的隐私计算任务在上述集群中的多个节点之间进行合理分配,以实现各节点的负载均衡。可以理解的是,虽然图中客户端和预言机服务器均连接至区块链网络中的某一区块链节点,但实际上二者可以分别连接同区块链网络中的不同区块链节点;而且,虽然将链下隐私计算节点(独立或集群)、预言机服务器和区块链节点分别绘制为不同的设备,但实际上三者可以位于相同或不同的物理实体中,本说明书对此并不进行限制。

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

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

[41] 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。

[42] 对应于图 1 所示的场景，一种情况下，客户端可以通过链下渠道直接向链下隐私计算节点发起挑战，即客户端向链下隐私计算节点发起链下挑战。另一种情况下，客户端可以通过区块链网络向链下隐私计算节点发起挑战，即客户端向链下隐私计算节点发起链上挑战。链上挑战的发起过程可以包括三个步骤：步骤①，客户端向区块链网络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内的某一区块链节点接收和执行；步骤②，区块链节点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，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，预言机服务器将挑战信息通过链下渠道发送至链下隐私计算节点。

[43] 客户端通过链上渠道向链下隐私计算节点发起挑战时，涉及到区块链网络与链下隐私计算节点之间的数据交互，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通过上述步骤②配合实现，该预言机合约与预言机服务器之间的配合机制即为预言机机制。其中，客户端向区块链节点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。

[44] 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。

[45] 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 1 所示的场景为例，所涉及的数据交互可以包括：客户端与链下隐私计算节点之间的数据交互（客户端向链下隐私计算节点发起链下挑战，链下隐私计算节点向客户端返回远程证明报告）、客户端与区块链节点之间的数据交互（客户端向区块链节点发送挑战交易、区块链节点向客户

端返回远程证明报告)、区块链节点与预言机服务器之间的数据交互(预言机服务器从区块链节点读取挑战信息、预言机服务器向区块链节点反馈远程证明报告)、预言机服务器与链下隐私计算节点之间的数据交互(预言机服务器向链下隐私计算节点发送挑战信息、链下隐私计算节点向预言机服务器返回远程证明报告)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,并且区块链节点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。

[46] 以客户端向区块链节点提交挑战交易为例。通过挑战交易向链下隐私计算节点发起链上挑战,使得区块链节点可以将客户端提交的挑战交易与其他节点进行共识后上链,对客户端的挑战行为进行存证。但是,如果客户端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。客户端可以对挑战交易进行加密,而区块链节点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。区块链节点处可以创建链上 TEE,并且区块链节点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。区块链节点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,区块链节点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。

[47] 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,客户端和区块链节点分别维护有相同的对称密钥,比如该对称密钥可由客户端与区块链节点通过诸如 DH (Diffie-Hellman) 或 ECDH (Elliptic Curve Diffie-Hellman) 等算法协商得到,或者由 KMS (Key Management Service, 密钥管理服务) 服务器分发至客户端和区块链节点,本说明书并不限制密钥来源。当密钥由 KMS 服务器分发时, KMS 服务器可以通过远程证明的方式确定区块链节点处的链上 TEE 可信,然后将密钥加密传输至该链上 TEE 内,远程证明的方式与上述客户端对链下隐私计算节点的远程证明过程类似,此处暂不赘述。那么,客户端可以通过上述的对称密钥对挑战交易进行加密,而区块链节点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。

[48] 当采用非对称加密时,区块链节点维护有非对称密钥的私钥,比如称之为区块链节点身份私钥,而客户端可以获得该区块链节点身份私钥相匹配的区块链节点身份公钥。非对称密钥可由区块链节点在链上 TEE 内生成,或者由 KMS 服务器分发至该区块链节点,本说明书并不限制密钥来源。类似地,当密钥由 KMS 服务器分发时, KMS 服务器可以通过远程证明的方式确定区块链节点处的链上 TEE 可信,然后将密钥加密传输至该链上 TEE 内。那么,客户端可以通过区块链节点身份公钥对挑战交易进行加密,而区块链节点将区块链节点身份私钥维护于链上 TEE 中,因而将经过加密的挑战交易读入链上 TEE 内,并通过区块链节点身份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。

[49] 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。客户端可以维护一对称密钥,比如该对称密钥可由客户端随机生成,且客户端可以获得上述非对称密钥中的区块链节点身份公钥。客户端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,然后客户端同时将加密后挑战交易与加密后密钥传输至区块链节点。相应的,区块链节点将加密后挑战交易与加密后密钥读入链上 TEE 内,首先使用区块链节点身份私钥对加密后密

钥进行解密、得到对称密钥，然后使用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。

[50] 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。

[51] 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。

[52] 仍以如图 1 所示的场景为例。一种情况下，客户端可以通过链下渠道直接向控制节点发起挑战，即客户端向控制节点发起链下挑战。另一种情况下，客户端可以通过区块链网络向控制节点发起挑战，即客户端向控制节点发起链上挑战。链上挑战的发起过程可以包括三个步骤：步骤①，客户端向区块链网络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内的某一节点接收和执行；步骤②，区块链节点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，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，预言机服务器将挑战信息通过链下渠道发送至控制节点。

[53] 客户端向控制节点发起挑战时，可以将挑战目标设定为控制节点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  $n$ ，那么控制节点会根据收到的挑战，向客户端返回链下隐私计算节点  $n$  对应的远程证明报告。客户端也可以不设定挑战目标，那么控制节点收到挑战后，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  $n$  的情况下，向客户端返回该链下隐私计算节点  $n$  对应的远程证明报告。

[54] 其中，控制节点在收到客户端发起的挑战后，可以将该挑战转发至链下隐私计算节点  $n$ ，使得链下隐私计算节点  $n$  临时触发远程证明过程，以产生相应的远程证明报告，然后通过控制节点反馈至客户端。或者，控制节点在收到客户端发起的挑战后，可以将该挑战转发至链下隐私计算节点  $n$ ，而如果链下隐私计算节点  $n$  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  $n$  将该远程证明报告返回控制节点，由控制节点提供至客户端，而无需临时触发远程证明过程。或者，控制节点在收到客户端发起的挑战后，如果本地已经存在预先生成的对应于链下隐私计算节点  $n$  的远程证明报告，那么链下隐私计算节点  $n$  将该远程证明报告提供至客户端，而无需向链下隐私计算节点  $n$  转发挑战，也无需链下隐私计算节点  $n$  因此临时触发远程证明过程。其中，链下隐私计算节点  $n$  本地存在的远程证明报告，可以是该链下隐私计算节点  $n$  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、控制节点、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  $n$  通过控制节点将远程证明报告提供至上述的其他挑战者时，控制节点可以对收到的远程证明报告进行缓存。因此，控制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，否则将挑战转发至链下隐私计

算节点 n; 以及, 链下隐私计算节点 n 在收到挑战后, 可以首先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, 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, 控制节点或链下隐私计算节点 n 也可以主动清除已失效的远程证明报告以避免将其反馈至客户端。

[55] 在图 1 所示的场景中, 客户端与控制节点之间、控制节点与链下隐私计算节点 n 之间、客户端与链下隐私计算节点 n 之间、链下隐私计算节点 n 与预言机服务器之间、预言机服务器与控制节点之间等, 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。

[56] 客户端通过获取针对链下隐私计算节点上创建的链下 TEE 的远程证明报告, 在验证该链下隐私计算节点可信, 即该链下隐私计算节点上部署的链下 TEE 可信的情况下, 可以在链下隐私计算节点中部署链下合约, 也就是在链下隐私计算节点中部署链下合约的字节码, 部署过程如下:

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

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

[59] 通过上述方式完成针对链下隐私计算节点的远程证明以及链下合约的部署之后, 即可以通过调用链下隐私计算节点基于链上数据进行链下隐私计算。在图 1 所示场景下, 区块链节点将链上数据通过客户端或预言机机制传输给链下隐私计算节点 (独立的链下隐私计算节点或链下隐私计算集群中的某一链下隐私计算节点), 以由链下隐私计算节点使用链上数据在链下 TEE 中执行预部署的链下合约, 然后再将计算结果反馈至区块链节点, 使得区块链节点在计算结果验证可信的情况下按照计算结果更新区块链账本数据。

[60] 图 2 是一示例性实施例提供的一种区块链节点侧的链上数据的链下隐私计算方法的流程图。如图 2 所示, 该方法可以包括步骤 202~步骤 206。

[61] 步骤 202, 区块链节点根据客户端提交的交易, 确定用于隐私计算的链上数据。

[62] 客户端向区块链节点提交交易。该交易可以以明文的形式传输给区块链节点, 也

可以采用如前文所述的加密数据传输方案进行传输，包括对称加密、非对称加密或两者结合的形式，以保证该交易在提交过程中的私密性，此处不再赘述。在加密传输的情况下，区块链节点可以将客户端提交的加密后的交易读入链上 TEE 内，并通过相应秘钥执行解密操作得到上述的交易，然后在链上 TEE 中执行该交易。

[63] 客户端生成的交易中可以直接包含经过加密的调用请求，那么区块链节点可以在链上 TEE 内解密交易、得到调用请求密文，然后区块链节点可以通过预言机机制将该调用请求密文传输至链下隐私计算节点。通常，上述调用请求中还包括调用信息，该调用信息可以由客户端生成后携带在上述交易中发送给区块链节点，也可以在区块链节点接收到上述调用请求后生成，本说明书对此并不进行限制。

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

[65] 针对调用请求中入参数据的信息，客户端生成的交易中可以直接包含入参数据，那么区块链节点可以在链上 TEE 内解密交易、得到入参数据。然后通过链上 TEE 内部署的虚拟机执行被调用的链上合约，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含入参数据的描述信息，比如该描述信息可以为存储地址等，那么区块链节点可以通过执行链上合约查询到相应的入参数据，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含初始数据，那么区块链节点可以通过执行链上合约对初始数据进行处理以获得相应的入参数据，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密。或者，客户端生成的交易中可以包含初始数据的描述信息，比如该描述信息可以为存储地址等，那么区块链节点可以通过执行链上合约查询到相应的初始数据，并由链上合约对初始数据进行处理，链上合约被执行后可以将上述标识信息和入参数据打包为调用请求并对该调用请求进行加密，因而客户端可以不直接将标识信息或者入参数据添加在交易中，客户端对于调用链下合约执行链下隐私计算的过程是透明的，客户端只需要获得链下隐私计算节点所反馈的计算结果即可，而不需要关注调用的链下合约的标识信息或者入参数据的信息等。

[66] 在上述交易执行前或执行过程中，需要利用某些链上数据进行链下隐私计算，因此需要根据上述交易确定相应的链上数据。链上数据可以是上述交易携带的入参数据，如位于上述交易的 data 字段中的数据；也可以是上述交易指定的数据，如在上述交易调用链上合约的情况下，被调用的链上合约基于上述交易在其 data 字段中指定的交易信息查询相应的链上数据；还可以在上述交易调用链上合约的情况下，将被调用的链上合约在执行过程中的中间值或最终结果作为上述的链上数据，上述中间值或最终结果是由链上合约对上述交易携带的数据或者按照其指定信息查询到的链上数据进行处理而生成的。另外，区块链节点确定出的链上数据可能具有多种类型，如位于区块链上的区块链数据、区块链节点维护的状态数据或区块链节点维护的收据数据等，本说明书对此并不进行限制。

[67] 步骤 204，所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境。

[68] 为保证链上数据在传输过程中的私密性，需要对链上数据进行加密。如果链上数据由客户端提供，比如该链上数据是上述交易携带的入参数据，那么该链上数据可能已经被客户端加密，而无需区块链节点进行加密。而如果链上数据由区块链节点查询得到或通过链上合约计算生成，那么应当由区块链节点在链上 TEE 内对该链上数据进行加

密；其中，如果区块链节点查询到的链上数据本身就处于加密状态，那么区块链节点需要在链上 TEE 内解密得到明文的链上数据，然后重新采用其他的密钥进行加密，以确保链下隐私计算节点能够顺利解密。当然，即便链上数据由客户端提供，客户端也可以将链上数据传输至区块链节点后，由区块链节点在链上 TEE 内进行加密。针对链上数据进行加密的过程可以使用上述的对称加密、非对称加密或两者结合的数字信封等方式进行，具体的加密过程不再一一赘述。

[69] 区块链节点还可以使用区块链节点身份私钥对链上数据进行签名；其中，签名验证成功被客户端或预言机服务器作为将经过加密的上述链上数据传输至链下隐私计算节点的前提条件。客户端或预言机服务器在接收到区块链节点发送的链上数据后，使用预先获取的区块链节点身份公钥对链上数据的签名进行验证（验签过程），只有链上数据通过验签，客户端或预言机服务器才能够确定链上数据确实是由区块链节点发送的，且传输过程中未发生数据丢失或被篡改，进而将该链上数据传输至链下隐私计算节点。

[70] 针对链上数据的不同来源和原始加密情况，区块链节点对链上数据进行加密和签名的操作顺序可以存在多种情况。下面以非对称加密场景为例，将所涉及设备的非对称密钥对的公钥简称为公钥，与之匹配的非对称密钥对的私钥简称为私钥，对上述情况进行说明。

[71] 如果链上数据由客户端提供，则在链上数据未被客户端加密的情况下，区块链节点可以先使用区块链节点的私钥对明文的链上数据进行签名，再对明文的链上数据进行加密；区块链节点也可以先对明文的链上数据进行加密，再使用区块链节点的私钥对密文的链上数据进行签名。在链上数据已经被客户端加密的情况下，若客户端使用客户端、预言机服务器或链下隐私计算节点的公钥对链上数据进行加密，则区块链节点直接对加密后的链上数据进行签名；若客户端使用区块链节点的公钥对链上数据进行加密，则区块链节点在链上 TEE 中解密得到明文的链上数据，然后可以先对明文的链上数据进行加密，再使用区块链节点的私钥对密文的链上数据进行签名，也可以先使用区块链节点的私钥对明文的链上数据进行签名，再对明文的链上数据进行加密。如果链上数据由区块链节点查询得到，则链上数据本身可能就处于加密状态，在链上数据被客户端或预言机服务器的公钥加密的情况下，区块链节点可以直接对加密后的链上数据进行签名；在链上数据被链上合约或其他交易的公钥进行加密的情况下，区块链节点可以在链上 TEE 中解密得到明文的链上数据，然后可以先对明文的链上数据进行加密，再使用区块链节点的私钥对密文的链上数据进行签名，或者先使用区块链节点的私钥对明文的链上数据进行签名，再对明文的链上数据进行加密。如果链上数据通过链上合约计算生成，则通常链上数据尚未被加密，此时区块链节点可以先对明文的链上数据进行加密，再使用区块链节点的私钥对密文的链上数据进行签名，或者先使用区块链节点的私钥对明文的链上数据进行签名，再对明文的链上数据进行加密。

[72] 在上述各实施例中，对签名前或签名后的明文的链上数据进行加密，可以使用客户端、预言机服务器或链下隐私计算节点的公钥，相应的，若使用客户端的公钥进行加密，则后续区块链节点经过客户端将加密和签名后的链上数据传输给链下隐私计算节点；若使用预言机服务器的公钥进行加密，则后续区块链节点经过预言机服务器将加密和签名后的链上数据传输给链下隐私计算节点；若使用链下隐私计算节点的公钥进行加密，则后续区块链节点可以经过客户端或预言机服务器将加密和签名后的链上数据传输给链下隐私计算节点。

[73] 在上述链上数据传输过程中，用于调用链下隐私计算节点中预部署的链下合约的调用信息可以与链上数据关联传输至链下隐私计算节点，该调用信息用于指示链下隐私计算节点在链下 TEE 内执行上述链下合约，以实现利用链上数据进行隐私计算的目的。具体的，区块链节点可以指定链下隐私计算节点中的链下合约使用链上数据在链下 TEE 中进行隐私计算。上述计算过程可以执行链下合约中的函数，该链下合约的调用信息被

与上述链上数据关联传输至链下隐私计算节点中，上述调用信息中可以包括所调用链下合约的合约 ID，也可以包括所调用链下合约的合约 ID 和该链下合约内至少一个函数的函数名。可以理解的是，在区块链节点或客户端指定上述调用信息的情况下，调用信息与链上数据关联传输前，可以针对调用信息执行与上述针对链上数据相似的加密与签名操作，具体方式不再赘述；而且，上述关联传输表示的是二者之间的逻辑关联，如通过预设的传输间隔时长或合约 ID 等关联标识信息将二者进行关联，而实际传输时可以将二者相邻并先后传输，也可以不相邻传输，本说明书对调用信息和链上数据的具体传输时序并不进行限制，下文仅以链上数据的传输为对象进行示例性说明。

[74] 区块链节点可以通过预言机机制将经过加密的链上数据传输至链下隐私计算节点，即区块链节点所执行的交易调用预言机合约，或者该交易调用的链上合约进一步调用预言机合约，预言机合约针对链上数据产生合约事件，而预言机服务器通过监听预言机合约产生的合约事件读取上述的链上数据，并进而将该链上数据传输至链下隐私计算节点。或者，区块链节点可以通过客户端处预部署的链下隐私计算调用组件，将经过加密的链上数据传输至链下隐私计算节点；客户端中可以预部署链下隐私计算调用组件，区块链节点将加密的链上数据发送给客户端，由客户端中的链下隐私计算调用组件调用链下隐私计算节点，并将加密后的链上数据传输至链下隐私计算节点。

[75] 在链下隐私计算节点为独立节点的情况下，区块链节点可以通过前述的预言机机制或者调用客户端处的链下隐私计算调用组件，将链上数据直接传输给链下隐私计算节点。而在链下隐私计算节点属于链下隐私计算集群的情况下，区块链节点虽然也可以直接将链上数据传输至该链下隐私计算节点，但通常会将链上数据首先传输至链下隐私计算集群的控制节点，比如通过上述的预言机机制或者客户端处的链下隐私计算调用组件将链上数据传输至控制节点，进而由控制节点将链上数据转发给执行隐私计算的链下隐私计算节点。其中，控制节点转发链上数据的方式可以为：客户端或预言机服务器将链下隐私计算节点的指定信息（如节点 ID）与链上数据关联发送至控制节点，控制节点接收上述指定信息与链上数据后，确定与上述指定信息匹配的链下隐私计算节点，然后将链上数据发送给该节点；或者，控制节点接收上述数据后，按照集群内各节点的当前负载值（如当前运算量、当前时刻起预设时间段内的预期运算量、当前计算任务的个数等）确定目标节点，如将当前负载值最小的节点确定为目标节点、将当前负载值小于某一负载值阈值的所有节点中的任一节点确定为目标节点等；然后将链上数据发送给上述目标节点，以由上述目标节点使用链上数据执行隐私计算。

[76] 区块链节点对链上数据进行加密（或进行加密和签名）后，将密文的链上数据经过客户端或预言机服务器传输至链下隐私计算节点。具体的，在链上数据被使用对称密钥加密的情况下，若链下隐私计算节点拥有该对称密钥，则客户端或预言机服务器可以直接将加密后的链上数据转发给链下隐私计算节点；若仅客户端（或预言机服务器）拥有该对称密钥，则客户端（或预言机服务器）将其在客户端（或预言机服务器）的链下 TEE 中解密得到明文的链上数据后，再使用与链下隐私计算节点协商的其他密钥加密链上数据并发送给链下隐私计算节点。在链上数据被使用非对称密钥的公钥加密的情况下，若链下隐私计算节点拥有与上述非对称密钥的公钥相匹配的私钥，则客户端（或预言机服务器）可以将上述加密后的链上数据直接转发给链下隐私计算节点；若仅客户端（或预言机服务器）拥有与上述非对称密钥的公钥相匹配的私钥，则客户端（或预言机服务器）将其在客户端（或预言机服务器）的链下 TEE 中解密得到明文的链上数据后，再使用与链下隐私计算节点协商的其他密钥加密链上数据并发送给链下隐私计算节点。在链上数据被使用上述数字信封加密的情况下，若链下隐私计算节点拥有该数字信封中非对称密钥的私钥，则客户端（或预言机服务器）可以将上述数字信封加密后的链上数据直接发送给链下隐私计算节点，或者使用与链下隐私计算节点协商的密钥将上述加密后的链上数据二次加密后发送给链下隐私计算节点；若客户端（或预言机服务器）拥有

该非对称秘钥的私钥，则客户端（或预言机服务器）可以将其在客户端（或预言机服务器）的链下 TEE 中解密得到对称秘钥后，使用与链下隐私计算节点协商的秘钥加密该对称秘钥后再发送给链下隐私计算节点；客户端（或预言机服务器）也可以将其在客户端（或预言机服务器）的链下 TEE 中解密得到链上数据后，再使用链下隐私计算节点的节点加密公钥构建的数字信封重新对链上数据进行加密后发送给链下隐私计算节点。

[77] 在链下隐私计算节点为独立节点的情况下，客户端或预言机服务器通常直接与链下隐私计算节点相连。链下隐私计算节点接收到客户端或预言机服务器使用链下隐私计算节点的节点加密公钥加密的链上数据后，可以先在预创建的链下 TEE 中使用与上述节点加密公钥相匹配的节点加密私钥对密文的链上数据进行解密，再使用区块链节点的区块链节点身份公钥对明文的链上数据进行验签，并在验签通过后使用链上数据进行隐私计算；也可以先使用区块链节点的区块链节点身份公钥对接收到的密文的链上数据进行验签，再在验签通过后使用区块链节点身份公钥相匹配的区块链节点身份私钥对密文的链上数据进行解密，并使用链上数据进行隐私计算。

[78] 在链下隐私计算节点属于链下隐私计算集群的情况下，与加密链上数据的节点加密公钥对应的节点加密私钥可以仅被链下隐私计算节点所维护，也可以链下隐私计算集群内的所有链下隐私计算节点共同维护，或者仅被该链下隐私计算集群的控制节点所维护。在上述节点加密私钥仅被链下隐私计算节点所维护的情况下，仅有链上数据的最终目的方（即该链下隐私计算节点）能够成功解密并获取上述链上数据，而其他设备即便获取加密后的该链上数据也无法对其进行解密，从而保证了链上数据在传输过程中的私密性。因为链下隐私计算节点所归属集群的控制节点会在任一节点加入集群时即通过远程证明对该节点进行可信验证，从而保证该集群中的所有链下隐私计算节点都是可信的，所以在上述节点加密私钥被链下隐私计算集群内的所有链下隐私计算节点所维护的情况下，一方面，控制节点接收到区块链节点使用节点加密私钥加密的链上数据后，可以直接将其转发给所确定的任一目标节点并由后者进行解密，而不需要控制节点进行解密和二次加密操作，从而缩短了控制节点的转发时间，提高了转发效率；另一方面，由于所有链下隐私计算节点均维护有上述节点加密私钥，对于客户端来说，链下隐私计算集群可视为一个设备，因此不需要保存各节点的公钥，减少了公钥的维护数量，一定程度上减轻了客户端的数据维护负担。而在节点加密私钥仅被该链下隐私计算集群的控制节点所维护的情况下，控制节点接收到密文的链上数据后，与上述链上数据的签名和加密的操作顺序相对应，控制节点可以先使用区块链节点的节点加密公钥对密文的链上数据进行验签，在验签通过后，再在控制节点中预部署的链下 TEE 中对密文的链上数据进行解密；也可以先在控制节点中预创建的链下 TEE 中对密文的链上数据进行解密以得到明文的链上数据，再使用区块链节点的节点加密公钥对明文的链上数据进行验签。在上述验签并加密（或验签）通过后，可以使用与目标节点预协商的秘钥将明文的链上数据进行再次加密后发送给目标节点，以使目标节点在解密后使用上述链上数据进行隐私计算。在上述过程中验签失败的情况下，进行验签的设备（链下隐私计算节点或控制节点）可以将上述链上数据丢弃；也可以提取链上数据的数据信息生成数据验签日志，并将该数据验签日志保存在本地或反馈给区块链节点；还可以向区块链节点或其他预设对象返回错误信息或告警信息等，本说明书对此并不进行限制。

[79] 链下隐私计算节点利用验签通过的链上数据在创建的链下 TEE 中执行预部署的链下合约，即进行隐私计算。具体的，链下隐私计算节点可以解密与链上数据相关联的链下合约调用请求得到标识信息，然后链下隐私计算节点可以根据标识信息调用预先部署的链下合约的字节码，而在链下可信执行环境中部署有若干执行引擎的情况下，链下隐私计算节点可以根据字节码确定对应的执行引擎，并且通过确定出的执行引擎执行上述字节码以对链上数据进行链下隐私计算。

[80] 在链下隐私计算节点处创建的链下 TEE 中，可以部署有若干执行引擎，比如 EVM、

WASM 虚拟机等中的一个或多个,在同时部署了多种执行引擎的情况下,客户端或区块链节点除了在链下隐私计算节点处安全存储链下合约的字节码之外,还可以向链下隐私计算节点指明用于执行该字节码的执行引擎。链下隐私计算节点可以接收客户端或区块链节点发送的与链下合约的字节码相关联的执行引擎指定信息,并根据执行引擎指定信息为字节码设定相应的执行引擎。因而链下隐私计算节点可以在链下 TEE 中根据确定出的执行引擎对链上数据进行链下隐私计算。值得说明的是,上述指定信息可以包含在上述调用请求中。

[81] 本说明书中链下隐私计算节点可以使用链上数据实现用户定义的任何计算逻辑。例如,链下隐私计算节点可以通过链下合约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,链下隐私计算节点可以通过链下合约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。

[82] 步骤 206,所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果,并根据所述计算结果更新区块链账本数据。

[83] 链下隐私计算节点在链下 TEE 中执行计算得到链下隐私计算结果,可以包括以下至少之一:响应码、响应信息、合约调用的返回值、合约调用的过程输出,链下隐私计算节点可以根据调用请求返回相应的链下隐私计算结果,本说明书中并不对此进行限制。对于上述计算结果,链下隐私计算节点可以先在链下 TEE 中对计算结果进行加密,然后将加密后的计算结果反馈至区块链节点。具体的,区块链节点可以通过预言机机制获取链下隐私计算节点在链下可信执行环境内生成并加密后反馈的计算结果,即上述计算结果作为被调用的预言机合约的响应反馈给区块链节点。或者,区块链节点也可以通过客户端处预部署的链下隐私计算调用组件获取链下隐私计算节点在链下可信执行环境内生成并加密后反馈的计算结果,即上述计算结果作为被调用的链下隐私计算调用组件的响应反馈给客户端,然后由客户端将计算结果发送给区块链节点以实现计算结果的反馈。

[84] 相应的,链下隐私计算节点可以通过链下隐私计算节点的节点签名私钥对计算结果进行签名或者可以采用被调用的链下合约的合约签名私钥对计算结果进行签名,也可以同时采用节点签名私钥和合约签名私钥对链下隐私计算结果进行签名,本说明书中并不对此进行限制。客户端或者区块链节点可以通过节点签名公钥或者合约签名公钥进行验签,从而确定该链下隐私计算结果确实是由链下隐私计算节点调用相应的链下合约所产生,并且传输过程中未发生数据丢失或被篡改。值得说明的是,链下隐私计算节点对计算结果进行签名所使用的节点签名私钥,与上述区块链节点、客户端或预言机服务器对链上数据进行加密使用的节点加密公钥,可以是一对相互匹配的非对称秘钥,也可以是不相匹配的非对称秘钥,本说明书对此并不进行限制。在调用请求中还包括指定对象的身份公钥的信息的情况下,链下隐私计算节点可以采用该身份公钥对计算结果进行加密,使得只有维护有与上述身份公钥相对应的身份私钥的指定对象才能对该链下隐私计算结果进行解密,可以限制能够查看计算结果的用户,而其他用户直接查看链下隐私计算结果时仅能够获得加密后的计算结果,从而实现了对于计算结果的隐私保护。

[85] 链下隐私计算节点针对计算结果的加密和签名的操作顺序可以存在多种情况。链下隐私计算节点可以在链下 TEE 中先使用区块链节点的区块链节点身份公钥对计算结果进行加密,再使用执行隐私计算的链下合约的合约签名私钥或隐私计算节点的节点签名私钥对密文的计算结果进行签名;也可以先使用上述合约签名私钥或上述节点签名私钥对明文的计算结果进行签名,再使用上述区块链节点身份公钥对密文的计算数据进行加密。在加密和签名完后,将上述签名和密文计算结果通过客户端或预言机服务器关联传输至区块链节点,后者接收之后在链上 TEE 中对其进行先解密后验签或先验签后解密以获取计算结果。链下隐私计算节点也可以在链下 TEE 中先使用客户端(或预言机

服务器)的公钥对计算结果进行加密,再使用执行隐私计算的链下合约的合约签名私钥或隐私计算节点的节点签名私钥对密文的计算结果进行签名;也可以先使用上述合约签名私钥或上述节点签名私钥对明文的计算结果进行签名,再使用客户端(或预言机服务器)的公钥对明文的计算结果进行加密;在加密和签名完后,由客户端(或预言机服务器)将上述签名和密文的计算结果传输至区块链节点,后者接收之后在链上 TEE 中对其进行先解密后验签或先验签后解密以获取计算结果。

[86] 在链下隐私计算节点属于链下隐私计算集群的情况下,因为链下隐私计算节点在使用链上数据进行隐私计算前已经通过了该集群控制节点的认证,因此链下隐私计算节点可以在计算得到上述计算结果后,先使用执行隐私计算的链下合约的合约签名私钥或链下隐私计算节点的节点签名私钥对计算结果进行签名,然后将签名后的计算结果发送至控制节点,由控制节点使用区块链节点的节点身份公钥进行加密;或者先使用上述合约签名私钥或上述节点签名私钥对计算结果进行签名,再使用区块链节点的节点身份公钥对其进行加密后发送给控制节点,最后由控制节点将上述加密和签名后的计算结果通过客户端或预言机服务器传输至区块链节点。当然,上述实施例中链下隐私计算节点或控制节点也可以使用客户端(或预言机服务器)的公钥对链上数据进行加密,然后由控制节点发送给客户端(或预言机服务器),客户端(或预言机服务器)接收后在链下 TEE 中解密,然后再使用区块链节点的区块链节点身份公钥进行二次加密后发送给区块链节点。

[87] 区块链节点在接收到链下隐私计算节点反馈的被签名的计算结果后,对该签名进行验签,区块链节点在确定针对计算结果的签名匹配于上述合约签名私钥或节点签名私钥的情况下,判定上述计算结果可信,且计算结果可信为区块链节点更新账本数据的前提条件。区块链节点使用预先获取的匹配于上述合约签名私钥或节点签名私钥的合约签名公钥或节点签名公钥对上述签名进行验证,以确定上述计算结果是否可信;在验证通过的情况下,判定上述计算结果可信,即该计算结果确实是在指定的链下隐私计算节点的 TEE 中使用链上数据执行指定的链下合约生成的,并且传输过程中未发生数据丢失或被篡改,因此区块链节点将上述签名验证通过作为使用计算结果更新账本数据的前提条件。

[88] 以区块链节点接收到的计算结果被链下隐私计算结果先使用区块链节点身份公钥加密,再使用节点加密私钥签名为例,对区块链节点针对计算结果的验签过程进行说明:首先使用与上述区块链节点身份公钥对应的区块链节点加密私钥解密上述签名,获得第一哈希值;然后使用与上述节点加密私钥对应的节点加密公钥解密上述密文的计算结果,再计算解密后所得明文的计算结果的第二哈希值,比较上述第一哈希值和第二哈希值:若上述第一哈希值与第二哈希值相等,则说明上述打包数据确实为区块链节点发送的,并且传输过程中未发生数据丢失或被篡改,验签成功;否则,若上述第一哈希值与第二哈希值不相等,则验签失败。

[89] 在验签成功的情况下,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。否则,在验签失败的情况下,客户端可以将上述链上数据丢弃;也可以提取链上数据的数据信息生成数据验签日志,并将该数据验签日志保存在本地或反馈给区块链节点;还可以向区块链节点或其他预设对象返回错误信息或告警信息等。

[90] 特殊的,在链下隐私计算节点通过预言机机制将计算结果反馈至区块链节点之后,在区块链节点对计算结果验签通过之后,还可以将上述密文的计算结果发送给客户端,或者将上述明文的计算结果重新加密后发送给客户端;可以理解的是,将上述计算结果发送给客户端的过程中,还可以将与上述计算结果相关的被客户端所提交的交易的相关

信息关联发送至客户端，以使客户端获知其所提交交易的相关计算结果。

[91] 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）的树根取值发生变化，而该状态树的树根会被包含于最新区块的区块头，从而实现区块链账本数据的更新，亦即相当于将该计算结果上链。

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

[93] 图 3 是一示例性实施例提供的一种链下隐私计算节点侧的链上数据的链下隐私计算方法的流程图。如图 3 所示，该方法可以包括步骤 302~步骤 306。

[94] 步骤 302，链下隐私计算节点接收区块链节点传输的经过加密的链上数据，所述链下隐私计算节点处部署了链下可信执行环境，所述链上数据由所述区块链节点根据客户端提交的交易确定。

[95] 如前所述，链下隐私计算节点可以通过预言机机制接收区块链节点传输的经过加密的链上数据；或者，链下隐私计算节点可以接收区块链节点通过客户端处预部署的链下隐私计算调用组件传输的经过加密的链上数据。

[96] 如前所述，链下隐私计算节点接收的链上数据可以被区块链节点使用区块链节点身份私钥进行签名。其中，签名验证成功被客户端或预言机服务器作为将经过加密的上述链上数据传输至链下隐私计算节点的前提条件。

[97] 如前所述，链上数据可以在被节点加密公钥加密后传输至链下隐私计算节点，且链下隐私计算节点维护有上述节点加密公钥对应的节点加密私钥。

[98] 如前所述，在链下隐私计算节点属于链下隐私计算集群的情况下，上述节点加密私钥仅被链下隐私计算节点所维护，或者上述节点加密私钥被链下隐私计算集群内的所有链下隐私计算节点共同维护。

[99] 如前所述，链下隐私计算节点接收区块链节点传输的被区块链节点使用节点加密公钥加密的链上数据；或者，链下隐私计算节点接收客户端传输的被客户端使用节点加密公钥加密的链上数据，其中链上数据是被上述区块链节点加密后传输给上述客户端的。

[100] 如前所述，链下隐私计算节点可以直接接收区块链节点发送的链上数据；或者，在链下隐私计算节点属于链下隐私计算集群的情况下，链下隐私计算节点可以接收区块链节点经过链下隐私计算集群的控制节点转发的链上数据。

[101] 步骤 304，所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果。

[102] 如前所述，链下合约的调用信息被链下隐私计算节点与链上数据关联接收，上述调用信息用于指示链下隐私计算节点通过在链下可信执行环境内执行上述链下合约对链上数据实现隐私计算；其中，调用信息包括：上述链下合约的合约 ID，或者上述链下合约的合约 ID 和链下合约内至少一个函数的函数名。

[103] 步骤 306，所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果，所述计算结果用于更新区块链账本数据。

[104] 如前所述，链下隐私计算节点可以通过预言机机制向区块链节点反馈加密后的计算结果；或者，链下隐私计算节点可以通过客户端处预部署的链下隐私计算调用组件向区块链节点反馈加密后的计算结果。

[105] 如前所述，链上数据由链下隐私计算节点在链下可信执行环境内执行预先部署的

链下合约实现隐私计算,且链下隐私计算节点维护有对应于上述链下合约的合约签名私钥;链下隐私计算节点可以使用上述合约签名私钥对计算结果进行签名,其中,区块链节点在确定针对计算结果的签名匹配于合约签名私钥的情况下,判定该计算结果可信,且将计算结果可信作为区块链节点更新账本数据的前提条件。

[106] 图 4 是一示例性实施例提供的一种客户端侧的链上数据的链下隐私计算方法的流程图。如图 4 所示,该方法可以包括步骤 402~步骤 406。

[107] 步骤 402,客户端向区块链节点提交交易,以由所述区块链节点根据所述交易确定用于隐私计算的链上数据。

[108] 步骤 404,所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下,将所述链上数据加密传输至链下隐私计算节点,所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境。

[109] 如前所述,客户端接收到的链上数据可以被区块链节点使用区块链节点身份私钥进行签名;其中,签名验证成功被客户端作为将经过加密的链上数据传输至链下隐私计算节点的前提条件。

[110] 如前所述,链下隐私计算节点维护有节点加密公钥对应的节点加密私钥,客户端可以使用上述节点加密公钥将链上数据加密后发送给链下隐私计算节点。

[111] 如前所述,客户端处预部署了链下隐私计算调用组件,客户端可以调用链下隐私计算调用组件将所述链上数据加密传输至链下隐私计算节点。

[112] 步骤 406,所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下,将所述计算结果发送给所述区块链节点用于更新区块链账本数据。

[113] 如前所述,客户端处预部署了链下隐私计算调用组件,客户端可以调用所述链下隐私计算调用组件将所述计算结果发送给所述区块链节点。

[114] 至此,链上数据下链参与链下隐私计算和链下隐私计算的计算结果上链的完整过程说明完毕。下面结合图 5 和图 6 所示的两个具体实施例对上述方法进行进一步说明。

[115] 图 5 是一示例性实施例提供的一种链上数据的链下隐私计算方法对应的各设备之间的交互流程图。如图 5 所示,由客户端向区块链节点提交交易以进行隐私计算,该方法可以包括以下步骤。

[116] 步骤 502,客户端向区块链节点发送交易。

[117] 在满足相应的触发条件后,客户端将对应的交易发送至区块链节点,上述触发条件可以为用户执行的预设操作、客户端上运行的应用程序的预设功能开启、预设时刻达到等。其中,上述用户执行的预设操作可以有多种形式,如提交交易请求、执行交易部署或反馈交易响应等;相应的,上述交易具体可以为转账、接收转账、查询历史交易信息等,本说明书对此并不进行限制。

[118] 步骤 504,区块链节点确定链上数据并将链上数据发送给客户端。

[119] 区块链节点可以在交易执行前或交易执行过程中根据接收到的交易确定用于链下隐私计算的链上数据。链上数据可以是上述交易携带的入参数据,如位于上述交易的 data 字段中的数据;也可以是上述交易指定的数据,如在上述交易调用链上合约的情况下,被调用的链上合约基于上述交易在其 data 字段中指定的交易信息查询相应的链上数据;还可以在上述交易调用链上合约的情况下,将被调用的链上合约在执行过程中的中间值或最终结果作为上述的链上数据,上述中间值或最终结果是由链上合约对上述交易携带的数据或者按照其指定信息查询到的链上数据进行处理而生成的。另外,区块链节点确定出的链上数据可能具有多种类型,如位于区块链上的区块链数据、区块链节点维护的状态数据或区块链节点维护的收据数据等,本说明书对此并不进行限制。

[120] 区块链节点在确定了链上数据后,可以先使用链下隐私计算节点的节点加密公钥对链上数据进行加密,然后使用区块链节点的区块链节点身份私钥对加密后的链上数据

进行签名,最后将上述签名和加密后的链上数据关联发送给客户端或打包后发送给客户端。也可以先使用区块链节点的节点加密私钥对链上数据进行签名,然后使用客户端的加密公钥对链上数据进行加密,最后将上述签名和加密后的链上数据关联发送给客户端或打包后发送给客户端。还可以先使用区块链节点的节点加密私钥对链上数据进行签名,然后将上述签名和明文的链上数据打包后使用客户端的加密公钥进行加密,最后将加密后的打包文件发送给客户端。另外,区块链节点除了向链下隐私计算节点结果传输链上数据之外,还可以将与上述链上数据相关联的链下合约调用请求传输给链下隐私计算节点,针对调用请求的加密和签名可以与上述链上数据关联进行,针对调用请求的加密和签名的操作方式及顺序可以针对计算结果的上述处理过程相同,对此不再赘述。

[121] 步骤 506,客户端验签通过后将链上数据转发给链下隐私计算节点。

[122] 客户端接收到上述打包数据后,首先对其中的链上数据进行验签,然后在验签成功的情况下将链上数据转发给链下隐私计算节点。对应于上述步骤 504 中的实施例,在客户端接收到关联发送的签名和加密后的链上数据的情况下,或者对接收到的打包文件进行拆分得到签名和加密后的链上数据后,一方面使用区块链节点的节点加密公钥对上述签名进行解密得到第一哈希值,另一方面,可以直接计算加密后的链上数据的第二哈希值,也可以使用客户端的加密私钥对加密后的链上数据进行解密以获取明文的链上数据,然后计算链上数据的第二哈希值。在客户端接收到加密的打包文件,且该打包文件中包含签名和非加密的链上数据的情况下,客户端可以首先使用客户端的加密私钥对上述打包文件进行解密,以得到上述签名和链上数据,然后一方面使用区块链节点的节点加密公钥解压上述签名获得链上数据对应的第一哈希值,另一方面计算链上数据的第二哈希值。在获得上述第一哈希值和第二哈希值后,将二者进行比较:若上述第一哈希值与第二哈希值相等,则说明上述打包数据确实为区块链节点发送的,且并未被其他设备篡改,验签成功;否则,若上述第一哈希值与第二哈希值不相等,则验签失败。

[123] 该实施例中,链下隐私计算节点是独立的链下隐私计算节点,在验签成功的情况下,客户端将上述链上数据转发给链下隐私计算节点。对应于上述实施例,客户端可以直接将使用链下隐私计算节点的节点加密公钥进行加密的上述链上数据转发给链下隐私计算节点。客户端也可以先使用链下隐私计算节点的节点加密公钥对上述链上数据进行加密,然后将密文的链上数据转发给链下隐私计算节点。否则,在验签失败的情况下(图中未标注),客户端可以将上述链上数据丢弃;也可以提取链上数据的数据信息生成数据验签日志,并将该数据验签日志保存在本地或反馈给区块链节点;还可以向区块链节点或其他预设对象返回错误信息或告警信息等。

[124] 该实施例中,独立的链下隐私计算节点中维护有节点加密私钥,客户端可以直接将加密后的链上数据发送给该链下隐私计算节点,由该链下隐私计算节点使用其维护的节点加密私钥在预创建的链下 TEE 中解密密文的链上数据。

[125] 步骤 508,链下隐私计算节点执行隐私计算。

[126] 链下隐私计算节点利用验签通过的链上数据在创建的链下 TEE 中执行预部署的链下合约,即进行隐私计算。具体的,链下隐私计算节点可以解密与链上数据相关联的链下合约调用请求得到标识信息等信息,然后链下隐私计算节点可以根据标识信息调用预先部署的链下合约的字节码,而在链下可信执行环境中部署有若干执行引擎的情况下,链下隐私计算节点可以根据字节码确定对应的执行引擎,并且通过确定出的执行引擎执行所述字节码以对链上数据进行链下隐私计算。

[127] 在链下隐私计算节点处创建的链下 TEE 中,可以部署有若干执行引擎,比如 EVM、WASM 虚拟机等中的一个或多个,在同时部署了多种执行引擎的情况下,客户端或区块链节点除了在链下隐私计算节点处安全存储链下合约的字节码之外,还可以向链下隐私计算节点指明用于执行该字节码的执行引擎。链下隐私计算节点可以接收客户端或区块链节点发送的与链下合约的字节码相关联的执行引擎指定信息,并根据执行引擎指定

信息为字节码设定相应的执行引擎。因而链下隐私计算节点可以在链下 TEE 中根据确定出的执行引擎对链上数据进行链下隐私计算。

[128] 本说明书中链下隐私计算节点可以使用链上数据实现用户定义的任何计算逻辑。例如，链下隐私计算节点可以通过链下合约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，链下隐私计算节点可以通过链下合约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区块链节点等，此处不再一一赘述。

[129] 上述链下合约中字节码的执行结果即为链下隐私计算的计算结果。如前所述，上述隐私计算是在链下 TEE 中进行的，相应的，上述计算结果在出链下 TEE 之前也需要进行加密。链下隐私计算节点可以使用客户端的加密公钥对计算结果进行加密，也可以使用区块链节点的节点加密公钥对计算结果进行加密。当然，计算结果也可以使用被调用链下合约的合约签名私钥或该链下隐私计算节点的节点签名私钥对计算结果进行签名，具体的加密和签名的操作顺序可以有多种可能，具体方式可参见上述实施例，此处不再一一赘述。

[130] 步骤 510，客户端将计算结果转发给区块链节点。

[131] 对应于前述由客户端将链上数据转发给链下隐私计算节点，在链下隐私计算节点完成隐私计算后，可以由客户端将计算结果转发给区块链节点。在使用链上数据进行隐私计算的链下隐私计算节点为独立的链下隐私计算节点的情况下，链下隐私计算节点直接将上述计算结果发送给客户端。在使用链上数据进行隐私计算的链下隐私计算节点归属于链下隐私计算集群的情况下，链下隐私计算节点将计算结果经过上述集群的控制节点转发给客户端。客户端接收到链下隐私计算节点或控制节点发送的计算结果后，将上述计算结果转发给区块链节点。

[132] 链下隐私计算节点除了对链下隐私计算结果进行反馈之外，链下隐私计算节点还可以对接收到与上述链上数据相关联的调用请求进行哈希运算得到第三哈希值，链下隐私计算节点将第三哈希值与上述链下隐私计算结果进行关联反馈。客户端或者区块链节点将接收到的三哈希值与生成的调用请求的第四哈希值进行比较，根据比较结果确定链下隐私计算结果是否可靠。

[133] 若第三哈希值与第四哈希值的比较结果不一致，则表明与该第三哈希值关联反馈的链下隐私计算结果不可靠；若第三哈希值与第四哈希值的比较结果一致，则需要进一步验证链下隐私计算节点或者被调用合约的签名等其他参考信息，在参考信息均正确的情况下，才能确定该链下隐私计算结果可靠。

[134] 步骤 512，区块链节点验签并将计算结果上链。

[135] 区块链节点接收到上述隐私计算的计算结果后，首先对该计算结果的签名进行可信验证。

[136] 在验签成功的情况下将计算结果上链。上链的具体方式可以包括：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）的树根取值发生变化，而该状态树的树根会被包含于最新区块的区块头，从而实现区块链账本数据的更新，亦即相当于将该计算结果上链。

[137] 在验签失败的情况下（图中未标注），区块链节点可以将上述计算结果丢弃；也可以提取计算结果的数据信息生成结果验签日志，并将该结果验签日志保存在本地，也可以向其他预设对象返回错误信息或告警信息等。

[138] 图 6 是一示例性实施例提供的另一种链上数据的链下隐私计算方法对应的各设备之间的交互流程图。如图 6 所示，由区块链节点内运行的链上合约主动调用链上数据进

行链下隐私计算，该过程实际上为通过预言机机制调用链下隐私计算的过程，该方法可以包括以下步骤。

[139] 步骤 602，链上合约主动调用链下隐私计算。

[140] 预部署在区块链节点中的链上合约在运行时，可以主动调用链下隐私计算。具体的，可以由链上合约指定需要调用的链下隐私计算节点、链下合约和/或链上数据，也可以由链上合约调用预言机合约，然后由预言机合约确定需要调用的链下隐私计算节点、链下合约和/或链上数据。其中，链上数据可以是上述交易携带的数据，如位于上述交易的 data 字段中的数据；也可以是上述交易指定的数据，如在上述交易调用链上合约的情况下，被调用的链上合约基于上述交易在其 data 字段中指定的交易信息查询相应的链上数据；还可以在上述交易调用链上合约的情况下，将被调用的链上合约在执行过程中的中间值或最终结果作为上述的链上数据，上述中间值或最终结果是由链上合约对上述交易携带的数据或者按照其指定信息查询到的链上数据进行处理而生成的。另外，区块链节点确定出的链上数据可能具有多种类型，如位于区块链上的区块链数据、区块链节点维护的状态数据或区块链节点维护的收据数据等。

[141] 步骤 604，预言机合约预处理链上数据。

[142] 针对确定的链上数据，预言机合约对其进行预处理，具体的，在链上合约处于加密状态的情况下，对上述加密的链上数据进行打包等预处理。在链上合约处于非加密状态的情况下，首先对上述未加密的链上数据进行加密，可以使用上述指定的链下隐私计算节点的节点加密公钥进行加密，也可以使用上述指定的链下隐私计算节点所归属链下隐私计算集群的控制节点的加密公钥进行加密，然后使用区块链节点的节点加密私钥对加密后的链上数据进行签名。最后，还可以对上述加密后的链上数据和对应的签名进行打包处理。

[143] 预言机合约进行的上述打包操作会触发预设的区块链事件，并被预言机服务器监听到，然后由区块链节点将经过上述预处理的打包数据以加密的方式发送给预言机服务器。该过程中，可以在预言机服务器监听到区块链事件后，向区块链节点发送链上数据获取请求并接收区块链节点返回的处于加密状态的链上数据。其中，对链上数据的具体加密方式可以为对称秘钥加密、非对称秘钥加密或数字信封加密等，可参见上文此处不再赘述。

[144] 步骤 606，预言机服务器验签并转发链上数据。

[145] 预言机服务器对接收到的链上数据进行验签，并在验签成功的情况下将密文的链上数据发送给链下隐私计算集群的控制节点。对链上数据进行验签的具体方法，请参见上述步骤 506 的记载，此处不再赘述。

[146] 步骤 608，链下隐私计算集群的控制节点接收链上数据并分配至目标节点。

[147] 该实施例中，链下隐私计算集群包含一控制节点，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。在接收到链上数据后，控制节点首先从集群中确定某一链下隐私计算节点作为使用链上数据进行隐私计算的节点（记为目标节点），然后将上述链上数据发送至该目标节点。

[148] 在接收到与上述链上数据关联发送的链下隐私计算节点的节点 ID 或节点编号等指定信息的情况下，控制节点将与上述指定信息确定相匹配的链下隐私计算节点作为目标节点；在未接收到与上述链上数据相关联的指定信息的情况下，控制节点按照集群内各节点的当前负载值（如当前运算量、当前时刻起预设时间段内的预期计算量、当前计算任务个数等）确定目标节点，如将当前负载值最小的节点确定为目标节点、将当前负载值小于某一负载值阈值的所有节点中的任一节点确定为目标节点等。

[149] 在确定了目标节点后，控制节点将链上数据发送至目标节点。在目标节点维护有加密链上数据所使用的节点加密公钥对应的节点加密私钥的情况下，控制节点直接将上述链上数据转发至目标节点。在目标节点并未维护加密链上数据所使用的节点加密公钥

对应的节点加密私钥的情况下，控制节点首先在自身的链下 TEE 中使用上述节点加密私钥解密密文的链上数据，然后在链下 TEE 中使用与目标节点预协商的秘钥将明文的链上数据再次加密后发送给目标节点。

[150] 步骤 610，链下隐私计算节点执行隐私计算。

[151] 链下隐私计算节点使用接收到的链上数据执行隐私计算的具体方法，请参见上述步骤 508 的记载，此处不再赘述。

[152] 步骤 612，控制节点接收计算结果并将其发送至预言机服务器。

[153] 控制节点接收到的计算结果通常已经被目标节点所加密，控制节点首先需要根据该计算结果加密使用的秘钥不同进行不同的处理。在计算结果被目标节点使用区块链节点身份公钥或预言机服务器的公钥加密的情况下，控制节点直接将该计算结果转发给预言机服务器。在计算结果被目标节点使用控制节点的公钥加密的情况下，控制节点首先在自身的链下 TEE 中使用与上述公钥对应的私钥解密密文的计算结果，然后在链下 TEE 中使用预言机服务器的公钥或区块链节点的区块链节点身份公钥将明文的链上数据再次加密后发送给预言机服务器。

[154] 步骤 614，预言机服务器转发计算结果。

[155] 预言机服务器接收到控制节点发送的加密状态的计算结果后，根据该计算结果加密使用的秘钥不同进行不同的处理。在计算结果被目标节点或控制节点使用区块链节点身份公钥加密的情况下，预言机服务器直接将该计算结果转发给区块链节点。在计算结果被控制节点所维护的公钥加密的情况下，预言机服务器首先在自身的链下 TEE 中使用与上述公钥对应的私钥解密密文的计算结果，然后在链下 TEE 中使用区块链节点的区块链节点身份公钥将明文的链上数据再次加密后发送给区块链节点。

[156] 步骤 616，区块链节点验签并将计算结果上链。

[157] 区块链节点接收计算结果后，首先对计算结果进行验签，然后在验签通过的情况下根据计算结果更新区块链账本数据，即将计算结果上链。上链的具体过程请参见上述步骤 512 的记载，此处不再赘述。

[158] 图 7 是本说明书一示例性实施例示出的一种电子设备的结构示意图。请参考图 7，在硬件层面，该电子设备包括处理器 702、内部总线 704、网络接口 706、内存 708 以及非易失性存储器 710，当然还可能包括其他业务所需要的硬件。处理器 702 从非易失性存储器 710 中读取对应的计算机程序到内存 708 中并运行，在逻辑层面上形成链上数据的链下隐私计算装置。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[159] 请参考图 8，在区块链节点侧的软件实施方式中，该链上数据的链下隐私计算装置可以包括：链上数据确定单元 801，使区块链节点根据客户端提交的交易，确定用于隐私计算的链上数据；链上数据传输单元 802，使所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；计算结果获取单元 803，使所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，并根据所述计算结果更新区块链账本数据。

[160] 可选的，所述链上数据传输单元 802 具体用于：使所述区块链节点通过预言机机制将经过加密的所述链上数据传输至链下隐私计算节点；或者，使所述区块链节点通过所述客户端处预部署的链下隐私计算调用组件，将经过加密的所述链上数据传输至所述链下隐私计算节点。

[161] 可选的，还包括：链上数据签名单元 804，使所述区块链节点使用区块链节点身份私钥对所述链上数据进行签名；其中，签名验证成功被所述客户端或预言机服务器作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件。

[162]可选的,所述链上数据被节点加密公钥加密后传输至所述链下隐私计算节点,且所述链下隐私计算节点维护有所述节点加密公钥对应的节点加密私钥。

[163]可选的,在所述链下隐私计算节点属于链下隐私计算集群的情况下,所述节点加密私钥仅被所述链下隐私计算节点所维护,或者所述节点加密私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

[164]可选的,所述链上数据传输单元 802 具体用于:使所述区块链节点使用所述节点加密公钥加密所述链上数据,并将经过加密的所述链上数据传输至所述链下隐私计算节点;或者,使所述区块链节点将所述链上数据加密后发送给所述客户端,所述链上数据由所述客户端使用所述节点加密公钥加密后传输至所述链下隐私计算节点。

[165]可选的,所述链上数据传输单元 802 具体用于:使所述区块链节点将所述链上数据直接发送给所述链下隐私计算节点;或者,在所述链下隐私计算节点属于链下隐私计算集群的情况下,使所述区块链节点将所述链上数据经过所述链下隐私计算集群的控制节点转发给所述链下隐私计算节点。

[166]可选的,所述计算结果获取单元 803 具体用于:使所述区块链节点通过预言机机制获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果;或者,使所述区块链节点通过所述客户端处预部署的链下隐私计算调用组件获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果。

[167]可选的,所述链上数据由所述链下隐私计算节点在链下可信执行环境内执行预先部署的链下合约实现隐私计算,且所述链下隐私计算节点维护有对应于所述链下合约的合约签名私钥;还包括:计算结果验签单元 805,使所述区块链节点在确定针对计算结果的签名匹配于合约签名私钥的情况下,判定所述计算结果可信,且计算结果可信为区块链节点更新账本数据的前提条件。

[168]请参考图 9,在链下隐私计算节点侧的软件实施方式中,该链上数据的链下隐私计算装置可以包括:链上数据接收单元 901,使链下隐私计算节点接收区块链节点传输的经过加密的链上数据,所述链下隐私计算节点处部署了链下可信执行环境,所述链上数据由所述区块链节点根据客户端提交的交易确定;隐私计算执行单元 902,使所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果;计算结果反馈单元 903,使所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果,所述计算结果用于更新区块链账本数据。

[169]可选的,所述链上数据接收单元 901 具体用于:使链下隐私计算节点通过预言机机制接收区块链节点传输的经过加密的链上数据;或者,使链下隐私计算节点接收区块链节点通过客户端处预部署的链下隐私计算调用组件传输的经过加密的链上数据。

[170]可选的,所述链下隐私计算单元接收的所述链上数据被所述区块链节点使用区块链节点身份私钥进行签名;其中,签名验证成功被所述客户端或预言机服务器作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件。

[171]可选的,所述链上数据被节点加密公钥加密后传输至所述链下隐私计算节点,且所述链下隐私计算节点维护有所述节点加密公钥对应的节点加密私钥。

[172]可选上,所述在所述链下隐私计算节点属于链下隐私计算集群的情况下,所述节点加密私钥仅被所述链下隐私计算节点所维护,或者所述节点加密私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

[173]可选的,所述链上数据接收单元 901 具体用于:使所述链下隐私计算节点接收所述区块链节点传输的被所述区块链节点使用所述节点加密公钥加密的所述链上数据;或者,

[174]使所述链下隐私计算节点接收所述客户端传输的被所述客户端使用所述节点加密公钥加密的所述链上数据,其中所述链上数据是被所述区块链节点加密后传输给所述客户端的。

[175]可选的,所述链上数据接收单元 901 具体用于:使所述链下隐私计算节点直接接收所述区块链节点发送的所述链上数据;或者,在所述链下隐私计算节点属于链下隐私计算集群的情况下,使所述链下隐私计算节点接收所述区块链节点经过所述控制节点转发的所述链上数据。

[176]可选的,所述计算结果反馈单元 903 具体用于:使所述链下隐私计算节点通过预言机机制向所述区块链节点反馈加密后的所述计算结果;或者,使所述链下隐私计算节点通过所述客户端处预部署的链下隐私计算调用组件向所述区块链节点反馈加密后的所述计算结果。

[177]可选的,所述链上数据由所述链下隐私计算节点在链下可信执行环境内执行预先部署的链下合约实现隐私计算,且所述链下隐私计算节点维护有对应于所述链下合约的合约签名私钥;还包括:计算结果签名单元 904,使所述链下隐私计算节点使用所述合约签名私钥对所述计算结果进行签名,其中,所述区块链节点在确定针对计算结果的签名匹配于合约签名私钥的情况下,判定所述计算结果可信,且将计算结果可信作为区块链节点更新账本数据的前提条件。

[178]可选的,所述链下合约的调用信息被所述链下隐私计算节点与所述链上数据关联接收,所述调用信息用于指示链下隐私计算节点通过在链下可信执行环境内执行所述链下合约对链上数据实现隐私计算;其中,所述调用信息包括:所述链下合约的合约 ID,或者所述链下合约的合约 ID 和所述链下合约内至少一个函数的函数名。

[179]请参考图 10,在客户端侧的软件实施方式中,该链上数据的链下隐私计算装置可以包括:交易提交单元 1001,使客户端向区块链节点提交交易,以由所述区块链节点根据所述交易确定用于隐私计算的链上数据;链上数据转发单元 1002,使所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下,将所述链上数据加密传输至链下隐私计算节点,所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境;计算结果转发单元 1003,使所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下,将所述计算结果发送给所述区块链节点,用于更新区块链账本数据。

[180]可选的,还包括:链上数据验签单元 1004,使所述客户端使用所述区块链节点公钥对接收到的所述链上数据进行签名验证,签名验证成功被所述客户端作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件,其中,所述链上数据被所述区块链节点使用区块链节点身份私钥进行签名。

[181]可选的,所述链下隐私计算节点维护有节点加密公钥对应的节点加密私钥,所述链上数据转发单元 1002 具体用于:使所述客户端使用所述节点加密公钥将所述链上数据加密后发送给所述链下隐私计算节点。

[182]可选的,所述客户端处预部署了链下隐私计算调用组件,所述链上数据转发单元 1002 具体用于:使所述客户端调用所述链下隐私计算调用组件将所述链上数据加密传输至链下隐私计算节点。

[183]可选的,所述客户端处预部署了链下隐私计算调用组件,所述计算结果转发单元 1003 具体用于:使所述客户端调用所述链下隐私计算调用组件将所述计算结果发送给所述区块链节点。

[184]上述装置中各个单元的功能和作用的实现过程详见上述方法中对应步骤的实现过程,在此不再赘述。

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

[186] 在一个典型的配置中，电子设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[187] 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。

[188] 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，磁带磁盘存储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。

[189] 对于上述装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[190] 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，第一哈希值也可以被称为第二哈希值，类似地，第二哈希值也可以被称为第一哈希值。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”。

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

## 权利要求书

1、一种链上数据的链下隐私计算方法，包括：

区块链节点根据客户端提交的交易，确定用于隐私计算的链上数据；

所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；

所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，并根据所述计算结果更新区块链账本数据。

2、根据权利要求1所述的方法，所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，包括：

所述区块链节点通过预言机机制将经过加密的所述链上数据传输至链下隐私计算节点；或者，

所述区块链节点通过所述客户端处预部署的链下隐私计算调用组件，将经过加密的所述链上数据传输至所述链下隐私计算节点。

3、根据权利要求2所述的方法，还包括：

所述区块链节点使用区块链节点身份私钥对所述链上数据进行签名；

其中，签名验证成功被所述客户端或预言机服务器作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件。

4、根据权利要求1所述的方法，所述链上数据被节点加密公钥加密后传输至所述链下隐私计算节点，且所述链下隐私计算节点维护有所述节点加密公钥对应的节点加密私钥。

5、根据权利要求4所述的方法，在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述节点加密私钥仅被所述链下隐私计算节点所维护，或者所述节点加密私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

6、根据权利要求4所述的方法，所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，包括：

所述区块链节点使用所述节点加密公钥加密所述链上数据，并将经过加密的所述链上数据传输至所述链下隐私计算节点；或者，

所述区块链节点将所述链上数据加密后发送给所述客户端，所述链上数据由所述客户端使用所述节点加密公钥加密后传输至所述链下隐私计算节点。

7、根据权利要求1所述的方法，所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，包括：

所述区块链节点将所述链上数据直接发送给所述链下隐私计算节点；或者，

在所述链下隐私计算节点属于链下隐私计算集群的情况下，所述区块链节点将所述链上数据经过所述链下隐私计算集群的控制节点转发给所述链下隐私计算节点。

8、根据权利要求1所述的方法，所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，包括：

所述区块链节点通过预言机机制获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果；或者，

所述区块链节点通过所述客户端处预部署的链下隐私计算调用组件获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果。

9、根据权利要求1所述的方法，所述链上数据由所述链下隐私计算节点在链下可信执行环境内执行预先部署的链下合约实现隐私计算，且所述链下隐私计算节点维护有对应于所述链下合约的合约签名私钥；所述方法还包括：

所述区块链节点在确定针对计算结果的签名匹配于合约签名私钥的情况下，判定所述计算结果可信，且计算结果可信为区块链节点更新账本数据的前提条件。

10、根据权利要求9所述的方法，所述链下合约的调用信息被与所述链上数据关联

传输至链下隐私计算节点,所述调用信息用于指示链下隐私计算节点通过在链下可信执行环境内执行所述链下合约对链上数据实现隐私计算;其中,所述调用信息包括:所述链下合约的合约ID,或者所述链下合约的合约ID和所述链下合约内至少一个函数的函数名。

11、一种链上数据的链下隐私计算方法,包括:

链下隐私计算节点接收区块链节点传输的经过加密的链上数据,所述链下隐私计算节点处部署了链下可信执行环境,所述链上数据由所述区块链节点根据客户端提交的交易确定;

所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果;

所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果,所述计算结果用于更新区块链账本数据。

12、根据权利要求11所述的方法,所述链下隐私计算节点接收区块链节点传输的经过加密的链上数据,包括:

链下隐私计算节点通过预言机机制接收区块链节点传输的经过加密的链上数据;或者,

链下隐私计算节点接收区块链节点通过客户端处预部署的链下隐私计算调用组件传输的经过加密的链上数据。

13、根据权利要求12所述的方法,还包括:

所述链下隐私计算节点接收的所述链上数据被所述区块链节点使用区块链节点身份私钥进行签名;

其中,签名验证成功被所述客户端或预言机服务器作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件。

14、根据权利要求11所述的方法,所述链上数据被节点加密公钥加密后传输至所述链下隐私计算节点,且所述链下隐私计算节点维护有所述节点加密公钥对应的节点加密私钥。

15、根据权利要求14所述的方法,在所述链下隐私计算节点属于链下隐私计算集群的情况下,所述节点加密私钥仅被所述链下隐私计算节点所维护,或者所述节点加密私钥被所述链下隐私计算集群内的所有链下隐私计算节点共同维护。

16、根据权利要求14所述的方法,所述链下隐私计算节点接收区块链节点传输的经过加密的链上数据,包括:

所述链下隐私计算节点接收所述区块链节点传输的被所述区块链节点使用所述节点加密公钥加密的所述链上数据;或者,

所述链下隐私计算节点接收所述客户端传输的被所述客户端使用所述节点加密公钥加密的所述链上数据,其中所述链上数据是被所述区块链节点加密后传输给所述客户端的。

17、根据权利要求11所述的方法,所述链下隐私计算节点接收区块链节点传输的经过加密的链上数据,包括:

所述链下隐私计算节点直接接收所述区块链节点发送的所述链上数据;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区块链节点经过所述链下隐私计算集群的控制节点转发的所述链上数据。

18、根据权利要求11所述的方法,所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果,包括:

所述链下隐私计算节点通过预言机机制向所述区块链节点反馈加密后的所述计算结果;或者,

所述链下隐私计算节点通过所述客户端处预部署的链下隐私计算调用组件向所述

区块链节点反馈加密后的所述计算结果。

19、根据权利要求 11 所述的方法，所述链上数据由所述链下隐私计算节点在链下可信执行环境内执行预先部署的链下合约实现隐私计算，且所述链下隐私计算节点维护有对应于所述链下合约的合约签名私钥；所述方法还包括：

所述链下隐私计算节点使用所述合约签名私钥对所述计算结果进行签名，其中，所述区块链节点在确定针对计算结果的签名匹配于合约签名私钥的情况下，判定所述计算结果可信，且将计算结果可信作为区块链节点更新账本数据的前提条件。

20、根据权利要求 19 所述的方法，所述链下合约的调用信息被所述链下隐私计算节点与所述链上数据关联接收，所述调用信息用于指示链下隐私计算节点通过在链下可信执行环境内执行所述链下合约对链上数据实现隐私计算；其中，所述调用信息包括：所述链下合约的合约 ID，或者所述链下合约的合约 ID 和所述链下合约内至少一个函数的函数名。

21、一种链上数据的链下隐私计算方法，包括：

客户端向区块链节点提交交易，以由所述区块链节点根据所述交易确定用于隐私计算的链上数据；

所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下，将所述链上数据加密传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；

所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下，将所述计算结果发送给所述区块链节点用于更新区块链账本数据。

22、根据权利要求 21 所述的方法，还包括：

所述客户端接收到的所述链上数据被所述区块链节点使用区块链节点身份私钥进行签名；

其中，签名验证成功被所述客户端作为将经过加密的所述链上数据传输至所述链下隐私计算节点的前提条件。

23、根据权利要求 21 所述的方法，所述链下隐私计算节点维护有节点加密公钥对应的节点加密私钥，所述将所述链上数据加密传输至链下隐私计算节点，包括：

所述客户端使用所述节点加密公钥将所述链上数据加密后发送给所述链下隐私计算节点。

24、根据权利要求 21 所述的方法，所述客户端处预部署了链下隐私计算调用组件，所述将所述链上数据加密传输至链下隐私计算节点，包括：

调用所述链下隐私计算调用组件将所述链上数据加密传输至链下隐私计算节点。

25、根据权利要求 21 所述的方法，所述客户端处预部署了链下隐私计算调用组件，所述将所述计算结果发送给所述区块链节点，包括：

调用所述链下隐私计算调用组件将所述计算结果发送给所述区块链节点。

26、一种链上数据的链下隐私计算装置，包括：

链上数据确定单元，使区块链节点根据客户端提交的交易，确定用于隐私计算的链上数据；

链上数据传输单元，使所述区块链节点将经过加密的所述链上数据传输至链下隐私计算节点，所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境；

计算结果获取单元，使所述区块链节点获取所述链下隐私计算节点在所述链下可信执行环境内生成并加密后反馈的计算结果，并根据所述计算结果更新区块链账本数据。

27、一种链上数据的链下隐私计算装置，包括：

链上数据接收单元，使链下隐私计算节点接收区块链节点传输的经过加密的链上数

据,所述链下隐私计算节点处部署了链下可信执行环境,所述链上数据由所述区块链节点根据客户端提交的交易确定;

隐私计算执行单元,使所述链下隐私计算节点在所述链下可信执行环境内对所述链上数据执行隐私计算生成计算结果;

计算结果反馈单元,使所述链下隐私计算节点向所述区块链节点反馈加密后的所述计算结果,所述计算结果用于更新区块链账本数据。

28、一种链上数据的链下隐私计算装置,包括:

交易提交单元,使客户端向区块链节点提交交易,以由所述区块链节点根据所述交易确定用于隐私计算的链上数据;

链上数据转发单元,使所述客户端在接收到所述区块链节点发送的经过加密的所述链上数据的情况下,将所述链上数据加密传输至链下隐私计算节点,所述链下隐私计算节点处部署了用于对所述链上数据执行隐私计算的链下可信执行环境;

计算结果转发单元,使所述客户端在接收到所述链下隐私计算节点在所述链下可信执行环境中生成并加密传输的计算结果的情况下,将所述计算结果发送给所述区块链节点,用于更新区块链账本数据。

29、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,所述处理器被配置为实现如权利要求 1-25 中任一项所述的方法。

30、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 1-25 中任一项所述方法的步骤。

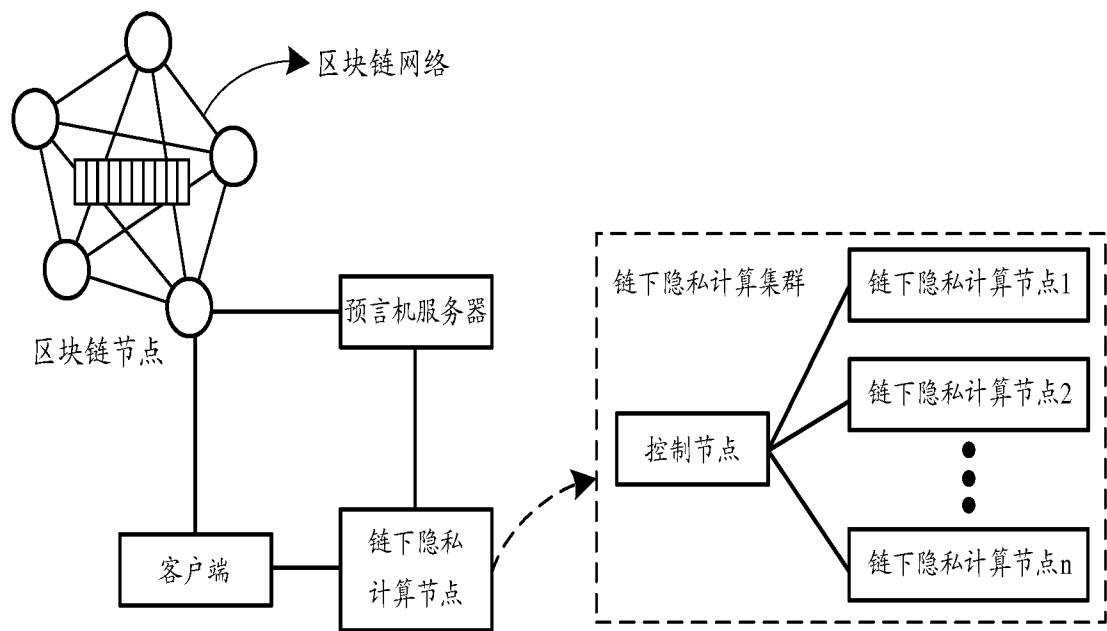


图 1

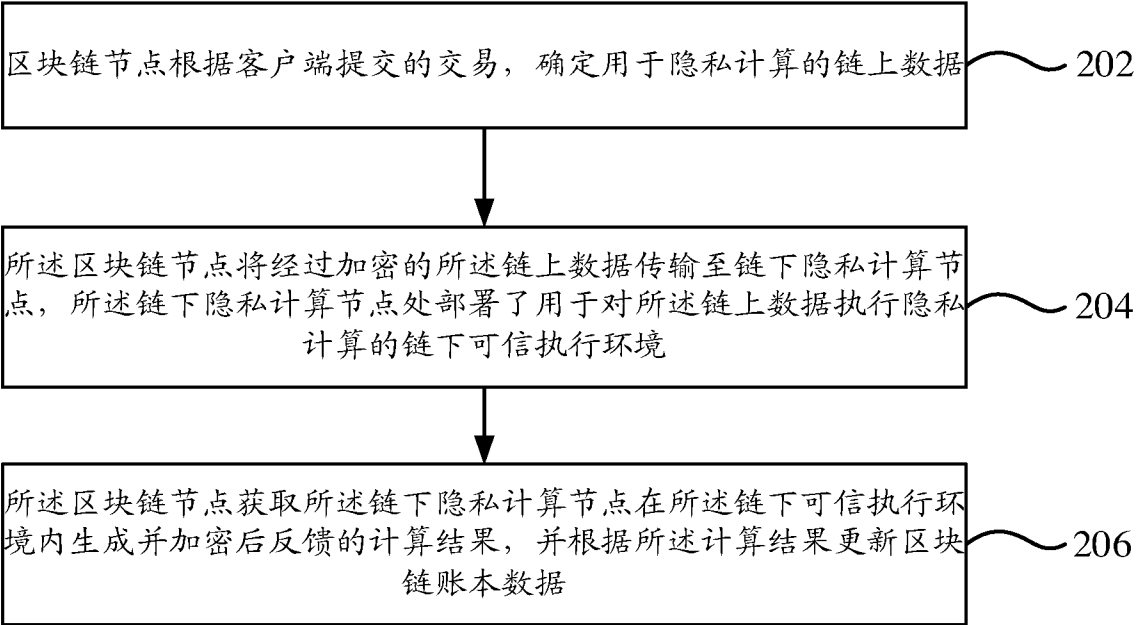


图 2

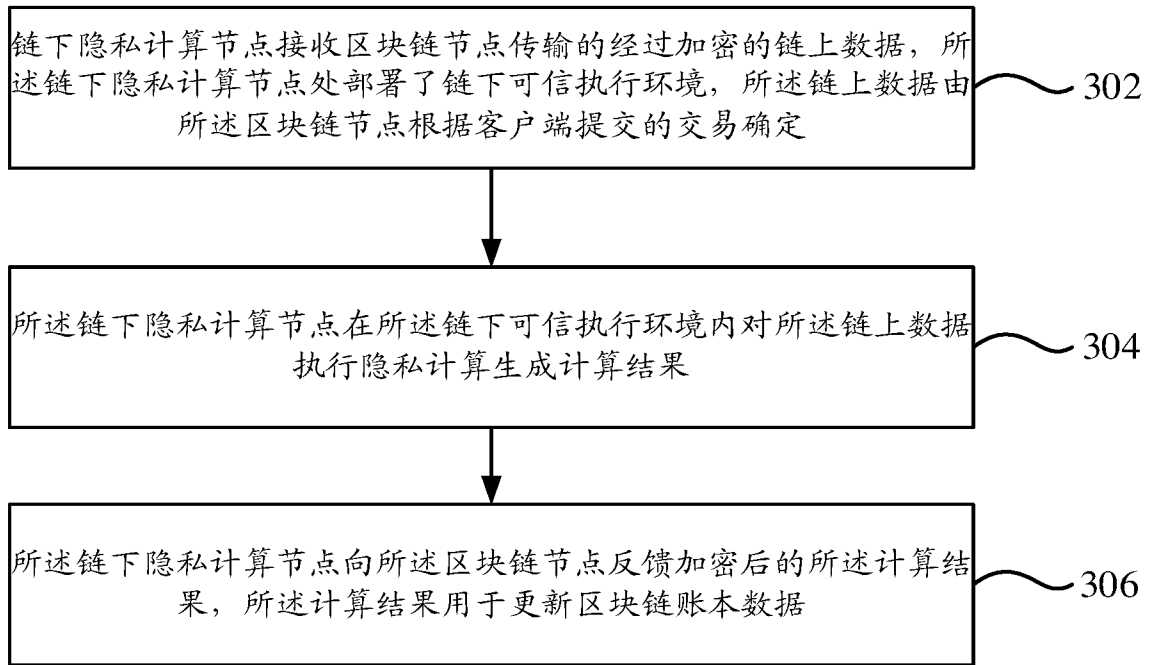


图 3

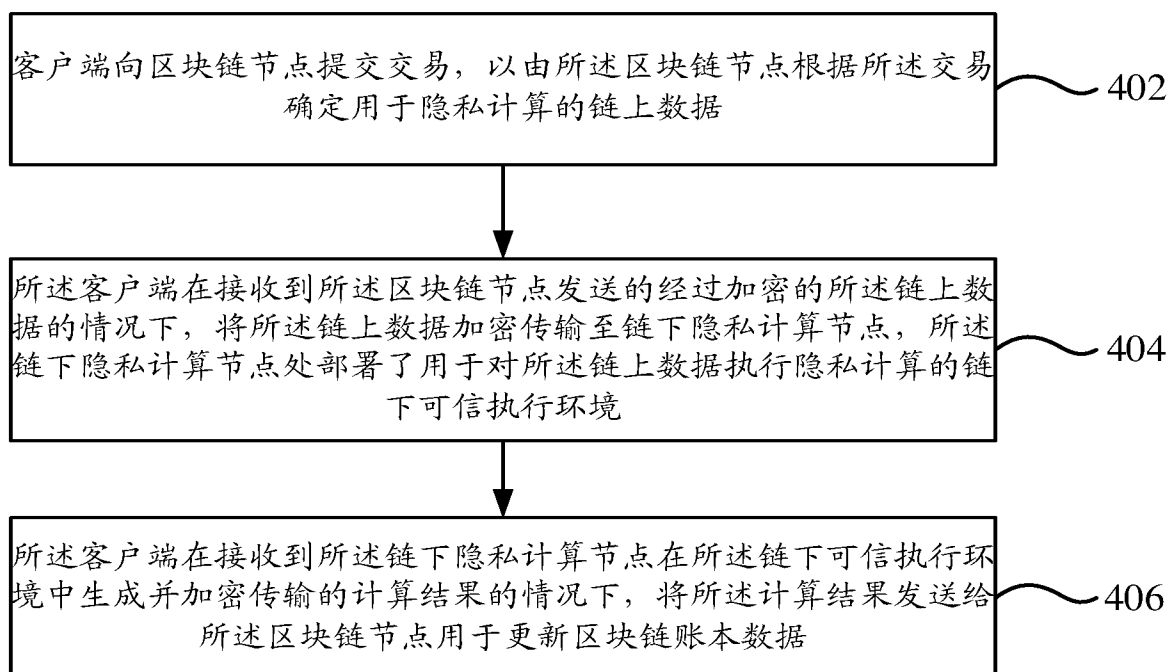


图 4

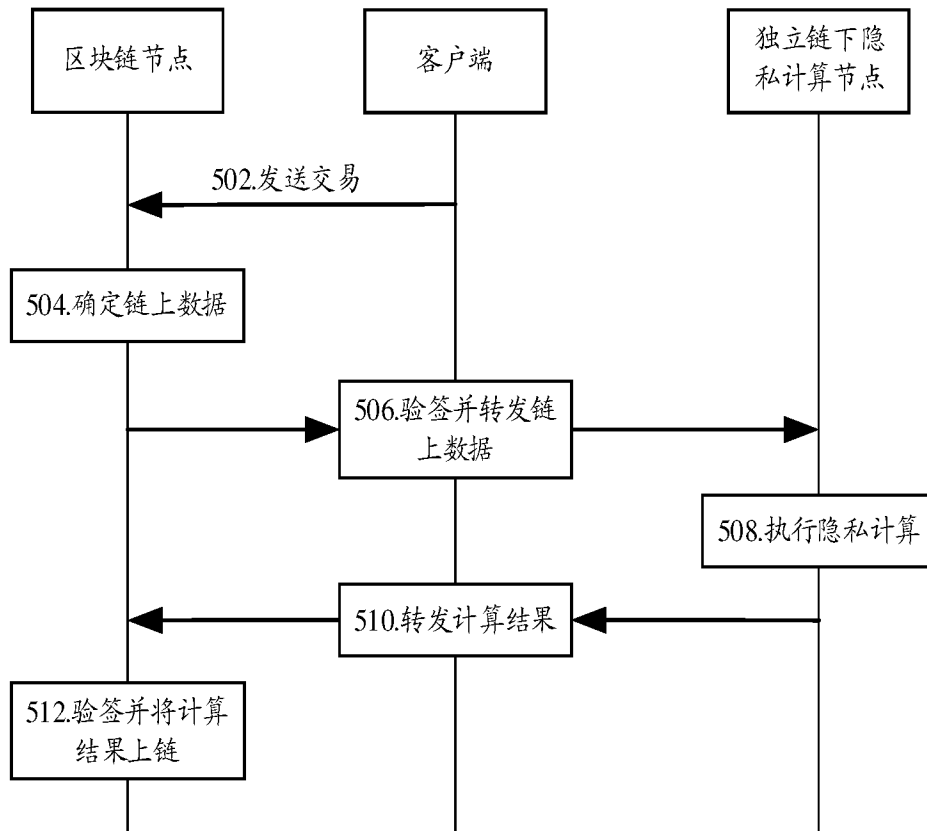


图 5

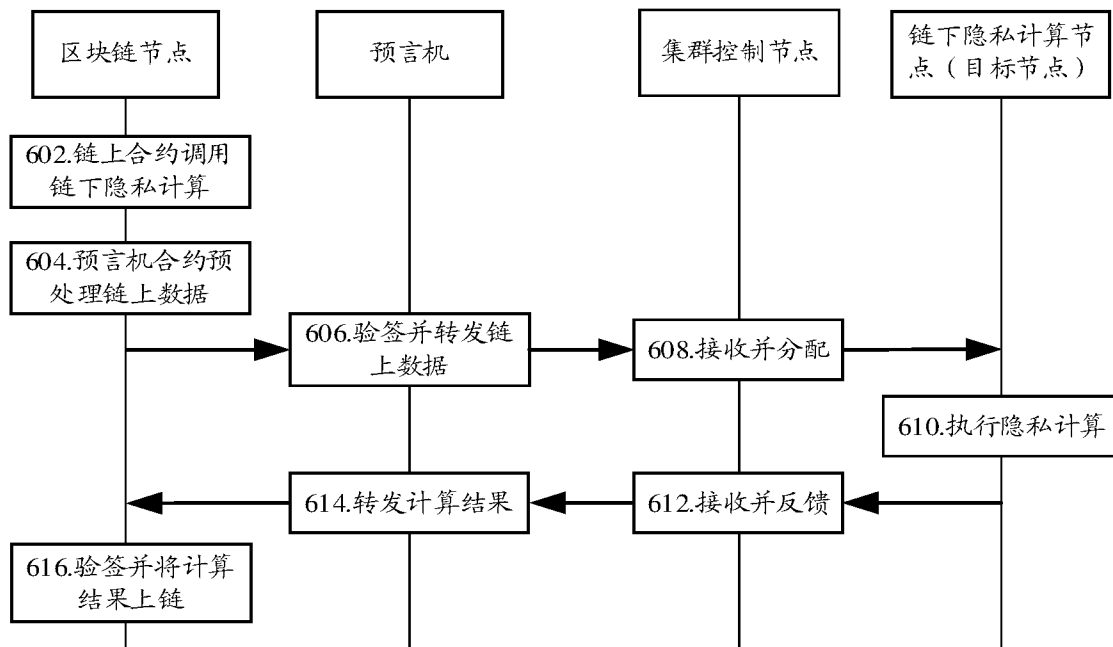


图 6

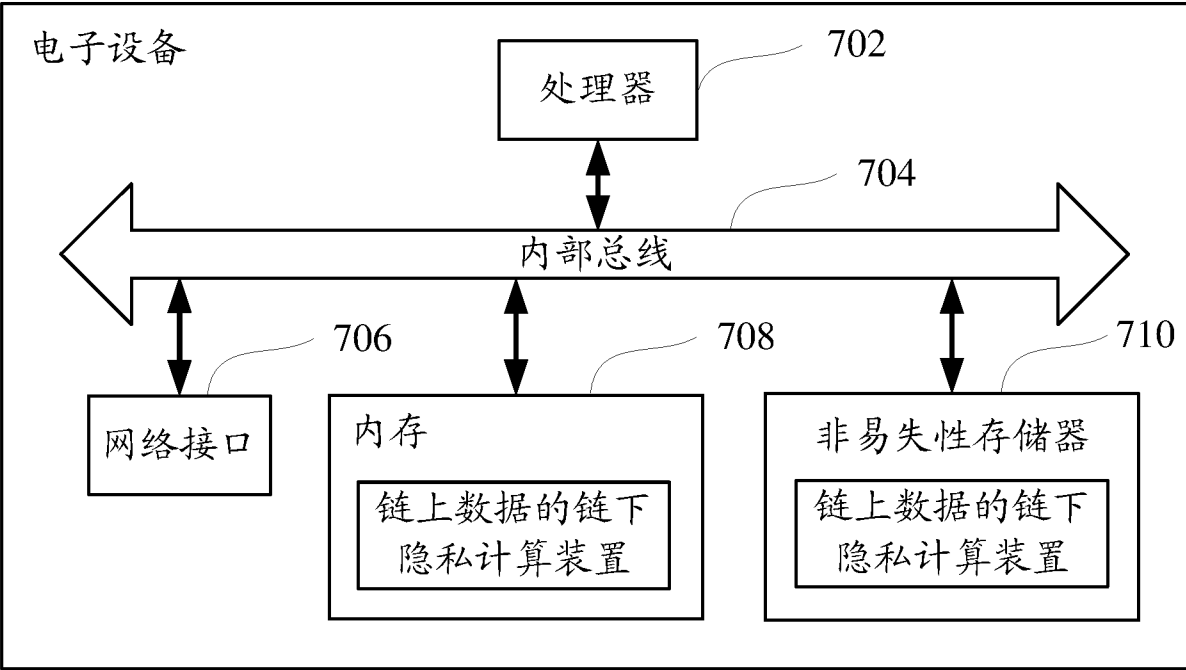


图 7

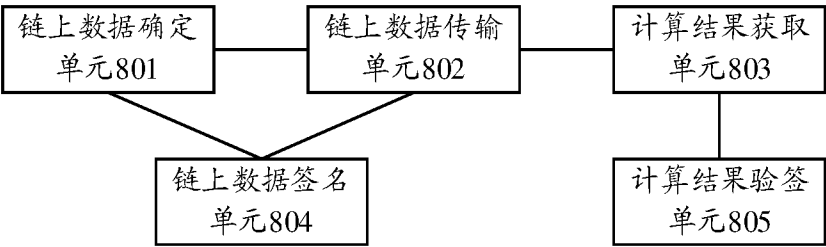


图 8



图 9

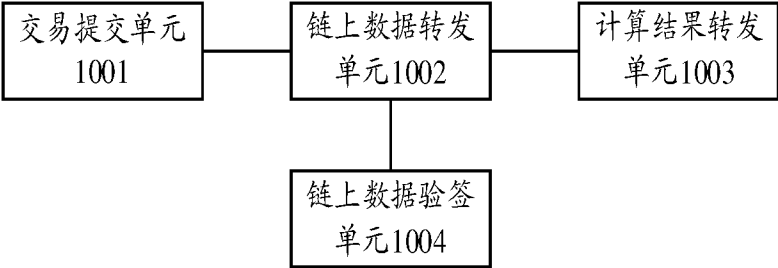


图 10

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/074245

**A. CLASSIFICATION OF SUBJECT MATTER**

G06Q 40/04(2012.01)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)

G06Q, G06F

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

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

CNPAT, CNKI, WPI, EPODOC, IEEE: 区块链, 可信执行环境, 隐私, 链上, 链下, 链外, block chain, trusted execution environment, private

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                      | Relevant to claim No.             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| PX        | CN 111047450 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.)<br>21 April 2020 (2020-04-21)<br>claims 1-30                                        | 1-30                              |
| X         | CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019<br>(2019-11-29)<br>description paragraphs [0063]-[0130], [0147], [0162], figures 1-4, 6 | 1, 3-7, 9-11, 13-17, 19-23, 26-30 |
| Y         | CN 110520884 A (ALIBABA GROUP HOLDING LIMITED) 29 November 2019<br>(2019-11-29)<br>description paragraphs [0063]-[0130], [0147], [0162], figures 1-4, 6 | 2, 8, 12, 18, 24-25               |
| Y         | CN 109670335 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.)<br>23 April 2019 (2019-04-23)<br>description, paragraph [0027]                      | 2, 8, 12, 18, 24-25               |
| A         | CN 110033368 A (ALIBABA GROUP HOLDING LIMITED) 19 July 2019 (2019-07-19)<br>entire document                                                             | 1-30                              |
| A         | CN 110851870 A (NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY OF PLA.) 28<br>February 2020 (2020-02-28)<br>entire document                                  | 1-30                              |



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

13 April 2021

Date of mailing of the international search report

29 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

International application No.

PCT/CN2021/074245

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages       | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------|-----------------------|
| A         | WO 2019182219 A1 (YOUMETECH CO., LTD.) 26 September 2019 (2019-09-26)<br>entire document | 1-30                  |
| <hr/>     |                                                                                          |                       |

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2021/074245**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |               |    | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|---------------|----|--------------------------------------|
| CN                                        | 111047450  | A  | 21 April 2020                        | None                    |               |    |                                      |
| CN                                        | 110520884  | A  | 29 November 2019                     | US                      | 2019279206    | A1 | 12 September 2019                    |
|                                           |            |    |                                      | WO                      | 2019072297    | A2 | 18 April 2019                        |
|                                           |            |    |                                      | EP                      | 3563329       | A2 | 06 November 2019                     |
|                                           |            |    |                                      | MX                      | 2019008597    | A  | 09 September 2019                    |
|                                           |            |    |                                      | CA                      | 3049924       | A1 | 18 April 2019                        |
|                                           |            |    |                                      | SG                      | 11201906754 S | A  | 27 August 2019                       |
|                                           |            |    |                                      | BR                      | 112019014847  | A2 | 14 April 2020                        |
|                                           |            |    |                                      | KR                      | 20200074910   | A  | 25 June 2020                         |
|                                           |            |    |                                      | PH                      | 12019501714   | A1 | 09 March 2020                        |
|                                           |            |    |                                      | AU                      | 2018347199    | A1 | 02 July 2020                         |
|                                           |            |    |                                      | JP                      | 2020516104    | A  | 28 May 2020                          |
|                                           |            |    |                                      | RU                      | 2729700       | C1 | 11 August 2020                       |
| CN                                        | 109670335  | A  | 23 April 2019                        | None                    |               |    |                                      |
| CN                                        | 110033368  | A  | 19 July 2019                         | WO                      | 2020108138    | A1 | 04 June 2020                         |
|                                           |            |    |                                      | CN                      | 111899102     | A  | 06 November 2020                     |
|                                           |            |    |                                      | TW                      | 202023235     | A  | 16 June 2020                         |
| CN                                        | 110851870  | A  | 28 February 2020                     | None                    |               |    |                                      |
| WO                                        | 2019182219 | A1 | 26 September 2019                    | KR                      | 102020986     | B1 | 04 November 2019                     |

## 国际检索报告

国际申请号

PCT/CN2021/074245

| <b>A. 主题的分类</b><br>G06Q 40/04 (2012.01) i<br><br>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>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>G06Q, G06F<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>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))<br>CNPAT, CNKI, WPI, EPODOC, IEEE: 区块链, 可信执行环境, 隐私, 链上, 链下, 链外, block chain, trusted execution environment, private                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                          |                                      |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| <b>C. 相关文件</b> <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 111047450 A (支付宝杭州信息技术有限公司) 2020年 4月 21日 (2020 - 04 - 21)<br/>权利要求1-30</td> <td>1-30</td> </tr> <tr> <td>X</td> <td>CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29)<br/>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6</td> <td>1, 3-7, 9-11, 13-17, 19-23, 26-30</td> </tr> <tr> <td>Y</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)<br/>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6</td> <td>2, 8, 12, 18, 24-25</td> </tr> <tr> <td>Y</td> <td>CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23)<br/>说明书第[0027]段</td> <td>2, 8, 12, 18, 24-25</td> </tr> <tr> <td>A</td> <td>CN 110033368 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19)<br/>全文</td> <td>1-30</td> </tr> <tr> <td>A</td> <td>CN 110851870 A (中国人民解放军国防科技大学) 2020年 2月 28日 (2020 - 02 - 28)<br/>全文</td> <td>1-30</td> </tr> <tr> <td>A</td> <td>WO 2019182219 A1 (YOUMETECH CO., LTD.) 2019年 9月 26日 (2019 - 09 - 26)<br/>全文</td> <td>1-30</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 111047450 A (支付宝杭州信息技术有限公司) 2020年 4月 21日 (2020 - 04 - 21)<br>权利要求1-30 | 1-30 | X | CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29)<br>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6 | 1, 3-7, 9-11, 13-17, 19-23, 26-30 | 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)<br>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6 | 2, 8, 12, 18, 24-25 | Y | CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23)<br>说明书第[0027]段 | 2, 8, 12, 18, 24-25 | A | CN 110033368 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19)<br>全文 | 1-30 | A | CN 110851870 A (中国人民解放军国防科技大学) 2020年 2月 28日 (2020 - 02 - 28)<br>全文 | 1-30 | A | WO 2019182219 A1 (YOUMETECH CO., LTD.) 2019年 9月 26日 (2019 - 09 - 26)<br>全文 | 1-30 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 引用文件, 必要时, 指明相关段落                                                                                        | 相关的权利要求                              |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| PX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CN 111047450 A (支付宝杭州信息技术有限公司) 2020年 4月 21日 (2020 - 04 - 21)<br>权利要求1-30                                 | 1-30                                 |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | CN 110520884 A (阿里巴巴集团控股有限公司) 2019年 11月 29日 (2019 - 11 - 29)<br>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6 | 1, 3-7, 9-11, 13-17, 19-23, 26-30    |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| 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)<br>说明书第[0063]-[0130]、[0147]、[0162]段, 图1-4、6 | 2, 8, 12, 18, 24-25                  |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | CN 109670335 A (众安信息技术服务有限公司) 2019年 4月 23日 (2019 - 04 - 23)<br>说明书第[0027]段                               | 2, 8, 12, 18, 24-25                  |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | CN 110033368 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19)<br>全文                                        | 1-30                                 |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | CN 110851870 A (中国人民解放军国防科技大学) 2020年 2月 28日 (2020 - 02 - 28)<br>全文                                       | 1-30                                 |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | WO 2019182219 A1 (YOUMETECH CO., LTD.) 2019年 9月 26日 (2019 - 09 - 26)<br>全文                               | 1-30                                 |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                          |                                      |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 同族专利的文件                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                          |                                      |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| 国际检索实际完成的日期<br>2021年 4月 13日                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                          | 国际检索报告邮寄日期<br>2021年 4月 29日           |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局 (ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                          | 授权官员<br>杨莹莹<br>电话号码 86-(10)-53961527 |      |                   |         |    |                                                                          |      |   |                                                                                                          |                                   |   |                                                                                                          |                     |   |                                                                            |                     |   |                                                                   |      |   |                                                                    |      |   |                                                                            |      |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2021/074245

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 | 公布日<br>(年/月/日)               |
|-------------|------------|----|----------------|------|------------------------------|
| CN          | 111047450  | A  | 2020年 4月 21日   | 无    |                              |
| CN          | 110520884  | A  | 2019年 11月 29日  | US   | 2019279206 A1 2019年 9月 12日   |
|             |            |    |                | WO   | 2019072297 A2 2019年 4月 18日   |
|             |            |    |                | EP   | 3563329 A2 2019年 11月 6日      |
|             |            |    |                | MX   | 2019008597 A 2019年 9月 9日     |
|             |            |    |                | CA   | 3049924 A1 2019年 4月 18日      |
|             |            |    |                | SG   | 11201906754S A 2019年 8月 27日  |
|             |            |    |                | BR   | 112019014847 A2 2020年 4月 14日 |
|             |            |    |                | KR   | 20200074910 A 2020年 6月 25日   |
|             |            |    |                | PH   | 12019501714 A1 2020年 3月 9日   |
|             |            |    |                | AU   | 2018347199 A1 2020年 7月 2日    |
|             |            |    |                | JP   | 2020516104 A 2020年 5月 28日    |
|             |            |    |                | RU   | 2729700 C1 2020年 8月 11日      |
| CN          | 109670335  | A  | 2019年 4月 23日   | 无    |                              |
| CN          | 110033368  | A  | 2019年 7月 19日   | WO   | 2020108138 A1 2020年 6月 4日    |
|             |            |    |                | CN   | 111899102 A 2020年 11月 6日     |
|             |            |    |                | TW   | 202023235 A 2020年 6月 16日     |
| CN          | 110851870  | A  | 2020年 2月 28日   | 无    |                              |
| WO          | 2019182219 | A1 | 2019年 9月 26日   | KR   | 102020986 B1 2019年 11月 4日    |