(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
2020 年 11 月 26 日 (26.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/233643 A1

(51) 国际专利分类号:
G06F 16/27 (2019.01) *G06F 16/22* (2019.01)

(21) 国际申请号: PCT/CN2020/091427

(22) 国际申请日: 2020 年 5 月 20 日 (20.05.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910419898.9 2019年5月20日 (20.05.2019) CN

(71) 申请人: 创新先进技术有限公司 (**ADVANCED NEW TECHNOLOGIES CO., LTD.**) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 刘琦 (**LIU, Qi**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 闫莺 (**YAN, Ying**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 魏长征 (**WEI, Changzheng**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (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,

(54) **Title:** RECEIPT STORAGE METHOD AND NODE EMPLOYING MULTI-DIMENSIONAL INFORMATION AND HAVING RESTRICTION

(54) 发明名称: 基于多维度信息且具有条件限制的收据存储方法和节点

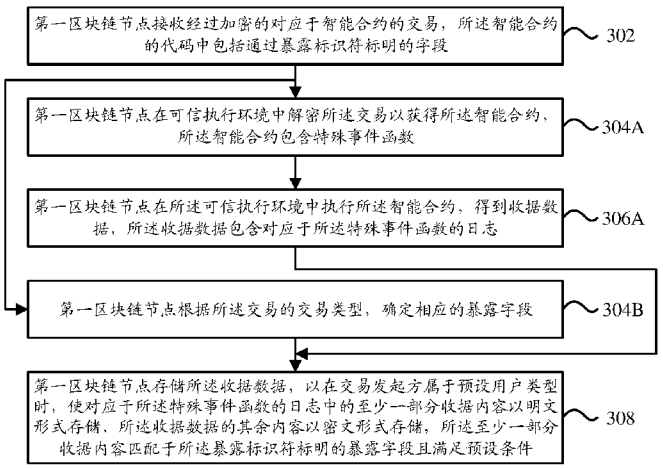

图 3

302 A first blockchain node receives an encrypted transaction corresponding to a smart contract, wherein code of the smart contract comprises a field marked with an exposure identifier

304A The first blockchain node decrypts the transaction in a trusted execution environment so as to obtain the smart contract, wherein the smart contract includes a special event function

304B The first blockchain node determines, according to a transaction type of the transaction, a corresponding exposure field

306A The first blockchain node executes the smart contract in the trusted execution environment so as to obtain receipt data, wherein the receipt data includes a log corresponding to the special event function

308 The first blockchain node stores the receipt data, such that when a transaction initiator is a preset user type, at least part of a receipt in the log corresponding to the special event function is stored as plaintext, and the rest of the receipt is stored as ciphertext, wherein the at least part of the receipt matches an exposure field marked with the exposure identifier and meets a preset condition

(57) **Abstract:** A receipt storage method and node employing multi-dimensional information and having a restriction, the method comprising: a first blockchain node receiving an encrypted transaction corresponding to a smart contract, wherein code of the smart contract comprises a field marked with an exposure identifier (302); the first blockchain node decrypting the transaction in a trusted execution environment so as to obtain the smart contract, wherein the smart contract includes a special event function (304A); the first blockchain node executing the smart contract in the trusted execution environment so as to obtain receipt data, wherein the receipt data includes a log corresponding to the special event function (306A); the first blockchain node determining, according to a transaction type of the transaction, a corresponding exposure field (304B); and the first blockchain node storing the receipt data, such that when a transaction initiator is a preset user type, at least part of a receipt in the log corresponding to the special event function is stored as plaintext, and the rest of the receipt is stored as ciphertext, wherein the at least part of the receipt matches an exposure field marked with the exposure identifier and meets a preset condition (308).

WO 2020/233643 A1

[见续页]

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

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种基于多维度信息且具有条件限制的收据存储方法和节点，包括：第一区块链节点接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段(302)；第一区块链节点在可信执行环境中解密交易以获得所述智能合约，所述智能合约包含特殊事件函数（304A）；第一区块链节点在所述可信执行环境中执行智能合约，得到的收据数据，所述收据数据包含对应于所述特殊事件函数对应的日志（306A）；第一区块链节点根据所述交易的交易类型，确定相应的暴露字段（304B）；第一区块链节点存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于暴露标识符标明的暴露字段且满足预设条件（308）。

基于多维度信息且具有条件限制的收据存储方法和节点

技术领域

[01]本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于多维度信息且具有条件限制的收据存储方法和节点。

背景技术

[02]区块链技术构建在传输网络（例如点对点网络）之上。传输网络中的网络节点利用链式数据结构来验证与存储数据，并采用分布式节点共识算法来生成和更新数据。

[03]目前企业级的区块链平台技术上最大的两个挑战就是隐私和性能，往往这两个挑战很难同时解决。大多解决方案都是通过损失性能换取隐私，或者不大考虑隐私去追求性能。常见的解决隐私问题的加密技术，如同态加密(Homomorphic encryption)和零知识证明(Zero-knowledge proof)等复杂度高，通用性差，而且还可能带来严重的性能损失。

[04]可信执行环境（Trusted Execution Environment, TEE）是另一种解决隐私问题的方式。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，因此与 TEE 相结合可以在性能损失较小的前提下很大程度上提升区块链的安全性和隐私性。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，包括软件方面的 TPM（Trusted Platform Module，可信赖平台模块）以及硬件方面的 Intel SGX（Software Guard Extensions, 软件保护扩展）、ARM Trustzone（信任区）和 AMD PSP（Platform Security Processor，平台安全处理器）。

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基于多维度信息且具有条件限制的收据存储方法和节点。

[06]为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[07]根据本说明书一个或多个实施例的第一方面，提出了一种基于多维度信息且具有条件限制的收据存储方法，包括：

[08]第一区块链节点接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段；

[09]第一区块链节点在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数；

[10]第一区块链节点在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志；

[11]第一区块链节点根据所述交易的交易类型，确定相应的暴露字段；

[12]第一区块链节点存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[13]根据本说明书一个或多个实施例的第二方面，提出了一种基于多维度信息且具有条件限制的收据存储节点，包括：

[14]接收单元，接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段；

[15]解密单元，在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数；

[16]执行单元，在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志；

[17]确定单元，根据所述交易的交易类型，确定相应的暴露字段；

[18]存储单元，存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[19]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：

[20]处理器；

[21]用于存储处理器可执行指令的存储器；

[22]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。

[23]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。

附图说明

[24]图 1 是一示例性实施例提供的一种创建智能合约的示意图。

[25]图 2 是一示例性实施例提供的一种调用智能合约的示意图。

[26]图 3 是一示例性实施例提供的一种基于多维度信息且具有条件限制的收据存储方法的流程图。

[27]图 4 是一示例性实施例提供的一种在区块链节点上实现隐私保护的示意图。

[28]图 5 是一示例性实施例提供的一种通过系统合约和链代码实现区块链网络的功能逻辑的示意图。

[29]图 6 是一示例性实施例提供的一种基于多维度信息且具有条件限制的收据存储节点的框图。

具体实施方式

[30]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[31]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[32]区块链一般被划分为三种类型：公有链（Public Blockchain），私有链（Private Blockchain）和联盟链（Consortium Blockchain）。此外，还有多种类型的结合，比如私

有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表，加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等。而且，各参与者（即节点）可自由加入以及退出网络，并进行相关操作。私有链则相反，该网络的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。这种类型的区块链更适合于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织；参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。

[33]不论是公有链、私有链还是联盟链，都可能提供智能合约的功能。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。

[34]以以太坊为例，支持用户在以太坊网络中创建并调用一些复杂的逻辑，这是以太坊区别于比特币区块链技术的最大挑战。以太坊作为一个可编程区块链的核心是以太坊虚拟机（EVM），每个以太坊节点都可以运行EVM。EVM是一个图灵完备的虚拟机，这意味着可以通过它实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。实际上，虚拟机直接运行的是虚拟机代码（虚拟机字节码，下简称“字节码”）。部署在区块链上的智能合约可以是字节码的形式。

[35]例如图1所示，Bob将一个包含创建智能合约信息的交易发送到以太坊网络后，节点1的EVM可以执行这个交易并生成对应的合约实例。图中1中的“0x6f8ae93...”代表了这个合约的地址，交易的data字段保存的可以是字节码，交易的to字段为空。节点间通过共识机制达成一致后，这个合约成功创建，并且可以在后续过程中被调用。合约创建后，区块链上出现一个与该智能合约对应的合约账户，并拥有一个特定的地址，合约代码将保存在该合约账户中。智能合约的行为由合约代码控制。换句话说，智能合约使得区块链上产生包含合约代码和账户存储（Storage）的虚拟账户。

[36]如图2所示，仍以以太坊为例，Bob将一个用于调用智能合约的交易发送到以太坊网络后，某一节点的EVM可以执行这个交易并生成对应的合约实例。图中2中交易的from字段是交易发起方（即Bob）的账户的地址，to字段中的“0x6f8ae93...”代表了被调用的智能合约的地址，value字段在以太坊中是以太币的值，交易的data字段保存的调用智能合约的方法和参数。智能合约以规定的方式在区块链网络中每个节点独立的执行，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。

[37] 区块链网络中的节点在执行 Bob 发起的交易后，会生成相应的收据（receipt）数据，以用于记录该交易相关的收据信息。以以太坊为例，节点执行交易所得的收据数据可以包括如下内容:

[38] Result 字段，表示交易的执行结果;

[39] Gas used 字段，表示交易消耗的 gas 值;

[40] Logs 字段，表示交易产生的日志，日志可以进一步包括 From 字段、To 字段、Topic 字段和 Log data 字段等，其中 From 字段表示调用的发起方的账户地址、To 字段表示被调用对象（如智能合约）的账户地址、Topic 字段表示日志的主题、Log data 字段表示日志数据;

[41] Output 字段，表示交易的输出。

[42] 一般的，交易执行后生成的收据数据以明文形式进行存储，任何人都可以看到收据数据所含的上述各个收据字段的内容，无隐私保护的设置和能力。而在一些区块链与 TEE 相结合的解决方案中，为了实现隐私保护，收据数据的全部内容均被当作需要隐私保护的数据存储在区块链上。所述区块链，是存储在节点的数据库中特定逻辑组织而成的数据集合。所述数据库，如后所述，其物理载体可以存储介质，例如持久性存储介质。实际上，收据数据中可能只有部分内容是敏感的，而其它内容并不敏感，只需要针对敏感的内容进行隐私保护、其他内容可以公开，甚至在一些情况下可能需要对部分内容实施检索以驱动相关操作的实施，那么针对这部分内容实施隐私保护将影响检索操作的实施。

[43] 以下结合图 3 所示说明本申请一基于多维度信息且具有条件限制的收据存储方法的实施例的实现过程:

[44] 步骤 302，第一区块链节点接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段。

[45] 暴露标识符为智能合约的编程语言中所定义的全局性标识，适用于采用该编程语言编写的所有智能合约。因此，通过在编程语言中定义暴露标识符，使得在任一智能合约的代码使用该暴露标识符，即可实现对收据数据的存储控制。例如，用户在编写智能合约的代码时，可以通过在代码中添加暴露标识符来标明一个或多个字段，以表明用户希望收据数据中对应于这部分字段的收据内容采用明文存储，而剩余未标注暴露标识符的

字段所对应的收据内容不允许采用明文存储、必须采用密文存储，以实现相应的隐私保护。

[46]换言之，对于暴露标识符标明的字段，从编程语言的维度上而言，允许将相应的收据内容以明文形式存储；但是，本说明书还可以进一步考量交易发起方所属的用户类型、交易的交易类型、智能合约所含的事件函数和收据内容对预设条件的满足情况，并从编程语言、用户类型、交易类型、事件函数和预设条件的维度上实现综合考量，确定是否将暴露标识符标明的字段所对应的收据内容以明文形式存储。与用户类型、交易类型、事件函数和预设条件相关的信息将在下文描述，此处暂不赘述。

[47]如上文所述，在用于创建智能合约的交易中，data 字段保存的可以是该智能合约的字节码。字节码由一连串的字节组成，每一字节可以标识一个操作。基于开发效率、可读性等多方面考虑，开发者可以不直接书写字节码，而是选择一门高级语言编写智能合约代码。高级语言编写的智能合约的代码，经过编译器编译而生成字节码，进而该字节码可以部署到区块链上。以太坊支持的高级语言很多，如 Solidity、Serpent、LLL 语言等。

[48]以 Solidity 语言为例，用其编写的合约与面向对象编程语言中的类（Class）很相似，在一个合约中可以声明多种成员，包括状态变量、函数、函数修改器、事件等。如下是以 Solidity 语言编写的一个简单的智能合约的代码示例 1：

```
Contract Example{
    int price;
    event currentPrice(int price);
    function get_price( ) returns(int){
        emit currentPrice(price);
        return price;
    }
}
```

[49]在基于 Solidity 语言编写的智能合约的代码中，可以通过暴露标识符来标明一个或多个字段，使得收据数据中对应于这部分字段的收据内容被允许以明文形式存储（需要进一步结合用户类型、交易类型、事件函数和预设条件的维度来确定实际是否采用明文存储），而其余的收据内容应当以密文形式存储。类似地，在基于 Serpent、LLL 语言

等编写的智能合约的代码中，同样可以通过暴露标识符来标明一个或多个字段，以实现相关收据内容的明文存储。

[50]暴露标识符可以为专用于标明允许明文存储的收据字段，例如可以采用关键字 plain 来表征该暴露标识符。那么，对于希望以明文形式存储的收据内容，可以在相应的字段之前添加 plain（或者，也可以采用其他方式与相应的字段进行关联）。

[51]暴露标识符标明的字段可以包括收据字段，比如上文所述的 Result 字段、Gas used 字段、Logs 字段、Output 字段等，或者 Logs 字段中进一步包含的 From 字段、To 字段、Topic 字段、Log data 字段等。例如，可以将上述的代码示例 1 调整为下述的代码示例 2:

```
plain Contract Example{
    int price;
    event currentPrice(int price);
    function get_price( ) returns(int){
        emit currentPrice(price);
        return price;
    }
}
```

[52]在上述的代码示例 2 中，在智能合约的代码最前方添加暴露标识符 plain，使得智能合约的代码被执行后，当交易发起方属于预设用户类型时，对于收据数据中由特殊事件函数产生的日志，允许该智能合约所属交易的交易类型对应的暴露字段且满足预设条件的收据内容以明文形式进行存储，比如当日志中的 From 字段属于暴露字段、To 字段并不属于暴露字段时，可以将收据数据中所有日志的 From 字段在满足预设条件时以明文形式存储、To 字段以密文形式存储，那么后续可以针对该 From 字段中的收据内容实施检索操作，比如可以统计某一账户所发起的交易量等。

[53]在一实施例中，第一区块链节点接收的交易对应的智能合约，可以是通过高级语言编写的智能合约，或者可以是字节码形式的智能合约。其中，当智能合约为高级语言编写的智能合约时，第一区块链节点还通过编译器对该高级语言编写的智能合约进行编译，生成字节码形式的智能合约，以在可信执行环境中执行。而当第一区块链节点接收的交易对应的智能合约为字节码形式的智能合约时，该字节码形式的智能合约可由客户端通过编译器对高级语言编写的智能合约进行编译而得到，而该高级语言编写的智能合约由

用户在客户端上编写得到。

[54]对于第一区块链节点接收的交易对应的智能合约，可以为用户在第一区块链节点上生成的智能合约。当用户采用高级语言编写得到上述的智能合约时，第一区块链节点还通过编译器将该高级语言编写的智能合约编译为字节码形式的智能合约；或者，用户也可能在第一区块链节点上直接编写得到字节码形式的智能合约。

[55]对于第一区块链节点接收的交易对应的智能合约，可以为用户在客户端上生成的智能合约。例如，用户通过对应的账户在客户端生成该交易后，通过该客户端将交易提交至第一区块链节点。以图 4 为例，第一区块链节点中包含交易/查询接口，该接口可与客户端对接，使得客户端可以向第一区块链节点提交上述交易。比如上文所述，用户可以采用高级语言在客户端上编写智能合约，然后由客户端通过编译器对该高级语言的智能合约进行编译，得到相应的字节码形式的智能合约。当然，客户端可以直接将高级语言编写的智能合约发送至第一区块链节点，使得第一区块链节点通过编译器编译为字节码形式的智能合约。

[56]对于第一区块链节点接收的交易对应的智能合约，可以为客户端通过第二区块链节点发来的交易中的智能合约，该智能合约通常为字节码形式；当然，该智能合约也可以为高级语言编写的智能合约，则第一区块链节点可以通过编译器编译为字节码形式的智能合约。

[57]在一实施例中，当智能合约的代码中包括暴露标识符时，高级语言编写的智能合约与字节码形式的智能合约可以具有相同的暴露标识符。而本领域技术人员应当理解的是：字节码可以采用不同于高级语言的暴露标识符，比如高级语言编写的智能合约的代码中包含第一标识符、字节码形式的智能合约的代码中包含第二标识符，则第一标识符与第二标识符之间存在对应关系，确保由高级语言编译为字节码后，不会影响暴露标识符的功能。

[58]步骤 304A，第一区块链节点在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数。

[59]在一实施例中，智能合约可以包含一个或多个事件，每一事件用于实现预定义的相关处理逻辑。智能合约所含的每一事件被调用执行后，均会生成对应的 Logs 字段，比如当智能合约包含事件 1 和事件 2 时，事件 1 可以生成对应的 Logs 字段、事件 2 可以生成对应的 Logs 字段，使得该智能合约对应的收据数据同时包含多个 Logs 字段。

[60]在一实施例中，智能合约所含的事件可以分为特殊事件函数和普通事件函数，其中：普通事件函数所产生的日志采用密文形式进行存储，以实现隐私保护；特殊事件函数所产生的日志则允许在满足隐私保护需求的前提下，将至少一部分日志字段以明文形式进行存储，从而可以针对该部分日志字段的内容实施检索，以驱动相关操作的实施。

[61]在一实施例中，可以在区块链网络的链代码或系统合约中记录属于“特殊事件函数”的事件函数，譬如可以记录在特殊事件函数列表中；相应地，通过将智能合约中包含的事件函数与上述的特殊事件函数列表进行对比，可以确定智能合约包含的事件函数是否为上述的特殊事件函数。

[62]在一实施例中，特殊事件函数可以为智能合约中自定义的任意函数，并通过在智能合约中添加针对事件函数的类型标识符，可以将该事件函数标记为特殊事件函数。以Solidity 语言为例，上述代码示例 1 中包含事件函数的代码示例如下：

```
event currentPrice(int price);
```

[63]在上述代码示例中，智能合约定义了事件：事件 currentPrice。但是，该事件未包含任何类型标识符，因而相应的事件函数属于普通事件函数。而对代码示例 1 中的事件函数进行调整后，可以得到事件函数的代码示例如下：

```
event currentPrice expose (int price);
```

[64]在上述修改后的代码示例中，智能合约定义了事件：事件 currentPrice。通过在事件 currentPrice 中添加类型标识符 “expose”，可以将该事件 currentPrice 标记为上述的特殊事件函数。

[65]以太坊支持的高级语言很多，如 Solidity、Serpent、LLL 语言等，均可以包含上述的类型标识符。通过编译器可以将高级语言编写的智能合约编译为相应的字节码，第一区块链节点最终在 EVM 虚拟机中执行字节码形式的智能合约。那么，上述的类型标识符在高级语言和字节码形式的智能合约代码中可以相同，或者高级语言的智能合约代码中为第一类型标识符、字节码形式的智能合约代码中为第二类型标识符，第一类型标识符与第二类型标识符之间可以相互对应。

[66]在一实施例中，通过对交易内容进行加密，可使上述经过加密的交易处于隐私保护的状态，避免交易内容发生暴露。譬如，交易内容中可能包含交易发起方的账户地址、交易目标的账户地址等信息，通过加密处理可以确保这些交易内容均无法被直接读取。

[67]在一实施例中，上述交易可以通过对称加密算法的方式进行加密，也可以采用非对

称算法的方式进行加密。对称加密采用的加密算法，例如是 DES 算法，3DES 算法，TDEA 算法，Blowfish 算法，RC5 算法，IDEA 算法等。非对称加密算法，例如是 RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。

[68]在一实施例中，上述交易可以通过对称加密算法结合非对称加密算法的方式进行加密。以客户端将上述交易提交至第一区块链节点为例，客户端可以采用对称加密算法加密交易内容，即采用对称加密算法的密钥加密交易内容，并用非对称加密算法加密对称加密算法中采用的密钥，譬如采用非对称加密算法的公钥加密对称加密算法中采用的密钥。这样，第一区块链节点接收到加密的交易后，可以先采用非对称加密算法的私钥进行解密，得到对称加密算法的密钥，进而用对称加密算法的密钥解密得到交易内容。

[69]当交易用于调用智能合约时，可以是多重嵌套结构的调用。例如，交易直接调用智能合约 1，而该智能合约 1 的代码调用了智能合约 2，且智能合约 2 中的代码指向了智能合约 3 的合约地址，使得交易实际上间接调用了智能合约 3 的代码，而智能合约 3 中包括某一事件函数。这样，相当于智能合约 1 中包含了该事件函数。具体实现过程与上述过程类似，在此不再赘述。

[70]步骤 306A，第一区块链节点在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志。

[71]如前所述，第一区块链节点在执行智能合约的代码时，针对代码所含的每一事件函数，将分别生成对应的 Logs 字段，即分别生成对应于每一事件函数的日志。因而在交易发起方属于预设用户类型的情况下，通过确定出特殊事件函数，可以进一步确定出特殊事件函数对应的日志，从而将特殊事件函数对应的至少一部分日志字段采用明文形式进行存储。

[72]在一实施例中，比如在以太坊中，第一区块链节点接收到客户端发来的调用智能合约的交易后，可以检查交易是否有效、格式是否正确，验证交易的签名是否合法等。

[73]一般来说，以太坊中的节点一般也是争夺记账权的节点，因此，第一区块链节点作为争夺记账权的节点可以在本地执行所述交易。如果争夺记账权的节点中的一个在本轮争夺记账权的过程中胜出，则成为记账节点。第一区块链节点如果在本轮争夺记账权的过程中胜出，就成为记账节点；当然，如果第一区块链节点如果在本轮争夺记账权的过程中没有胜出，则不是记账节点，而其它节点可能成为记账节点。

[74]智能合约类似于面向对象编程中的类，执行的结果生成对应该智能合约的合约实例，

类似于生成类对应的对象。执行交易中用于创建智能合约的代码的过程，会创建合约账户，并在账户空间中部署合约。以太坊中，智能合约账户的地址是由发送者的地址（如图 1-2 中的“0xf5e...”）和交易随机数（nonce）作为输入，通过加密算法生成的，比如图 1-2 中的合约地址“0x6f8ae93...”即由发送者的地址“0xf5e...”和交易中的 nonce 经加密算法生成。

[75]一般的，采用工作量证明（Proof of Work, POW）以及股权证明（Proof of Stake, POS）、委任权益证明（Delegated Proof of Stake，DPOS）等共识算法的支持智能合约的区块链网络中，争夺记账权的节点都可以在接收到包含创建智能合约的交易后执行所述交易。争夺记账权的节点中可能其中一个在本轮争夺记账权的过程中胜出，成为记账节点。记账节点可以将该包含智能合约的交易与其它交易一起打包并生成新的区块，并将生成的新的区块发送至其它节点进行共识。

[76]对于采用实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）等机制的支持智能合约的区块链网络中，具有记账权的节点在本轮记账前已经商定好。因此，第一区块链节点接收到上述交易后，如果自身不是本轮的记账节点，则可以将该交易发送至记账节点。对于本轮的记账节点（可以是第一区块链节点），在将该交易打包并生成新区块的过程中或者之前，或在将该交易与其它交易一起打包并生成新区块的过程中或者之前，可以执行该交易。所述记账节点将该交易打包（或还包括其它交易一起打包）并生成新的区块后，将生成的新的区块或者区块头发送至其它节点进行共识。

[77]如上所述，采用 POW 机制的支持智能合约的区块链网络中，或者采用 POS、DPOS、PBFT 机制的支持智能合约的区块链网络中，本轮的记账节点都可以将该交易打包并生成新的区块，并将生成的新的区块后区块头发送至其它节点进行共识。如果其它节点接收到所述区块后经验证没有问题，可以将该新的区块追加到原有的区块链末尾，从而完成记账过程，达成共识；若交易用于创建智能合约，则完成了智能合约在区块链网络上的部署，若交易用于调用智能合约，则完成了智能合约的调用和执行。其它节点验证记账节点发来的新的区块或区块头的过程中，也可以执行所述区块中的交易。

[78]所述执行过程，一般可以通过虚拟机执行。以以太坊为例，支持用户在以太坊网络中创建和/或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 ，Ethereum Virtual Machine），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。

[79]本实施例中，第一区块链节点可以在可信执行环境（Trusted Execution Environment，TEE）中执行解密的智能合约的代码。例如图 4 所示，第一区块链节点可以划分为常规执行环境（图中位于左侧）和 TEE，客户端提交的交易（如上文所述，交易可以存在其他来源；此处以客户端提交的交易为例进行说明）首先进入常规执行环境中的“交易/查询接口”进行识别，不存在隐私处理需求的交易可以被留在常规执行环境中进行处理（这里可以根据交易发起方的用户类型、交易类型、交易所含的标识符等识别是否存在隐私处理需求），而将存在隐私处理需求的交易传递至 TEE 中进行处理。TEE 与常规执行环境相互隔离。交易在进入 TEE 之前处于加密状态，在可信执行环境内则被解密为明文的交易内容，从而在确保数据安全的前提下，使得该明文的交易内容能够在 TEE 中实现高效处理，并在 TEE 中生成明文的收据数据。

[80]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。ARM 的 Trust Zone 技术最早实现了真正商用的 TEE 技术。伴随着互联网的高速发展，安全的需求越来越高，不仅限于移动设备，云端设备，数据中心都对 TEE 提出了更多的需求。TEE 的概念也得到了高速的发展和扩充。现在所说的 TEE 相比与最初提出的概念已经是更加广义的 TEE。例如，服务器芯片厂商 Intel，AMD 等都先后推出了硬件辅助的 TEE 并丰富了 TEE 的概念和特性，在工业界得到了广泛的认可。现在提起的 TEE 通常更多指这类硬件辅助的 TEE 技术。不同于移动端，云端访问需要远程访问，终端用户对硬件平台不可见，因此使用 TEE 的第一步就是要确认 TEE 的真实可信。因此现在的 TEE 技术都引入了远程证明机制，由硬件厂商(主要是 CPU 厂商) 背书并通过数字签名技术确保用户对 TEE 状态可验证。同时仅仅是安全的资源隔离也无法满足的安全需求，进一步的数据隐私保护也被提出。包括 Intel SGX， AMD SEV 在内的商用 TEE 也都提供了内存加密技术，将可信硬件限定在 CPU 内部，总线和内存的数据均是密文防止恶意用户进行窥探。例如，英特尔的软件保护扩展（SGX）等 TEE 技术隔离了代码执行、远程证明、安全配置、数据的安全存储以及用于执行代码的可信路径。在 TEE 中运行的应用程序受到安全保护，几乎不可能被第三方访问。

[81]以 Intel SGX 技术为例，SGX 提供了围圈（enclave，也称为飞地），即内存中一个加密的可信执行区域，由 CPU 保护数据不被窃取。以第一区块链节点采用支持 SGX 的 CPU 为例，利用新增的处理器指令，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），通过 CPU 内的加密引擎 MEE（Memory

Encryption Engine）对其中的数据进行加密。EPC 中加密的内容只有进入 CPU 后才会被解密成明文。因此，在 SGX 中，用户可以不信任操作系统、VMM（Virtual Machine Monitor，虚拟机监控器）、甚至 BIOS（Basic Input Output System，基本输入输出系统），只需要信任 CPU 便能确保隐私数据不会泄漏。实际应用中，可以将隐私数据加密后以密文形式传递至围圈中，并通过远程证明将对应的秘钥也传入围圈。然后，在 CPU 的加密保护下利用数据进行运算，结果会以密文形式返回。这种模式下，既可以利用强大的计算力，又不用担心数据泄漏。

[82]如上文所述，通过在 TEE 中执行解密后的交易内容，可以确保执行过程在可信环境内完成，以确保隐私信息不会发生泄漏。当上述存在隐私处理需求的交易用于创建智能合约时，该交易中包含智能合约的代码，第一区块链节点可以在 TEE 中对该交易进行解密得到其所含智能合约的代码，并进而在 TEE 中执行该代码。当上述存在隐私处理需求的交易用于调用智能合约时，第一区块链节点可以在 TEE 中执行该代码（若被调用的智能合约处理加密状态，则需要先在 TEE 中对该智能合约进行解密，以得到相应的代码）。具体的，第一区块链节点可以利用 CPU 中新增的处理器指令，在内存中分配一部分区域 EPC，通过 CPU 内的加密引擎 MEE 对上述的明文代码进行加密存入所述 EPC 中。EPC 中加密的内容进入 CPU 后被解密成明文。在 CPU 中，对明文的代码进行运算，完成执行过程。例如，在 SGX 技术中，执行智能合约的明文代码，可以将 EVM 加载进围圈中。在远程证明过程中，密钥管理服务器可以计算本地 EVM 代码的 hash 值，并与第一区块链节点中加载的 EVM 代码的 hash 值比对，比对结果正确作为通过远程证明的一个必要条件，从而完成对第一区块链节点 SGX 围圈加载的代码的度量。经过度量，正确的 EVM 可以在 SGX 中执行上述智能合约的代码。

[83]步骤 304B，第一区块链节点根据所述交易的交易类型，确定相应的暴露字段。

[84]在一实施例中，交易可以包括交易类型字段（如 TransType 字段），该交易类型字段的取值用于标明相应的交易类型。因此，通过读取交易所含交易类型字段的取值，可以确定出交易类型，比如存证类型、资产转移（如转账）类型、合约创建类型、合约调用类型等，本说明书并不对此进行限制。

[85]在一实施例中，不同类型的交易可以分别存在对应的暴露字段。暴露字段为收据数据中指定的一个或多个字段，在收据数据需要密文存储以保护隐私的前提下，可以结合前述的暴露标识符标明的字段与暴露字段之间的匹配情况，从而在交易发起方属于预设用户类型时，针对收据数据中由特殊事件函数产生的日志，选择性地将该日志中被暴露

标识符标明且满足预设条件的暴露字段对应的收据内容以明文形式进行存储，可以在满足隐私保护需求的同时，以便后续针对该明文形式存储的收据内容实施检索等操作。

[86]在一实施例中，可以预先定义每一交易类型与暴露字段之间的映射关系，并将该映射关系记录于区块链中，使得第一区块链节点可以获取该预定义的映射关系，并进一步根据上述交易的交易类型和该映射关系，确定收据数据中的暴露字段。例如，存证类型对应的暴露字段可以包括上述 From 字段之外的所有字段，资产转移类型对应的暴露字段可以包括上述的 To 字段，合约创建类型和合约调用类型对应的暴露字段可以包括上述 From 字段之外的所有字段，而对于其他交易类型的情况，此处不再一一赘述。

[87]其中，上述的映射关系具体可以记录于系统合约中。还可以将该映射关系记录于区块链网络的链代码中。通过将映射关系记录于系统合约中，便于后续针对该映射关系进行更新升级，而记录于链代码中的映射关系则相对不易实现更新升级，后续将针对两者的差异进行描述，此处暂不赘述。

[88]步骤 308，第一区块链节点存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[89]在一实施例中，用户在区块链上存在对应的外部账户，并基于该外部账户发起交易或实施其他操作。那么，交易发起方所属的用户类型，即该外部账户所属的用户类型。因此，第一区块链节点可以确定所述交易发起方对应的外部账户，并通过查询区块链上记录的所述外部账户对应的用户类型，以作为所述交易发起方所属的用户类型。

[90]在一实施例中，外部账户可以包括记录于区块链上的用户类型字段（如 UserType 字段），该用户类型字段的取值对应于用户类型。比如，当用户类型字段的取值为 00 时，用户类型为普通用户，当用户类型字段的取值为 01 时，用户类型为高级用户，当用户类型字段的取值为 11 时，用户类型为管理用户等。因此，第一区块链节点可以通过读取上述的外部账户的用户类型字段，即可基于取值确定相应的用户类型。

[91]在一实施例中，在创建上述的外部账户时，用户类型可以被配置为关联至该外部账户，使用户类型与外部账户之间的关联关系被记录于区块链中，比如通过用户类型与外部账户的账户地址来建立上述的关联关系，使得外部账户的数据结构并不需要改变，即外部账户无需包含上述的类型字段。因此，第一区块链节点可以通过读取区块链上记录

的关联关系，并基于交易发起方对应的外部账户，确定该外部账户对应的上述预设用户类型。

[92]在一实施例中，可以在一定条件下对外部账户的用户类型进行修改。例如，管理用户可以具备修改权项，使得第一区块链节点可以根据管理用户发起的更改请求，更改上述外部账户对应的用户类型。管理用户可以对应于创世块中预置的、具有管理权限的外部账户，使得管理用户可以对其他的普通用户、高级用户等进行类型更改，比如将普通用户更改为高级用户、将高级用户更改为普通用户等。

[93]第一区块链节点通过识别交易发起方所属的用户类型，可以确定交易发起方的隐私保护需求的强烈程度：当属于预设用户类型时，可以确定该交易发起方的隐私保护需求相对较弱，能够接受收据数据在一定程度上的暴露，以实现相应的功能扩展；当不属于预设用户类型时，可以确定该交易发起方的隐私保护需求相对较强，无法接受对收据数据的暴露。因而，基于对交易发起方所属的用户类型的识别，可使针对收据数据的存储方式满足交易发起方的实际需求，能够兼顾隐私保护和功能扩展。例如，普通用户的隐私保护的需求相对更低、对基于收据数据的功能扩展需求相对更高，那么对于普通用户发起的交易所产生的收据数据，可以允许部分收据内容采用明文形式存储，以便针对明文存储的收据内容实施功能扩展。再例如，高级用户和管理用户的隐私保护的需求相对更高、对基于收据数据的功能扩展需求相对更低，那么对于高级用户和管理用户发起的交易所产生的收据数据，可以将所有收据内容均采用密文形式存储。

[94]在智能合约的代码中，暴露标识符可以标明一个或多个字段，这些字段在收据数据中存在对应的收据内容。交易类型对应的暴露字段可以为收据数据中的一个或多个字段，这些字段在收据数据中存在对应的收据内容。特殊事件函数被执行后，收据数据中包含对应于特殊事件函数的日志，该日志实际为收据数据中的部分收据内容。通过选用预设条件，可以筛选出收据数据中满足该预设条件的收据内容。而本说明书中，在交易发起方属于预设用户类型的情况下，通过对暴露标识符、交易类型、特殊事件函数和预设条件进行综合考量，可以筛选出上述四部分收据内容的交叉内容，并针对该交叉内容实施明文存储，收据数据的其余内容均采用密文存储。

[95]预设条件的内容可以包括以下至少之一：相应的收据内容中包含预设内容、相应的收据内容的取值属于预设数值区间等。

[96]预设内容可以包括：指定的一个或多个关键词，比如该关键词可以包括预定义的状态变量、预定义的事件函数、表示交易执行结果的信息等，使得当收据内容包含作为关

键词的状态变量、事件函数或交易执行结果等信息时，可以判定该收据内容满足预设条件。

[97]预设内容可以包括：预设值。比如该预设值可以为数值，该数值可与状态变量的取值等进行比较，以确定状态变量的取值是否符合预期；再比如该预设值可以为数值、字母、特殊符号等构成的字符串，该字符串可与交易发起方的账户地址、交易目标方的账户地址、日志主题等进行比较，以识别出特定的交易发起方、特定的交易目标方或特定的日志主题等。以预设内容为字符串为例，假定该字符串为某一账户地址，在作为交易发起方的用户属于预设用户类型且 To 字段属于暴露字段的情况下，可使该用户在针对该账户地址发起交易且 To 字段被暴露标识符标明时，日志中的 To 字段可以在满足预设条件的情况下以明文形式存储、在不满足预设条件的情况下以密文形式存储，而其他的 From 字段等必然以密文形式存储，避免泄露隐私。

[98]预设数值区间可以表明相关收据字段的隐私保护需求情况，比如在转账场景中，预设数值区间可以为数值较小、隐私保护需求较低的数值区间，使得即便公开相关收据字段也不会造成严重的用户隐私泄露，但可以用于自动触发如 DAPP 客户端的相关操作，从而在隐私保护与便捷性之间取得一定平衡。

[99]在一实施例中，预设条件可以包括收据数据中的所有收据字段对应的通用条件，即暴露标识符标明的字段所对应的收据内容处于收据数据中的任意收据字段时，均被用于与该预设条件进行比较。例如，当预设条件为“包含预设关键词”时，可以将暴露标识符标明的字段所对应的收据内容与该预设条件所含的关键词进行比较，以确定出包含该关键词的收据内容，作为满足上述预设条件的收据内容；其中，当暴露标识符标明的字段所对应的收据内容属于某一收据字段时，该收据字段还可能包含其他收据内容，这些收据内容均以密文形式进行存储。

[100] 在一实施例中，预设条件可以包括收据数据中的每一收据字段分别对应的专用条件，即收据数据中的各个收据字段分别存在对应的预设条件，需要根据暴露标识符标明的字段所对应的收据内容所处的收据字段，确定相应的预设条件并实施比较。不同收据字段对应的预设条件之间相互独立，但可能相同，也可能不同。例如，From 字段对应的预设条件可以为“是否包含预设内容”，且该预设内容可以为预设的账户地址，表明由该账户地址发起的交易，Topic 字段对应的预设条件可以为“是否属于预设取值区间”，而 Topic 字段中可以记录相关事件引用的状态变量的取值，譬如转账场景下可以包括代表“转账金额”的状态变量，表明转账金额处于预设取值区间；那么：当暴露标

识符标明的对象所对应的收据内容同时处于 From 字段和 Topic 字段时，处于 From 字段中的收据内容适用于与预设条件“是否包含预设内容”进行比较、处于 Topic 字段中的收据内容适用于与预设条件“是否属于预设取值区间”进行比较。

[101] 由于暴露标识符为智能合约的编程语言中所定义的全局性标识，因而只要在智能合约中写入暴露标识符后，就难以修改该暴露标识符所标明的字段。而用户类型则取决于交易发起方、与编程语言无关，使得不同交易发起方即便调用同一智能合约时，对收据数据的存储方式（密文或明文）也可能存在不同。交易类型也可以由交易发起方根据需求而选取，以表明交易发起方的实际需求。预设条件可以由交易发起方根据实际需求而选取，与编程语言无关。同时，特殊事件函数的定义并不一定基于编程语言实现，比如在基于特殊事件函数列表等方式记录特殊事件函数时，即便智能合约中包含的某一事件函数原本属于特殊事件函数，也可以通过对特殊事件函数列表进行更改的方式，将原有的特殊事件函数更新为普通事件函数，从而避免该事件函数产生的日志以明文形式存储，或者将原有的普通事件函数更新为特殊事件函数，使得该事件函数产生的日志中的至少一部分内容以明文形式存储。因此，通过由不同用户对智能合约进行调用，或者发起不同类型的交易，或者调整智能合约所含事件函数的类型，或者选用不同的预设条件，可以跳脱暴露标识符的限制，调整需要明文或密文存储的收据内容。

[102] 以上述的代码示例 2 为例：假定事件 currentPrice 原本并未记录于特殊事件函数列表中，即事件 currentPrice 对应于普通事件函数，那么即便在智能合约的代码中添加了暴露标识符 plain 且交易发起方属于预设用户类型，事件 currentPrice 产生的日志中的各个字段（包括暴露字段）仍以密文形式存储。但是，如果将事件 currentPrice 添加至特殊事件函数列表中，那么代码示例 2 不需要调整的情况下，当交易发起方属于预设用户类型时，可使事件 currentPrice 对应的日志中的暴露字段在满足预设条件的情况下以明文形式存储。

[103] 需要指出的是：在上述的代码示例 2 中，通过在代码最前方声明“plain”，该暴露标识符“plain”所标明的字段为收据数据中的所有字段，且这些字段均为合约级字段，使得在交易发起方属于预设用户类型且该合约级字段属于暴露字段时，使事件 currentPrice 产生的日志中对应于该合约级字段且满足预设条件的收据内容均被允许以明文形式存储。当然，如果代码示例 2 中通过暴露标识符标注了譬如 From 字段，那么该 From 字段为上述的合约级字段，当该 From 字段进一步属于交易类型对应的暴露字段时，可在交易发起方属于预设用户类型的情况下，使第一区块链节点在存储收据数据

时，收据数据中所有对应于该 From 字段且满足预设条件的收据内容，均被允许以明文形式存储。

[104] 尤其是，当智能合约的代码中包含多个事件函数时，在多个事件函数分别产生的各自对应的 Logs 字段中，均可能存在合约级字段所对应的收据内容；进一步地，可以通过识别交易发起方所属的用户类型、交易的交易类型对应的暴露字段、各个事件函数的类型为普通事件函数或特殊事件函数以及收据内容对预设条件的满足情况，从而在交易发起方属于预设用户类型且合约级字段属于暴露字段的情况下，将所有特殊事件函数所产生的日志中对应于合约级字段且满足预设条件的收据内容以明文形式存储。例如，智能合约可以包括下述的代码示例 3:

```
plain Contract Example {
    int price;
    int price1;
    event currentPrice1(int price);
    event currentPrice2(int price1);
    ...
```

[105] 在上述的代码示例 3 中，与代码示例 2 相类似地，暴露标识符“plain”位于智能合约的代码最前方，使得收据数据中的所有字段均被标注为合约级字段；同时，智能合约中包含了事件 currentPrice1 和事件 currentPrice2：假定事件 currentPrice1 对应于特殊事件函数列表中定义的特殊事件函数、事件 currentPrice2 对应于普通事件函数，那么在交易发起方属于预设用户类型且 From 字段属于暴露字段的情况下，在事件 currentPrice1 和事件 currentPrice2 分别产生的日志 Log1、Log2 中，日志 Log1 包含的 From 字段在满足预设条件的情况下以明文形式存储、在未满足预设条件的情况下以密文形式存储，而日志 Log2 包含的 From 字段必然以密文形式存储；类似地，日志 Log1 中属于暴露字段的其他字段在满足预设条件时也以明文形式存储、非暴露字段以密文形式存储，而日志 Log2 的所有字段均以密文形式存储。并且，如果通过对特殊事件函数列表进行更新后，将事件 currentPrice2 更新为对应于特殊事件函数，那么日志 Log2 包含的属于暴露字段的所有字段可以在满足预设条件的情况下以明文形式存储、在未满足预设条件的情况下以密文形式存储，而无需对智能合约的代码做任何变动。

[106] 对于上述的合约级字段而言，可以通过前述的类型标识符来标明智能合约所含

的事件函数是否为特殊事件函数。例如，可以将上述的代码示例 3 调整为下述的代码示例 4:

```
plain Contract Example {
  int price;
  int price1;
  event currentPrice1 expose (int price);
  event currentPrice2(int price1);
  ...
```

[107] 在上述的代码示例 4 中，与代码示例 2 相类似地，合约级字段包括收据数据中的所有字段；同时，智能合约中包含了事件 currentPrice1 和事件 currentPrice2：由于事件 currentPrice1 在包含如前所述的类型标识符 expose，使得该事件 currentPrice1 被标注为对应于特殊事件函数，而事件 currentPrice2 并未包含类型标识符 expose，使得事件 currentPrice2 被标注为对应于普通事件函数，那么在交易发起方属于预设用户类型的情况下，在事件 currentPrice1 和事件 currentPrice2 分别产生的日志 Log1、Log2 中，日志 Log1 中对应于交易类型的所有暴露字段在满足预设条件的情况下以明文形式存储、在未满足预设条件的情况下以密文形式存储，而日志 Log2 包含的所有字段必然以密文形式存储。

[108] 除了合约级字段之外，暴露标识符标明的字段可以包括：对应于智能合约中定义的至少一个事件的事件级字段，使得在交易发起方属于预设用户类型且该事件级字段属于暴露字段的情况下，第一区块链节点将特殊事件函数产生的收据内容中对应于该事件级字段且满足预设条件的部分以明文形式存储。尤其是，当智能合约中包含多个事件时，可以针对至少一部分事件设定上述的事件级字段，使得这部分事件产生的日志中对应于上述事件级字段且满足预设条件的收据内容以明文形式存储，而这部分事件产生的日志中的其余收据内容、其余事件对应的收据内容均以密文形式存储。以 From 字段为例，可以将上述的代码示例 4 调整为下述的代码示例 5:

```
Contract Example {
int price;
int price1;
event currentPrice1(“from”,int price);
```

```
event currentPrice2(int price1);
...
```

[109] 在上述的代码示例 5 中，事件 currentPrice1 虽然未添加暴露标识符“plain”，但是包含了内容“from”，该内容“from”对应于 From 字段，用于表明事件 currentPrice1 所产生日志中的 From 字段需要以明文形式存储，因而该内容“from”既属于上述的暴露标识符，又标明了需要明文存储的 From 字段。并且，由于内容“from”位于事件 currentPrice1 中，因而 From 字段为事件级字段，使得在交易发起方属于预设用户类型且 From 字段属于暴露字段的情况下，当该事件 currentPrice1 对应于特殊事件函数时，在该事件 currentPrice1 对应产生的日志 Logs 中，From 字段在满足预设条件的情况下以明文形式进行存储、在未满足预设条件的情况下以密文形式存储，而其他字段必然以密文形式存储。而对于代码示例 8 所含的另一事件 currentPrice2，由于并未针对该事件 currentPrice2 添加暴露标识符，因而不论该事件 currentPrice2 对应于特殊事件函数或普通事件函数，所产生的日志 Logs 均以密文形式存储。该代码示例 5 对应的实施例中，即对于事件级字段而言，可以通过特殊事件函数列表或者类型标识符的方式识别智能合约所含的事件函数是否为特殊事件函数，此处不再一一赘述。

[110] 本说明书通过在一定程度上暴露收据内容，以用于实现对 DAPP 客户端的驱动或其他的功能扩展。并且，本说明书通过综合考虑交易发起方所属的用户类型、交易类型对应的暴露字段、暴露标识符标明的字段、特殊事件函数产生的日志和收据内容对预设条件的满足情况，可以准确选取用于明文存储的收据内容，即同时满足“交易发起方属于预设用户类型”、“属于交易类型对应的暴露字段”、“匹配于暴露标识符标明的字段”、“属于特殊事件函数产生的日志”和“满足预设条件”的收据内容，从而在满足上述功能扩展需求的同时，确保绝大部分的用户隐私能够得到保护。尤其是，当第一区块链节点是根据区块链网络上记载的信息（如特殊事件函数列表）来识别特殊事件函数时，可以在智能合约已经创建之后，通过对“特殊事件函数”进行更新，以调整收据数据的存储方式，比如将原本明文存储的收据内容改为密文存储，或者将原本密文存储的收据内容改为明文存储。

[111] 通过在计算设备（物理机或虚拟机）上运行区块链的程序代码（以下简称为链代码），可以将该计算设备配置为区块链网络中的区块链节点，比如上述的第一区块链节点等。换言之，第一区块链节点通过运行上述的链代码，以实现相应的功能逻辑。因此，可以在创建区块链网络时，将上文所述的与暴露标识符、用户类型、交易类型、事

件函数和预设条件相关的收据数据存储逻辑写入链代码中，使得各个区块链节点均可以实现该收据数据存储逻辑；以第一区块链节点为例，该与暴露标识符、用户类型、交易类型、事件函数和预设条件相关的收据数据存储逻辑可以包括：对用户类型的识别逻辑、对交易类型的识别逻辑、对事件函数的识别逻辑、对预设条件的确定逻辑、基于暴露标识符对收据内容进行存储的逻辑。

[112] 对用户类型的识别逻辑用于指示第一区块链节点：识别交易发起方的用户类型。比如：系统合约中可以记录有预定义的外部账户与用户类型之间的关联关系，或者系统合约中可以记录有用户类型字段的取值与用户类型之间的对应关系。具体可以参考上文中识别用户类型的相关描述，此处不再赘述。

[113] 对交易类型的识别逻辑用于指示第一区块链节点：识别交易发起方所发起的交易的类型。比如：根据交易所含的类型字段的取值，确定该交易对应的交易类型。具体可以参考上文中识别交易类型的相关描述，此处不再赘述。

[114] 对事件函数的识别逻辑用于指示第一区块链节点：识别交易对应的智能合约所含的事件函数的类型。比如：根据事件函数所含的类型标识符进行识别，或者根据区块链网络中记载的特殊事件函数列表进行识别。具体可以参考上文中识别特殊事件函数的相关描述，此处不再赘述。

[115] 对预设条件的确定逻辑用于指示第一区块链节点：获取暴露标识符标明的对象所对应的收据内容所适用的预设条件。比如：获取适用于所有收据字段的通用条件，或者获取适用于暴露标识符标明的对象所对应的收据内容的所处字段的专用条件等。具体可以参考上文中预设条件的相关描述，此处不再赘述。

[116] 基于暴露标识符对收据内容进行存储的逻辑用于指示第一区块链节点：针对暴露标识符标明的字段、暴露标识符未标明的字段等，分别采用何种方式存储相应的收据内容。比如：在交易发起方属于预设用户类型的情况下，对于识别出的特殊事件函数，将该特殊事件函数对应的日志中由暴露标识符标明且满足预设条件的暴露字段对应的收据内容采用明文形式进行存储，而收据数据中其他的收据内容均采用密文形式进行存储。

[117] 然而，链代码的升级更新相对较为困难，使得采用链代码实现对收据数据的存储存在灵活性低、可扩展性不足的问题。为了实现对链代码的功能扩展，如图 5 所示，可以采用链代码与系统合约相结合的方式：链代码用于实现区块链网络的基础功能，而

运行过程中的功能扩展可以通过系统合约的方式实现。与上述的智能合约相类似的，系统合约包括譬如字节码形式的代码，第一区块链节点可以通过运行系统合约的代码（比如，根据唯一对应的地址“0x53a98...”来读取该系统合约中的代码），实现对链代码的功能补充。相应地，第一区块链节点可以读取系统合约的代码，该系统合约的代码中定义了与暴露标识符、用户类型、交易类型、事件函数和预设条件相关的收据数据存储逻辑；然后，第一区块链节点可以执行系统合约的代码，从而基于与暴露标识符、用户类型、交易类型、事件函数和预设条件相关的收据数据存储逻辑，在交易发起方属于预设用户类型时，将所述特殊事件函数产生的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[118] 区别于上述由用户发布至区块链的智能合约，系统合约无法由用户自由发布。第一区块链节点读取的系统合约可以包括配置于区块链网络的创世块中的预置系统合约；以及，区块链网络中的管理员（即上述的管理用户）可以具有针对系统合约的更新权限，从而针对诸如上述的预置系统合约进行更新，则上述第一区块链节点读取的系统合约还可以包括相应的更新后系统合约。当然，更新后系统合约可以由管理员对预置系统合约实施一次更新后得到；或者，更新后系统合约可以由管理员对预置系统合约实施多次迭代更新后得到，比如由预置系统合约更新得到系统合约 1、对系统合约 1 更新得到系统合约 2、对系统合约 2 更新得到系统合约 3，该系统合约 1、系统合约 2、系统合约 3 均可以视为更新后系统合约，但第一区块链节点通常会以最新版本的系统合约为准，比如第一区块链节点会以系统合约 3 中的代码为准，而非系统合约 1 或系统合约 2 中的代码。

[119] 除了创世块中包含的预置系统合约之外，管理员还可以在后续区块内发布系统合约，以及针对所发布的系统合约进行更新。总之，应当通过诸如权限管理等方式，对系统合约的发布和更新实施一定程度的限制，以确保区块链网络的功能逻辑能够正常运作，并且避免对任何用户造成不必要的损失。

[120] 第一区块链节点通过密钥对至少一部分收据内容进行加密。所述加密，可以采用对称加密，也可以采用非对称加密。如果第一区块链节点用对称加密方式，即用对称加密算法的对称密钥对收据内容加密，则客户端（或其他持有密钥的对象）可以用该对称加密算法的对称密钥对加密后的收据内容进行解密。

[121] 第一区块链节点用对称加密算法的对称密钥对收据内容进行加密时，该对称密

钥可由客户端预先提供至第一区块链节点。那么，由于只有客户端（实际应当为客户端上的已登录账户对应的用户）和第一区块链节点掌握该对称密钥，使得仅该客户端能够解密相应的加密后的收据内容，避免无关用户甚至不法分子对加密后的收据内容进行解密。

[122] 例如，客户端在向第一区块链节点发起交易时，客户端可以用对称加密算法的初始密钥对交易内容进行加密，以得到该交易；相应地，第一区块链节点可以通过获得该初始密钥，以用于直接或间接对收据内容进行加密。譬如，该初始密钥可以由客户端与第一区块链节点预先协商得到，或者由密钥管理服务器发送至客户端和第一区块链节点，或者由客户端发送至第一区块链节点。当初始密钥由客户端发送至第一区块链节点时，客户端可以通过非对称加密算法的公钥对该初始密钥进行加密后，将加密后的初始密钥发送至第一区块链节点，而第一区块链节点通过非对称加密算法的私钥对该加密后的初始密钥进行解密，得到初始密钥，即上文所述的数字信封加密，此处不再赘述。

[123] 第一区块链节点可以采用上述的初始密钥对收据内容进行加密。不同交易采用的初始密钥可以相同，使得同一用户所提交的所有交易均采用该初始密钥进行加密，或者不同交易采用的初始密钥可以不同，比如客户端可以针对每一交易随机生成一初始密钥，以提升安全性。

[124] 第一区块链节点可以根据初始密钥与影响因子生成衍生密钥，并通过该衍生密钥对收据内容进行加密。相比于直接采用初始密钥进行加密，衍生密钥可以增加随机度，从而提升被攻破的难度，有助于优化数据的安全保护。影响因子可以与交易相关；例如，影响因子可以包括交易哈希值的指定位，比如第一区块链节点可以将初始密钥与交易哈希值的前 16 位（或前 32 位、后 16 位、后 32 位，或者其他位）进行拼接，并对拼接后的字符串进行哈希运算，从而生成衍生密钥。

[125] 第一区块链节点还可以采用非对称加密方式，即用非对称加密算法的公钥对收据内容加密，则相应地，客户端可以用所述非对称加密算法的私钥解密上述加密后的收据内容。非对称加密算法的密钥，例如可以是由客户端生成一对公钥和私钥，并将公钥预先发送至第一区块链节点，从而第一区块链节点可以将收据内容用该公钥加密。

[126] 第一区块链节点通过运行用于实现某一功能的代码，以实现该功能。因此，对于需要在 TEE 中实现的功能，同样需要执行相关代码。而对于在 TEE 中执行的代码，需要符合 TEE 的相关规范和要求；相应地，对于相关技术中用于实现某一功能的代码，需要结合 TEE 的规范和要求重新进行代码编写，不仅存在相对更大的开发量，而且容

易在重新编写过程中产生漏洞（bug），影响功能实现的可靠性和稳定性。

[127] 因此，第一区块链节点可以通过在 TEE 之外执行存储功能代码，将 TEE 中生成的收据数据（包括需要明文存储的明文形式的收据内容，以及需要密文存储的密文形式的收据内容）存储至 TEE 之外的外部存储空间，使得该存储功能代码可以为相关技术中用于实现存储功能的代码、不需要结合 TEE 的规范和要求重新进行代码编写，即可针对收据数据实现安全可靠的存储，不仅可以在不影响安全、可靠程度的基础上，减少相关代码的开发量，而且可以通过减少 TEE 的相关代码而降低 TCB (Trusted Computing Base，可信计算基)，使得 TEE 技术与区块链技术进行结合的过程中，额外造成的安全风险处于可控范围。

[128] 在一实施例中，第一区块链节点可以在 TEE 内执行写缓存功能代码，以将上述的收据数据存入 TEE 内的写缓存中，比如该写缓存可以对应于如图 2 所示的“缓存”。进一步的，第一区块链节点将写缓存中的数据从可信执行环境输出，以存储至外部存储空间。其中，写缓存功能代码可以以明文形式存储于 TEE 中，可以直接在 TEE 中执行该明文形式的缓存功能代码；或，写缓存功能代码可以以密文形式存储于 TEE 之外，比如存储于上述的外部存储空间（比如图 2 所示的“打包+存储”，其中“打包”表示第一区块链节点在可信执行环境之外对交易进行打包成块），可以将该密文形式的写缓存功能代码读入 TEE、在 TEE 中进行解密为明文代码，并执行该明文代码。

[129] 写缓存是指在将数据写入外部存储空间时，为了避免造成对外部存储空间的“冲击”而提供的“缓冲”机制。例如，可以采用 buffer 实现上述的写缓存；当然，写缓存也可以采用 cache 来实现，本说明书并不对此进行限制。实际上，由于 TEE 为隔离的安全环境，而外部存储空间位于 TEE 之外，使得通过采用写缓存机制，可以对缓存内的数据进行批量写入外部存储空间，从而减少 TEE 与外部存储空间之间的交互次数，提升数据存储效率。同时，TEE 在不断执行各条交易的过程中，可能需要调取已生成的数据，如果需调用的数据恰好位于写缓存中，可以直接从写缓存中读取该数据，这样一方面可以减少与外部存储空间之间的交互，另一方面免去了对从外部存储空间所读取数据的解密过程，从而提升在 TEE 中的数据处理效率。

[130] 当然，也可以将写缓存建立于 TEE 之外，比如第一区块链节点可以在 TEE 之外执行写缓存功能代码，从而将上述的收据数据存入 TEE 外的写缓存中，并进一步将写缓存中的数据存储至外部存储空间。

[131] 以下结合图 6 介绍本说明书一种基于多维度信息且具有条件限制的收据存储节

点的实施例，包括：

[132] 接收单元 61，接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段；

[133] 解密单元 62，在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数；

[134] 执行单元 63，在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志；

[135] 确定单元 64，根据所述交易的交易类型，确定相应的暴露字段；

[136] 存储单元 65，存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[137] 可选的，第一区块链节点接收的交易对应的智能合约，包括：

[138] 高级语言编写的智能合约；或，

[139] 字节码形式的智能合约。

[140] 可选的，当第一区块链节点接收的交易对应的智能合约为高级语言编写的智能合约时，所述节点还包括：

[141] 编译单元 66，通过编译器对所述高级语言编写的智能合约进行编译，生成字节码形式的智能合约，以在所述可信执行环境中执行。

[142] 可选的，当第一区块链节点接收的交易对应的智能合约为字节码形式的智能合约时，所述字节码形式的智能合约由客户端通过编译器对高级语言编写的智能合约进行编译而得到，所述高级语言编写的智能合约由用户在所述客户端上编写得到。

[143] 可选的，所述高级语言编写的智能合约与所述字节码形式的智能合约具有相同或对应的暴露标识符。

[144] 可选的，第一区块链节点接收的交易对应的智能合约，包括：

[145] 用户在第一区块链节点上生成的智能合约；或，

[146] 用户在客户端上生成的智能合约；或，

[147] 所述客户端通过第二区块链节点发来的交易中的智能合约。

[148] 可选的，所述暴露标识符标明的字段包括：合约级字段；存储单元 65 具体用于：

[149] 在交易发起方属于预设用户类型且所述合约级字段属于暴露字段时，将所有特殊事件函数产生的日志中对应于所述合约级字段且满足预设条件的部分以明文形式存储。

[150] 可选的，所述暴露标识符标明的字段包括：对应于所述智能合约中定义的至少一个事件的事件级字段；存储单元 65 具体用于：

[151] 在交易发起方属于预设用户类型且所述事件级字段属于暴露字段时，确定出所述至少一个事件对应的特殊事件函数产生的日志，并将确定出的日志中对应于所述事件级字段且满足预设条件的部分以明文形式存储。

[152] 可选的，所述智能合约中的事件函数包含类型标识符，所述类型标识符用于将所述事件函数标记为特殊事件函数。

[153] 可选的，当所述智能合约包含的事件函数位于区块链上记录的特殊函数列表中时，所述智能合约包含的事件函数被判定为特殊事件函数。

[154] 可选的，第一区块链节点通过下述方式确定所述交易发起方所属的用户类型：

[155] 第一区块链节点确定所述交易发起方对应的外部账户；

[156] 第一区块链节点查询区块链上记录的所述外部账户对应的用户类型，以作为所述交易发起方所属的用户类型。

[157] 可选的，所述外部账户包括记录于区块链上的用户类型字段，所述用户类型字段的取值对应于所述用户类型。

[158] 可选的，在创建所述外部账户时，所述用户类型被配置为关联至所述外部账户，使所述用户类型与所述外部账户之间的关联关系被记录于区块链中。

[159] 可选的，还包括：

[160] 更改单元 67，根据管理用户发起的更改请求，更改所述外部账户对应的用户类型。

[161] 可选的，所述交易包括交易类型字段，所述交易类型字段的取值用于标明相应的交易类型。

[162] 可选的，所述交易的交易类型包括：存证类型、资产转移类型、合约创建类型、合约调用类型。

[163] 可选的，区块链中存储有预定义的交易类型与暴露字段之间的映射关系，所述映射关系被用于确定所述交易的交易类型对应的暴露字段。

[164] 可选的，所述预设条件包括以下至少之一：相应的收据内容中包含预设内容、相应的收据内容的取值属于预设数值区间。

[165] 可选的，

[166] 所述预设条件包括所述收据数据中的所有收据字段对应的通用条件；或，

[167] 所述预设条件包括所述收据数据中的每一收据字段分别对应的专用条件。

[168] 可选的，

[169] 所述预设条件位于所述交易中；或，

[170] 所述预设条件位于所述交易对应的智能合约中，或所述交易对应的智能合约所调用的另一智能合约中；或，

[171] 所述预设条件位于系统合约或链代码中。

[172] 可选的，存储单元 65 具体用于：

[173] 读取系统合约的代码，所述系统合约的代码中定义了与暴露标识符、用户类型、交易类型、特殊事件函数和预设条件相关的收据数据存储逻辑；

[174] 执行所述系统合约的代码，以在交易发起方属于预设用户类型时，将对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

[175] 可选的，所述系统合约包括：记录于创世块中的预置系统合约，或所述预置系统合约对应的更新后系统合约。

[176] 可选的，存储单元 65 具体用于：

[177] 在所述可信执行环境之外执行存储功能代码，以将所述收据数据存储至所述可信执行环境之外的外部存储空间。

[178] 可选的，第一区块链节点对所述收据数据进行加密的密钥包括：对称加密算法

的密钥或非对称加密算法的密钥。

[179] 可选的，所述对称加密算法的密钥包括所述客户端提供的初始密钥；或，所述对称加密算法的密钥包括所述初始密钥与影响因子生成的衍生密钥。

[180] 可选的，所述交易由所述初始密钥进行加密，且所述初始密钥被非对称加密算法的公钥进行加密；解密单元 62 具体用于：

[181] 用所述非对称加密算法的私钥解密得到所述初始密钥，并用所述初始密钥对所述交易进行解密，以得到所述交易内容。

[182] 可选的，所述初始密钥由客户端生成；或，所述初始密钥由密钥管理服务器发送至所述客户端。

[183] 可选的，所述影响因子与所述交易相关。

[184] 可选的，所述影响因子包括：所述交易的哈希值的指定位。

[185] 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。

[186] 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。

[187] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

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

[189] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

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

行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

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

[192] 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。

[193] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。在一个典型的配置中，计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[194] 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。

[195] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[196] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排

他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[197] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[198] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

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

[200] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种基于多维度信息且具有条件限制的收据存储方法，包括:

第一区块链节点接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段;

第一区块链节点在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数;

第一区块链节点在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志;

第一区块链节点根据所述交易的交易类型，确定相应的暴露字段;

第一区块链节点存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

2. 根据权利要求 1 所述的方法，第一区块链节点接收的交易对应的智能合约，包括:

高级语言编写的智能合约；或，

字节码形式的智能合约。

3. 根据权利要求 2 所述的方法，当第一区块链节点接收的交易对应的智能合约为高级语言编写的智能合约时，所述方法还包括:

第一区块链节点通过编译器对所述高级语言编写的智能合约进行编译，生成字节码形式的智能合约，以在所述可信执行环境中执行。

4. 根据权利要求 2 所述的方法，当第一区块链节点接收的交易对应的智能合约为字节码形式的智能合约时，所述字节码形式的智能合约由客户端通过编译器对高级语言编写的智能合约进行编译而得到，所述高级语言编写的智能合约由用户在所述客户端上编写得到。

5. 根据权利要求 2 所述的方法，所述高级语言编写的智能合约与所述字节码形式的智能合约具有相同或对应的暴露标识符。

6. 根据权利要求 1 所述的方法，第一区块链节点接收的交易对应的智能合约，包括:

用户在第一区块链节点上生成的智能合约；或，

用户在客户端上生成的智能合约；或，

所述客户端通过第二区块链节点发来的交易中的智能合约。

7. 根据权利要求 1 所述的方法，所述暴露标识符标明的字段包括：合约级字段；第一区块链节点存储所述收据数据，包括：

第一区块链节点在交易发起方属于预设用户类型且所述合约级字段属于暴露字段时，将所有特殊事件函数产生的日志中对应于所述合约级字段且满足预设条件的部分以明文形式存储。

8. 根据权利要求 1 所述的方法，所述暴露标识符标明的字段包括：对应于所述智能合约中定义的至少一个事件的事件级字段；第一区块链节点存储所述收据数据，包括：

第一区块链节点在交易发起方属于预设用户类型且所述事件级字段属于暴露字段时，确定出所述至少一个事件对应的特殊事件函数产生的日志，并将确定出的日志中对应于所述事件级字段且满足预设条件的部分以明文形式存储。

9. 根据权利要求 1 所述的方法，所述智能合约中的事件函数包含类型标识符，所述类型标识符用于将所述事件函数标记为特殊事件函数。

10. 根据权利要求 1 所述的方法，当所述智能合约包含的事件函数位于区块链上记录的特殊函数列表中时，所述智能合约包含的事件函数被判定为特殊事件函数。

11. 根据权利要求 1 所述的方法，第一区块链节点通过下述方式确定所述交易发起方所属的用户类型：

第一区块链节点确定所述交易发起方对应的外部账户；

第一区块链节点查询区块链上记录的所述外部账户对应的用户类型，以作为所述交易发起方所属的用户类型。

12. 根据权利要求 11 所述的方法，所述外部账户包括记录于区块链上的用户类型字段，所述用户类型字段的取值对应于所述用户类型。

13. 根据权利要求 11 所述的方法，在创建所述外部账户时，所述用户类型被配置为关联至所述外部账户，使所述用户类型与所述外部账户之间的关联关系被记录于区块链中。

14. 根据权利要求 13 所述的方法，还包括：

第一区块链节点根据管理用户发起的更改请求，更改所述外部账户对应的用户类型。

15. 根据权利要求 1 所述的方法，所述交易包括交易类型字段，所述交易类型字段的取值用于标明相应的交易类型。

16. 根据权利要求 1 所述的方法，所述交易的交易类型包括：存证类型、资产转移类型、合约创建类型、合约调用类型。

17. 根据权利要求 1 所述的方法，区块链中存储有预定义的交易类型与暴露字段之间的映射关系，所述映射关系被用于确定所述交易的交易类型对应的暴露字段。

18. 根据权利要求 1 所述的方法，所述预设条件包括以下至少之一：相应的收据内容中包含预设内容、相应的收据内容的取值属于预设数值区间。

19. 根据权利要求 1 所述的方法，

所述预设条件包括所述收据数据中的所有收据字段对应的通用条件；或，

所述预设条件包括所述收据数据中的每一收据字段分别对应的专用条件。

20. 根据权利要求 1 所述的方法，

所述预设条件位于所述交易中；或，

所述预设条件位于所述交易对应的智能合约中，或所述交易对应的智能合约所调用的另一智能合约中；或，

所述预设条件位于系统合约或链代码中。

21. 根据权利要求 1 所述的方法，第一区块链节点存储所述收据数据，包括：

第一区块链节点读取系统合约的代码，所述系统合约的代码中定义了与暴露标识符、用户类型、交易类型、特殊事件函数和预设条件相关的收据数据存储逻辑；

第一区块链节点执行所述系统合约的代码，以在交易发起方属于预设用户类型时，将对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件。

22. 根据权利要求 21 所述的方法，所述系统合约包括：记录于创世块中的预置系统合约，或所述预置系统合约对应的更新后系统合约。

23. 根据权利要求 1 所述的方法，第一区块链节点存储所述收据数据，包括：

第一区块链节点在所述可信执行环境之外执行存储功能代码，以将所述收据数据存储至所述可信执行环境之外的外部存储空间。

24. 根据权利要求 1 所述的方法，第一区块链节点对所述收据数据进行加密的密钥包括：对称加密算法的密钥或非对称加密算法的密钥。

25. 根据权利要求 24 所述的方法，所述对称加密算法的密钥包括所述客户端提供的初始密钥；或，所述对称加密算法的密钥包括所述初始密钥与影响因子生成的衍生密钥。

26. 根据权利要求 25 所述的方法，所述交易由所述初始密钥进行加密，且所述初始密钥被非对称加密算法的公钥进行加密；第一区块链节点在可信执行环境中解密所述

交易，包括:

第一区块链节点用所述非对称加密算法的私钥解密得到所述初始密钥，并用所述初始密钥对所述交易进行解密，以得到所述交易内容。

27. 根据权利要求 25 所述的方法，所述初始密钥由客户端生成；或，所述初始密钥由密钥管理服务器发送至所述客户端。

28. 根据权利要求 25 所述的方法，所述影响因子与所述交易相关。

29. 根据权利要求 28 所述的方法，所述影响因子包括：所述交易的哈希值的指定位。

30. 一种基于多维度信息且具有条件限制的收据存储节点，包括:

接收单元，接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段;

解密单元，在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数;

执行单元，在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志;

确定单元，根据所述交易的交易类型，确定相应的暴露字段;

存储单元，存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段。

31. 一种电子设备，包括:

处理器;

用于存储处理器可执行指令的存储器;

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-29 中任一项所述的方法。

32. 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 1-29 中任一项所述方法的步骤。

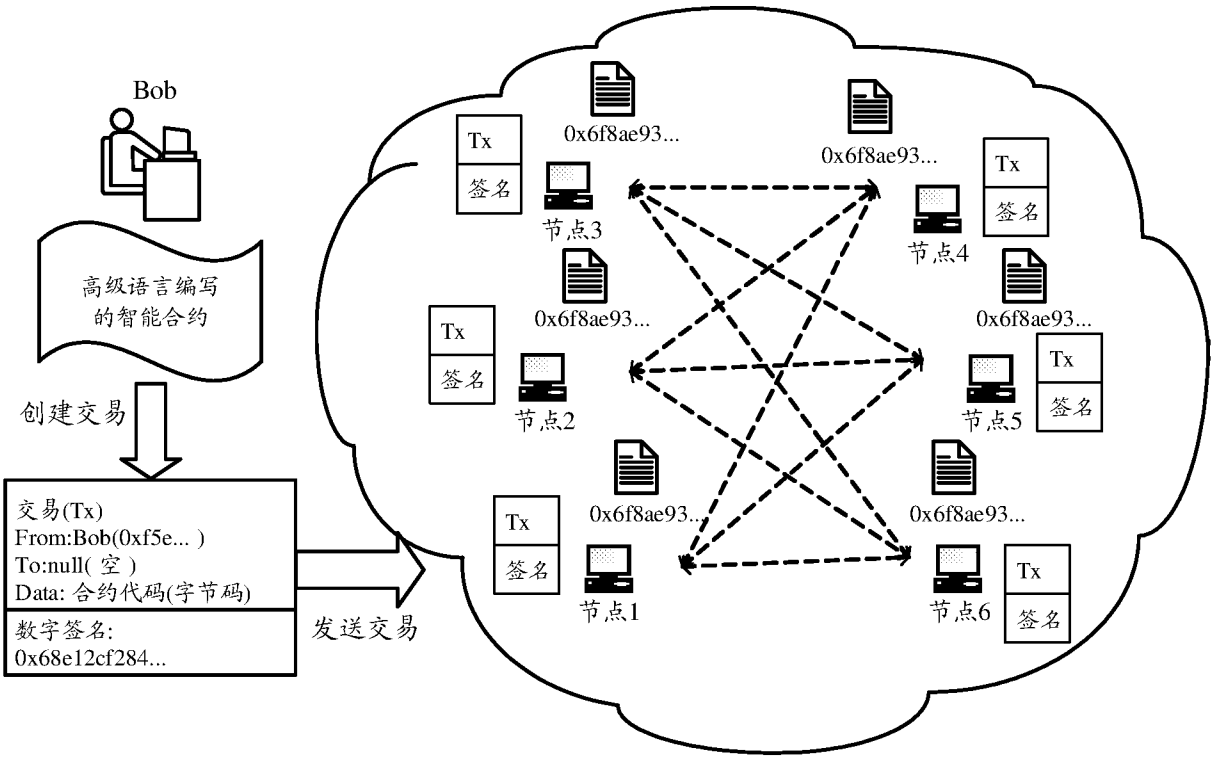
Bob
高级语言编写
的智能合约
创建交易
交易(Tx)
From:Bob(0xf5e...)
To:null(空)
Data: 合约代码(字节码)
数字签名:
0x68e12cf284...
发送交易
Tx
签名
0x6f8ae93...
节点1
节点2
节点3
节点4
节点5
节点6

图 1

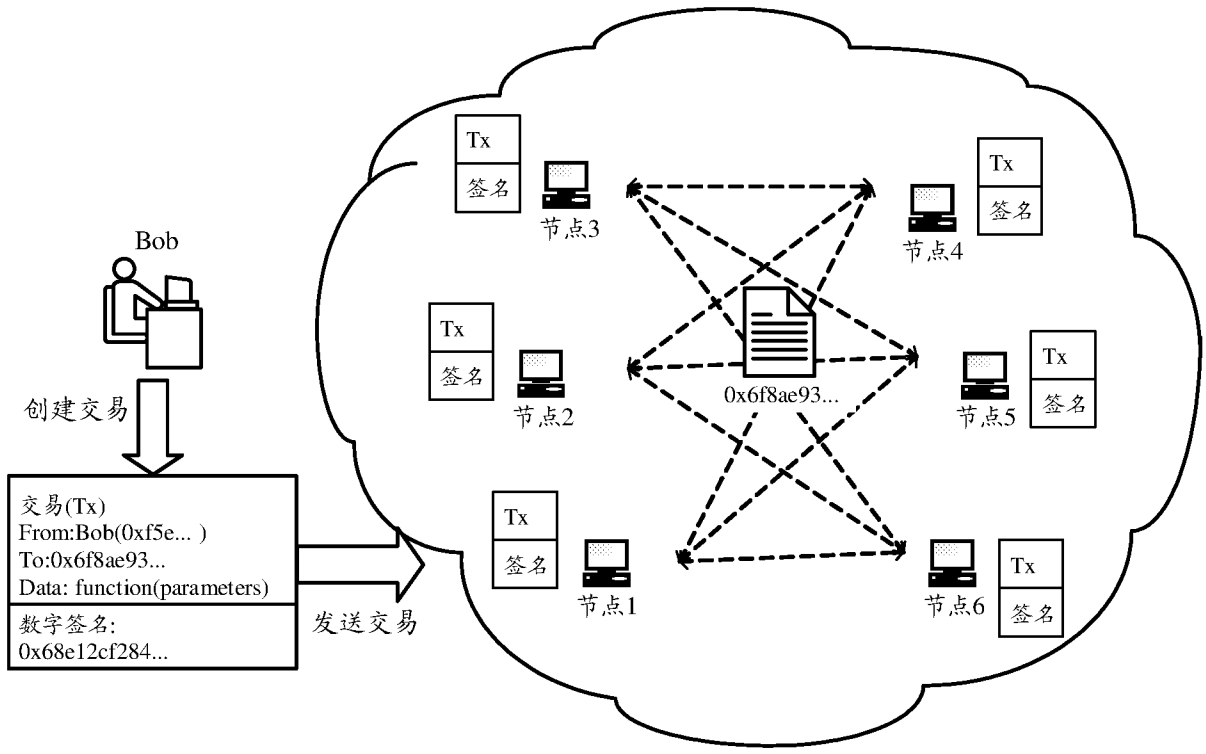
Bob
创建交易
交易(Tx)
From:Bob(0xf5e...)
To:0x6f8ae93...
Data: function(parameters)
数字签名:
0x68e12cf284...
发送交易
Tx
签名
0x6f8ae93...
节点1
节点2
节点3
节点4
节点5
节点6

图 2

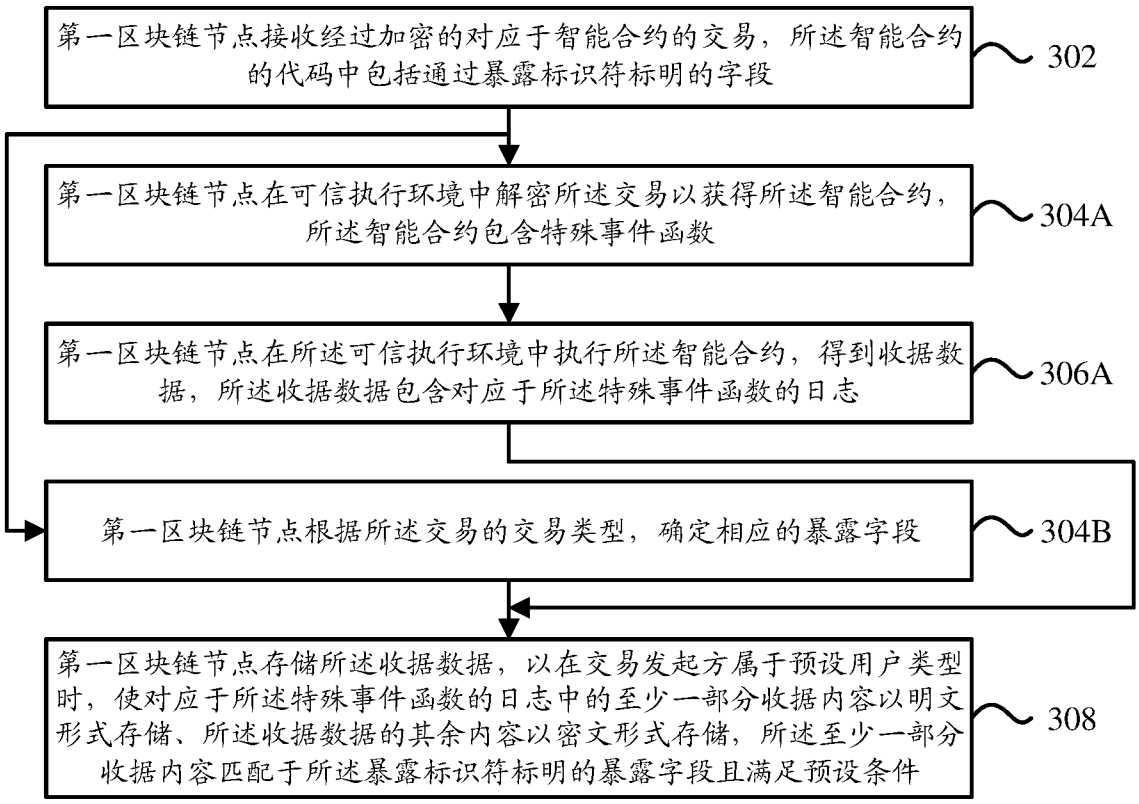
第一区块链节点接收经过加密的对应于智能合约的交易，所述智能合约的代码中包括通过暴露标识符标明的字段
302
第一区块链节点在可信执行环境中解密所述交易以获得所述智能合约，所述智能合约包含特殊事件函数
304A
第一区块链节点在所述可信执行环境中执行所述智能合约，得到收据数据，所述收据数据包含对应于所述特殊事件函数的日志
306A
第一区块链节点根据所述交易的交易类型，确定相应的暴露字段
304B
第一区块链节点存储所述收据数据，以在交易发起方属于预设用户类型时，使对应于所述特殊事件函数的日志中的至少一部分收据内容以明文形式存储、所述收据数据的其余内容以密文形式存储，所述至少一部分收据内容匹配于所述暴露标识符标明的暴露字段且满足预设条件
308

图 3

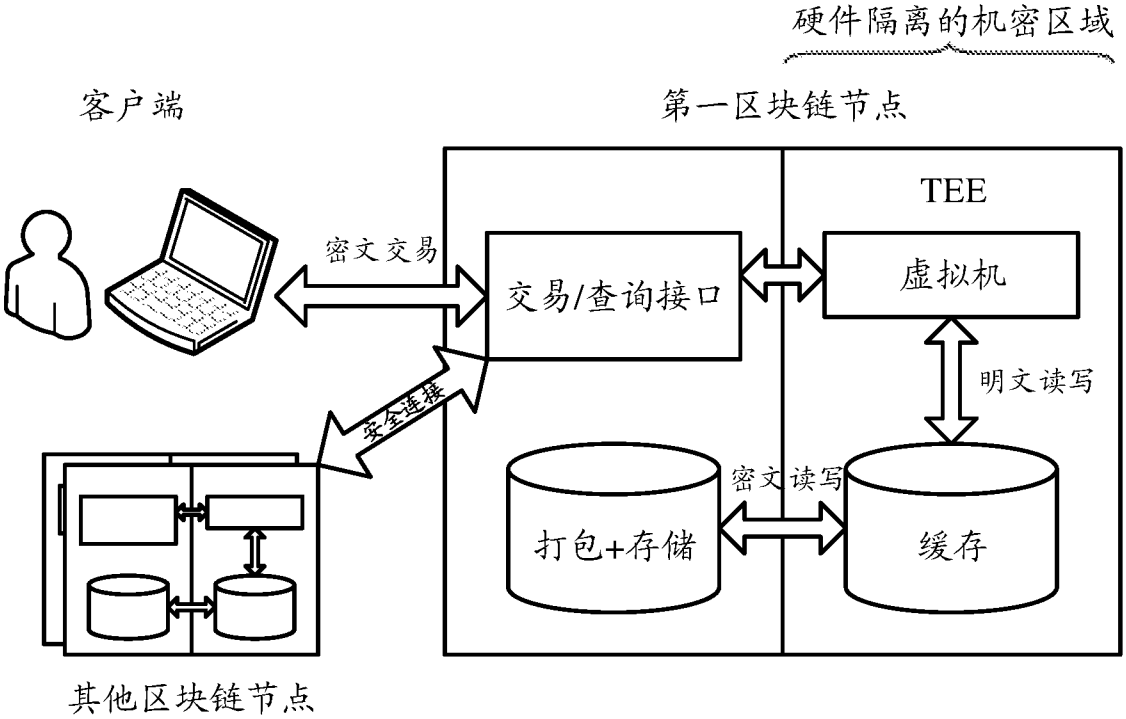
硬件隔离的机密区域
客户端
第一区块链节点
TEE
密文交易
交易/查询接口
虚拟机
明文读写
安全连接
密文读写
打包+存储
缓存
其他区块链节点

图 4

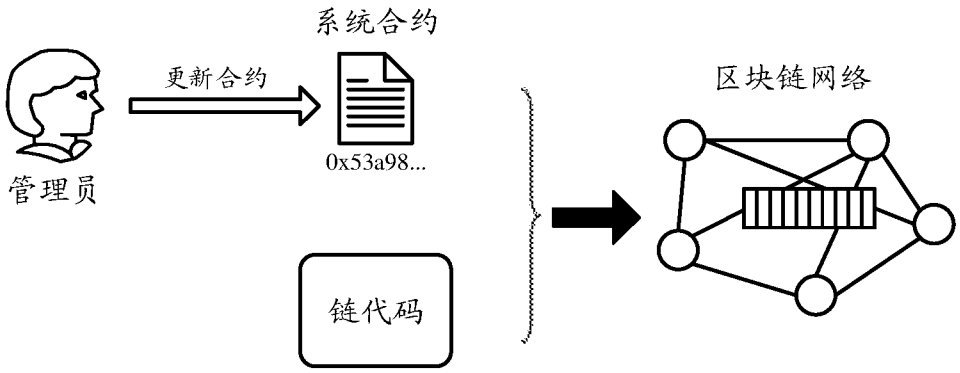
系统合约
更新合约
0x53a98...
管理员
区块链网络
链代码

图 5

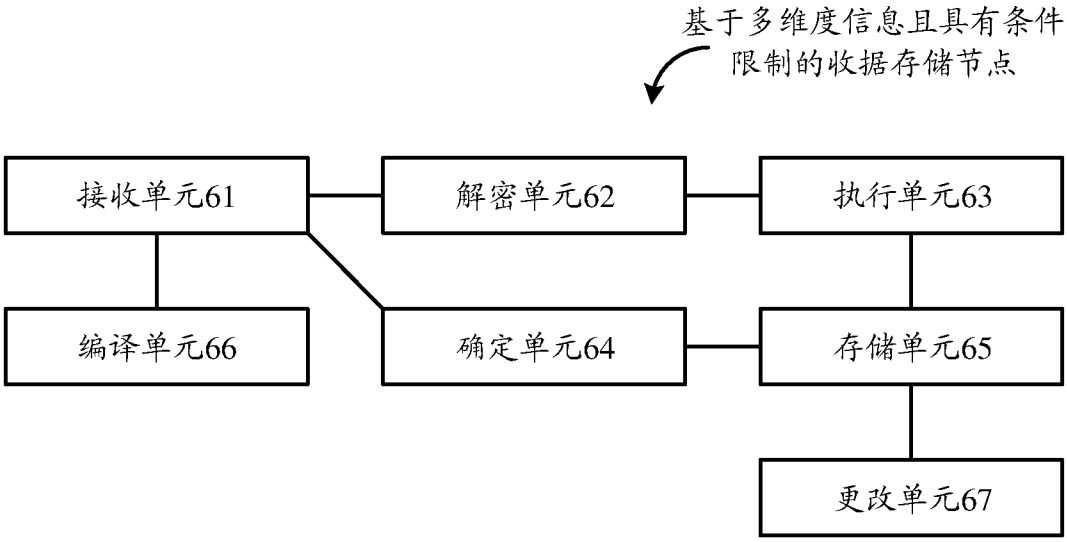
基于多维度信息且具有条件限制的收据存储节点
接收单元61
解密单元62
执行单元63
编译单元66
确定单元64
存储单元65
更改单元67

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/091427

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/27(2019.01)i; G06F 16/22(2019.01)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; G06Q

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)

CNKI, CNPAT, EPODOC, WPI, IEEE: 区块链, 节点, 可信执行环境, 交易, 加密, 解密, 字段, 域, 标识, 函数, 日志, 用户, 类型, 收据, block, chain, node, TEE, transaction, encrypt, decrypt, field, ID, mark, function, user, type, kind, receipt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110263087 A (ALIBABA GROUP HOLDING LIMITED) 20 September 2019 (2019-09-20) claims 1-32	1–32
A	CN 109493020 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.) 19 March 2019 (2019-03-19) description, paragraphs 27-58	1–32
A	CN 107294709 A (ALIBABA GROUP HOLDING LIMITED) 24 October 2017 (2017-10-24) description, paragraphs 59-80	1–32
A	CN 107342858 A (WUHAN PHOENIX BLOCKCHAIN TECHNOLOGY CO., LTD.) 10 November 2017 (2017-11-10) entire document	1–32
A	US 2019149325 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 16 May 2019 (2019-05-16) entire document	1-32

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 August 2020	**21 August 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/091427

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110263087 A	20 September 2019	None	
CN 109493020 A	19 March 2019	None	
CN 107294709 A	24 October 2017	None	
CN 107342858 A	10 November 2017	None	
US 2019149325 A1	16 May 2019	US 2020145204 A1	07 May 2020

国际检索报告

国际申请号
PCT/CN2020/091427

A. 主题的分类

G06F 16/27(2019.01)i; G06F 16/22(2019.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; G06Q

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））

CNKI, CNPAT, EPODOC, WPI, IEEE: 区块链，节点，可信执行环境，交易，加密，解密，字段，域，标识，函数，日志，用户，类型，收据，block, chain, node, TEE, transaction, encrypt, decrypt, field, ID, mark, function, user, type, kind, receipt

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 110263087 A (阿里巴巴集团控股有限公司) 2019年 9月 20日 (2019-09-20) 权利要求1-32	1-32
A	CN 109493020 A (众安信息技术服务有限公司) 2019年 3月 19日 (2019-03-19) 说明书第27-58段	1-32
A	CN 107294709 A (阿里巴巴集团控股有限公司) 2017年 10月 24日 (2017-10-24) 说明书第59-80段	1-32
A	CN 107342858 A (武汉凤链科技有限公司) 2017年 11月 10日 (2017-11-10) 全文	1-32
A	US 2019149325 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年 5月 16日 (2019-05-16) 全文	1-32

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 8月 4日	2020年 8月 21日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 宋朝 电话号码 86-(10)-53961349

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/091427

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 110263087 A	2019年 9月 20日	无	
CN 109493020 A	2019年 3月 19日	无	
CN 107294709 A	2017年 10月 24日	无	
CN 107342858 A	2017年 11月 10日	无	
US 2019149325 A1	2019年 5月 16日	US 2020145204 A1	2020年 5月 7日