

# (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)



(10) 国际公布号  
**WO 2020/233350 A1**

- (51) 国际专利分类号:  
**G06F 21/53** (2013.01)
- (21) 国际申请号: PCT/CN2020/087051
- (22) 国际申请日: 2020 年 4 月 26 日 (26.04.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201910419185.2 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, NODE AND SYSTEM BASED ON PLAINTEXT LOGS

(54) 发明名称: 基于明文日志的收据存储方法、节点和系统

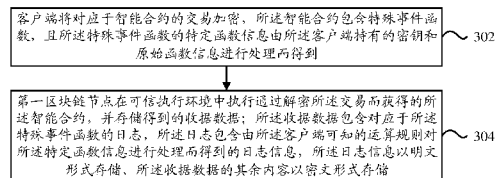


图 3

- 302 A client encrypts a transaction corresponding to an intelligent contract wherein the intelligent contract includes a special event function and specific function information of the special event function is obtained by means of a key held by the client and processing of original function information
- 304 A first blockchain node executes in a trusted execution environment the intelligent contract which is obtained by means of decrypting the transaction and stores obtained receipt data wherein the receipt data includes a log corresponding to the special event function the log includes log information which is obtained by means of processing the specific function information according to an operational rule knowable for the client and the log information is stored in the form of plaintext and the remaining content of the receipt data is stored in the form of ciphertext

(57) Abstract: Provided in one or one embodiments are a receipt storage method, node and system based on plaintext logs. The method may comprise: a client encrypting a transaction corresponding to an intelligent contract, wherein the intelligent contract includes a special event function, and specific function information of the special event function is obtained by means of a key held by the client and processing of original function information; a first blockchain node executing, in a trusted execution environment, the intelligent contract which is obtained by means of decrypting the transaction, and storing obtained receipt data, wherein the receipt data includes a log corresponding to the special event function, the log includes log information which is obtained by means of processing the specific function information according to an operational rule knowable for the client, and the log information is stored in the form of plaintext, and the remaining content of the receipt data is stored in the form of ciphertext.

(57) 摘要: 本说明书一个或多个实施例提供一种基于明文日志的收据存储方法、节点和系统, 该方法可以包括: 客户端将对应于智能合约的交易加密, 所述智能合约包含特殊事件函数, 且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到; 第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约, 并存储得到的收据数据; 所述收据数据包含对应于所述特殊事件函数的日志, 所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息, 所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

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))。

## 基于明文日志的收据存储方法、节点和系统

### 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，尤其涉及一种基于明文日志的收据存储方法、节点和系统。

### 5 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。太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明文日志的收据存储方法、节点和系统。

[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，提出了一种基于明文日志的收据存储方法，包括：

[08]客户端将对应于智能合约的交易加密,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

[09]第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约,并存储得到的收据数据;所述收据数据包含对应于所述特殊事件函数的日志,所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息,所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[10]根据本说明书一个或多个实施例的第二方面,提出了一种基于明文日志的收据存储方法,包括:

[11]第一区块链节点接收客户端发起的经过加密且对应于智能合约的交易,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

[12]第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约,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,所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息;

[13]第一区块链节点存储所述收据数据,使所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[14]根据本说明书一个或多个实施例的第三方面,提出了一种基于明文日志的收据存储系统,包括客户端和第一区块链节点,其中:

[15]客户端用于将对应于智能合约的交易加密,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

[16]第一区块链节点用于在可信执行环境中执行通过解密所述交易而获得的所述智能合约,并存储得到的收据数据;所述收据数据包含对应于所述特殊事件函数的日志,所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息,所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[17]根据本说明书一个或多个实施例的第四方面,提出了一种基于明文日志的收据存储节点,包括:

[18]接收单元,接收客户端发起的经过加密且对应于智能合约的交易,所述智能合约包

含特殊事件函数，且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到；

[19]解密单元，在可信执行环境中解密所述交易，得到所述智能合约；

5 [20]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，所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息；

[21]存储单元，存储所述收据数据，使所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[22]根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：

10 [23]处理器；

[24]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第一方面或第二方面所述的方法。

15 [26]根据本说明书一个或多个实施例的第六方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面或第二方面所述方法的步骤。

## 附图说明

[27]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。

[28]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。

20 [29]图 3 是一示例性实施例提供的一种基于明文日志的收据存储方法的流程图。

[30]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。

[31]图 5 是一示例性实施例提供的另一种基于明文日志的收据存储方法的流程图。

[32]图 6 是一示例性实施例提供的一种基于明文日志的收据存储系统的框图。

[33]图 7 是一示例性实施例提供的一种基于明文日志的收据存储节点的框图。

## 具体实施方式

[34]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发明说明书一个或多个实施例相一致的所有实施方式。

- 5 相反，它们仅是与如所附权利要求书中所详述的、本发明说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

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

[36]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。

[37]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。

25 [38]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。

[39]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。

[40]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。

[41]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:

[42]Result 字段, 表示交易的执行结果;

[43]Gas used 字段, 表示交易消耗的 gas 值;

[44]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;

[45]Output 字段, 表示交易的输出。

[46]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基于部分内容对收据数据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。

[47]以下结合图3所示说明本申请一基于明文日志的收据存储方法的实施例的实现过程：

[48]步骤302，客户端将对应于智能合约的交易加密，所述智能合约包含特殊事件函数，且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到。

[49]在一实施例中，智能合约可以包含一个或多个事件（event），每一事件在智能合约的代码中存在对应的事件函数，通过执行事件函数对相关事件的调用，以实现相关处理逻辑。

[50]在一实施例中，智能合约中的事件函数可以分为特殊事件函数和普通事件函数。普通事件函数可以与相关技术中的事件函数无异。特殊事件函数在数据结构、处理方式等方面均与普通事件函数相同，其差异在于：特殊事件函数所含的一项或多项函数信息存在特殊性，需要确保该函数信息的取值尽可能地具有唯一性，该一项或多项函数信息即上述的特定函数信息。由于在后续步骤中需要根据特定函数信息生成相应的日志信息，因而通过特定函数信息的唯一性，可以确保所生成的日志信息具有唯一性，从而能够基于该日志信息对相关日志或整个收据数据实施检索操作。

[51]在一实施例中，用户可以基于自身在区块链网络中对应的外部账户，在客户端处创建并发起上述交易。上述客户端持有的密钥，实际上是指该用户持有的密钥。由于密钥是由用户持有、并非公开信息，因而可以避免不同用户之间模仿借鉴或恶意抄袭，极大地降低了密钥的重复概率；因此，即便采用相同的原始函数信息时，也可以通过不同密钥处理得到差异化的特定函数信息，从而确保特定函数信息的唯一性。

[52]在一实施例中，密钥可由各个用户分别生成，比如由用户自定义生成，或者由用户通过预设随机算法而随机生成，只要符合诸如长度、所含字符的类型等方面的要求即可。当密钥由各个用户生成时，极小概率下可能存在不同用户生成相同密钥的情形，但该情形下不同用户可能采用不同的原始函数信息；即便采用的密钥和原始函数信息均恰好相

同，由于该情形的出现概率极小，因而能够据此检索到的日志数量也十分有限，可以根据其他维度的信息（比如交易时刻、交易所处区块高度等）加以综合判断，能够高效地分辨对应于不同用户的日志。

[53]在一实施例中，密钥可由密钥管理服务器分配。密钥管理服务器可以按照预设规则生成每个密钥，并且可以将每次生成的密钥与已经分配的所有密钥进行比对，以确保新分配的密钥与已经分配的所有密钥均不相同，从而确保每一密钥的唯一性。那么，即便采用的原始函数信息相同时，也可以基于不同密钥而产生差异化的特定函数信息。

[54]在一实施例中，每个用户分别持有一个密钥，通过该密钥为自身创建的所有智能合约生成相应的特定函数信息。因此，用户每次生成新的特定函数信息时，都需要确保所采用的原始函数信息区别于先前已生成的特定函数信息对应的原始函数信息，以确保该用户通过同一密钥分别生成不同的特定函数信息。例如，智能合约 1 中包含特定函数信息 A1，该特定函数信息 A1 由用户持有的密钥 K 与原始函数信息 B1 生成；智能合约 2 中包含特定函数信息 A21 和特定函数信息 A22，该特定函数信息 A21 由用户持有的密钥 K 与原始函数信息 B21 生成、该特定函数信息 A22 由用户持有的密钥 K 与原始函数信息 B22 生成，其中原始函数信息 B1、B21、B22 各不相同。

[55]在一实施例中，每个用户持有 N 个密钥，同一用户创建的不同智能合约对应于不同密钥，即智能合约与密钥之间一一对应。因此，当同一智能合约包含多个特定函数信息时，只要相应的原始函数信息之间不同，即可确保产生的多个特定函数信息存在差异；而对于不同智能合约而言，由于采用的密钥不同，因而即便采用相同的原始函数信息，生成的特定函数信息仍然存在差异，因而用户无需关注于不同智能合约中所采用的原始函数信息是否相同，可以简化对原始函数信息的设定过程。例如，智能合约 3 中包含特定函数信息 A3，该特定函数信息 A3 由用户持有的密钥 K1 与原始函数信息 B3 生成；智能合约 4 中包含特定函数信息 A4，该特定函数信息 A4 由用户持有的密钥 K2 与原始函数信息 B4 生成，且该原始函数信息 B3 与原始函数信息 B4 可以相同。

[56]在一实施例中，可以将密钥与原始函数信息拼接后，通过 CMAC128 算法进行计算，得到 128 位的特定函数信息。当然，在其他实施例中，也可以通过其他算法对密钥和原始函数信息进行计算，以得到相应的特定函数信息，本说明书并不对此进行限制。并且，特定函数信息的长度并不一定为 128 位，比如在其他实施例中可以为更短或更长的字符串，本说明书并不对此进行限制。

[57]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，避免交易内容被暴露。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。

5 [58]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。

10 [59]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。

15 [60]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。具体实现过程与上述过程类似，在此不再赘述。

20 [61]步骤 304，第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约，并存储得到的收据数据；所述收据数据包含对应于所述特殊事件函数的日志，所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息，所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[62]如前所述，第一区块链节点接收的交易，例如可以是创建和/或调用智能合约的交易。比如在以太坊中，第一区块链节点接收到客户端发来的创建和/或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。

25 [63]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。

[64] 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。

[65] 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。

[66] 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。

[67] 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。

[68] 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。

[69]在一实施例中，每一事件被调用后，相应的事件函数均会被执行并生成对应的日志，即上述 Logs 字段的内容。相应的，上述日志信息可以为日志中的任意信息，比如 Logs 字段所含的 Topic 字段等。根据日志信息的生成方式，可以将用于生成日志信息的一项或多项函数信息作为上述的特定函数信息。以日志信息包括 Topic 字段为例，特定函数信息可以包括特殊事件函数的函数名、特殊事件函数所含参数的参数类型，通过预设算法对该函数名和参数类型进行处理，即可生成该特殊事件函数对应日志中的 Topic 字段；例如，生成 Topic 字段的公式如下：

$$\text{Keccak256}(\text{func}(\text{int}, \text{int}))$$

[70]在上述公式中，“func()”代表特殊事件函数的函数名，“int, int”代表特殊事件函数所含参数的参数类型，而 Keccak256 代表所采用的散列算法。当然，在其他实施例中，所采用的散列算法和公式中采用的入参均可能发生变化，本说明书并不对此进行限制。例如，在一些实施例中，除了上述的函数名和参数类型之外，还可能涉及到特殊事件函数所含参数的参数名；或者，特定函数信息可以包括以下至少之一：特殊事件函数的函数名、特殊事件函数所含参数的参数名、特殊事件函数所含参数的参数类型等，从而基于这些信息的任意组合以用于生成上述的 Topic 字段或其他日志信息。

[71]当日志信息是基于函数名和参数类型而生成时，由于参数类型的表达方式通常已经在编程语言中预先定义（比如上述的“int”用于表示“有符号整型”的参数变量；当然，并不排除一些情况下，可以对参数类型进行自定义），因而用户可以针对函数名进行设定，以确保日志信息满足前述的唯一性需求。例如，用户可以通过诸如前述的特定函数

信息的生成方式，生成函数名：假定每一智能合约分别采用不同的密钥，用户只需要确保当前智能合约中的不同特殊事件函数分别采用不同的原始函数名（即原始函数信息），那么针对密钥和原始函数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的函数名；而假定用户仅持有一个密钥，即该用户创建的所有智能合约共用该

5 密钥，则该用户需要确保当前智能合约中的每一特殊事件函数对应的原始函数名在先前均未使用过（指该用户自身未使用过，而其他用户可以使用），从而针对密钥和原始函数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的函数名。

[72]当日志信息是基于参数名和参数类型而生成时，与上述情形相类似的，用户可以针对参数名进行设定，以确保日志信息满足前述的唯一性需求。例如，用户可以通过诸如

10 前述的特定函数信息的生成方式，生成参数名：假定每一智能合约分别采用不同的密钥，用户只需要确保当前智能合约中的不同特殊事件函数分别采用不同的原始参数名（即原始函数信息），那么针对密钥和原始参数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的参数名；而假定用户仅持有一个密钥，即该用户创建的所有智能合约共用该密钥，则该用户需要确保当前智能合约中的每一特殊事件函数对应的原

15 始参数名在先前均未使用过（指该用户自身未使用过，而其他用户可以使用），从而针对密钥和原始参数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的参数名。

[73]当日志信息是基于函数名和参数名而生成时，用户可以针对函数名和参数名中至少之一进行设定，只要确保函数名或参数名具有唯一性，即可确保日志信息满足前述的唯一性需求。生成具有唯一性的函数名或参数名的过程可以参考上述实施例，此处不再赘述。

20

[74]通过在创建智能合约时，在智能合约的代码中添加具有唯一性的特定函数信息（至少一部分特定函数信息具有唯一性），使得交易在调用该智能合约、生成相应的日志后，日志中可以包含根据特定函数信息生成的日志信息，并且该特定函数信息的唯一性可以

25 传递给日志信息，使得日志信息具有唯一性。同时，由于将特定函数信息生成为相应的日志信息的运算规则对客户端可知（即客户端具有获知该运算规则的能力；具体的，可以在生成日志之前、生成日志之后或其他任意时刻获知，本说明书并不对此进行限制），因而客户端可以根据特定函数信息和运算规则自行生成检索关键词，该检索关键词与上述的日志信息的内容相同，因而在上述日志信息采用明文存储的情况下，可以基于检索

30 关键词与日志信息之间的匹配，实现对相关日志的精准检索，以用于根据检索到的日志

实施相关操作。

[75]在一实施例中，特定函数信息由第一规则对密钥和原始函数信息进行处理得到，日志信息由第二规则对特定函数信息进行处理得到；其中，第一规则和第二规则中至少之一为不可逆的运算规则。

- 5 [76]当第一规则为不可逆的运算规则时，即便第二规则并非不可逆的运算规则，或者智能合约所含的特定函数信息遭到泄露，也可以避免用户使用的密钥被根据特定函数信息而反向推导出来。用户在生成原始函数信息时，往往会根据其所使用的功能或代表的含义而赋予名称，导致原始函数信息的取值容易被猜测或推演出来，因而通过采用不可逆的第一规则，尤其是在同一密钥被应用于多个智能合约的情况下，可以避免密钥被其他
- 10 用户冒用或滥用。

- [77]由于智能合约的代码在交易中处于加密状态，并且解密过程仅在可信执行环境内实施，因而智能合约的代码中所含的特定函数信息处于保密状态、无法被直接读取。因此，当第二规则为不可逆的运算规则时，可以避免反向推导出用于生成日志信息的特定函数信息，防止被其他用户应用于其他的智能合约中而破坏其唯一性。例如，当采用
- 15 Keccak256 算法对特定函数信息进行散列计算得到相应的日志信息（即散列值）时，由于散列计算本身不可逆，因而即便对日志信息采取明文存储，也可以确保特定函数信息的内容不会泄露，与其他加密存储的收据内容均能够满足安全性需求。

- [78]在一实施例中，除了对特殊函数信息对应的日志信息采用明文加密之外，第一区块链节点需要在可信执行环境中对收据数据的其余收据内容加密后存储。所述加密，可以
- 20 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。

- [79]在一实施例中，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
- 25 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。

[80]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。

[81]在一实施例中，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。

[82]在一实施例中，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。

[83]在一实施例中，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。

[84]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。

[85]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。

[86]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 1 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 4 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。

[87]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。

[88]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。

[89]以下结合图 5 介绍本说明书一种基于明文日志的收据存储方法的实施例，该实施例侧重于从第一区块链节点的角度进行描述。如图 5 所示，该方法可以包括以下步骤：

[90]步骤 502，第一区块链节点接收客户端发起的经过加密且对应于智能合约的交易，所述智能合约包含特殊事件函数，且所述特殊事件函数的特定函数信息由所述客户端持

有的密钥和原始函数信息进行处理而得到。

[91]在一实施例中，智能合约可以包含一个或多个事件，每一事件在智能合约的代码中存在对应的事件函数，通过执行事件函数对相关事件的调用，以实现相关处理逻辑。

[92]在一实施例中，智能合约中的事件函数可以分为特殊事件函数和普通事件函数。普通事件函数可以与相关技术中的事件函数无异。特殊事件函数在数据结构、处理方式等方面均与普通事件函数相同，其差异在于：特殊事件函数所含的一项或多项函数信息存在特殊性，需要确保该函数信息的取值尽可能地具有唯一性，该一项或多项函数信息即上述的特定函数信息。由于在后续步骤中需要根据特定函数信息生成相应的日志信息，因而通过特定函数信息的唯一性，可以确保所生成的日志信息具有唯一性，从而能够基于该日志信息对相关日志或整个收据数据实施检索操作。

[93]在一实施例中，用户可以基于自身在区块链网络中对应的外部账户，在客户端处创建并发起上述交易。上述客户端持有的密钥，实际上是指该用户持有的密钥。由于密钥是由用户持有、并非公开信息，因而可以避免不同用户之间模仿借鉴或恶意抄袭，极大地降低了密钥的重复概率；因此，即便采用相同的原始函数信息时，也可以通过不同密钥处理得到差异化的特定函数信息，从而确保特定函数信息的唯一性。

[94]在一实施例中，密钥可由各个用户分别生成，比如由用户自定义生成，或者由用户通过预设随机算法而随机生成，只要符合诸如长度、所含字符的类型等方面的要求即可。当密钥由各个用户生成时，极小概率下可能存在不同用户生成相同密钥的情形，但该情形下不同用户可能采用不同的原始函数信息；即便采用的密钥和原始函数信息均恰好相同，由于该情形的出现概率极小，因而能够据此检索到的日志数量也十分有限，可以根据其他维度的信息（比如交易时刻、交易所处区块高度等）加以综合判断，能够高效地分辨对应于不同用户的日志。

[95]在一实施例中，密钥可由密钥管理服务器分配。密钥管理服务器可以按照预设规则生成每个密钥，并且可以将每次生成的密钥与已经分配的所有密钥进行比对，以确保新分配的密钥与已经分配的所有密钥均不相同，从而确保每一密钥的唯一性。那么，即便采用的原始函数信息相同时，也可以基于不同密钥而产生差异化的特定函数信息。

[96]在一实施例中，每个用户分别持有一个密钥，通过该密钥为自身创建的所有智能合约生成相应的特定函数信息。因此，用户每次生成新的特定函数信息时，都需要确保所采用的原始函数信息区别于先前已生成的特定函数信息对应的原始函数信息，以确保该

用户通过同一密钥分别生成不同的特定函数信息。例如，智能合约 1 中包含特定函数信息 A1，该特定函数信息 A1 由用户持有的密钥 K 与原始函数信息 B1 生成；智能合约 2 中包含特定函数信息 A21 和特定函数信息 A22，该特定函数信息 A21 由用户持有的密钥 K 与原始函数信息 B21 生成、该特定函数信息 A22 由用户持有的密钥 K 与原始函数信息 B22 生成，其中原始函数信息 B1、B21、B22 各不相同。

[97]在一实施例中，每个用户持有 N 个密钥，同一用户创建的不同智能合约对应于不同密钥，即智能合约与密钥之间一一对应。因此，当同一智能合约包含多个特定函数信息时，只要相应的原始函数信息之间不同，即可确保产生的多个特定函数信息存在差异；而对于不同智能合约而言，由于采用的密钥不同，因而即便采用相同的原始函数信息，生成的特定函数信息仍然存在差异，因而用户无需关注于不同智能合约中所采用的原始函数信息是否相同，可以简化对原始函数信息的设定过程。例如，智能合约 3 中包含特定函数信息 A3，该特定函数信息 A3 由用户持有的密钥 K1 与原始函数信息 B3 生成；智能合约 4 中包含特定函数信息 A4，该特定函数信息 A4 由用户持有的密钥 K2 与原始函数信息 B4 生成，且该原始函数信息 B3 与原始函数信息 B4 可以相同。

[98]在一实施例中，可以将密钥与原始函数信息拼接后，通过 CMAC128 算法进行计算，得到 128 位的特定函数信息。当然，在其他实施例中，也可以通过其他算法对密钥和原始函数信息进行计算，以得到相应的特定函数信息，本说明书并不对此进行限制。并且，特定函数信息的长度并不一定为 128 位，比如在其他实施例中可以为更短或更长的字符串，本说明书并不对此进行限制。

[99]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，避免交易内容被暴露。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。

[100] 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，也可以采用非对称加密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。

[101] 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。

[102] 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。具体实现过程与上述过程类似，在此不再赘述。

[103] 步骤 504，第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约，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，所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息。

[104] 如前所述，第一区块链节点接收的交易，例如可以是创建和/或调用智能合约的交易。比如在以太坊中，第一区块链节点接收到客户端发来的创建和/或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。进一步地，与交易或智能合约的执行过程相关的描述，可以参考上述图 3 所示的实施例，此处不再赘述。

[105] 在一实施例中，每一事件被调用后，相应的事件函数均会被执行并生成对应的日志，即上述 Logs 字段的内容。相应的，上述日志信息可以为日志中的任意信息，比如 Logs 字段所含的 Topic 字段等。根据日志信息的生成方式，可以将用于生成日志信息的一项或多项函数信息作为上述的特定函数信息。以日志信息包括 Topic 字段为例，特定函数信息可以包括特殊事件函数的函数名、特殊事件函数所含参数的参数类型，通过预设算法对该函数名和参数类型进行处理，即可生成该特殊事件函数对应日志中的 Topic 字段；例如，生成 Topic 字段的公式如下：

Keccak256(func(int, int))

[106] 在上述公式中，“func()”代表特殊事件函数的函数名，“int, int”代表特殊事件函数所含参数的参数类型，而 Keccak256 代表所采用的散列算法。当然，在其他实施例中，所采用的散列算法和公式中采用的入参均可能发生变化，本说明书并不对此进行限制。例如，在一些实施例中，除了上述的函数名和参数类型之外，还可能涉及到特殊事件函数所含参数的参数名；或者，特定函数信息可以包括以下至少之一：特殊事件函

数的函数名、特殊事件函数所含参数的参数名、特殊事件函数所含参数的参数类型等，从而基于这些信息的任意组合以用于生成上述的 Topic 字段或其他日志信息。

[107] 当日志信息是基于函数名和参数类型而生成时，由于参数类型的表达方式通常已经在编程语言中预先定义（比如上述的“int”用于表示“有符号整型”的参数变量；

5 当然，并不排除一些情况下，可以对参数类型进行自定义），因而用户可以针对函数名进行设定，以确保日志信息满足前述的唯一性需求。例如，用户可以通过诸如前述的特定函数信息的生成方式，生成函数名：假定每一智能合约分别采用不同的密钥，用户只需要确保当前智能合约中的不同特殊事件函数分别采用不同的原始函数名（即原始函数信息），那么针对密钥和原始函数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的函数名；而假定用户仅持有一个密钥，即该用户创建的所有智能合约共用该密钥，则该用户需要确保当前智能合约中的每一特殊事件函数对应的原始函数名在先前均未使用过（指该用户自身未使用过，而其他用户可以使用），从而针对密钥和原始函数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的函数名。

15 [108] 当日志信息是基于参数名和参数类型而生成时，与上述情形相类似的，用户可以针对参数名进行设定，以确保日志信息满足前述的唯一性需求。例如，用户可以通过诸如前述的特定函数信息的生成方式，生成参数名：假定每一智能合约分别采用不同的密钥，用户只需要确保当前智能合约中的不同特殊事件函数分别采用不同的原始参数名（即原始函数信息），那么针对密钥和原始参数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的参数名；而假定用户仅持有一个密钥，即该用户创建的所有智能合约共用该密钥，则该用户需要确保当前智能合约中的每一特殊事件函数对应的原始参数名在先前均未使用过（指该用户自身未使用过，而其他用户可以使用），从而针对密钥和原始参数名进行 CMAC128 运算后，即可为相应的特殊事件函数生成具有唯一性的参数名。

25 [109] 当日志信息是基于函数名和参数名而生成时，用户可以针对函数名和参数名中至少之一进行设定，只要确保函数名或参数名具有唯一性，即可确保日志信息满足前述的唯一性需求。生成具有唯一性的函数名或参数名的过程可以参数上述实施例，此处不再赘述。

[110] 在一实施例中，特定函数信息由第一规则对密钥和原始函数信息进行处理得到，

日志信息由第二规则对特定函数信息进行处理得到；其中，第一规则和第二规则中至少之一为不可逆的运算规则。

[111] 当第一规则为不可逆的运算规则时，即便第二规则并非不可逆的运算规则，或者智能合约所含的特定函数信息遭到泄露，也可以避免用户使用的密钥被根据特定函数信息而反向推导出来。用户在生成原始函数信息时，往往会根据其所使用的功能或代表的含义而赋予名称，导致原始函数信息的取值容易被猜测或推演出来，因而通过采用不可逆的第一规则，尤其是在同一密钥被应用于多个智能合约的情况下，可以避免密钥被其他用户冒用或滥用。

[112] 由于智能合约的代码在交易中处于加密状态，并且解密过程仅在可信执行环境内实施，因而智能合约的代码中所含的特定函数信息处于保密状态、无法被直接读取。因此，当第二规则为不可逆的运算规则时，可以避免反向推导出用于生成日志信息的特定函数信息，防止被其他用户应用于其他的智能合约中而破坏其唯一性。例如，当采用 Keccak256 算法对特定函数信息进行散列计算得到相应的日志信息（即散列值）时，由于散列计算本身不可逆，因而即便对日志信息采取明文存储，也可以确保特定函数信息的内容不会泄露，与其他加密存储的收据内容均能够满足安全性需求。

[113] 步骤 506, 第一区块链节点存储所述收据数据, 使所述日志信息以明文形式存储, 所述收据数据的其余内容以密文形式存储。

[114] 通过在创建智能合约时，在智能合约的代码中添加具有唯一性的特定函数信息（至少一部分特定函数信息具有唯一性），使得交易在调用该智能合约、生成相应的日志后，日志中可以包含根据特定函数信息生成的日志信息，并且该特定函数信息的唯一性可以传递给日志信息，使得日志信息具有唯一性。同时，由于将特定函数信息生成为相应的日志信息的运算规则对客户端可知（即客户端具有获知该运算规则的能力；具体的，可以在生成日志之前、生成日志之后或其他任意时刻获知，本说明书并不对此进行限制），因而客户端可以根据特定函数信息和运算规则自行生成检索关键词，该检索关键词与上述的日志信息的内容相同，因而在上述日志信息采用明文存储的情况下，可以基于检索关键词与日志信息之间的匹配，实现对相关日志的精准检索，以用于根据检索到的日志实施相关操作。

[115] 在一实施例中，除了对特殊函数信息对应的日志信息采用明文加密之外，第一区块链节点需要在可信执行环境中对收据数据的其余收据内容加密后存储。关于内容可

以参考图 3 所示实施例中的相关描述，此处不再赘述。

[116] 在一实施例中，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。相关内容可以参考图 3 所示实施例中的相关描述，此处不再赘述。

[117] 以下结合图 6 介绍本说明书一种基于明文日志的收据存储系统的实施例，该系统包括客户端 601 和第一区块链节点 602，其中：

[118] 客户端 601 用于将对应于智能合约的交易加密，所述智能合约包含特殊事件函数，且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到；

[119] 第一区块链节点 602 用于在可信执行环境中执行通过解密所述交易而获得的所述智能合约，并存储得到的收据数据；所述收据数据包含对应于所述特殊事件函数的日志，所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息，所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[120] 可选的，所述特定函数信息包括以下至少之一：所述特殊事件函数的函数名、所述特殊事件函数所含参数的参数名、所述特殊事件函数所含参数的参数类型。

[121] 可选的，所述密钥被应用于所述客户端创建的所有智能合约，且不同特殊事件函数对应于不同的原始函数信息。

[122] 可选的，所述客户端创建的不同智能合约对应于不同密钥。

[123] 可选的，所述密钥由所述客户端随机生成；或者，所述密钥由密钥管理服务器分发。

[124] 可选的，所述特定函数信息由第一规则对所述密钥和所述原始函数信息进行处理得到，所述日志信息由第二规则对所述特定函数信息进行处理得到；其中，所述第一规则 and 所述第二规则中至少之一为不可逆的运算规则。

[125] 可选的，第一区块链节点接收的交易对应的智能合约，包括：

[126] 用户在第一区块链节点上生成的智能合约；或，

[127] 用户在客户端上生成的智能合约；或，

[128] 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。

[129] 可选的,所述交易用于创建和/或调用智能合约。

[130] 以下结合图7介绍本说明书一种基于明文日志的收据存储节点的实施例,包括:

[131] 接收单元71,接收客户端发起的经过加密且对应于智能合约的交易,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

[132] 解密单元72,在可信执行环境中解密所述交易,得到所述智能合约;

[133] 执行单元73,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,所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息;

[134] 存储单元74,存储所述收据数据,使所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

[135] 可选的,所述特定函数信息包括以下至少之一:所述特殊事件函数的函数名、所述特殊事件函数所含参数的参数名、所述特殊事件函数所含参数的参数类型。

[136] 可选的,所述密钥被应用于所述客户端创建的所有智能合约,且不同特殊事件函数对应于不同的原始函数信息。

[137] 可选的,所述客户端创建的不同智能合约对应于不同密钥。

[138] 可选的,所述密钥由所述客户端随机生成;或者,所述密钥由密钥管理服务器分发。

[139] 可选的,所述特定函数信息由第一规则对所述密钥和所述原始函数信息进行处理得到,所述日志信息由第二规则对所述特定函数信息进行处理得到;其中,所述第一规则和所述第二规则中至少之一为不可逆的运算规则。

[140] 可选的,第一区块链节点接收的交易对应的智能合约,包括:

[141] 用户在第一区块链节点上生成的智能合约;或,

[142] 用户在客户端上生成的智能合约;或,

[143] 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。

[144] 可选的，所述交易用于创建和/或调用智能合约。

[145] 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。

[146] 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。

[147] 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。

[148] 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。

10 [149] 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。

15 [150] 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。

20 [151] 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。

25 [152] 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。

[153] 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。

[154] 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。

[155] 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。

[156] 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。

[157] 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。

[158] 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。

- 5 [159] 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”。
- 10 [160] 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. 一种基于明文日志的收据存储方法, 包括:

客户端将对应于智能合约的交易加密, 所述智能合约包含特殊事件函数, 且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

5 第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约, 并存储得到的收据数据; 所述收据数据包含对应于所述特殊事件函数的日志, 所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息, 所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

10 2. 根据权利要求 1 所述的方法, 所述特定函数信息包括以下至少之一: 所述特殊事件函数的函数名、所述特殊事件函数所含参数的参数名、所述特殊事件函数所含参数的参数类型。

3. 根据权利要求 1 所述的方法, 所述密钥被应用于所述客户端创建的所有智能合约, 且不同特殊事件函数对应于不同的原始函数信息。

4. 根据权利要求 1 所述的方法, 所述客户端创建的不同智能合约对应于不同密钥。

15 5. 根据权利要求 1 所述的方法, 所述密钥由所述客户端随机生成; 或者, 所述密钥由密钥管理服务器分发。

6. 根据权利要求 1 所述的方法, 所述特定函数信息由第一规则对所述密钥和所述原始函数信息进行处理得到, 所述日志信息由第二规则对所述特定函数信息进行处理得到; 其中, 所述第一规则 and 所述第二规则中至少之一为不可逆的运算规则。

20 7. 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。

25 8. 根据权利要求 1 所述的方法, 所述交易用于创建和/或调用智能合约。

9. 一种基于明文日志的收据存储方法, 包括:

第一区块链节点接收客户端发起的经过加密且对应于智能合约的交易, 所述智能合约包含特殊事件函数, 且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

30 第一区块链节点在可信执行环境中执行通过解密所述交易而获得的所述智能合约, 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, 所述日志包含由所

述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息;

第一区块链节点存储所述收据数据,使所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

5 10. 根据权利要求9所述的方法,所述特定函数信息包括以下至少之一:所述特殊事件函数的函数名、所述特殊事件函数所含参数的参数名、所述特殊事件函数所含参数的参数类型。

11. 根据权利要求9所述的方法,所述密钥被应用于所述客户端创建的所有智能合约,且不同特殊事件函数对应于不同的原始函数信息。

12. 根据权利要求9所述的方法,所述客户端创建的不同智能合约对应于不同密钥。

10 13. 根据权利要求9所述的方法,所述密钥由所述客户端随机生成;或者,所述密钥由密钥管理服务器分发。

14. 根据权利要求9所述的方法,所述特定函数信息由第一规则对所述密钥和所述原始函数信息进行处理得到,所述日志信息由第二规则对所述特定函数信息进行处理得到;其中,所述第一规则 and 所述第二规则中至少之一为不可逆的运算规则。

15 15. 根据权利要求9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。

20 16. 根据权利要求9所述的方法,所述交易用于创建和/或调用智能合约。

17. 一种基于明文日志的收据存储系统,包括客户端和第一区块链节点,其中:

客户端用于将对应于智能合约的交易加密,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始函数信息进行处理而得到;

25 第一区块链节点用于在可信执行环境中执行通过解密所述交易而获得的所述智能合约,并存储得到的收据数据;所述收据数据包含对应于所述特殊事件函数的日志,所述日志包含由所述客户端可知的运算规则对所述特定函数信息进行处理而得到的日志信息,所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

18. 一种基于明文日志的收据存储节点,包括:

30 接收单元,接收客户端发起的经过加密且对应于智能合约的交易,所述智能合约包含特殊事件函数,且所述特殊事件函数的特定函数信息由所述客户端持有的密钥和原始

函数信息进行处理而得到;

解密单元, 在可信执行环境中解密所述交易, 得到所述智能合约;

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, 所述日志包含由所述客户端可知的运算规则对

5 所述特定函数信息进行处理而得到的日志信息;

存储单元, 存储所述收据数据, 使所述日志信息以明文形式存储、所述收据数据的其余内容以密文形式存储。

19. 一种电子设备, 包括:

处理器;

10 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 9-16 中任一项所述的方法。

20. 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 9-16 中任一项所述方法的步骤。

15

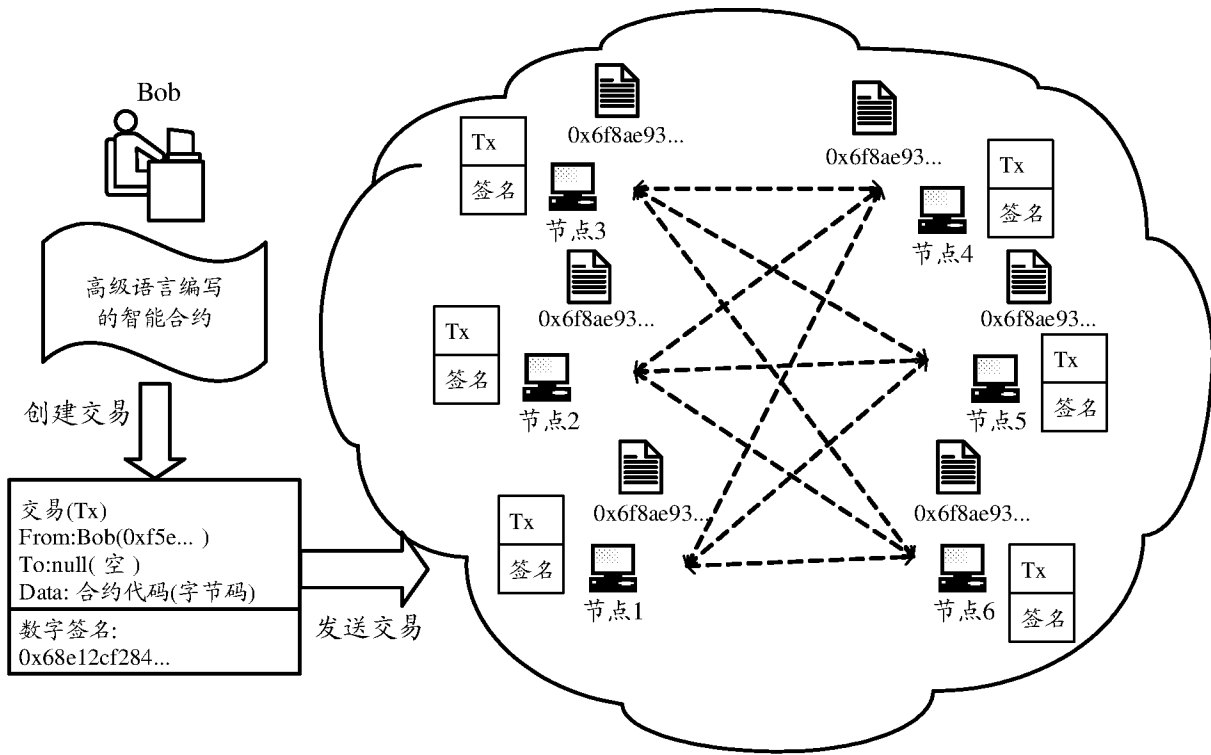


图 1

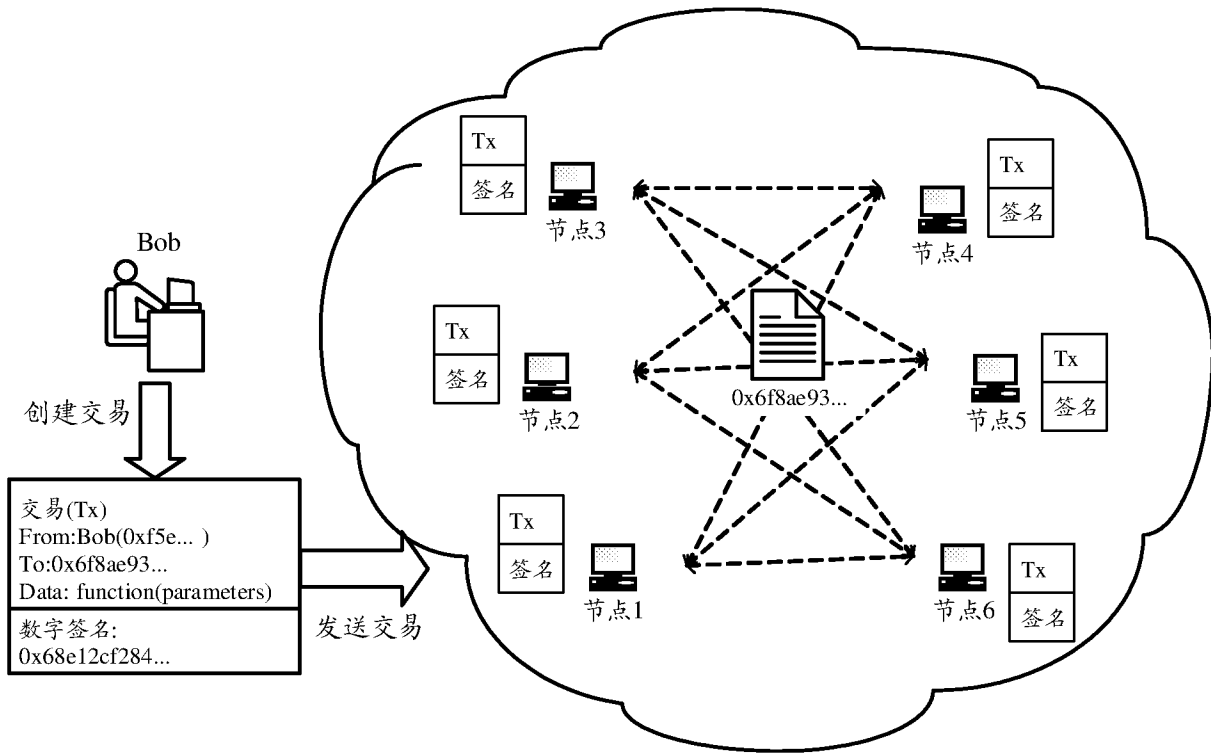


图 2

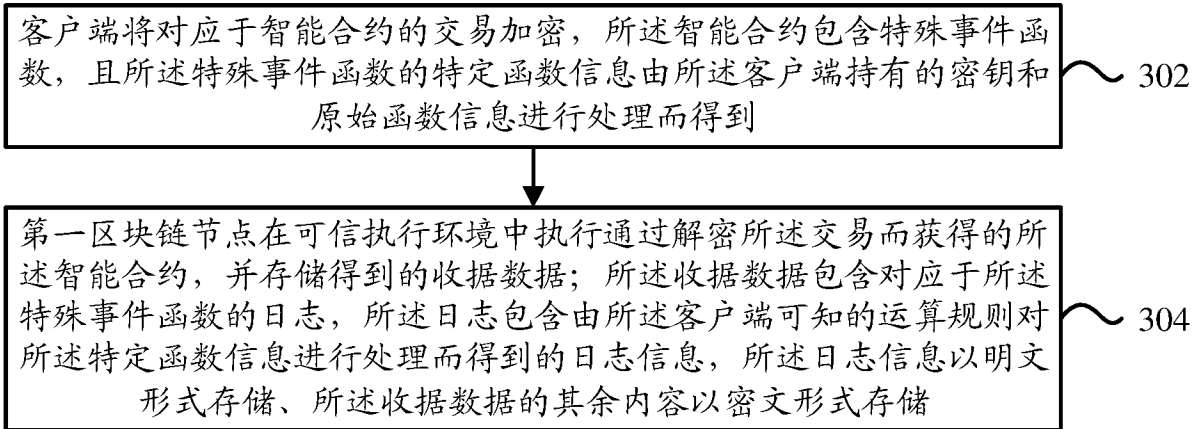


图 3

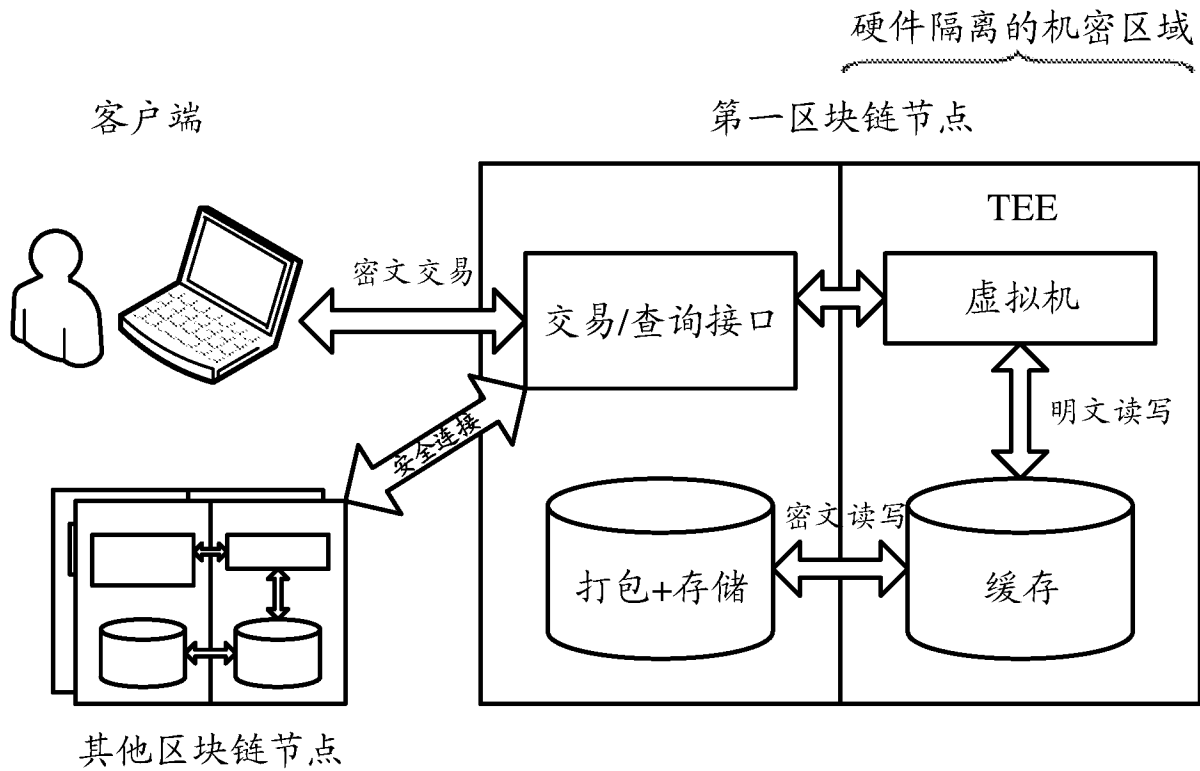


图 4

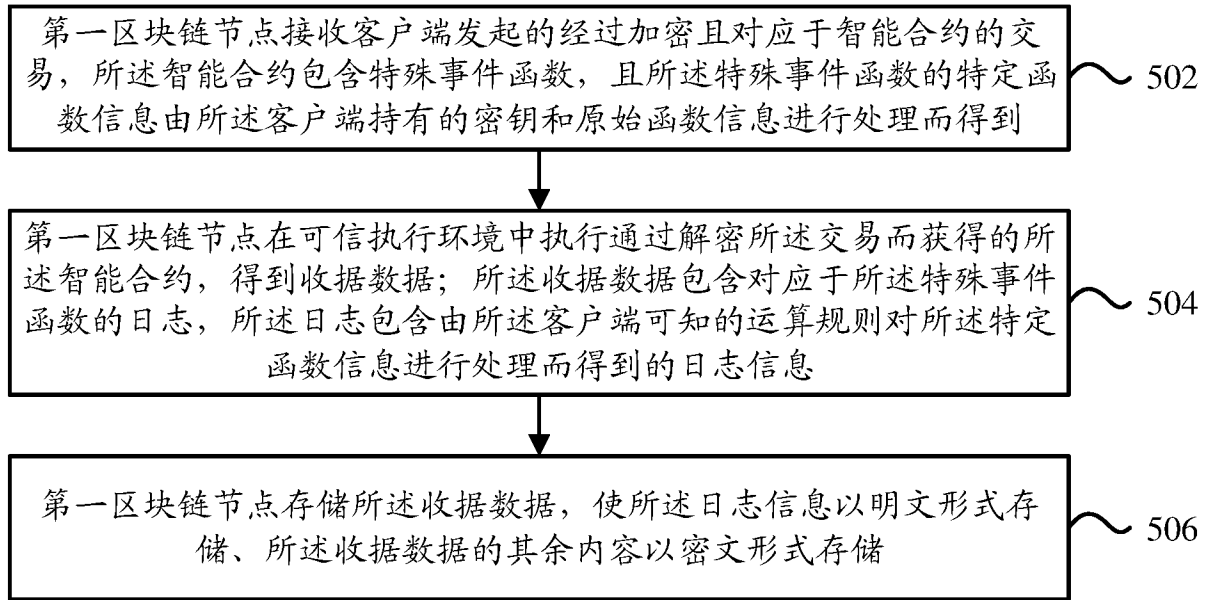


图 5

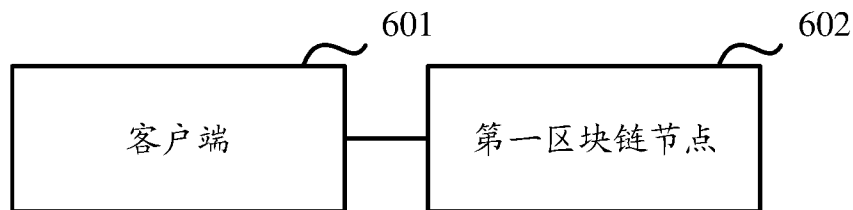


图 6

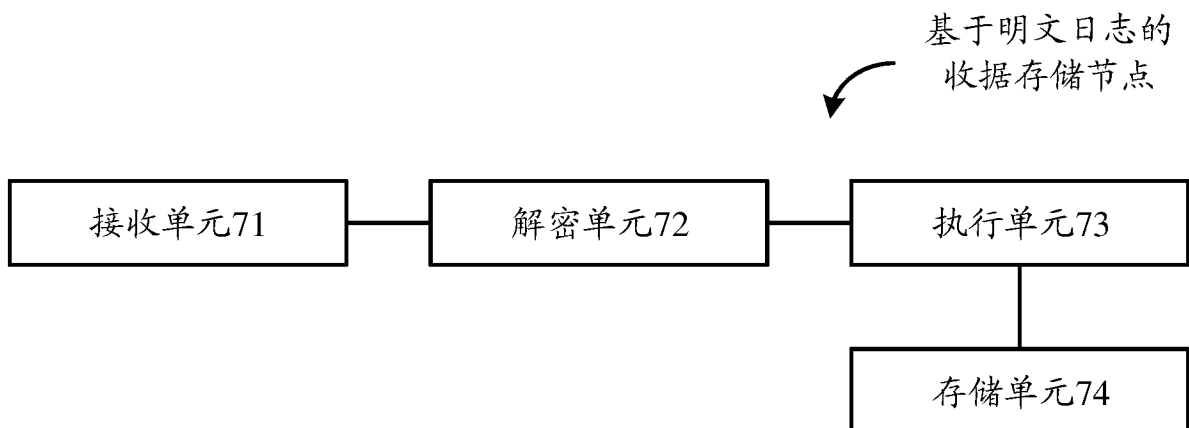


图 7

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/087051

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 21/53(2013.01)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; H04L

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

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

DWPI; CNABS; SIPOABS; CNKI; CNTXT: 明文, 日志, 收据, 客户端, 智能, 合约, 交易, 加密, 函数, 密钥, 区块链, 节点, 解密, 日志, 明文, 密文, plaintext, log, receipt, client, intelligent, contract, transaction, encryption, function, key, blockchain, node, decryption

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                       | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PX        | CN 110245489 A (ALIBABA GROUP HOLDING LIMITED) 17 September 2019<br>(2019-09-17)<br>claims 1-20                                          | 1-20                  |
| X         | CN 107342858 A (WUHAN PHOENIX BLOCKCHAIN TECHNOLOGY CO., LTD.) 10<br>November 2017 (2017-11-10)<br>description, paragraphs [0068]-[0098] | 1-20                  |
| A         | CN 108681898 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 19 October 2018<br>(2018-10-19)<br>entire document                                   | 1-20                  |



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

06 July 2020

Date of mailing of the international search report

20 July 2020

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

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

International application No.

**PCT/CN2020/087051**

| Patent document<br>cited in search report |           |   | Publication date<br>(day/month/year) | Patent family member(s) |           | Publication date<br>(day/month/year) |
|-------------------------------------------|-----------|---|--------------------------------------|-------------------------|-----------|--------------------------------------|
| CN                                        | 110245489 | A | 17 September 2019                    | None                    |           |                                      |
| CN                                        | 107342858 | A | 10 November 2017                     | CN                      | 107342858 | B 10 September 2019                  |
| CN                                        | 108681898 | A | 19 October 2018                      | None                    |           |                                      |

## 国际检索报告

国际申请号

PCT/CN2020/087051

| <b>A. 主题的分类</b><br>G06F 21/53 (2013.01) i<br><br>按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                     |                             |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|----|-------------------------------------------------------------------------|------|---|-------------------------------------------------------------------------------------|------|---|--------------------------------------------------------------|------|
| <b>B. 检索领域</b><br>检索的最低限度文献(标明分类系统和分类号)<br>G06F; H04L<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))<br>DWPI; CNABS; SIPOABS; CNKI; CNTXT: 明文, 日志, 收据, 客户端, 智能, 合约, 交易, 加密, 函数, 密钥, 区块链, 节点, 解密, 日志, 明文, 密文, plaintext, log, receipt, client, intelligent, contract, transaction, encryption, function, key, blockchain, node, decryption                                                                                                                                                                                                                              |                                                                                                                                                                                     |                             |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| <b>C. 相关文件</b> <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 110245489 A (阿里巴巴集团控股有限公司) 2019年 9月 17日 (2019 - 09 - 17)<br/>权利要求1-20</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>CN 107342858 A (武汉凤链科技有限公司等) 2017年 11月 10日 (2017 - 11 - 10)<br/>说明书第[0068]段至第[0098]段</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 108681898 A (广东工业大学) 2018年 10月 19日 (2018 - 10 - 19)<br/>全文</td> <td>1-20</td> </tr> </tbody> </table>                                                                              |                                                                                                                                                                                     |                             | 类 型*                                                                                                                                                                                                      | 引用文件, 必要时, 指明相关段落                                                                                                                                                                   | 相关的权利要求 | PX | CN 110245489 A (阿里巴巴集团控股有限公司) 2019年 9月 17日 (2019 - 09 - 17)<br>权利要求1-20 | 1-20 | X | CN 107342858 A (武汉凤链科技有限公司等) 2017年 11月 10日 (2017 - 11 - 10)<br>说明书第[0068]段至第[0098]段 | 1-20 | A | CN 108681898 A (广东工业大学) 2018年 10月 19日 (2018 - 10 - 19)<br>全文 | 1-20 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 引用文件, 必要时, 指明相关段落                                                                                                                                                                   | 相关的权利要求                     |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| PX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | CN 110245489 A (阿里巴巴集团控股有限公司) 2019年 9月 17日 (2019 - 09 - 17)<br>权利要求1-20                                                                                                             | 1-20                        |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CN 107342858 A (武汉凤链科技有限公司等) 2017年 11月 10日 (2017 - 11 - 10)<br>说明书第[0068]段至第[0098]段                                                                                                 | 1-20                        |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CN 108681898 A (广东工业大学) 2018年 10月 19日 (2018 - 10 - 19)<br>全文                                                                                                                        | 1-20                        |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                     |                             |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| <table border="0"> <tr> <td>           * 引用文件的具体类型:<br/>           “A” 认为不特别相关的表示了现有技术一般状态的文件<br/>           “E” 在国际申请日的当天或之后公布的在先申请或专利<br/>           “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)<br/>           “O” 涉及口头公开、使用、展览或其他方式公开的文件<br/>           “P” 公布日先于国际申请日但迟于所要求的优先权日的文件         </td> <td>           “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件<br/>           “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性<br/>           “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性<br/>           “&amp;” 同族专利的文件         </td> </tr> </table> |                                                                                                                                                                                     |                             | * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“P” 公布日先于国际申请日但迟于所要求的优先权日的文件 | “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件<br>“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性<br>“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性<br>“&” 同族专利的文件 |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“P” 公布日先于国际申请日但迟于所要求的优先权日的文件                                                                                                                                                                                                                                                                                                                                                                                          | “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件<br>“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性<br>“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性<br>“&” 同族专利的文件 |                             |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| 国际检索实际完成的日期<br>2020年 7月 6日                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                     | 国际检索报告邮寄日期<br>2020年 7月 20日  |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                     | 授权官员<br>王燕<br>电话号码 62089117 |                                                                                                                                                                                                           |                                                                                                                                                                                     |         |    |                                                                         |      |   |                                                                                     |      |   |                                                              |      |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2020/087051

| 检索报告引用的专利文件 |           |   | 公布日<br>(年/月/日) | 同族专利         | 公布日<br>(年/月/日) |
|-------------|-----------|---|----------------|--------------|----------------|
| CN          | 110245489 | A | 2019年 9月 17日   | 无            |                |
| CN          | 107342858 | A | 2017年 11月 10日  | CN 107342858 | B 2019年 9月 10日 |
| CN          | 108681898 | A | 2018年 10月 19日  | 无            |                |