

(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
2024 年 1 月 4 日 (04.01.2024)



(10) 国际公布号
WO 2024/001028 A1

(51) 国际专利分类号:

G06F 16/27 (2019.01) **G06F 21/60** (2013.01)
G06F 21/64 (2013.01) **G06F 11/14** (2006.01)

(21) 国际申请号: PCT/CN2022/135413

(22) 国际申请日: 2022 年 11 月 30 日 (30.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

202210761451.1 2022年6月29日 (29.06.2022) CN

(71) 申请人: 蚂蚁区块链科技(上海)有限公司
(**ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.**) [CN/CN]; 中国上海市黄浦区外马路
618号8层803室, Shanghai 200010 (CN)。

(72) 发明人: 闫莺(**YAN, Ying**); 中国上海市黄浦区外马
路618号8层803室, Shanghai 200010 (CN)。 魏长

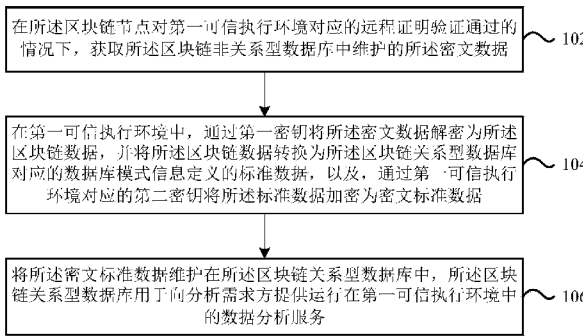
征(**WEI, Changzheng**); 中国上海市黄浦区外马路
618号8层803室, Shanghai 200010 (CN)。

(74) 代理人: 北京智信禾专利代理有限公司
(**CHISPO ATTORNEYS AT LAW**); 中国北京市东
城区崇文门外大街8号哈德门广场西塔
9层901, Beijing 100062 (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,
CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ,
IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ,
LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,
PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,
SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** METHOD AND APPARATUS FOR MAINTAINING BLOCKCHAIN DATA, AND ELECTRONIC DEVICE AND
STORAGE MEDIUM

(54) 发明名称: 一种维护区块链数据的方法、装置、电子设备和存储介质



102 When remote attestation corresponding to a first trusted execution environment passes verification of a blockchain node, acquire ciphertext data, which is maintained in a blockchain non-relational database

104 In the first trusted execution environment, decrypt the ciphertext data into blockchain data by means of a first key, convert the blockchain data into standard data, which is defined by database mode information corresponding to a blockchain relational database, and encrypt the standard data into ciphertext standard data by means of a second key corresponding to the first trusted execution environment

106 Maintain the ciphertext standard data in the blockchain relational database, wherein the blockchain relational database is used for providing an analysis demander with a data analysis service, which is run in the first trusted execution environment

(57) **Abstract:** Provided in the present description are a method and apparatus for maintaining blockchain data, and an electronic device and a storage medium. The method is applied to a node device, which is deployed with a blockchain node and a first trusted execution environment, wherein the node device maintains a blockchain non-relational database and a blockchain relational database, the blockchain non-relational database is used for maintaining ciphertext data, and the ciphertext data is obtained by the blockchain node encrypting, by means of a first key corresponding to a second trusted execution environment, blockchain data which is generated when a blockchain service is run in the second trusted execution environment. The method comprises: when remote attestation corresponding to a first trusted execution environment passes verification of a blockchain node, acquiring ciphertext data, which is maintained in a blockchain non-relational database; in the first trusted execution environment, decrypting, converting and encrypting the ciphertext data into ciphertext standard data; and maintaining the ciphertext standard data in a blockchain relational database, wherein the blockchain relational database is used for providing a data analysis service for an analysis demander.

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本说明书提供一种维护区块链数据的方法、装置、电子设备和存储介质, 应用于部署有区块链节点和第一可信执行环境的节点设备, 节点设备维护有区块链非关系型数据库和区块链关系型数据库, 区块链非关系型数据库用于维护密文数据, 密文数据由区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到; 该方法包括: 在区块链节点对第一可信执行环境对应的远程证明验证通过的情况下, 获取区块链非关系型数据库中维护的密文数据; 在第一可信执行环境中, 将密文数据解密、转换并加密为密文标准数据; 将密文标准数据维护在区块链关系型数据库中, 区块链关系型数据库用于向分析需求方提供数据分析服务。

一种维护区块链数据的方法、装置、电子设备和存储介质

本申请要求于 2022 年 06 月 29 日提交中国专利局、申请号为 202210761451.1、发明名称为“一种维护区块链数据的方法、装置、电子设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本说明书实施例属于区块链技术领域，尤其涉及一种维护区块链数据的方法、装置、电子设备和存储介质。

背景技术

区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链系统中按照时间顺序将数据区块以顺序相连的方式组合成链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

在传统区块链技术中，为了契合区块链节点在运行区块链服务过程中对大量数据的存储需求，区块链节点通常使用具有高效的存取效率的非关系型数据库进行数据存储，然而，非关系型数据库由于缺乏事务关系，数据之间缺乏联系且未标准化，不利于进行数据分析。关系型数据库具有完整的事务关系，数据之间具有联系且具有严格的标准化结构，如果将传统区块链技术中的非关系型数据库替换为关系型数据库，虽然利于进行数据分析，但在区块链底层系统直接使用关系型数据库又会对区块链节点运行区块链服务过程中的在线读写性能带来巨大挑战。因此，如何在确保区块链服务执行过程具有高效存取效率的情况下实现便捷的数据分析服务是本领域亟待解决的问题。

发明内容

本发明的目的在于提供一种维护区块链数据的方法、装置、电子设备和存储介质。

根据本说明书一个或多个实施例的第一方面，提出了一种维护区块链数据的方法，应用于部署有区块链节点和第一可信执行环境的节点设备，所述节点设备维护有区块链非关系型数据库和区块链关系型数据库，所述区块链非关系型数据库用于维护密文数据，所述密文数据由所述区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到；所述方法包括：

在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，获取所述区块链非关系型数据库中维护的所述密文数据；

在第一可信执行环境中，通过第一密钥将所述密文数据解密为所述区块链数据，并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，以及，通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据；

将所述密文标准数据维护在所述区块链关系型数据库中，所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

根据本说明书一个或多个实施例的第二方面，提出了一种维护区块链数据的装置，应用于部署有区块链节点和第一可信执行环境的节点设备，所述节点设备维护有区块链非关系型数据库和区块链关系型数据库，所述区块链非关系型数据库用于维护密文数据，所述密文数据由所述区块链节点将在第二可信

—2—

执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到；所述装置包括：

区块链数据获取单元，用于在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，获取所述区块链非关系型数据库中维护的所述密文数据；

- 5 区块链数据获取单元，用于在第一可信执行环境中，通过第一密钥将所述密文数据解密为所述区块链数据，并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，以及，通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据；

标准数据维护单元，用于将所述密文标准数据维护在所述区块链关系型数据库中，所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

- 10 根据本说明书一个或多个实施例的第三方面，提出了一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

- 15 根据本说明书一个或多个实施例的第四方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

- 本说明书实施例通过在节点设备上分别部署区块链非关系型数据库和区块链关系型数据库，一方面，由于区块链非关系型数据库用于维护将区块链节点运行区块链服务时生成的区块链数据加密得到的密文数据，这使得区块链节点运行区块链服务时能够对区块链数据加密后进行高效存储以及对密文数据进行高效读取；另一方面，通过将从区块链非关系型数据库中维护的密文数据解密、转换并加密为密文标准数据以同步维护于区块链关系型数据库中，从而利用区块链关系型数据库实现便捷的数据分析服务。另外，无论是区块链节点运行的区块链服务，或是节点设备对密文数据解密、转换并加密的过程均在相应的可信执行环境中进行，同时区块链节点在提供密文数据前需要提前对第一可信执行环境对应的远程证明进行验证，从而确保了数据处理、数据传输和数据存储的系统级别的数据安全。本说明书实施例涉及的维护区块链数据的方法实现了一份数据两处备份，客观上提高了容灾能力，在确保区块链服务执行过程具有高效存取效率的情况下实现便捷的数据分析服务；同时由于结合了可信执行环境技术，因此实现了从链上的区块链服务到链下的数据转换和数据分析服务的全流程的可信数据流转与可信数据处理的过程，尽可能地减少了数据泄露风险。
- 20
- 25

附图说明

- 30 为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1是一示例性实施例提供的一种维护区块链数据的方法的流程图。

图2是一示例性实施例提供的一种维护区块链数据的系统架构图。

图3是一示例性实施例提供的一种设备的结构示意图。

- 35 图4是一示例性实施例提供的一种维护区块链数据的装置的框图。

具体实施方式

为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

图1是一示例性实施例提供的一种维护区块链数据的方法的流程图。该方法应用于部署有区块链节点和第一可信执行环境的节点设备，所述节点设备维护有区块链非关系型数据库和区块链关系型数据库，所述区块链非关系型数据库用于维护密文数据，所述密文数据由所述区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到；所述方法包括：

S102：在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，获取所述区块链非关系型数据库中维护的所述密文数据。

图2是一示例性实施例提供的一种维护区块链数据的系统架构图。如图2所示，区块链网络中的每个区块链节点都部署于对应的节点设备上，每个节点设备都会同时维护有区块链非关系型数据库和区块链关系型数据库，同时，节点设备也部署有第一可信执行环境（Trusted execution environment，TEE）和第二可信执行环境。在本说明书实施例中，区块链非关系型数据库属于非关系型数据库，而区块链关系型数据库属于关系型数据库，另外，第二可信执行环境用于承担区块链节点运行区块链服务，而第一可信执行环境用于承担节点设备运行数据分析服务，同时第一可信执行环境也用于承担节点设备对密文数据进行解密、转换和再加密的过程，具体而言，节点设备链下部署有运行在第一可信执行环境中的数据转换引擎与数据分析引擎，其中，数据转换引擎用于执行对密文数据进行解密、转换和再加密的过程，而数据分析引擎则用于运行数据分析服务。

本说明书实施例中，对于可信执行环境内部的数据需要处于明文状态的，而当数据出域时，即数据需要被输出至可信执行环境外部时则需要确保数据被加密并处于密文状态，因此，可信执行环境维护有对应的密钥以用于将内部数据加密后输出到外部，或者从外部读入密文以在内部解密为明文，通常情况下可信执行环境对应的密钥属于对称密钥。例如在本说明书实施例中，第一可信执行环境维护有第二密钥，以用于从区块链非关系型数据库存取数据的过程进行加解密，而第二可信执行环境维护有第一密钥，以用于从区块链关系型数据库存取数据的过程中进行加解密。

一方面，区块链非关系型数据库作为区块链节点运行区块链服务的原生数据库，即作为区块链底层系统的基础架构的一部分，用于对区块链节点运行区块链服务的过程中生成的区块链数据进行高效存取，而为了确保数据安全，区块链节点在需要向区块链非关系型数据库中存储区块链数据时，作为直接存储区块链数据的代替，区块链节点可以先在第二可信执行环境中对区块链数据进行加密得到密文数据（通过第二可信执行环境对应的第一密钥），然后将密文数据存储在区块链非关系型数据库，从而避免直接存储明文数据而诱发数据泄露的风险，当然，所述区块链非关系型数据库除了可以维护密文数据外，还用于维护所述区块链节点将运行区块链服务时生成的区块链数据，也就是说对于一些隐私需求较低的区块链数据，可以直接在区块链非关系型数据库中以明文状态存取。区块链非关系型数据库可以具体采用 Key-Value 数据库（键值对数据库，一种典型的非关系型数据库，简称 K-V 数据库），不同于关系型数据库，K-V 数据库并不清楚存储数据的值，而且也没有像 MySQL（关系型数据库管理系统）和 PostgreSQL（一种特性非常齐全的自由软件的对象-关系型数据库管理系统）中 schema（数据库模式信息）的概念。这也就意味着它不能像关系型数据库一样通过使用带 where 的 SQL（Structured Query Language，结构化查询语句）来过滤并查询所存数据的部分内容。如果你不知道该从哪查询，你需要遍历所有的 key 值，找到对应的 value，对其进行过滤，最终只保留你想要的那部分数据。这样一来计算量会非常大，同时也意味着只有在 key 已知的情况下，K-V 数据库才能保证高性能，否则其性能明显不足。因此，虽然在绝对访问速度方面 K-V 数据库优于关系型数据库，但需要已知 key 值的要求限制了其应用场景。上述描述虽然仅涉及对 K-V 数据库的介绍，但实质上适用于大多数非关系型数据库，总的来说，就是非关系型

数据库具有高效的访问速度但缺乏数据分析能力，例如缺乏基于索引、数据间关系的查询能力。

在本说明书实施例中，由于节点设备部署的区块链底层系统（包含区块链节点与对应的区块链数据库）沿用了具有高效的访问速度的非关系型数据库（即区块链非关系型数据库），因此可以使区块链节点在运行区块链服务时，能够高效地从区块链非关系型数据库中存取数据，从而确保区块链服务的高效运行，同时由于存储的是区块链数据加密后的得到密文数据，因此还可以避免数据泄露带来的安全风险。

另一方面，本说明书实施例涉及的节点设备还额外维护有区块链关系型数据库，以作为对用户提供数据分析服务的原生数据库，即作为数据分析系统的基础架构的一部分，用于向分析需求方提供数据分析服务。例如，区块链非关系型数据库可以具体采用 oracle 数据库、MySQL 等关系型数据库。关系型数据库，是指采用了关系模型来组织数据的数据库，其以行和列的形式存储数据，以便于用户理解，关系型数据库这一系列的行和列被称为表，一组表组成了数据库。用户通过查询来检索数据库中的数据，而查询是一个用于限定数据库中某些区域的执行代码。关系模型可以简单理解为二维表格模型，而一个关系型数据库就是由二维表及其之间的关系组成的一个数据组织，关系型数据库需要提前定义好表的结构、表的关系、规范化的数据结构等数据库模式信息，再根据数据库模式信息存入数据，支持 SQL，具有强大的数据分析能力，但由于关系型数据库十分强调数据的一致性，并为此降低读写性能付出了巨大的代价，虽然关系型数据库存储数据和处理数据的可靠性很不错，但一旦面对海量数据的处理的时候效率就会变得很差，特别是遇到高并发读写的时候性能就会下降的非常厉害。总的来说，就是关系型数据库具有强大的数据分析能力但访问速度、读写性能较差，不适用于大规模并发读写的应用场景。

在本说明书实施例中，由于节点设备链下部署的数据分析系统（包括图 2 中未示出的数据分析引擎与对应的数据库）采用了具有高效的访问速度的非关系型数据库（即区块链关系型数据库），因此可以使节点设备在通过调用数据分析引擎而运行数据分析服务时，能够利用区块链非关系型数据库强大的数据分析能力，从而确保向分析需求方提供便捷的数据分析服务。

本说明书实施例涉及的区块链关系型数据库中维护的数据是通过区块链非关系型数据库中的数据转换、迁移得到的。下面将具体介绍这个数据转换、迁移的过程。

在本说明书实施例中，只有在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，节点设备才能获取到所述区块链非关系型数据库中维护的所述密文数据。对于区块链节点而言，其需要对任何向其请求获取区块链非关系型数据库中数据的数据需求方验证访问权限，以在数据需求方具有访问权限的情况下才允许向该数据需求方提供数据，在本实施例中，节点设备（具体为节点设备部署的数据转换引擎）就属于数据需求方，因此，区块链节点需要验证节点设备是否具备区块链非关系型数据库的访问权限，本说明书实施例通过验证节点设备部署的第一可信执行环境对应的远程证明是否有效，来判断节点设备是否具备区块链非关系型数据库的访问权限。具体而言，第一可信执行环境对应的远程证明包含第一可信执行环境使用第一可信执行环境对应的 CPU 私钥对其环境中运行的全部程序（这些程序对应的哈希值）进行签名得到的数字签名，区块链节点在获取到该远程证明后，可以通过本地维护的第一可信执行环境对应的 CPU 公钥对该远程证明中包含的数字签名进行验签，在验签通过的情况下可以确认节点设备的确运行有第一可信执行环境且第一可信执行环境中运行的程序合法可信、未被篡改，从而判断节点设备具备区块链非关系型数据库的访问权限；或者，区块链节点在获取到该远程证明后，可能由于不具备第一可信执行环境对应的 CPU 公钥，因此也可以将该远程证明发送至持有第一可信执行环境对应的 CPU 公钥的鉴权第三方，由鉴权第三方在验证远程证明通过后向区块链节点返回对应的远程认证报告，区块链节点在通过鉴权第三方对应的公钥验证该远程认证报告有效、且该远程认证报告用于表明所述远程证明有效的情况下，可以确认节点设备的确运行有第一可信执行环境且第一可信执行环境中运行的程序合法可信、未被篡改，从而判断节点设备具备区块链非关系型数据库的访问权限。

在本说明书实施例中，所述获取所述区块链非关系型数据库中维护的所述密文数据，包括：接收所述区块链节点主动推送的所述密文数据；和/或，向所述区块链节点发送区块链数据请求，接收所述区块链节点响应于所述区块链数据请求返回的所述密文数据。

本说明书实施例所涉及的维护区块链数据的方法应用于节点设备，具体应用于节点设备链下部署的数据转换引擎。节点设备可以通过两种方式中至少一种方式获取区块链非关系型数据库中维护的密文数据，这两种方式包括：其一，通过接收区块链节点的主动推送的密文数据，例如每次区块链节点在第二可信执行环境中运行区块链服务的过程中向区块链非关系型数据库中新增或修改密文数据的情况下，区块链节点都会向链下的数据转换引擎主动推送携带有最新新增或修改的密文数据的数据更新消息，本方式可以及时将区块链非关系型数据库中的数据转换并同步至区块链关系型数据库中，从而确保区块链关系型数据库中数据的对称性和时效性；其二，通过节点设备向区块链节点发送区块链数据请求以获取所述区块链节点响应于所述区块链数据请求返回的密文数据，本方式通过请求-响应模式来获取密文数据，可以有效控制请求的密文数据的范围从而屏蔽一些不需要维护在区块链关系型数据库中的数据。

在本说明书实施例中，所述远程证明包含于所述区块链数据请求；或者，所述远程证明预先维护于所述区块链节点。当远程认证包含于区块链数据请求中时，相当于区块链节点对第一可信执行环境对应的最新远程证明进行验证，从而确保了远程证明的时效性。而当远程证明预先维护于区块链节点时，相当于区块链节点事先就可以通过预先维护在区块链节点的远程证明来判断节点设备是否具备区块链非关系型数据库的访问权限，因此可以减少节点设备获取密文数据过程的中间环节，增加密文数据的获取效率。

可选的，所述向所述区块链节点发送区块链数据请求，包括：向所述区块链节点部署的智能合约发起针对所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的所述区块链数据请求；或者，向所述区块链节点发起针对所述区块链非关系型数据库中维护的所述密文数据的所述区块链数据请求。

本说明书实施例所涉及的区块链数据包括区块数据、状态数据和事件数据。其中，区块数据是指区块链网络中每个区块链节点所维护的区块链账本，区块链账本和/或区块链账本对应的密文数据实质被维护在区块链非关系型数据库中，由于区块链账本是一种特殊的数据结构，其是由多个区块通过哈希锚定首尾相连而成，具有不可篡改性，每个区块由区块头和区块体组成，任一区块的区块头中包含有该个区块的状态树根、交易数根、收据树根、区块高度和对应父区块的哈希值等信息，而区块体中包含有该个区块包含的交易数据（交易哈希）。本说明书实施例所涉及的区块数据指的就是区块链账本中包含的数据。本说明书实施例涉及的状态数据和事件数据则是由区块链节点所部署的各个智能合约所维护，实质上状态数据、事件数据和/或状态数据、事件数据对应的密文数据是维护在区块链非关系型数据库中对应于各个智能合约的合约存储空间。

在一实施例中，区块链节点部署有若干的智能合约，任一智能合约中都维护有相应的状态数据，这些状态数据被以在第二可信执行环境中通过第一密钥加密为密文数据的形式维护在区块链非关系型数据库中对应于所述任一智能合约的合约存储空间内。而节点设备可以向区块链节点部署的智能合约（事实上，任一智能合约部署在区块链网络中每个区块链节点上）发起区块链数据请求，该区块链数据请求在形式上属于一种区块链交易，该区块链交易在由区块链节点接收到后，区块链节点会进一步调用该区块链交易所指示的智能合约执行该区块链交易。智能合约在执行该区块链交易时，从区块链非关系型数据库中对应于该智能合约的合约存储空间查找并获取区块链交易所指示的密文数据，并将该密文数据作为区块链数据请求对应的响应消息（如以区块链事件的形式）回调至节点设备，从而实现以调用智能合约的方式来获取区块链非关系型数据库中维护的密文数据。

在另一实施例中，节点设备可以向区块链节点直接发起区块链数据请求，例如通过区块链节点的数据查询接口发起区块链数据请求，该区块链数据请求用于使区块链节点从区块链非关系型数据库中调取区块链数据请求所指示的密文数据（由区块数据在第二可信执行环境中经过第一密钥加密得到的）并回调至节点设备。

在又一实施例中，节点设备可以直接向区块链非关系型数据库发起区块链数据请求，例如通过区块链非关系型数据库的数据库接口发起区块链数据请求，此时相当于节点设备链下的本地调用而无需经过区块链节点，区块链非关系型数据库直接响应于接收到的区块链数据请求返回区块链数据请求指示的密

文数据。

需要注意的是，虽然区块链数据请求在形式上与区块链交易相同，但不一定具有区块链交易的所有性质，例如区块链节点在接收到区块链数据请求后不一定会将其在区块链网络中进行共识，而是作为本地调用请求进行处理，这种不进行共识仅会在本地区块链节点内部执行的区块链交易称为本地交易；当然，区块链数据请求也可以具有区块链交易的所有性质，即作为共识交易在区块链网络中完成共识后，由区块链网络中的每个区块链节点各自分别执行。

S104：在第一可信执行环境中，通过第一密钥将所述密文数据解密为所述区块链数据，并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，以及，通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据。

节点设备在获取到密文数据后，会将其读入第一可信执行环境中，同时调用运行在第一可信执行环境中的数据转换引擎在第一可信执行环境中执行有关密文数据的解密、转换和加密任务。具体而言，节点设备通过第一密钥首先将所述密文数据解密为明文数据，也即前述的所述区块链数据，然后将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，最后通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据。由于上述过程均在第一可信执行环境中实现，因此可以有效避免数据泄露问题，提高系统的安全性。

在本说明书实施例中，第一密钥由所述区块链节点对所述远程证明验证通过的情况下提供至所述节点设备部署的第一可信执行环境；或者，第一密钥预先维护于第一可信执行环境中。第一密钥可以由区块链节点在验证远程证明的情况下（即区块链节点确认节点设备具备区块链非关系型数据库的访问权限的情况下）及时地提供给节点设备中的第一可信执行环境，或预先维护在第一可信执行环境中，例如历史上节点设备已经被区块链节点确认具有相应访问权限而第一密钥已由区块链节点提供给了第一可信执行环境，那么第一可信执行环境就会预先维护有该第一密钥。

本说明书实施例所涉及的数据库模式信息具体是指数据库 schema，schema 是元数据的一个抽象集合，包含一套 schema component（模式组件）：主要是元素与属性的声明、复杂与简单数据类型的定义，具体包括：定义可出现在文档中的元素；定义可出现在文档中的属性；定义哪个元素是子元素；定义子元素的次序；定义子元素的数目；定义元素是否为空，或者是否可包含文本；定义元素和属性的数据类型；定义元素和属性的默认值以及固定值。而在数据库中，schema 是数据库的组织结构和结构。数据库模式信息中包含了 schema 对象，能够是表(table)、列(column)、数据类型(data type)、视图(view)、存储过程(stored procedures)、关系(relationships)、主键(primary key)、外键(foreign key)等。数据库模式信息能够用一个可视化的图来表示，它显示了数据库对象及其相互之间的关系。由于数据库模式信息用于描述数据库的结构，能够作为创建一个数据库的蓝图，因此通过规定一个数据库对应的数据库模式信息，可以指导该数据库中数据是如何进行储存。

节点设备在解密得到区块链数据后，将在第一可信执行环境中基于区块链关系型数据库对应的数据库模式信息，将区块链数据转换为该数据库模式信息所定义的标准数据，这意味着转换得到的标准数据能够被按照一定的规则维护在区块链关系型数据库中，并且标准数据也已经具备了规范化的结构以及被定义有与区块链关系型数据库中其他数据之间的关系。区块链数据到标准数据的转换过程包括但不限于数据表、行、列的转换，例如通过 ETL（Extract-Transform-Load，基于数据抽取、转换和加载的数据仓库技术）机制实现了区块链数据到标准数据的转换，其具体实现方式现有技术均有所记载，这里不再赘述。由于密文标准数据是通过对标准数据进行加密得到的，其只是在数值上脱敏处理了，但仍然保留有标准数据状态时的结构、以及标准数据状态时与其他数据之间的关系，即密文标准数据和加密前的标准数据一样，能够被按照一定的规则维护在区块链关系型数据库。

可选的，在所述区块链数据请求针对于所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的情况下，所述方法还包括：

向所述智能合约发起模式信息查询请求，将所述智能合约响应于所述模式信息查询请求返回的记录

于所述智能合约中的第一数据库模式信息确定为所述区块链关系型数据库对应的所述数据库模式信息。

在本说明书实施例中，区块链关系型数据库对应的数据库模式信息可以被预先维护在节点设备处（例如由节点设备的管理员用户所设置），或者，向智能合约请求获取得到。如前所述，由于区块链节点部署的每个智能合约在区块链非关系型数据库中都有对应的合约存储空间，且每个智能合约在处理数据、组织数据、存储数据时具有不同的特性，因此不同智能合约在区块链非关系型中对应的合约存储空间具有不同的数据组织形式，而这个数据组织形式包括数据组织的格式、关系和内涵等，它同样是以数据库模式信息的形式被维护在智能合约中。因此，为了正确应对不同智能合约在区块链非关系型数据库所维护的具有不同组织特性的密文数据，本说明书实施例通过向对应智能合约请求获取该智能合约中维护的对应于该智能合约维护在非关系型数据库中的密文数据的第一数据库模式信息，来作为在区块链关系型数据库中维护该智能合约涉及的密文数据解密、转换并加密（本说明书中也可以将解密、转换并加密的过程简称为转换）得到的密文标准数据的组织模式，从而在区块链关系型数据库中正确地维护该智能合约涉及的密文标准数据。当区块链节点包含多个智能合约时，且不同的智能合约具有不同的数据组织形式的情况下，通过本说明书实施例可以获取每个智能合约对应的数据库模式信息，并按照对应智能合约的数据库模式信息，来作为所述区块链关系型数据库对应的所述数据库模式信息实现对应智能合约涉及的密文数据到密文标准数据的转换，并最终按照不同智能合约各自的数据库模式信息，实现多个智能合约涉及的密文标准数据在区块链关系型数据库中的正确维护。此时相当于区块链关系型数据库应用有多种不同的数据库模式信息，且任一智能合约对应的数据库模式信息仅支持维护该任一智能合约涉及的密文标准数据（即来自该任一智能合约中密文数据解密、转换并加密得到的密文标准数据），从而支持多个采用不同数据组织形式的智能合约维护在区块链非关系型数据库中的密文数据正确地转换为密文标准数据后，最终以密文标准数据的形式迁移至区块链关系型数据库中维护。

S106：将所述密文标准数据维护在所述区块链关系型数据库中，所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

节点设备在第一可信环境中加密得到密文标准数据后，便可以按照区块链关系型数据库对应的区块链模式信息将密文标准数据存储于区块链关系型数据库中，以实现区块链非关系型数据库中的密文数据到区块链关系型数据库中密文标准数据的转换迁移。由于区块链关系型数据库支持多种 SQL，具有强大的数据分析能力（例如基于各类条件、索引、关系的数据查询能力），因此区块链关系型数据库可以方便地向分析需求方提供便捷的数据分析服务，同时由于数据分析服务运行在第一可信执行环境中，因此实际上是在第一可信执行环境中将密文标准数据解密后再进行分析以获取的分析结果，对明文数据进行分析可以保证分析的效率，同时在 TEE 中运行数据分析服务也能确保数据安全。例如，通过节点设备上链下部署的运行在第一可信执行环境中的数据分析引擎向外部提供数据分析接口，来向外部调用该分析接口的分析需求方提供针对区块链关系型数据库的数据分析服务。

本说明书实施例通过在节点设备上分别部署区块链非关系型数据库和区块链关系型数据库，一方面，由于区块链非关系型数据库用于维护将区块链节点运行区块链服务时生成的区块链数据加密得到的密文数据，这使得区块链节点运行区块链服务时能够对区块链数据加密后进行高效存储以及对密文数据进行高效读取；另一方面，通过将从区块链非关系型数据库中维护的密文数据解密、转换并加密为密文标准数据以同步维护于区块链关系型数据库中，从而利用区块链关系型数据库实现便捷的数据分析服务。另外，无论是区块链节点运行的区块链服务，或是节点设备对密文数据解密、转换并加密的过程均在相应的可信执行环境中进行，同时区块链节点在提供密文数据前需要提前对第一可信执行环境对应的远程证明进行验证，从而确保了数据处理、数据传输和数据存储的系统级别的数据安全。本说明书实施例涉及的维护区块链数据的方法实现了一份数据两处备份，客观上提高了容灾能力，在确保区块链服务执行过程具有高效存取效率的情况下实现便捷的数据分析服务；同时由于结合了可信执行环境技术，因此实现了从链上的区块链服务到链下的数据转换和数据分析服务的全流程的可信数据流转与可信数据处理的过程，尽可能地减少了数据泄露风险。

可选的，还包括：

接收所述分析需求方发送的数据分析请求；

将所述区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境，通过第二密钥将所述至少一个密文标准数据分别解密为至少一个标准数据，将基于所述数据分析请求对所述至少一个标准数据进行分析得到的分析结果返回所述分析需求方。

作为一种提供数据分析服务的实施例，节点设备上链下部署的数据分析引擎还可以用于接收分析需求方发送的数据分析请求，然后基于所述数据分析引擎调取区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境，使用第二密钥将所述至少一个密文标准数据分别解密为至少一个标准数据，并在第一可信执行环境中搭建基于至少一个标准数据（明文状态）构成的内存数据库，并基于所述数据分析请求对该内存数据库进行分析并将分析得到的分析结果返回所述分析需求方，分析结果可以通过第二密钥加密后返回分析需求方，或者以明文状态直接返回分析需求方，本说明书对此并不做任何限制，至此实现一次完整的数据分析服务。例如，数据分析请求是针对同时满足条件A与条件B的数据查询请求，那么数据分析引擎将在区块链关系型数据库中查询同时具备条件A与条件B的密文标准数据，并将这些密文标准数据读入第一可信执行环境中通过第二密钥解密为标准数据后以作为分析结果返回分析需求方。

可选的，所述将所述区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境，包括：

在确定所述分析需求方属于所述数据分析服务的合法用户的情况下，将所述区块链关系型数据库中维护的所述数据分析请求对应的所述至少一个密文标准数据读入第一可信执行环境。

在本说明书实施例中，节点设备需要首先验证分析请求方的分析权限，并在确认分析请求方具有分析权限的情况下，才会响应该分析请求方发送的数据分析请求执行后续的步骤。节点设备在第一可信执行环境中维护有数据分析服务对应的合法用户列表，节点设备——具体为数据分析引擎可以在验证分析需求方身份后（例如通过第一分析需求方对应的第一公钥对数据分析请求中包含的数字签名进行验签，在验签通过的情况下确认该数据分析请求确实来自第一公钥对应的第一分析需求方），通过在检查合法用户列表中包含该分析需求方的标识信息的情况下，确定该分析请求方具有分析权限，而在合法用户列表中不包含该分析需求方的标识信息的情况下，确定该分析请求方不具有分析权限。

可选的，所述合法用户对应的第一用户列表密文维护在所述区块链关系型数据库中，第一用户列表密文由所述节点设备在第一可信执行环境中通过第二密钥对第一用户列表进行加密后得到，第一用户列表由所述节点设备在第一可信执行环境中通过第一密钥对第二用户列表密文进行解密并基于所述数据库模式信息进行转换后得到，其中，第二用户列表密文由所述区块链节点部署的用户授权合约维护在所述区块链非关系型数据库中。

在本说明书实施例中，所述合法用户对应的合法用户列表是由节点设备从区块链关系型数据库中读取第一用户列表密文后在第一可信执行环境中使用第二密钥解密得到，而区块链关系型数据库中维护的第一用户列表密文同样也是通过本说明书实施例所涉及的维护区块链数据的方法从区块链非关系型数据库中的第二用户列表密文迁移过来的。具体而言，所述合法用户对应的合法用户列表其实是维护在区块链节点所部署的用户授权合约中，其可以通过区块链交易的方式实现修改、更新、增加等操作，如前所述，用户授权合约维护的合法用户列表实际上是被区块链节点通过第二密钥加密为第二用户列表密文后，被维护于区块链非关系型数据库中对应于所述用户授权合约的合约存储空间内，因此，第二用户列表密文可以作为本说明书实施例所涉及的密文数据，通过本说明书实施例所涉及的维护区块链数据的方法，被节点设备上部署的数据转换引擎所获取，在第一可信执行环境中通过第二密钥解密为明文状态的合法用户列表，合法用户列表又进一步被转换为所述区块链关系型数据库对应的数据库模式信息定义的标准合法用户列表（其包含的数据内涵与合法用户列表一致），以使标准合法用户列表最终通过第一密钥加密为第二用户列表密文后备维护在区块链关系数据库中。运行在第一可信执行环境中的数据分析引

擎在需要获取合法用户列表的情况下，可以从区块链关系数据库读取第一用户列表密文并使用第二密钥解密得到标准合法用户列表。本说明书实施例中，合法用户对应的合法用户列表实质上是区块链节点上部署的用户授权合约所维护，而节点设备通过本说明书实施例所涉及的维护区块链数据的方法可以将区块链非关系型数据库中以第二用户列表密文形式存储的合法用户列表以第一用户列表密文的形式同步维护于区块链关系数据库中，从而使得节点设备无需调用链上的用户授权合约而可以通过链下方式获取合法用户列表。

图3是一示例性实施例提供的一种设备的示意结构图。请参考图3，在硬件层面，该设备包括处理器302、内部总线303、网络接口306、内存308以及非易失性存储器310，当然还可能包括其他功能所需要的硬件。本说明书一个或多个实施例可以基于软件方式来实现，比如由处理器302从非易失性存储器310中读取对应的计算机程序到内存308中然后运行。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

如图4所示，图4是本说明书根据一示例性实施例提供的一种维护区块链数据的装置的框图，该装置可以应用于如图3所示的设备中，以实现本说明书的技术方案；该装置应用于部署有区块链节点和第一可信执行环境的节点设备，所述节点设备维护有区块链非关系型数据库和区块链关系型数据库，所述区块链非关系型数据库用于维护密文数据，所述密文数据由所述区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到；所述装置包括：

密文数据获取单元401，用于在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，获取所述区块链非关系型数据库中维护的所述密文数据；

数据转换单元402，用于在第一可信执行环境中，通过第一密钥将所述密文数据解密为所述区块链数据，并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，以及，通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据；

密文标准数据维护单元403，用于将所述密文标准数据维护在所述区块链关系型数据库中，所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

可选的，所述密文数据获取单元401具体用于：

接收所述区块链节点主动推送的所述密文数据；和/或，

向所述区块链节点发送区块链数据请求，接收所述区块链节点响应于所述区块链数据请求返回的所述密文数据。

可选的，所述密文数据获取单元401进一步用于：

向所述区块链节点部署的智能合约发起针对所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的所述区块链数据请求；或者，

向所述区块链节点发起针对所述区块链非关系型数据库中维护的所述密文数据的所述区块链数据请求。

可选的，在所述区块链数据请求针对于所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的情况下，所述装置还包括：

模式信息查询请求发送单元404，用于向所述智能合约发起模式信息查询请求，将所述智能合约响应于所述模式信息查询请求返回的记录于所述智能合约中的第一数据库模式信息确定为所述区块链关系型数据库对应的所述数据库模式信息。

可选的，所述远程证明包含于所述区块链数据请求；或者，

所述远程证明预先维护于所述区块链节点。

可选的，所述区块链数据包括区块数据、状态数据和事件数据。

可选的，第一密钥由所述区块链节点对所述远程证明验证通过的情况下提供至所述节点设备部署的第一可信执行环境；或者，第一密钥预先维护于第一可信执行环境中。

可选的, 还包括:

数据分析请求接收单元 405, 用于接收所述分析需求方发送的数据分析请求;

分析结果返回单元 406, 用于将所述区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境, 通过第二密钥将所述至少一个密文标准数据分别解密为至少一个标准数据, 将基于所述数据分析请求对所述至少一个标准数据进行分析得到的分析结果返回所述分析需求方。

可选的, 所述分析结果返回单元 406 进一步用于:

在确定所述分析需求方属于所述数据分析服务的合法用户的情况下, 将所述区块链关系型数据库中维护的所述数据分析请求对应的所述至少一个密文标准数据读入第一可信执行环境。

可选的, 所述合法用户对应的第一用户列表密文维护在所述区块链关系型数据库中, 第一用户列表密文由所述节点设备在第一可信执行环境中通过第二密钥对第一用户列表进行加密后得到, 第一用户列表由所述节点设备在第一可信执行环境中通过第一密钥对第二用户列表密文进行解密并基于所述数据库模式信息进行转换后得到, 其中, 第二用户列表密文由所述区块链节点部署的用户授权合约维护在所述区块链非关系型数据库中。

在 20 世纪 90 年代, 对于一个技术的改进可以很明显地区分是硬件上的改进 (例如, 对二极管、晶体管、开关等电路结构的改进) 还是软件上的改进 (对于方法流程的改进)。然而, 随着技术的发展, 当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此, 不能说一个方法流程的改进就不能用硬件实体模块来实现。例如, 可编程逻辑器件 (Programmable Logic Device, PLD) (例如现场可编程门阵列 (Field Programmable Gate Array, FPGA)) 就是这样一种集成电路, 其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统 “集成” 在一片 PLD 上, 而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且, 如今, 取代手工地制作集成电路芯片, 这种编程也多半改用 “逻辑编译器 (logic compiler)” 软件来实现, 它与程序开发撰写时所用的软件编译器相类似, 而要编译之前的原始代码也得用特定的编程语言来撰写, 此称之为硬件描述语言 (Hardware Description Language, HDL), 而 HDL 也并非仅有一种, 而是有许多种, 如 ABEL (Advanced Boolean Expression Language)、AHDL (Altera Hardware Description Language)、Confluence、CUPL (Cornell University Programming Language)、HDCal、JHDL (Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL (Ruby Hardware Description Language) 等, 目前最普遍使用的是 VHDL (Very-High-Speed Integrated Circuit Hardware Description Language) 与 Verilog。本领域技术人员也应该清楚, 只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中, 就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现, 例如, 控制器可以采取例如微处理器或处理器以及存储可由该 (微) 处理器执行的计算机可读程序代码 (例如软件或固件) 的计算机可读介质、逻辑门、开关、专用集成电路 (Application Specific Integrated Circuit, ASIC)、可编程逻辑控制器和嵌入微控制器的形式, 控制器的例子包括但不限于以下微控制器: ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320, 存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道, 除了以纯计算机可读程序代码方式实现控制器以外, 完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件, 而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至, 可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

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服务器系统。当然, 本发明不排除随着未来计算机技术的发展, 实现上述实施例功能的计算机例如可以为个人计算机、膝上型计算机、车载人机交互设备、蜂窝电

话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

虽然本说明书一个或多个实施例提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或终端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境，甚至为分布式数据处理环境)。术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、产品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。例如若使用到第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现等。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

本发明是参照根据本发明实施例的方法、装置(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算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。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。

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，磁带磁磁盘存储、石墨烯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。

本领域技术人员应明白，本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机

可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述,例如程序模块。一般地,程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个实施例,在这些分布式计算环境中,由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中,程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本说明书的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

以上所述仅为本说明书一个或多个实施例的实施例而已,并不用于限制本说明书一个或多个实施例。对于本领域技术人员来说,本说明书一个或多个实施例可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在权利要求范围之内。

权 利 要 求

1. 一种维护区块链数据的方法，应用于部署有区块链节点和第一可信执行环境的节点设备，所述节点设备维护有区块链非关系型数据库和区块链关系型数据库，所述区块链非关系型数据库用于维护密文数据，所述密文数据由所述区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到；所述方法包括：

在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下，获取所述区块链非关系型数据库中维护的所述密文数据；

在第一可信执行环境中，通过第一密钥将所述密文数据解密为所述区块链数据，并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据，以及，通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据；

将所述密文标准数据维护在所述区块链关系型数据库中，所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

2. 根据权利要求 1 所述的方法，所述获取所述区块链非关系型数据库中维护的所述密文数据，包括：

接收所述区块链节点主动推送的所述密文数据；和/或，

向所述区块链节点发送区块链数据请求，接收所述区块链节点响应于所述区块链数据请求返回的所述密文数据。

3. 根据权利要求 2 所述的方法，所述向所述区块链节点发送区块链数据请求，包括：

向所述区块链节点部署的智能合约发起针对所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的所述区块链数据请求；或者，

向所述区块链节点发起针对所述区块链非关系型数据库中维护的所述密文数据的所述区块链数据请求。

4. 根据权利要求 3 所述的方法，在所述区块链数据请求针对于所述智能合约维护在所述区块链非关系型数据库中的所述密文数据的情况下，所述方法还包括：

向所述智能合约发起模式信息查询请求，将所述智能合约响应于所述模式信息查询请求返回的记录于所述智能合约中的第一数据库模式信息确定为所述区块链关系型数据库对应的所述数据库模式信息。

5. 根据权利要求 2 所述的方法，所述远程证明包含于所述区块链数据请求；或者，

所述远程证明预先维护于所述区块链节点。

6. 根据权利要求 1 所述的方法，所述区块链数据包括区块数据、状态数据和事件数据。

7. 根据权利要求 1 所述的方法，第一密钥由所述区块链节点对所述远程证明验证通过的情况下提供至所述节点设备部署的第一可信执行环境；或者，第一密钥预先维护于第一可信执行环境中。

8. 根据权利要求 1 所述的方法，还包括：

接收所述分析需求方发送的数据分析请求；

将所述区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境，通过第二密钥将所述至少一个密文标准数据分别解密为至少一个标准数据，将基于所述数

据分析请求对所述至少一个标准数据进行分析得到的分析结果返回所述分析需求方。

9. 根据权利要求 8 所述的方法, 所述将所述区块链关系型数据库中维护的所述数据分析请求对应的至少一个密文标准数据读入第一可信执行环境, 包括:

5 在确定所述分析需求方属于所述数据分析服务的合法用户的情况下, 将所述区块链关系型数据库中维护的所述数据分析请求对应的所述至少一个密文标准数据读入第一可信执行环境。

10 10. 根据权利要求 9 所述的方法, 所述合法用户对应的第一用户列表密文维护在所述区块链关系型数据库中, 第一用户列表密文由所述节点设备在第一可信执行环境中通过第二密钥对第一用户列表进行加密后得到, 第一用户列表由所述节点设备在第一可信执行环境中通过第一密钥对第二用户列表密文进行解密并基于所述数据库模式信息进行转换后得到, 其中, 第二用户列表密文由所述区块链节点部署的用户授权合约维护在所述区块链非关系型数据库中。

11. 一种维护区块链数据的装置, 应用于部署有区块链节点和第一可信执行环境的节点设备, 所述节点设备维护有区块链非关系型数据库和区块链关系型数据库, 所述区块链非关系型数据库用于维护密文数据, 所述密文数据由所述区块链节点将在第二可信执行环境中运行区块链服务时生成的区块链数据通过第二可信执行环境对应的第一密钥加密得到; 所述装置包括:

15 区块链数据获取单元, 用于在所述区块链节点对第一可信执行环境对应的远程证明验证通过的情况下, 获取所述区块链非关系型数据库中维护的所述密文数据;

区块链数据获取单元, 用于在第一可信执行环境中, 通过第一密钥将所述密文数据解密为所述区块链数据, 并将所述区块链数据转换为所述区块链关系型数据库对应的数据库模式信息定义的标准数据, 以及, 通过第一可信执行环境对应的第二密钥将所述标准数据加密为密文标准数据;

20 标准数据维护单元, 用于将所述密文标准数据维护在所述区块链关系型数据库中, 所述区块链关系型数据库用于向分析需求方提供运行在第一可信执行环境中的数据分析服务。

12. 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;

25 其中, 所述处理器通过运行所述可执行指令以实现如权利要求 1-10 中任一项所述的方法。

13. 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 1-10 中任一项所述方法的步骤。

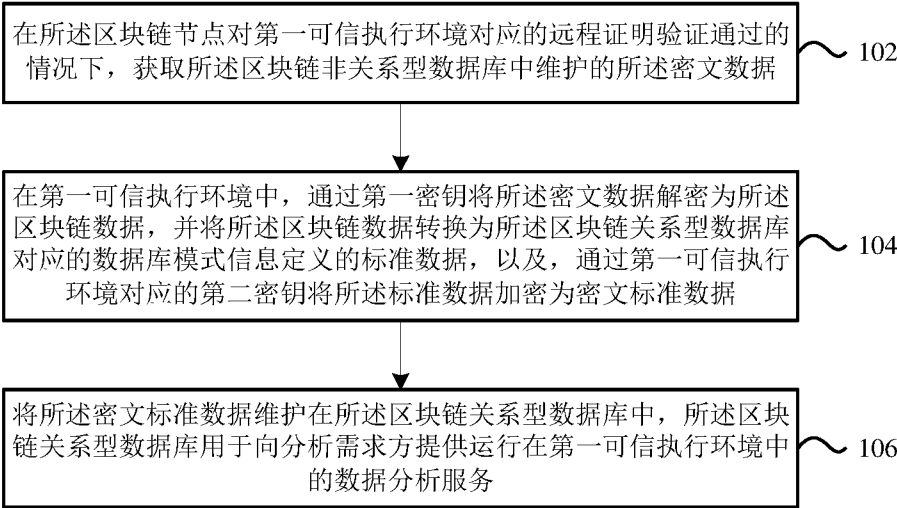


图 1

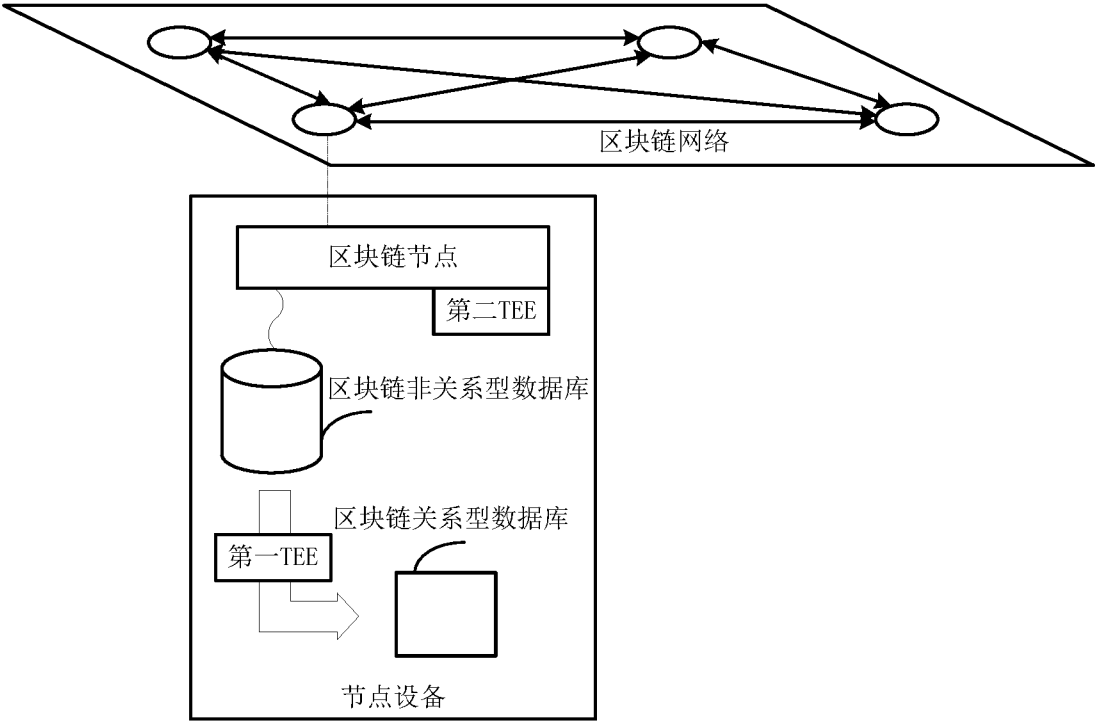


图 2

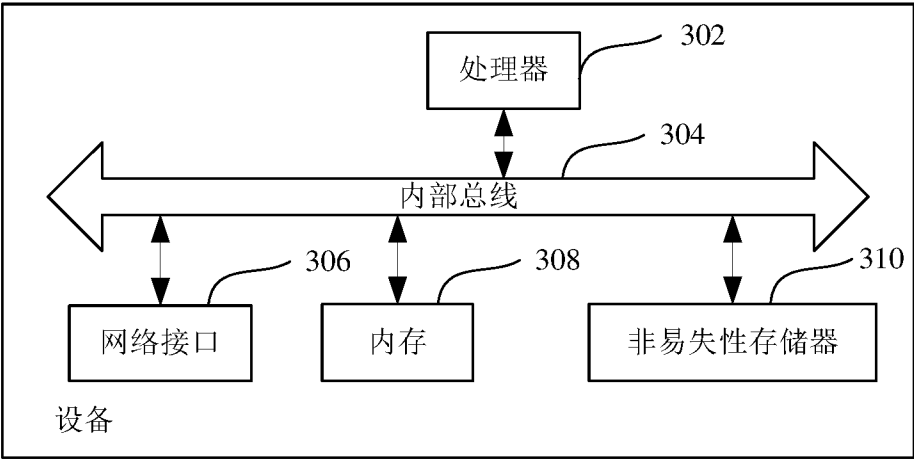


图 3

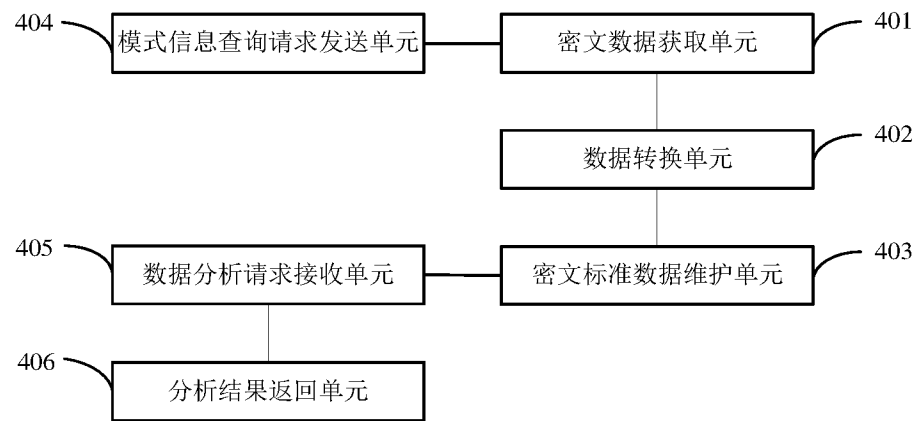


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/135413

A. CLASSIFICATION OF SUBJECT MATTER

G06F16/27(2019.01)i;G06F21/64(2013.01)i;G06F21/60(2013.01)i;G06F11/14(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)

VEN, CNTXT, ENTXT, DWPI, CNKI, IEEE: 区块链, 可信执行环境, 关系型, 非关系型, 数据库, 加密, 密文, 秘钥, 远程证明, blockchain, trusted execution environment, TEE, relational, non-relational, database, encryption, ciphertext, key, remote attestation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115129785 A (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) 30 September 2022 (2022-09-30) claims 1-13	1-13
A	CN 111899017 A (ADVANCED NEW TECHNOLOGIES CO., LTD.) 06 November 2020 (2020-11-06) description, paragraphs [0025]-[0049]	1-13
A	CN 110880972 A (FUDAN UNIVERSITY) 13 March 2020 (2020-03-13) entire document	1-13
A	CN 113742370 A (ALIBABA CLOUD COMPUTING LTD.) 03 December 2021 (2021-12-03) entire document	1-13
A	US 2020134209 A1 (ALIBABA GROUP HOLDING LIMITED) 30 April 2020 (2020-04-30) entire document	1-13



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

“D” document cited by the applicant in the international application

“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

22 March 2023

Date of mailing of the international search report

28 March 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/135413

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115129785	A	30 September 2022	None			
CN	111899017	A	06 November 2020	None			
CN	110880972	A	13 March 2020	None			
CN	113742370	A	03 December 2021	HK	40064001	A0	30 June 2022
US	2020134209	A1	30 April 2020	SG	11202100863	XA	25 February 2021
				EP	3814946	A1	05 May 2021
				WO	2020092502	A1	07 May 2020
				TW	202018571	A	16 May 2020
				US	2021081551	A1	18 March 2021
				US	2020272746	A1	27 August 2020
				HK	40006557	A0	22 May 2020
				CN	109583230	A	05 April 2019

国际检索报告

国际申请号

PCT/CN2022/135413

A. 主题的分类 G06F16/27(2019.01);G06F21/64(2013.01);G06F21/60(2013.01);G06F11/14(2006.01) 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称,和使用的检索词(如使用)) VEN, CNTXT, ENTXT, DWPI, CNKI, IEEE: 区块链, 可信执行环境, 关系型, 非关系型, 数据库, 加密, 密文, 密钥, 远程证明, blockchain, trusted execution environment, TEE, relational, non-relational, database, encryption, ciphertext, key, remote attestation		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 115129785 A (蚂蚁区块链科技(上海)有限公司) 2022年9月30日 (2022 - 09 - 30) 权利要求1-13	1-13
A	CN 111899017 A (创新先进技术有限公司) 2020年11月6日 (2020 - 11 - 06) 说明书第[0025]-[0049]段	1-13
A	CN 110880972 A (复旦大学) 2020年3月13日 (2020 - 03 - 13) 全文	1-13
A	CN 113742370 A (阿里云计算有限公司) 2021年12月3日 (2021 - 12 - 03) 全文	1-13
A	US 2020134209 A1 (ALIBABA GROUP HOLDING LIMITED) 2020年4月30日 (2020 - 04 - 30) 全文	1-13
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “D” 申请人在国际申请中引证的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2023年3月22日		国际检索报告邮寄日期 2023年3月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 孔昕 电话号码 (+86) 010-53961371

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/135413

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	115129785	A	2022年9月30日	无			
CN	111899017	A	2020年11月6日	无			
CN	110880972	A	2020年3月13日	无			
CN	113742370	A	2021年12月3日	HK	40064001	A0	2022年6月30日
US	2020134209	A1	2020年4月30日	SG	11202100863	XA	2021年2月25日
				EP	3814946	A1	2021年5月5日
				WO	2020092502	A1	2020年5月7日
				TW	202018571	A	2020年5月16日
				US	2021081551	A1	2021年3月18日
				US	2020272746	A1	2020年8月27日
				HK	40006557	A0	2020年5月22日
				CN	109583230	A	2019年4月5日