(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 4 月 1 日 (01.04.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/057005 A1

(51) 国际专利分类号:
G06F 16/27 (2019.01)

(21) 国际申请号: PCT/CN2020/082673

(22) 国际申请日: 2020 年 4 月 1 日 (01.04.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910904526.5 2019年9月24日 (24.09.2019) CN

(71) 申请人: 北京海益同展信息科技有限公司 (**BEIJING HAI YI TONG ZHAN INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市北京经济技术开发区科创十一街18号院2号楼6层601, Beijing 100176 (CN)。

(72) 发明人: 邵珠光(**SHAO, Zhuguang**); 中国北京市北京经济技术开发区科创十一街18号院2号楼6层601, Beijing 100176 (CN)。 王哲(**WANG, Zhe**); 中国北京市北京经济技术开发区科创十一街18号院2号楼6层601, Beijing 100176 (CN)。

(74) 代理人: 北京英赛嘉华知识产权代理有限责任公司 (**INSIGHT INTELLECTUAL PROPERTY LIMITED**); 中国北京市朝阳区建外大街光华东里8号中海广场中楼7层, Beijing 100020 (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, 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,

(54) **Title:** METHOD AND DEVICE FOR PUBLISHING SMART CONTRACT

(54) **发明名称**: 用于发布智能合约的方法和装置

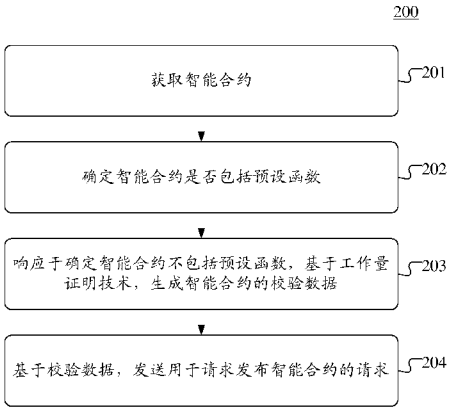

图 2

201 Obtain a smart contract
202 Determine whether the smart contract comprises a preset function
203 In response to determining that the smart contract does not comprise the preset function, generate verification data of the smart contract on the basis of a proof of work technology
204 Send, on the basis of the verification data, a request of requesting to publish the smart contract

(57) **Abstract:** Disclosed are a method and device for publishing a smart contract. A specific embodiment of the method comprises: obtaining a smart contract; determining whether the smart contract comprises a preset function; in response to determining that the smart contract does not comprise the preset function, generating verification data of the smart contract on the basis of a proof of work technology; and sending, on the basis of the verification data, a request of requesting to publish the smart contract. The embodiment can ensure the security of subsequent processes of the smart contract such as publishing and executing.

(57) **摘要**: 本公开的实施例公开了用于发布智能合约的方法和装置。该方法的一具体实施方式包括: 获取智能合约; 确定智能合约是否包括预设函数; 响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据; 基于校验数据，发送用于请求发布智能合约的请求。该实施方式可以保证后续智能合约的发布、执行等过程的安全性。

WO 2021/057005 A1

[见续页]

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))。

用于发布智能合约的方法和装置

本专利申请要求于 2019 年 9 月 24 日提交的、申请号为 201910904526.5、申请人为北京海益同展信息科技有限公司、发明名称为“用于发布智能合约的方法和装置”的中国专利申请的优先权，该申请的全文以引用的方式并入本申请中。

技术领域

本公开的实施例涉及计算机技术领域，具体涉及用于发布智能合约的法和装置。

背景技术

目前，智能合约与区块链的结合应用是当前区块链技术领域的一个研究方向。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

随着区块链技术的成熟发展，用户可以通过智能合约来操作数据。由于用户需求的多样性，许多区块链系统（如 Fabric、以太坊、CITA 等）如今都开始采用图灵完备性语言（如 Java、Python、C、C++等）开发智能合约。

发明内容

本公开的实施例提出了用于发布智能合约的方法和装置。

第一方面，本公开的实施例提供了一种用于发布智能合约的方法，该方法包括：获取智能合约；确定智能合约是否包括预设函数；响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据；基于校验数据，发送用于请求发布智能合约的请求。

在一些实施例中，预设函数包括破坏区块链系统的安全性的函数。

在一些实施例中，上述方法还包括：响应于确定智能合约包括预设函数，输出提示信息以提示智能合约异常。

在一些实施例中，预设函数包括以下至少一项：使用时变性变量的函数、执行文件的输入/输出（I/O）操作的函数、调用脚本以控制系统的函数、执行网络相关的操作的函数、控制系统的环境变量的函数。

在一些实施例中，基于工作量证明技术，生成智能合约的校验数据，包括：基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据，其中，标识数据包括以下至少一项：随机数组、区块链系统的预设标识。

在一些实施例中，基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据，包括：执行如下运算步骤：对标识数据和智能合约进行哈希运算，得到运算结果；确定得到的运算结果是否满足预设的工作量要求；响应于确定得到的运算结果满足预设的工作量要求，确定得到的运算结果作为智能合约的校验数据；响应于确定得到的运算结果不满足预设的工作量要求，继续执行运算步骤。

在一些实施例中，基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据，包括：响应于确定智能合约属于正式发布的智能合约，基于工作量证明技术，根据标识数据，生成智能合约的校验数据。

在一些实施例中，确定智能合约是否包括预设函数，包括：确定智能合约中的目标自定义函数是否包括预设函数，其中，目标自定义函数包括智能合约中的、除库函数和预设的免检函数之外的函数。

第二方面，本公开的实施例提供了一种用于发布智能合约的装置，该装置包括：获取单元，被配置成获取智能合约；确定单元，被配置成确定智能合约是否包括预设函数；生成单元，被配置成响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据；发送单元，被配置成基于校验数据，发送用于请求发布智能合约的请求。

在一些实施例中，预设函数包括破坏区块链系统的安全性的函数。

在一些实施例中，上述装置还包括：输出单元，被配置成响应于确定智能合约包括预设函数，输出提示信息以提示智能合约异常。

在一些实施例中，预设函数包括以下至少一项：使用时变性变量的函数、执行文件的输入/输出 I/O 操作的函数、调用脚本以控制系统的函数、执行网络相关的操作的函数、控制系统的环境变量的函数。

在一些实施例中，上述生成单元进一步被配置成基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据，其中，标识数据包括以下至少一项：随机数组、区块链系统的预设标识。

在一些实施例中，上述生成单元进一步被配置成执行如下运算步骤：对标识数据和智能合约进行哈希运算，得到运算结果；确定得到的运算结果是否满足预设的工作量要求；响应于确定得到的运算结果满足预设的工作量要求，确定得到的运算结果作为智能合约的校验数据；响应于确定得到的运算结果不满足预设的工作量要求，继续执行运算步骤。

在一些实施例中，上述生成单元进一步被配置成响应于确定智能合约属于正式发布的智能合约，基于工作量证明技术，根据标识数据，生成智能合约的校验数据。

在一些实施例中，上述确定单元进一步被配置成确定智能合约中的目标自定义函数是否包括预设函数，其中，目标自定义函数包括智能合约中的、除库函数和预设的免检函数之外的函数。

第三方面，本公开的实施例提供了一种终端设备，该终端设备包括：一个或多个处理器；存储装置，用于存储一个或多个程序；当一个或多个程序被一个或多个处理器执行，使得一个或多个处理器实现如第一方面中任一实现方式描述的方法。

第四方面，本公开的实施例提供了一种计算机可读介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如第一方面中任一实现方式描述的方法。

本公开的实施例提供的用于发布智能合约的方法和装置，通过在请求发布智能合约之前，先对智能合约进行检查以确定其中是否包括预设函数，从而可以对智能合约的处理逻辑进行控制，避免智能合约的执行导致非预期的结果产生。在确定智能合约不包括预设函数之后，可以进一步基于工作量证明技术，生成智能合约的校验数据，以保证

后续智能合约的发布、执行等过程的安全性。

附图说明

通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本公开的其它特征、目的和优点将会变得更明显：

图 1 是本公开的一个实施例可以应用于其中的示例性系统架构图；

图 2 是根据本公开的用于发布智能合约的方法的一个实施例的流程图；

图 3 是根据本公开的实施例的用于发布智能合约的方法的一个应用场景的示意图；

图 4 是根据本公开的用于发布智能合约的方法的又一个实施例的流程图；

图 5 是根据本公开的用于发布智能合约的装置的一个实施例的结构示意图；

图 6 是适于用来实现本公开的实施例的电子设备的结构示意图。

具体实施方式

下面结合附图和实施例对本公开作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本公开。

图 1 示出了可以应用本公开的用于发布智能合约的方法或用于发布智能合约的装置的实施例的示例性架构 100。

如图 1 所示，系统架构 100 可以包括终端设备 101、102、103，网络 104 和区块链系统 105。区块链系统 105 可以包括一个或多个节点，节点之间可以通信连接。网络 104 用以在终端设备 101、102、103

和区块链系统 105 之间提供通信链路的介质。网络 104 可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

终端设备 101、102、103 通过网络 104 与区块链系统 105 交互，以接收或发送消息等。终端设备 101、102、103 上可以安装有各种通讯客户端应用。例如，智能合约开发平台、区块链应用平台等等。

终端设备 101、102、103 可以是硬件，也可以是软件。当终端设备 101、102、103 为硬件时，可以是各种电子设备，包括但不限于智能手机、平板电脑、电子书阅读器、膝上型便携计算机和台式计算机等等。当终端设备 101、102、103 为软件时，可以安装在上述所列举的电子设备中。其可以实现成多个软件或软件模块（例如用来提供分布式服务的多个软件或软件模块），也可以实现成单个软件或软件模块。在此不做具体限定。

区块链系统 105 中的一个或多个节点可以提供各种服务，例如可以接收终端设备 101、102、103 上发送的智能合约发布请求，并生成对应的智能合约执行交易，以完成智能合约的执行。

需要说明的是，本公开的实施例所提供的种用于发布智能合约的方法一般由终端设备 101、102、103 执行，相应地，用于发布智能合约的装置一般设置于终端设备 101、102、103 中。

需要指出的是，区块链系统 105 中的节点可以是单一服务器，也可以由多个服务器或多个服务器集群构成。其中，上述服务器可以是硬件，也可以是软件。当服务器为硬件时，可以实现成多个服务器组成的分布式服务器集群，也可以实现成单个服务器。当服务器为软件时，可以实现成多个软件或软件模块（例如用来提供分布式服务的多个软件或软件模块），也可以实现成单个软件或软件模块。在此不做具体限定。

应该理解，图 1 中的终端设备、网络和区块链系统的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和区块链系统。

继续参考图 2，其示出了根据本公开的用于发布智能合约的方法

的一个实施例的流程 200。该用于发布智能合约的方法包括以下步骤：

步骤 201，获取智能合约。

在本实施例中，用于发布智能合约的方法的执行主体（如图 1 所示的终端设备 101、102、103）可以从本地或其它设备获取智能合约。其中，智能合约可以由技术人员根据实际的应用需求预先开发。智能合约的开发语言可以根据实际的应用需求灵活选择。例如，开发语言可以为各种图灵完备性语言（如 Java、Python、C、C++等等）。

步骤 202，确定智能合约是否包括预设函数。

在本实施例中，预设函数可以由技术人员根据实际的应用需求预先指定。由此，可以通过对智能合约的检查，可以及时了解智能合约中是否包括可能导致非预期情况产生的函数，进而可以在发布之前对智能合约的处理逻辑进行控制。

在本实施例的一些可选的实现方式中，预设函数包括破坏智能合约的安全性的函数。例如，出于智能合约的代码安全性考虑，预设函数可以为以下至少一项：可能导致智能合约无效的函数、可能导致无限循环的函数、可能导致递归栈耗尽的函数、可能导致重要信息泄露的函数、可能导致越权访问的函数、可能引发智能合约的逻辑漏洞的函数等等。

在本实施例的一些可选的实现方式中，预设函数包括破坏区块链系统的安全性的函数。应当可以理解，区块链系统可以指用于完成智能合约的执行的操作的区块链系统。例如，预设函数可以为影响区块链系统中个各节点的共识的函数。

可选地，预设函数包括以下至少一项：使用时变性变量的函数、执行文件的输入/输出 I/O 操作的函数、调用脚本以控制系统的函数、执行网络相关的操作的函数、控制系统的环境变量的函数。

其中，时变性变量可以指每次执行结果可能不一致的变量。例如，随机数、时间戳等。使用时变性变量的函数可能导致同时执行智能合约的各个节点的执行结果不一致。

其中，执行文件的输入/输出 I/O 操作的函数容易影响数据一致性。例如，可能会导致错误的信息写入区块链数据库中。其中，执行网络

相关的操作的函数（如指示访问网络资源的函数、指示发送网络请求的函数等）容易影响区块链系统的通信安全。

其中，调用脚本以控制系统的函数、控制系统的环境变量的函数容易影响区块链系统的权限控制。例如，可能导致如越权访问等的情况发生，从而造成对区块链系统的恶意攻击。

应当可以理解，针对不同的应用需求，智能合约的具体内容可能具有较大差异。例如，不同的智能合约可能存在的安全性问题，以及可能对区块链系统改成的危害也可能不同。因此，预设函数可以基于实际的应用需求灵活设置。

在本实施例中，可以灵活选取各种方法检测智能合约中是否包括预设函数。例如，可以利用各种程序分析方法或程序分析应用获取智能合约包括的各函数的标识信息。然后检测获取的各函数的标识信息总是否包括预设函数的标识信息。

其中，函数的标识信息可以基于函数所属的类名、函数名、函数的参数信息等确定。例如，可以采用函数所属的类名、函数名和函数的参数信息组成的三元组作为函数的标识信息。应当理解，针对不同的开发语言，可以采用不同的方法检测智能合约中是否包括预设函数，也可以设计不同的标识方法以标识函数。

若获取的各函数的标识信息中包括预设函数的标识信息，则表征智能合约包括预设函数。相反地，若获取的各函数的标识信息中不包括预设函数的标识信息，则表征智能合约不包括预设函数。

可选地，可以确定智能合约中的目标自定义函数是否包括预设函数。其中，目标自定义函数可以包括智能合约中的、除库函数和预设的免检函数之外的函数。其中，库函数可以为智能合约的开发语言本身提供的底层函数。免检函数可以指由技术人员预先设置的、无需检测的函数。其中，目标自定义函数可以指智能合约中的各种由开发人员编写的函数。例如，目标自定义函数可以是符合预设条件的由开发人员编写的函数。

可选地，可以通过如下步骤确定智能合约是否包括预设函数：先解析智能合约的入口函数以确定入口函数所调用的各个内部函数。然

后可以确定入口函数所调用的各个内部函数作为目标内部函数集，以及从目标内部函数集中选取一个内部函数作为目标函数，执行如下检测步骤：

步骤一，确定目标函数是否已被检测过。

先判断目标函数是否已被检测过，可以避免函数递归式调用或嵌入式调用情况下无法跳出循环的情况。

步骤二，响应于确定目标函数已被检测过，且目标内部函数集中未被选取过的内部函数的数目不为 0，从目标内部函数集中选取未被选取过的一个内部函数作为目标函数，继续执行上述检测步骤；响应于确定目标函数已被检测过，且目标内部函数集中未被选取过的内部函数的数目为 0，确定智能合约不包括预设函数。

步骤三，响应于确定目标函数未被检测过，确定目标函数是否是预设函数，以及将目标函数标记为已检测。

步骤四，响应于确定目标函数是预设函数，输出提示信息以提示智能合约异常。

步骤五，响应于确定目标函数不是预设函数，确定目标函数是否是库函数或预设的免检函数；

步骤六，响应于确定目标函数是库函数或预设的免检函数，且目标内部函数集中未被选取过的内部函数的数目不为 0，从目标内部函数集中选取未被选取过的一个内部函数作为目标函数，继续执行上述检测步骤；响应于确定目标函数是库函数或预设的免检函数，且目标内部函数集中未被选取过的内部函数的数目为 0，确定智能合约不包括预设函数。

步骤七，响应于确定目标函数不是库函数或预设的免检函数，解析获取目标函数所调用的各个内部函数作为目标内部函数集，以及从目标内部函数集中选取一个内部函数作为目标函数，执行上述检测步骤。

步骤 203，响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据。

在本实施例中，工作量证明（Proof-of-Work，PoW）是一种对应

服务与资源滥用、或是阻断服务攻击的经济对策。一般是要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源作为担保成本，以确保服务与资源是被真正的需求所使用。目前，工作量证明技术常用的技术原理是散列函数。工作量证明技术是目前广泛研究和应用的公知技术，在此不再赘述。

在本实施例中，基于工作量证明技术，可以生成需要耗费一定成本（如时间、计算资源等等）才能得到的校验数据。其中，校验数据可以用于在后续对智能合约的各种处理过程中对智能合约的校验，以避免不法人士恶意伪造智能合约等情况。

应当可以理解，工作量证明技术的技术原理多种多样，采用不同技术原理的工作量技术，生成智能合约的校验数据的方式也可以不同。

作为示例，采用基于散列函数的工作量证明技术，可以对智能合约不断进行哈希运算，直到得到符合预设要求的运算结果，进而可以将得到的符合预设要求的运算结果作为智能合约的校验数据。其中，预设要求可以由技术人员根据实际应用场景设置。例如，预设要求可以为：得到的运算结果的前 N 位为 0。

在本实施例的一些可选的实现方式中，响应于确定智能合约包括预设函数，可以输出提示信息以提示智能合约异常，以便于用户可以及时对智能合约进行检测和调整。

步骤 204，基于校验数据，发送用于请求发布智能合约的请求。

在本实施例中，在得到校验数据之后，可以进一步对智能合约进行编译，并结合校验数据进行打包，从而可以基于期望使用的区块链平台发送请求以完成智能合约的发布。其中，发送的用于请求发布智能合约的请求中可以包含用于指示智能合约的校验数据的信息。例如，用于请求发布智能合约的请求中可以包含智能合约的校验数据，也可以包含智能合约的校验数据的标识信息（如地址等）。

继续参见图 3，图 3 是根据本实施例的用于发布智能合约的方法的一个示意性的应用场景 300。在图 3 的应用场景中，可以先获取开发人员预先编写的智能合约，然后解析智能合约中的各个函数，并分析智能合约中的各个函数是否有预先指定的各预设函数中的预设函

数。若智能合约中的各个函数没有预先指定的任一预设函数，则可以对智能合约进行哈希运算，以得到满足 PoW 要求的运算结果作为智能合约的校验数据。进一步地，可以请求对智能合约和校验数据进行编译打包等操作以完成智能合约的发布。

本公开的上述实施例提供的方法通过在请求发布智能合约之前，先对智能合约进行检查以确定其中是否包括预设函数，从而可以对智能合约的处理逻辑进行控制，避免智能合约的执行导致非预期的结果产生。在确定智能合约不包括预设函数之后，可以进一步基于工作量证明技术，生成智能合约的校验数据，以保证后续智能合约的发布、执行等过程的安全性，避免了可能危害区块链系统的智能合约的发布。

进一步参考图 4，其示出了用于发布智能合约的方法的又一个实施例的流程 400。该用于发布智能合约的方法的流程 400，包括以下步骤：

步骤 401，获取智能合约。

步骤 402，确定智能合约是否包括预设函数。

上述步骤 401 和 402 的具体的执行过程可参考图 2 对应实施例中的步骤 201 和 202 的相关说明，在此不再赘述。

步骤 403，响应于确定智能合约不包括预设函数，基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据。

在本实施例中，标识数据可以包括以下至少一项：随机数组、区块链系统的预设标识。其中，随机数组可以利用现有的各种随机算法生成。其中，区块链系统的预设标识可以指区块链系统预先设置的标识。

此时，可以结合标识数据和智能合约以生成符合预设工作量要求的校验数据。由此，可以进一步增加生成智能合约的校验数据的难度，从而进一步增强伪造智能合约的难度，提升智能合约的后续处理过程的安全性。

在本实施例中，可以基于哈希运算、卷积求导、大质数分解等运算实现工作量证明。以哈希运算作为示例，可以通过如下步骤生成智

能合约的校验数据：

执行如下运算步骤：对标识数据和智能合约进行哈希运算，得到运算结果；确定得到的运算结果是否满足预设的工作量要求；响应于确定得到的运算结果满足预设的工作量要求，确定得到的运算结果作为智能合约的校验数据；响应于确定得到的运算结果不满足预设的工作量要求，继续执行上述运算步骤。

例如，预设的工作量要求为：得到的运算结果的前 N 位均为 1。此时，可以生成第一随机数组，然后对第一随机数组、区块链系统的预设标识和智能合约进行哈希运算，得到第一运算结果。若第一运算结果的前 N 位不均为 1，则可以生成第二随机数组，然后对第二随机数组、区块链系统的预设标识和智能合约进行哈希运算，得到第二运算结果。若第二运算结果的前 N 位均为 1，则可以将第二运算结果作为智能合约的校验数据。

可选地，可以确定智能合约是否属于正式发布的智能合约。响应于确定智能合约属于正式发布的智能合约，可以基于工作量证明技术，根据随机数组，生成智能合约的校验数据。响应于确定智能合约不属于正式发布的智能合约（如测试发布的智能合约），可以基于工作量证明技术，仅利用智能合约生成校验数据，以减少测试发布过程中的资源消耗。

步骤 404，基于校验数据，发送用于请求发布智能合约的请求。

在本实施例中，在得到校验数据之后，可以进一步对智能合约进行编译，并结合随机数组和/或区块链系统的预设标识、校验数据进行打包，从而可以基于期望使用的区块链平台发送请求以完成智能合约的发布。

基于上述生成智能合约的校验数据的具体方式，对应可以设置在发布智能合约时的检测方式。作为示例，在发布智能合约前，可以先根据用于请求发布智能合约的请求，获取智能合约对应的随机数组和/或区块链系统的预设标识，以及智能合约的校验数据。

应当可以理解，若基于随机数组生成智能合约的校验数据，则可以根据用于请求发布智能合约的请求，获取智能合约对应的随机数组

和校验数据，若基于随机数组和区块链系统的预设标识生成智能合约的校验数据，则可以根据用于请求发布智能合约的请求，获取智能合约对应的随机数组、区块链系统的预设标识和校验数据。

之后，可以根据获取的智能合约对应的随机数组和/或区块链系统的预设标识，以及智能合约的校验数据校验智能合约是否异常。例如，若基于随机数组和区块链系统的预设标识生成智能合约的校验数据，则可以计算获取的随机数组、区块链系统、智能合约的哈希运算结果，然后确定计算得到的哈希运算结果是否与获取的校验数据是否相同。

若计算得到的哈希运算结果与获取的校验数据不同，则可以表征智能合约异常（如可能是不法人士伪造的智能合约等），进而可以输出提示信息以提示智能合约异常，暂不能完成发布。

若计算得到的哈希运算结果与获取的校验数据相同，则可以进一步校验获取的校验数据是否符合预设的 PoW 要求。若获取的校验数据不符合预设的 PoW 要求，则可以表征智能合约异常，进而可以输出提示信息以提示智能合约异常，暂不能完成发布。若获取的校验数据符合预设的 PoW 要求，则可以表征智能合约正常，可以进一步对智能合约进行处理以完成智能合约的发布。

本公开的上述实施例提供的方法在确定智能合约不包括预设函数之后，可以基于工作量证明技术，根据智能合约的标识数据如随机数组、区块链系统的预设标识等生成智能合约的校验数据，从而增加生成智能合约的校验数据的难度，有助于减少随意发布智能合约的情况。同时，在智能合约发布前，还可以根据随机数组、区块链系统的预设标识等还可以对智能合约进行校验，从而可以有效的检测伪造智能合约等情况，进一步保证发布的智能合约的安全性。

进一步参考图 5，作为对上述各图所示方法的实现，本公开提供了用于发布智能合约的装置的一个实施例，该装置实施例与图 2 所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

如图 5 所示，本实施例提供的用于发布智能合约的装置 500 包括智能合约获取单元 501、确定单元 502、生成单元 503 和发送单元 504。

其中，智能合约获取单元 501 被配置成获取智能合约；确定单元 502 被配置成确定智能合约是否包括预设函数；生成单元 503 被配置成响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据；发送单元 504 被配置成基于校验数据，发送用于请求发布智能合约的请求。

在本实施例中，用于发布智能合约的装置 500 中：获取单元 501、确定单元 502、生成单元 503 和发送单元 504 的具体处理及其所带来的技术效果可分别参考图 2 对应实施例中的步骤 201、步骤 202、步骤 203 和步骤 204 的相关说明，在此不再赘述。

在本实施例的一些可选的实现方式中，预设函数包括破坏区块链系统的安全性的函数。

在本实施例的一些可选的实现方式中，上述用于发布智能合约的装置 500 还包括：输出单元（图中未示出）被配置成响应于确定智能合约包括预设函数，输出提示信息以提示智能合约异常。

在本实施例的一些可选的实现方式中，预设函数包括以下至少一项：使用时变性变量的函数、执行文件的输入/输出 I/O 操作的函数、调用脚本以控制系统的函数、执行网络相关的操作的函数、控制系统的环境变量的函数。

在本实施例的一些可选的实现方式中，上述生成单元 503 进一步被配置成基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据，其中，标识数据包括以下至少一项：随机数组、区块链系统的预设标识。

在本实施例的一些可选的实现方式中，上述生成单元 503 进一步被配置成执行如下运算步骤：对标识数据和智能合约进行哈希运算，得到运算结果；确定得到的运算结果是否满足预设的工作量要求；响应于确定得到的运算结果满足预设的工作量要求，确定得到的运算结果作为智能合约的校验数据；响应于确定得到的运算结果不满足预设的工作量要求，继续执行运算步骤。

在本实施例的一些可选的实现方式中，上述生成单元 503 进一步被配置成响应于确定智能合约属于正式发布的智能合约，基于工作量

证明技术，根据标识数据，生成智能合约的校验数据。

在本实施例的一些可选的实现方式中，上述确定单元 502 进一步被配置成确定智能合约中的目标自定义函数是否包括预设函数，其中，目标自定义函数包括智能合约中的、除库函数和预设的免检函数之外的函数。

本公开的上述实施例提供的装置，通过获取单元获取智能合约；确定单元确定智能合约是否包括预设函数；生成单元响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据；发送单元基于校验数据，发送用于请求发布智能合约的请求，从而可以在请求发布智能合约之前，对智能合约的处理逻辑进行控制，避免智能合约的执行导致非预期的结果产生。

下面参考图 6，其示出了适于用来实现本公开的实施例的电子设备（例如图 1 中的终端设备）600 的结构示意图。本公开的实施例中的终端设备可以包括但不限于诸如移动电话、笔记本电脑、数字广播接收器、PDA（个人数字助理）、PAD（平板电脑）、PMP（便携式多媒体播放器）、车载终端（例如车载导航终端）等等的移动终端以及诸如数字 TV、台式计算机等等的固定终端。图 6 示出的终端设备仅仅是一个示例，不应对本公开的实施例的功能和使用范围带来任何限制。

如图 6 所示，电子设备 600 可以包括处理装置（例如中央处理器、图形处理器等）601，其可以根据存储在只读存储器（ROM）602 中的程序或者从存储装置 608 加载到随机访问存储器（RAM）603 中的程序而执行各种适当的动作和处理。在 RAM 603 中，还存储有电子设备 600 操作所需的各种程序和数据。处理装置 601、ROM 602 以及 RAM 603 通过总线 604 彼此相连。输入/输出（I/O）接口 605 也连接至总线 604。

通常，以下装置可以连接至 I/O 接口 605：包括例如触摸屏、触摸板、键盘、鼠标、摄像头、麦克风、加速度计、陀螺仪等的输入装置 606；包括例如液晶显示器（LCD）、扬声器、振动器等的输出装置 607；包括例如磁带、硬盘等的存储装置 608；以及通信装置 609。通信装置

609 可以允许电子设备 600 与其他设备进行无线或有线通信以交换数据。虽然图 6 示出了具有各种装置的电子设备 600，但是应理解的是，并不要求实施或具备所有示出的装置。可以替代地实施或具备更多或更少的装置。图 6 中示出的每个方框可以代表一个装置，也可以根据需要代表多个装置。

特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信装置 609 从网络上被下载和安装，或者从存储装置 608 被安装，或者从 ROM 602 被安装。在该计算机程序被处理装置 601 执行时，执行本公开的实施例的方法中限定的上述功能。

需要说明的是，本公开的实施例所述的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑磁盘只读存储器（CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。在本公开的实施例中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本公开的实施例中，计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读信号介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当

的介质传输，包括但不限于：电线、光缆、RF（射频）等等，或者上述的任意合适的组合。

上述计算机可读介质可以是上述终端设备中所包含的；也可以是单独存在，而未装配入该终端设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被该终端设备执行时，使得该终端设备：获取智能合约；确定智能合约是否包括预设函数；响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据；基于校验数据，发送用于请求发布智能合约的请求。

可以以一种或多种程序设计语言或其组合来编写用于执行本公开的实施例的操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网（LAN）或广域网（WAN）——连接到用户计算机，或者，可以连接到外部计算机（例如利用因特网服务提供商来通过因特网连接）。

附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

描述于本公开的实施例中所涉及到的单元可以通过软件的方式实

现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括获取单元、确定单元、生成单元和发送单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定，例如，获取单元还可以被描述为“获取智能合约的单元”。

以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本公开的实施例中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离上述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开的实施例中公开的（但不限于）具有类似功能的技术特征进行互相替换而形成的技术方案。

权 利 要 求

1、一种用于发布智能合约的方法，包括:

获取智能合约;

确定所述智能合约是否包括预设函数;

响应于确定所述智能合约不包括预设函数，基于工作量证明技术，生成所述智能合约的校验数据;

基于所述校验数据，发送用于请求发布所述智能合约的请求。

2、根据权利要求 1 所述的方法，其中，所述预设函数包括破坏区块链系统的安全性的函数。

3、根据权利要求 2 所述的方法，其中，所述方法还包括:

响应于确定所述智能合约包括预设函数，输出提示信息以提示所述智能合约异常。

4、根据权利要求 2 所述的方法，其中，所述预设函数包括以下至少一项：使用时变性变量的函数、执行文件的输入/输出（I/O）操作的函数、调用脚本以控制系统的函数、执行网络相关的操作的函数、控制系统的环境变量的函数。

5、根据权利要求 1 所述的方法，其中，所述基于工作量证明技术，生成所述智能合约的校验数据，包括:

基于工作量证明技术，根据所述智能合约的标识数据，生成所述智能合约的校验数据，其中，标识数据包括以下至少一项：随机数组、区块链系统的预设标识。

6、根据权利要求 5 所述的方法，其中，所述基于工作量证明技术，根据所述智能合约的标识数据，生成所述智能合约的校验数据，包括:

执行如下运算步骤：对标识数据和智能合约进行哈希运算，得到

运算结果；确定得到的运算结果是否满足预设的工作量要求；响应于确定得到的运算结果满足预设的工作量要求，确定得到的运算结果作为所述智能合约的校验数据；响应于确定得到的运算结果不满足预设的工作量要求，继续执行所述运算步骤。

7、根据权利要求 5 所述的方法，其中，所述基于工作量证明技术，根据所述智能合约的标识数据，生成所述智能合约的校验数据，包括：

响应于确定所述智能合约属于正式发布的智能合约，基于工作量证明技术，根据所述智能合约的标识数据，生成所述智能合约的校验数据。

8、根据权利要求 1 所述的方法，其中，所述确定所述智能合约是否包括预设函数，包括：

确定所述智能合约中的目标自定义函数是否包括预设函数，其中，所述目标自定义函数包括所述智能合约中的、除库函数和预设的免检函数之外的函数。

9、一种用于发布智能合约的装置，包括：

获取单元，被配置成获取智能合约；

确定单元，被配置成确定所述智能合约是否包括预设函数；

生成单元，被配置成响应于确定所述智能合约不包括预设函数，基于工作量证明技术，生成所述智能合约的校验数据；

发送单元，被配置成基于所述校验数据，发送用于请求发布所述智能合约的请求。

10、一种终端设备，包括：

一个或多个处理器；

存储装置，其上存储有一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求 1-8 中任一所述的方法。

11、一种计算机可读介质，其上存储有计算机程序，其中，该程序被处理器执行时实现如权利要求 1-8 中任一所述的方法。

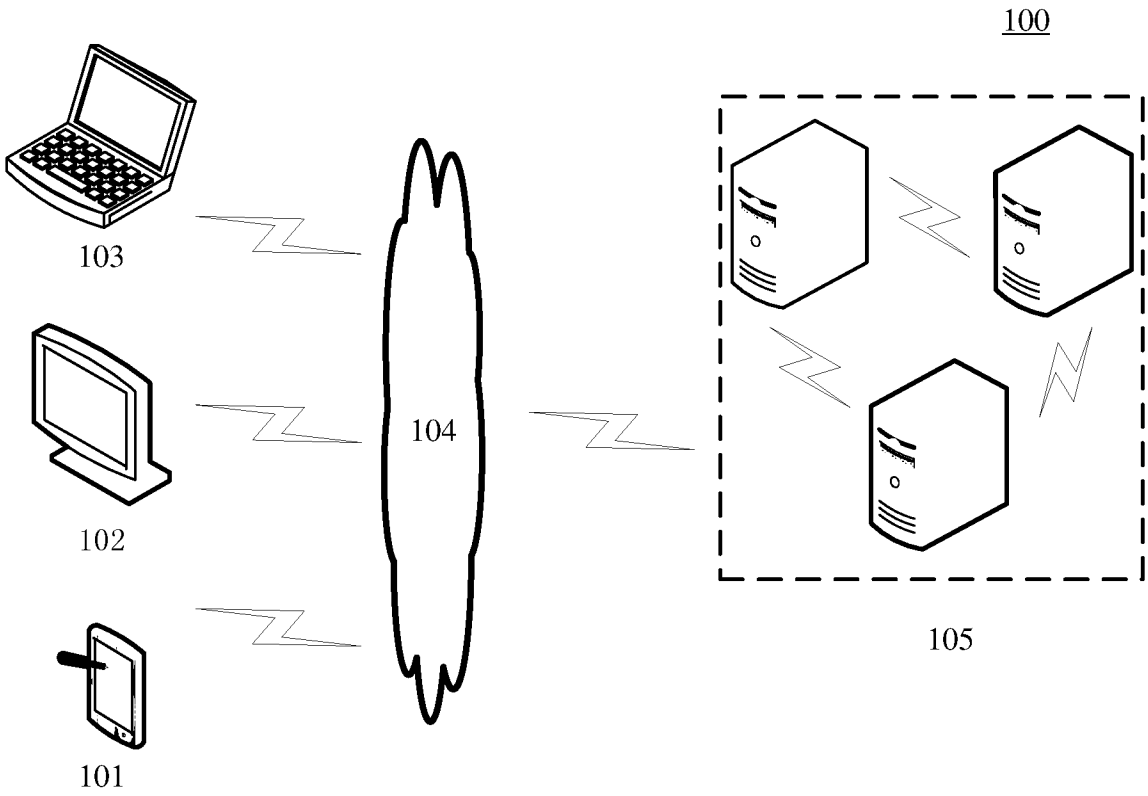

图 1

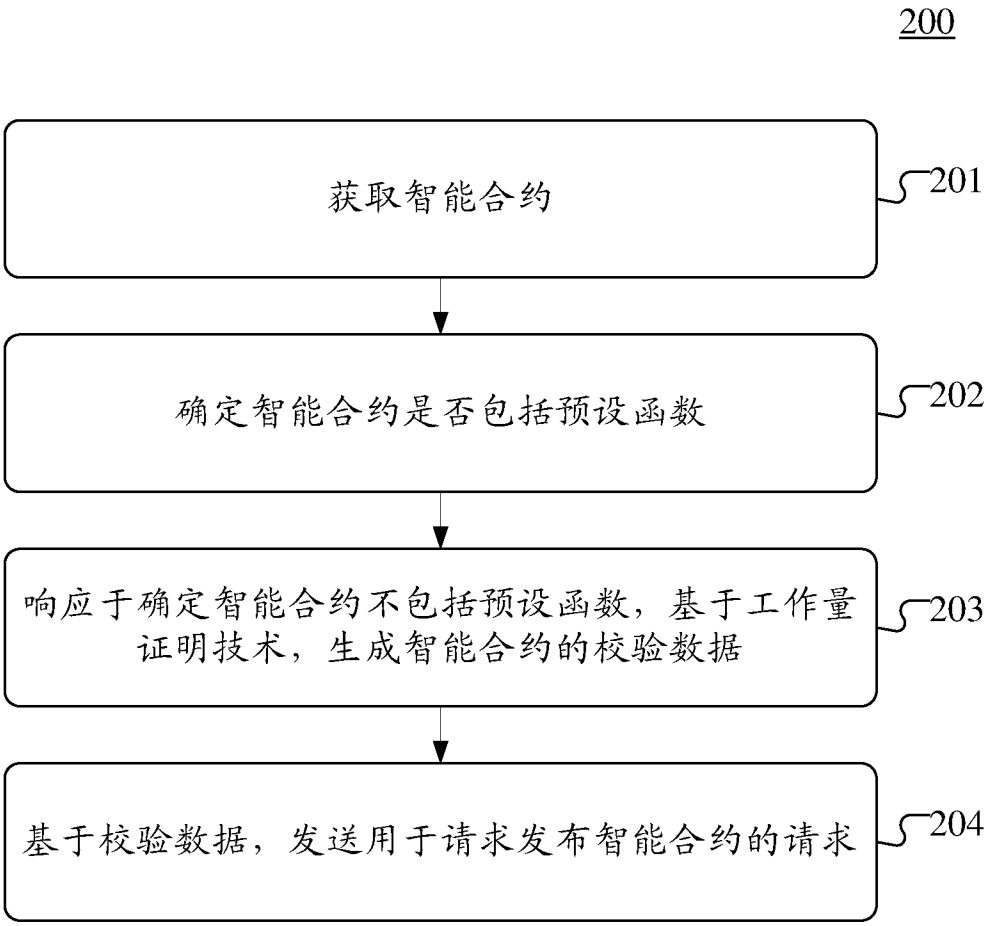
200
获取智能合约
201
确定智能合约是否包括预设函数
202
响应于确定智能合约不包括预设函数，基于工作量证明技术，生成智能合约的校验数据
203
基于校验数据，发送用于请求发布智能合约的请求
204

图 2

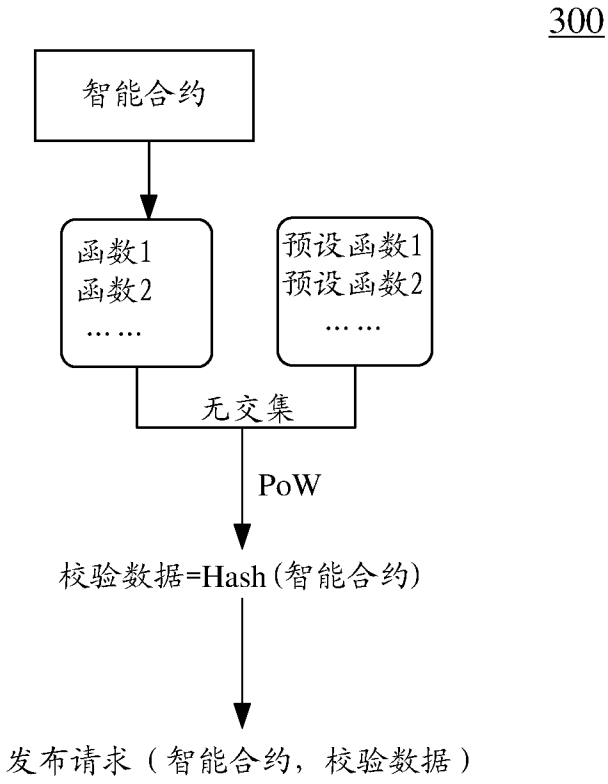
300
智能合约
函数1
函数2
……
预设函数1
预设函数2
……
无交集
PoW
校验数据=Hash（智能合约）
发布请求（智能合约，校验数据）

图 3

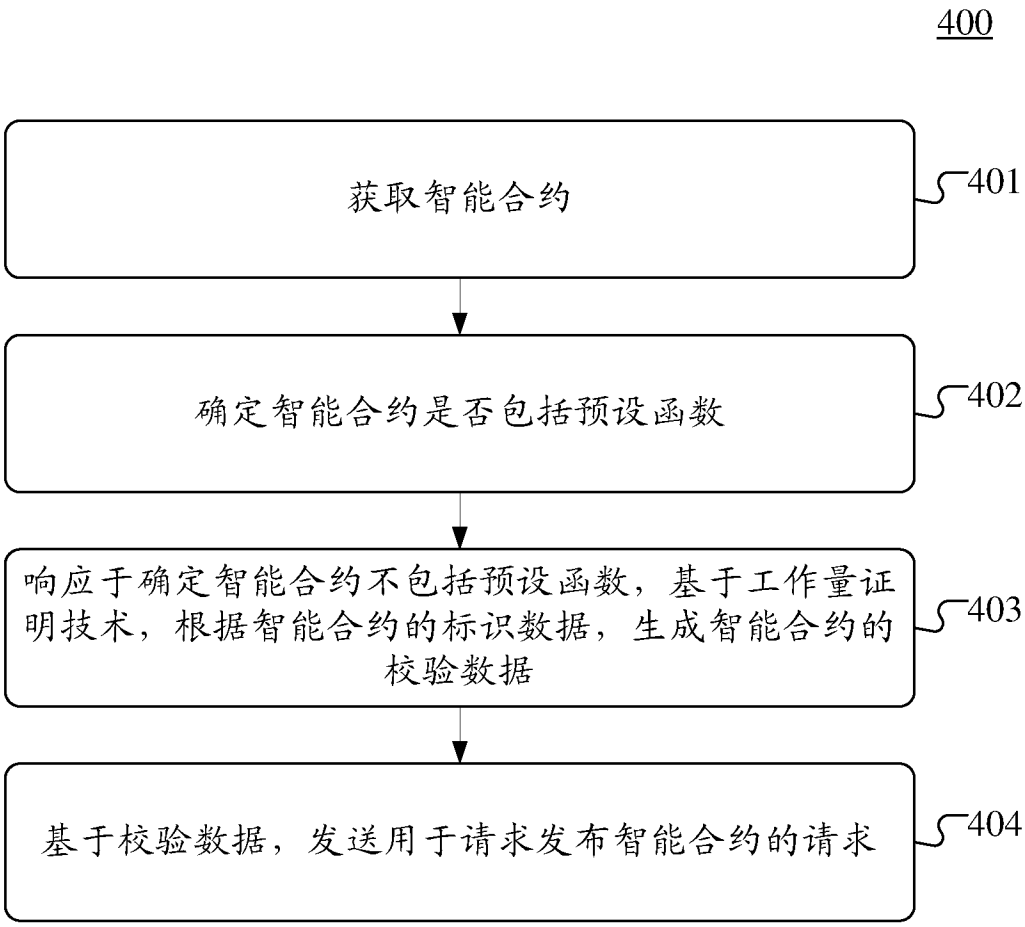
400
获取智能合约
401
确定智能合约是否包括预设函数
402
响应于确定智能合约不包括预设函数，基于工作量证明技术，根据智能合约的标识数据，生成智能合约的校验数据
403
基于校验数据，发送用于请求发布智能合约的请求
404

图 4

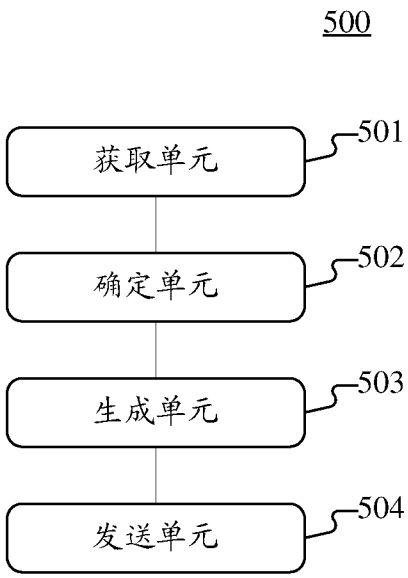
500
获取单元
501
确定单元
502
生成单元
503
发送单元
504

图 5

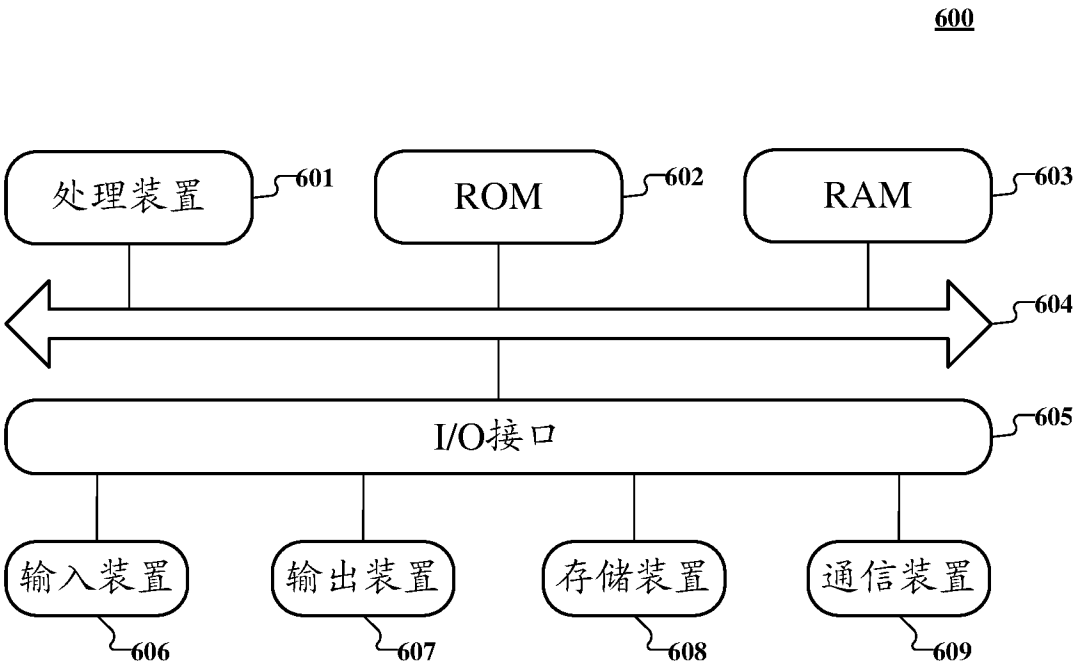
600
处理装置
601
ROM
602
RAM
603
604
I/O接口
605
输入装置
606
输出装置
607
存储装置
608
通信装置
609

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/082673

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/27(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

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)

CNABS, VEN, DWPI, SIPOABS, CNKI: 安全, 错误, 智能合约, 上传, 函数, 产生, 审核, 校验, 发送, 生成, 发布, 验证, security, error, contract, send, function, check, verification, generate, correct

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 109829296 A (SINOCHEM TECHNOLOGY CO., LTD.) 31 May 2019 (2019-05-31) claims 1-7	1-11
A	CN 110111104 A (JUZIX TECHNOLOGY CO., LTD.) 09 August 2019 (2019-08-09) entire document	1-11
A	CN 109542421 A (QUARK CHAIN TECHNOLOGY CO., LIMITED) 29 March 2019 (2019-03-29) entire document	1-11
PX	CN 110688428 A (BEIJING HAIYI TONGZHAN INFORMATION TECHNOLOGY CO., LTD.) 14 January 2020 (2020-01-14) entire document	1-11

☐ 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
11 June 2020	**23 June 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/CN2020/082673

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109829296 A	31 May 2019	None	
CN 110111104 A	09 August 2019	None	
CN 109542421 A	29 March 2019	None	
CN 110688428 A	14 January 2020	None	

国际检索报告

国际申请号
PCT/CN2020/082673

A. 主题的分类

G06F 16/27(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

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））

CNABS, VEN, DWPI, SIPOABS, CNKI:安全，错误，智能合约，上传，函数，产生，审核，校验，发送，生成，发布，验证，security, error, contract, send, function, check, verification, generate,correct

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
X	CN 109829296 A (中化能源科技有限公司) 2019年 5月 31日 (2019-05-31) 权利要求1-7	1-11
A	CN 110111104 A (矩阵元技术深圳有限公司) 2019年 8月 9日 (2019-08-09) 全文	1-11
A	CN 109542421 A (夸克链科技深圳有限公司) 2019年 3月 29日 (2019-03-29) 全文	1-11
PX	CN 110688428 A (北京海益同展信息科技有限公司) 2020年 1月 14日 (2020-01-14) 全文	1-11

☐ 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 6月 11日	2020年 6月 23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 王丹 电话号码 62412062

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/082673

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 109829296 A	2019年 5月 31日	无	
CN 110111104 A	2019年 8月 9日	无	
CN 109542421 A	2019年 3月 29日	无	
CN 110688428 A	2020年 1月 14日	无	