

基于区块链的数据交易方法及装置、计算设备及存储介质

5 技术领域

本申请涉及数据安全技术领域，具体涉及一种基于区块链的数据交易方法及装置、计算设备及计算机存储介质。

背景技术

10 现有基于区块链技术的数据交易方法主要是运用区块链技术的不可篡改特性来保障数据交易的合法性、安全性。首先由数据交易的参与方共同加入交易区块链，然后将要交易的数据、摘要等内容，通过不同的加密方式上传至区块链，交易双方协定好交易后，数据的解密方法或者仅数据需求方能解密的数据才会被数据需求方获取，然后解密后使用。

15

发明内容

鉴于上述问题，提出了本申请以便提供一种克服上述数据交易存在的交易数据泄露和被滥用问题的基于区块链的数据交易方法及装置、计算设备及计算机存储介质。

20 根据本申请的一个方面，提供了一种基于区块链的数据交易方法，包括：
将与第一数据对应的第二数据上传至区块链，以供数据需求方下载所述第二数据；其中，所述第一数据为原始数据；
从区块链中下载数据处理程序，所述数据处理程序由数据需求方上传至区块链；

25 利用所述数据处理程序对所述第一数据进行处理，得到数据处理结果，将所述数据处理结果上传至区块链，以通过区块链将所述数据处理结果返回给所述数据需求方。

在一种可选的方式中，所述第二数据包括以下多者中的至少一者：
样例数据、属性数据、脱敏数据、伪数据。

30 在一种可选的方式中，在将与第一数据对应的第二数据上传至区块链之后，所述方法还包括：

经由数据监管方对所述第二数据进行审核，以供所述数据需求方下载经审核后的第二数据；

在所述从区块链中下载数据处理程序之前，所述方法还包括：

经由数据监管方对所述数据处理程序进行审核；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：

经由数据监管方对所述数据处理结果进行审核。

- 5 在一种可选的方式中，在所述从区块链中下载数据处理程序之前，所述方法还包括：

所述数据处理程序在由所述数据需求方上传至所述区块链之前经由数据监管方增加发布许可；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：

- 10 对所述数据处理结果进行公钥加密；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：经由数据监管方给所述数据处理结果增加发布许可。

在一种可选的方式中，在所述从区块链中下载数据处理程序之后，所述方法还包括：

- 15 通过区块链生成测试合约，将所述数据处理程序处理得到的测试结果上传至区块链；

基于所述测试结果通过数据监管方审核以及数据需求方同意之后，生成正式的交易合约。

在一种可选的方式中，所述审核的过程包括：

- 20 所述审核以自动或半自动的方式完成，并经过多方确认后生成完整的代码合约，所述多方包括所述区块链中的数据提供方、数据需求方和数据监管方。

在一种可选的方式中，所述区块链包括：身份链、样例链和合约链；

所述身份链，用于对所述区块链中的数据提供方、数据需求方和数据监管方进行身份认证；

- 25 所述样例链，用于对所述第二数据、所述数据处理程序进行存储；

所述合约链，用于对所述数据处理程序和所述数据处理结果进行合约交易。

根据本申请的另一方面，提供了一种基于区块链的数据交易装置，包括：

- 30 数据上传模块，用于将与第一数据对应的第二数据上传至区块链，以供数据需求方下载所述第二数据；其中，所述第一数据为原始数据；

下载模块，用于从区块链中下载数据处理程序，所述数据处理程序由数据需求方上传至区块链；

数据处理模块，用于利用所述数据处理程序对所述第一数据进行处理，得

到数据处理结果，将所述数据处理结果上传至区块链，以通过区块链将所述数据处理结果返回给所述数据需求方。

根据本申请的又一方面，提供了一种计算设备，包括：处理器、存储器、通信接口和通信总线，所述处理器、所述存储器和所述通信接口通过所述通信总线完成相互间的通信；

所述存储器用于存放至少一可执行指令，所述可执行指令使所述处理器执行上述基于区块链的数据交易方法对应的操作。

根据本申请的再一方面，提供了一种计算机存储介质，所述存储介质中存储有至少一可执行指令，所述可执行指令使处理器执行如上述基于区块链的数据交易方法对应的操作。

根据本申请提供的方案，将与第一数据对应的第二数据上传至区块链，以供数据需求方下载第二数据；其中，第一数据为原始数据；从区块链中下载数据处理程序，数据处理程序由数据需求方上传至区块链；利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。本申请数据提供方不再将第一数据（即原始数据）上传区块链，而是将第二数据（即与原始数据对应的伪数据、脱敏数据）上传至区块链，通过数据提供方代替数据需求方完成对需求数据的计算，将数据处理结果返回给数据需求方，数据供求双方不交易原始数据，将原始数据交易转化为数据处理程序与数据处理结果的交易，确保了原始数据不出网，有效避免了交易数据未按约定目的使用的风险，避免了交易数据泄露和被滥用的安全问题。

上述说明仅是本申请技术方案的概述，为了能够更清楚了解本申请的技术手段，而可依照说明书的内容予以实施，并且为了让本申请的上述和其它目的、特征和优点能够更明显易懂，以下特举本申请的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本申请的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

- 图 1 示出了本申请实施例的基于区块链的数据交易方法的流程示意图；
- 图 2 示出了本申请实施例的区块链网络示意图；
- 图 3 示出了本申请实施例的基于区块链的数据提供方参与示意图；
- 图 4 示出了本申请实施例的基于区块链的数据需求方参与示意图；
- 图 5 示出了本申请实施例的基于区块链的数据监管方参与示意图；

图 6 示出了本申请实施例的基于区块链的数据交易步骤示意图；
图 7 示出了本申请实施例的基于区块链的数据交易装置的结构示意图；
图 8 示出了本申请实施例的计算设备的结构示意图。

5 具体实施方式

下面将参照附图更详细地描述本申请的示例性实施例。虽然附图中显示了本申请的示例性实施例，然而应当理解，可以以各种形式实现本申请而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本申请，并且能够将本申请的范围完整的传达给本领域的技术人员。

10 现有基于区块链技术的数据交易方法主要是运用区块链技术的不可篡改特性来保障数据交易的合法性、安全性。首先由数据交易的参与方共同加入交易区块链，然后将要交易的数据、摘要等内容，通过不同的加密方式上传至区块链，交易双方协定好交易后，数据的解密方法或者仅数据需求方能解密的数据才会被数据需求方获取，然后解密后使用，但数据交易后，数据获得者是否
15 超出交易目的使用数据已然不受交易控制，存在一定的数据滥用风险。基于全同态加密的数据处理方式不需要访问数据本身就可以加工数据，但受加密方式限制，数据分析速度缓慢，数据交易本质上涉及的仍是目标数据，无法保证加密后的数据不会被破解。目前数据交易的技术方案均是交易原始数据，只是在交易时对数据的加密方式略有差异。

20 现有基于区块链的数据交易方法存在以下问题需要进一步优化：一是数据泄露风险仍然存在的问题，无论是用哈希算法、对称加密技术还是非对称加密技术，最终结果都是需求方获取到一份完整的原始数据，但是这份原始数据在需求方手中是否被妥善保护无法追踪；二是数据滥用风险仍然存在的问题，需求方在获取到目标数据后，是否按约定对目标数据进行加工处理无法追踪，
25 不能保证交易的数据被合法的使用；三是监管滞后的问题，虽然利用了区块链的不可篡改特性保证了数据交易的可追溯性，但对于数据交易的合理性、合规性、合法性无法保证，对于不合理的数据交易仅能通过事后追溯，而不能在事前阻止重要交易数据的流通。

在实施本申请实施例之前，对下文中涉及的技术术语在此进行统一解释：

30 区块链：本文中指联盟区块链，是由若干组织或机构共同参与管理的区块链，其中的每个组织或机构控制一个或多个节点，共同记录交易数据，并且只有这些组织或机构能够对联盟链中的数据进行读写和发送交易。

数据提供方：数据生产单位，为数据归属者。

数据需求方：数据需求单位，利用数据做各种计算以满足相应的业务需求。

35 数据监管方（也简称为监管方）：数据生产单位的管理单位，负责对数据

计算需求进行合理性、合规性、合法性判断。

样例数据：数据提供方上传至区块链的脱敏数据（其中脱敏是指对某些敏感信息通过脱敏规则对数据变形，以实现敏感隐私数据的可靠性保护）、伪数据。

5 数据的数据属性：也称为属性数据，包括标称属性（nominal attribute）、二元属性（binary attribute）、序数属性（ordinal attribute）、数值属性（numerical attribute）、离散属性与连续属性。

10 标称属性：标称属性的值是一些符号或实物的名称，每个值代表某种类别、编码或状态，所以标称属性又被看做是分类型的属性（categorical），这些值不必具有有意义的序，并且不是定量的。

二元属性：二元属性是一种标称属性，只有两个类别或状态：0 或 1，其中，0 常表示不出现，1 表示出现，如果将 0 和 1 对应于 false 和 true，二元属性则为布尔属性。

15 序数属性：序数属性可能的取值之间具有有意义的序或秩评定，但相继值之间的差是未知的，例如，学生的成绩属性可以分为优、良、中、差四个等级，某快餐店的饮料杯具有大、中、小三个可能值，然而，具体“大”比“中”大多少是未知的。

数值属性：数值属性是可度量的量，用整数或实数值表示。

20 离散属性与连续属性：具有有限个或无限个可数个数，可以用或不用整数表示，如果一个属性不是离散的，则它是连续的。

图 2 示出了本申请实施例的区块链网络示意图。如图 2 所示，可信区块链网络由数据提供方、数据需求方、监管方三方共同组成。数据提供方和数据需求方将自己的公钥上传，监管方作为信任中心对区块链上参与者的身份进行确认，增加区块链中参与者的可信度。同时数据提供方不再将原始数据（本文也称第一数据）上传区块链，而是将伪数据、脱敏数据（本文也称第二数据）上传至区块链，并且将第二数据的数据属性同步上传至区块链，由多个参与者、监管者对其进行校验和验证，保证数据的真实可用性。数据需求者根据业务需求，在区块链上查看数据提供者上传的数据属性，而后上传数据处理程序，经监管方确认后公开在区块链上。即每一个的环节的审计方法可以自动、半自动或者全人工的方式完成，但数据处理结果上链，需要多方达成一致意见，否则退回或者修改后重来。图 1 示出了本申请实施例的基于区块链的数据交易方法的流程示意图。本方法的执行主体可以为图 2 中所示的数据提供方，通过数据提供方代替数据需求方完成对需求数据的计算，将数据处理结果返回给数据需求方，将对原始数据的交易转化为对数据处理程序与数据处理结果的交易。具体地，如图 1 所示，包括以下步骤：

步骤 S101，将与第一数据对应的第二数据上传至区块链，以供数据需求

方下载第二数据；其中，第一数据为原始数据。

在大数据的业务场景下，将原始数据上传至区块链，不仅会给区块链的存储容量造成压力，还存在数据泄露的风险。因此，数据提供方不再将原始数据上传至区块链，而是将原始数据脱敏，上传具有代表性的数据样例。也可以参照原始数据进行数据伪造，将保留有原数据特征的伪数据上传至区块链，以供区块链上的其他用户查看。为保持数据的完整性，在上传脱敏数据、伪数据的同时，将该部分数据的范围、规模等数据属性信息一并上传。

本实施例中，参与区块链的数据提供方不上传原始数据，即，在区块链上不保存原始数据，仅将与原始数据对应的样例数据、属性数据、脱敏数据、伪数据上传至区块链中，供数据需求方查看和下载。其中，与原始数据对应的样例数据、属性数据、脱敏数据与伪数据称为第二数据。可选地，第二数据包括以下多者中的至少一者：样例数据、属性数据、脱敏数据、伪数据。

进一步地，为了增强交易数据（例如第二数据、数据处理程序、数据处理结果）的可信性、可靠性，保障数据交易的合法性、合规性，在数据交易过程或环节中增加数据监管角色，解决在数据交易过程中存在的缺乏公信力、数据获取困难的问题。数据监管方可由交易双方共同信任的第三方机构、政府指定的组织担任。交易数据只有在通过数据监管方认可的前提下才可以进行下一个流程的流转。

进一步地，为了对交易数据进行交易处理、存储与管理，按照数据交易的应用场景将区块链分为以下垂直领域的区块链或行业链：身份链、样例链和合约链。其中，身份链，用于对区块链中的数据提供方、数据需求方和数据监管方进行身份认证，通过身份链将数据提供方、数据需求方、数据监管方三方共同组成可信区块链网络，不仅明确了参与者的身份，还确定了区块链中的资产归属；样例链，用于对第二数据、数据处理程序进行存储；合约链，用于对数据处理程序和数据处理结果进行合约交易，合约链包括合约的交互准则、法律条文、业务逻辑规则以及交易双方协商一致的合约条款，并可按照预置的规则执行。如图3所示，以数据提供方将样例数据上传至样例链为例，数据提供方通过身份链进行签名认证之后，将样例数据上传至样例链中，供数据需求方下载样例数据。

在一种可选的方式中，在数据需求方下载第二数据之前，所述方法还包括：经由监管方对所述第二数据进行审核。为了进一步增强交易数据的安全性，交易双方分别对自己的交易数据进行公钥加密，其中数据需求方使用数据提供方公钥对数据处理程序进行加密，数据提供方使用数据需求方公钥对数据处理结果进行加密；并经由监管方给交易数据增加发布许可，交易双方使用自己的私钥解密后获得相应的交易数据。

步骤 S102，从区块链中下载数据处理程序，数据处理程序由数据需求方

上传至区块链。

参与区块链的数据需求方查阅到数据需求数据（即第二数据）之后，根据业务需求，依据第二数据设计数据处理程序，将数据处理程序上传至区块链中，再由数据提供方从区块链中下载数据处理程序。如图 3 所示，数据提供方从
5 样例链中下载由数据需求方根据样例数据上传的交易程序（即数据处理程序）。

在一种可选的方式中，在从区块链中下载数据处理程序之前，方法还包括：经由监管方对所述数据处理程序进行审核，在审核通过后，监管方给数据处理程序增加发布许可。

数据交易中涉及的数据处理程序、代码分析的结果在通过监管方认可的前提下才可以进行流转，例如，数据需求方首先把数据处理程序、需求样例数据、样例计算结果上传至区块链中，然后由监管方检查审核，监管方对数据处理程序的安全风险进行审计，主要在于三个部分：代码本身、输入参数、返回值进行合理性、合规性、合法性进行审计。在通过监管方审计之后，再将数据处理程序交易给数据提供方。
10

进一步地，在数据提供方使用数据处理程序对数据处理程序、代码分析的结果进行处理时，为确保数据或程序的安全性与合规性，数据处理程序的源码完全开放，并且严格明确程序参数的变化范围。
15

步骤 S103，利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。
20

在一种可选的方式中，在将数据处理结果上传至区块链之前，方法还包括：经由监管方对所述数据处理结果进行审核。

本实施例中，数据供求双方不交易原始数据，而是利用区块链的能力，由数据提供方代替数据需求方完成对需求数据的计算，通过区块链将计算结果返回数据需求方，由于数据需求方对原始数据的需求被转化为数据需求方对数据处理结果的需求，数据处理这一过程需要由数据提供方完成，从而将数据交易转化为数据处理程序与数据处理结果的交易，确保了原始数据不出网，同时也避免了交易数据泄露和被滥用的安全问题。同时，由于处理后的数据处理结果对数据需求方而言，仅对本次需求数据的分析有效，不再具有进一步分析处理的价值，有效避免了交易数据不按照约定目的使用的风险。
25
30

具体地，数据提供方利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。数据提供方利用数据处理程序对第一数据中的样例数据或第二数据进行处理得到的数据处理结果为测试数据处理结果，对第一数据进行处理得到的数据处理结果为正式的数据处理结果。如图 3 所示，数据提供方从
35 样例链中下载由数据需求方根据样例数据上传的交易程序之后，根据交易程

序对样例数据进行处理得到测试结果。数据提供方通过合约链生成测试合约，然后将测试结果上传至合约链。测试结果通过数据监管方审核以及数据需求方一致同意后，再生成正式的交易合约，然后将正式的数据处理结果上传至区块链进行数据交易。

5 在一种可选的方式中，在经由监管方对数据处理程序进行审核之后，通过区块链生成测试合约，将数据处理程序处理得到的测试结果上传至区块链；测试结果通过监管方审核以及数据需求方同意之后，生成正式的交易合约。

10 在一种可选的方式中，审核以自动或半自动的方式完成，并经过多方确认后生成完整的代码合约。以下结合图 3、图 4、图 5 对图 2 中本申请实施例的基于区块链的数据交易参与者的数据交易步骤或过程作具体描述：

15 数据提供方将样例数据上传至区块链的过程，如图 3 所示，例如，数据提供方将脱敏后的原始数据、具有代表性的数据样例、伪数据上传至区块链，供其他用户查看。数据提供方下载经过数据监管方审计后的数据处理程序，通过区块链生成的测试合约，将测试结果上传。测试结果通过监管方审核以及数据需求方一致同意后，生成正式的交易合约，然后将正式的数据处理结果上传至区块链进行数据交易。

20 数据需求方将数据处理程序上传区块链的过程，如图 4 所示，数据需求方下载可以交易的样例数据，根据样例数据设计数据处理程序，然后将数据处理程序上传至区块链，经由监管方审核后，生成测试合约。然后下载经由数据监管方审核通过的由数据提供方反馈的测试结果，在确认无误之后发起正式数据交易合约，最后通过区块链进行数据处理结果的交易。

25 监管方确认交易的合法性与合规性的过程，如图 5 所示，当数据监管方确认数据需求方的数据处理请求合理之后，数据监管方对数据提供方提供的数据、数据需求方提供的数据处理程序进行合法性与合规性确认，当确认无误后将认证后的合约发布到区块链中，然后对数据提供方上传的正式数据处理结果进行验证。其中，数据交易涉及的数据处理程序的本身代码、输入参数、返回值也具有一定的安全风险，需要监管方与数据提供方共同确认程序的安全性、合规性，才能使用数据处理程序对目标数据进行处理，将处理结果交易给数据需求方。例如，对于数据处理程序与代码分析的结果，在通过监管方认可的的前提下才可以进行流转，即数据需求方首先把数据处理程序、需求样例数据、样例计算结果上传区块链中，并严格明确参数的变化范围，然后由监管方检查审核，监管方对数据处理程序的安全风险进行审计，主要对代码本身、输入参数与返回值进行合理性、合规性、合法性审计。通过监管方审计之后，再将数据处理程序交易至数据提供方，数据提供方认同该数据处理程序的合理计算需求之后，利用该数据处理程序对原始数据进行处理，并将计算结果返回至监管方，最后再由监管方将计算结果交易给数据需求方。通过在区块链中增加监管角色，保护了交易过程中进行数据交易的双方主体，对数据交易提前治

理，将不合规的数据交易在流通之前进行有效阻断。

图 6 示出了本申请实施例的基于区块链的数据交易步骤示意图。交易双方分别对自己的交易数据进行公钥加密，并经由监管方给交易数据增加发布许可，进一步增强了交易数据的安全性。具体包括以下步骤：

5 步骤 1，数据需求方使用数据提供方的公钥加密数据处理程序和样例结果，并交易至监管方。

步骤 2，监管方对数据处理程序增加发布许可，然后发布到区块链中。

10 步骤 3，数据提供方从区块链中获取已发布的数据处理程序，使用自己的私钥解密后，利用自己的真实数据（第一数据）进行数据处理，然后将数据处理结果使用数据需求方的公钥加密，然后交易至监管方。

步骤 4，监管方对数据处理结果增加发布许可，然后发布到区块链中。

步骤 5，数据需求方从区块链中获取已发布的数据处理结果，使用自己的私钥解密后，获取期望的数据处理结果，交易结束。

15 本申请上述实施例提供的方案，将与第一数据对应的第二数据上传至区块链，以供数据需求方下载第二数据；其中，第一数据为原始数据；从区块链中下载数据处理程序，数据处理程序由数据需求方上传至区块链；利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。本申请数据供求双方不交易原始数据，将原始数据交易转化为数据处理程序与数据处理结果的交易，
20 确保原始数据不出网，有效避免了交易数据未按约定目的使用的风险，避免了交易数据泄露和被滥用的安全问题。通过增加数据监管方角色，进一步增强了交易数据的可信性、可靠性，保障了数据交易的合法性、合规性，增加了数据交易的公信力。由于区块链中不保留原始数据，规避了区块链容量不足的风险，同时也降低了数据被泄露的可能性。通过对交易数据进行公钥加密并经由监
25 管方给交易数据增加发布许可的方式，进一步增强了交易数据的安全性。

图 7 示出了本申请实施例的基于区块链的数据交易装置的结构示意图。基于区块链的数据交易装置 700 包括：数据上传模块 710、下载模块 720 和数据处理模块 730。

30 所述数据上传模块 710，用于将与第一数据对应的第二数据上传至区块链，以供数据需求方下载所述第二数据；其中，所述第一数据为原始数据；

所述下载模块 720，用于从区块链中下载数据处理程序，所述数据处理程序由数据需求方上传至区块链；

35 所述数据处理模块 730，用于利用所述数据处理程序对所述第一数据进行处理，得到数据处理结果，将所述数据处理结果上传至区块链，以通过区块链将所述数据处理结果返回给所述数据需求方。

在一种可选的方式中，所述第二数据包括以下多者中的至少一者：

样例数据、属性数据、脱敏数据、伪数据。

在一种可选的方式中，在将与第一数据对应的第二数据上传至区块链之后，经由监管方对所述第二数据进行审核；

- 5 所述下载模块 720 在所述从区块链中下载数据处理程序之前，经由监管方对所述数据处理程序进行审核；

所述数据处理模块 730 在所述将所述数据处理结果上传至区块链之前，经由监管方对所述数据处理结果进行审核。

- 10 在一种可选的方式中，所述数据处理程序在由所述数据需求方上传至所述区块链之前经由监管方增加发布许可；

所述数据处理模块 730 在所述将所述数据处理结果上传至区块链之前，对所述数据处理结果进行公钥加密；在所述将所述数据处理结果上传至区块链之后，经由监管方给所述数据处理结果增加发布许可。

在一种可选的方式中，在所述从区块链中下载数据处理程序之后，还包括：

- 15 通过区块链生成测试合约，将所述数据处理程序处理得到的测试结果上传至区块链；

所述测试结果通过监管方审核以及数据需求方同意之后，生成正式的交易合约。

在一种可选的方式中，所述审核的过程包括：

- 20 所述审核以自动或半自动的方式完成，并经过多方确认后生成完整的代码合约，所述多方包括所述区块链中的数据提供方、数据需求方和数据监管方。

在一种可选的方式中，所述区块链包括：身份链、样例链和合约链；

所述身份链，用于对所述区块链中的数据提供方、数据需求方和数据监管方进行身份认证；

- 25 所述样例链，用于对所述第二数据、所述数据处理程序进行存储；

所述合约链，用于对所述数据处理程序和所述数据处理结果进行合约交易。

- 30 本申请上述实施例提供的方案，将与第一数据对应的第二数据上传至区块链，以供数据需求方下载第二数据；其中，第一数据为原始数据；从区块链中下载数据处理程序，数据处理程序由数据需求方上传至区块链；利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。本申请数据供求双方不交易原始数据，将原始数据交易转化为数据处理程序与数据处理结果的交易，确保原始数据不出网，有效避免了交易数据未按约定目的使用的风险，避免了

交易数据泄露和被滥用的安全问题。通过增加数据监管方角色,进一步增强了交易数据的可信性、可靠性,保障了数据交易的合法性、合规性,增加了数据交易的公信力。由于区块链中不保留原始数据,规避了区块链容量不足的风险,同时也降低了数据被泄露的可能性。通过对交易数据进行公钥加密并经由监管方给交易数据增加发布许可的方式,进一步增强了交易数据的安全性。

图 8 示出了本申请计算设备实施例的结构示意图,本申请具体实施例并不对计算设备的具体实现做限定。

如图 8 所示,该计算设备可以包括:处理器(processor)802、通信接口(Communications Interface) 804、存储器(memory) 806、以及通信总线 808。

其中:处理器 802、通信接口 804、以及存储器 806 通过通信总线 808 完成相互间的通信。通信接口 804,用于与其它设备比如客户端或其它服务器等的网元通信。处理器 802,用于执行程序 810,具体可以执行上述基于区块链的数据交易方法实施例中的相关步骤。

具体地,程序 810 可以包括程序代码,该程序代码包括计算机操作指令。

处理器 802 可能是中央处理器 CPU,或者是特定集成电路 ASIC (Application Specific Integrated Circuit),或者是被配置成实施本申请实施例的一个或多个集成电路。计算设备包括的一个或多个处理器,可以是同一类型的处理器,如一个或多个 CPU;也可以是不同类型的处理器,如一个或多个 CPU 以及一个或多个 ASIC。

存储器 806,用于存放程序 810。存储器 806 可能包含高速 RAM 存储器,也可能还包括非易失性存储器(non-volatile memory),例如至少一个磁盘存储器。

程序 810 具体可以用于使得处理器 802 执行以下操作:

将与第一数据对应的第二数据上传至区块链,以供数据需求方下载所述第二数据;其中,所述第一数据为原始数据;

从区块链中下载数据处理程序,所述数据处理程序由数据需求方上传至区块链;

利用所述数据处理程序对所述第一数据进行处理,得到数据处理结果,将所述数据处理结果上传至区块链,以通过区块链将所述数据处理结果返回给所述数据需求方。

在一种可选的方式中,所述第二数据包括以下多者中的至少一者:

样例数据、属性数据、脱敏数据、伪数据。

在一种可选的方式中,所述程序 810 使所述处理器执行以下操作:

在将与第一数据对应的第二数据上传至区块链之后,经由监管方对所述

第二数据进行审核；

在所述从区块链中下载数据处理程序之前，经由监管方对所述数据处理程序进行审核；

5 在所述将所述数据处理结果上传至区块链之前，经由监管方对所述数据处理结果进行审核。

在一种可选的方式中，所述程序 810 使所述处理器执行以下操作：

所述数据处理程序在由所述数据需求方上传至所述区块链之前经由监管方给所述数据处理程序增加发布许可；

10 在所述将所述数据处理结果上传至区块链之前，对所述数据处理结果进行公钥加密；

在所述将所述数据处理结果上传至区块链之前，经由监管方给所述数据处理结果增加发布许可。

在一种可选的方式中，所述程序 810 使所述处理器执行以下操作：

15 在所述从区块链中下载数据处理程序之后，通过区块链生成测试合约，将所述数据处理程序处理得到的测试结果上传至区块链；

所述测试结果通过监管方审核以及数据需求方同意之后，生成正式的交易合约。

在一种可选的方式中，所述审核的过程包括：

20 所述审核以自动或半自动的方式完成，并经过多方确认后生成完整的代码合约，所述多方包括所述区块链中的数据提供方、数据需求方和数据监管方。

在一种可选的方式中，所述区块链包括：身份链、样例链和合约链；

所述身份链，用于对所述区块链中的数据提供方、数据需求方和数据监管方进行身份认证；

所述样例链，用于对所述第二数据、所述数据处理程序进行存储；

25 所述合约链，用于对所述数据处理程序和所述数据处理结果进行合约交易。

30 本申请上述实施例提供的方案，将与第一数据对应的第二数据上传至区块链，以供数据需求方下载第二数据；其中，第一数据为原始数据；从区块链中下载数据处理程序，数据处理程序由数据需求方上传至区块链；利用数据处理程序对第一数据进行处理，得到数据处理结果，将数据处理结果上传至区块链，以通过区块链将数据处理结果返回给数据需求方。本申请数据供求双方不交易原始数据，将原始数据交易转化为数据处理程序与数据处理结果的交易，确保原始数据不出网，有效避免了交易数据未按约定目的使用的风险，避免了交易数据泄露和被滥用的安全问题。通过增加数据监管方角色，进一步增强了

交易数据的可信性、可靠性，保障了数据交易的合法性、合规性，增加了数据交易的公信力。由于区块链中不保留原始数据，规避了区块链容量不足的风险，同时也降低了数据被泄露的可能性。通过对交易数据进行公钥加密并经由监管方给交易数据增加发布许可的方式，进一步增强了交易数据的安全性。

- 5 本申请实施例提供了一种非易失性计算机存储介质，所述计算机存储介质存储有至少一可执行指令，该计算机可执行指令可执行上述任意方法实施例中的基于区块链的数据交易方法。

10 在此提供的算法或显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本申请实施例也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本申请的内容，并且上面对特定语言所做的描述是为了披露本申请的最佳实施方式。

15 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本申请的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

20 类似地，应当理解，为了精简本申请并帮助理解各个发明方面中的一个或多个，在上面对本申请的示例性实施例的描述中，本申请实施例的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本申请要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本申请的单独实施例。

25 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

30

35 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本申请的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本申请的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本申请实施例的一些或者全部部件的一些或者全部功能。本申请还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本申请的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

10 应该注意的是上述实施例对本申请进行说明而不是对本申请进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本申请可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，15 这些装置中的若干个可以通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。上述实施例中的步骤，除有特殊说明外，不应理解为对执行顺序的限定。

权 利 要 求 书

1. 一种基于区块链的数据交易方法，其特征在于，所述方法包括：

将与第一数据对应的第二数据上传至区块链，以供数据需求方下载所述第二数据；其中，所述第一数据为原始数据；

从所述区块链中下载数据处理程序，所述数据处理程序由所述数据需求方根据所述第二数据设计并由所述数据需求方上传至所述区块链；

利用所述数据处理程序对所述第一数据进行处理，得到数据处理结果，将所述数据处理结果上传至所述区块链，以通过所述区块链将所述数据处理结果返回给所述数据需求方。

2. 根据权利要求 1 所述的方法，其特征在于，所述第二数据包括以下多者中的至少一者：

样例数据、属性数据、脱敏数据、伪数据。

3. 根据权利要求 1 所述的方法，其特征在于，在将与第一数据对应的第二数据上传至区块链之后，所述方法还包括：

经由数据监管方对所述第二数据进行审核，以供所述数据需求方下载经审核后的第二数据；

在所述从区块链中下载数据处理程序之前，所述方法还包括：

经由数据监管方对所述数据处理程序进行审核；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：

经由数据监管方对所述数据处理结果进行审核。

4. 根据权利要求 1 所述的方法，其特征在于，

所述数据处理程序在由所述数据需求方上传至所述区块链之前经由数据监管方增加发布许可；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：对所述数据处理结果进行公钥加密；

在所述将所述数据处理结果上传至区块链之前，所述方法还包括：

经由数据监管方给所述数据处理结果增加发布许可。

5. 根据权利要求 3 所述的方法，其特征在于，在所述从区块链中下载数据处理程序之后，所述方法还包括：

通过区块链生成测试合约，将所述数据处理程序处理得到的测试结果上传至区块链；

基于所述测试结果通过所述数据监管方审核以及所述数据需求方同意，生成正式的交易合约。

6. 根据权利要求 3 所述的方法，其特征在于，所述审核的过程包括：

所述审核以自动或半自动的方式完成，并经过多方确认后生成完整的代码合约，所述多方包括所述区块链中的数据提供方、数据需求方和数据监管方。

7. 根据权利要求 1-6 中任一项所述的方法，其特征在于，所述区块链包括：身份链、样例链和合约链；

所述身份链，用于对所述区块链中的数据提供方、数据需求方和数据监管方进行身份认证；

所述样例链，用于对所述第二数据、所述数据处理程序进行存储；

所述合约链，用于对所述数据处理程序和所述数据处理结果进行合约交易。

8. 一种基于区块链的数据交易装置，其特征在于，包括：

数据上传模块，用于将与第一数据对应的第二数据上传至区块链，以供数据需求方下载所述第二数据；其中，所述第一数据为原始数据；

下载模块，用于从区块链中下载数据处理程序，所述数据处理程序由数据需求方上传至区块链；

数据处理模块，用于利用所述数据处理程序对所述第一数据进行处理，得到数据处理结果，将所述数据处理结果上传至区块链，以通过区块链将所述数据处理结果返回给所述数据需求方。

9. 一种计算设备，包括：处理器、存储器、通信接口和通信总线，所述处理器、所述存储器和所述通信接口通过所述通信总线完成相互间的通信；

所述存储器用于存放至少一可执行指令，所述可执行指令使所述处理器执行如权利要求 1-7 中任一项所述的基于区块链的数据交易方法对应的操作。

10. 一种计算机存储介质，所述存储介质中存储有至少一可执行指令，所述可执行指令使处理器执行如权利要求 1-7 中任一项所述的基于区块链的数据交易方法对应的操作。