

(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
2023 年 1 月 5 日 (05.01.2023)



(10) 国际公布号
WO 2023/274398 A1

- (51) 国际专利分类号:
G06Q 20/40 (2012.01)
- (21) 国际申请号: PCT/CN2022/103305
- (22) 国际申请日: 2022 年 7 月 1 日 (01.07.2022)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202110749282.5 2021 年 7 月 1 日 (01.07.2021) CN
- (71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。蚂蚁区块链科技 (上海) 有限公司 (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) [CN/CN]; 中国上海市黄浦区外马路 618 号 8 层 803 室, Shanghai 200010 (CN)。
- (72) 发明人: 傅滢(FU, Ying); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000

(CN)。王海军(WANG, Haijun); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。邬萌(WU, Meng); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京亿腾知识产权代理事务所 (普通合伙) (E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国北京市海淀区中关村紫金数码园 3 号楼 707, Beijing 100190 (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, IQ, IR, IS, IT, JM, 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,

(54) Title: SECURITY DETECTION METHOD AND APPARATUS FOR SMART CONTRACT

(54) 发明名称: 智能合约的安全检测方法及装置

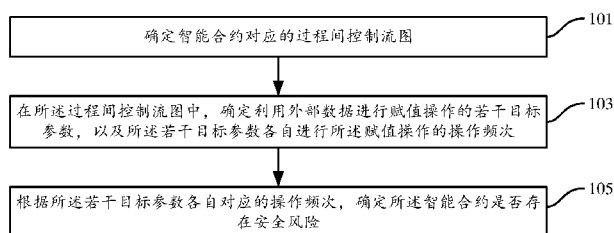


图 1

- 101 Determine an inter-process control flow graph corresponding to a smart contract
- 103 In the inter-process control flow graph, determine a plurality of target parameters for performing assignment operation by using external data, and operation frequencies of respective assignment operation of the plurality of target parameters
- 105 Determine whether the smart contract has a security risk according to the operation frequencies corresponding to the plurality of target parameters

(57) Abstract: A security detection method and apparatus for a smart contract, related to the technical field of blockchains. The method comprises: determining an inter-process control flow graph corresponding to a smart contract (101); in the inter-process control flow graph, determining a plurality of target parameters for performing assignment operation by using external data, and operation frequencies of respective assignment operation of the plurality of target parameters (103), the plurality of target parameters belonging to world state parameters of the block chain, and the external data being input into the smart contract from the outside; and determining whether the smart contract has a security risk according to the operation frequencies corresponding to the plurality of target parameters (105).

(57) 摘要: 一种智能合约的安全检测方法及装置, 涉及区块链技术领域, 该方法包括: 确定智能合约对应的过程间控制流图 (101); 在过程间控制流图中, 确定利用外部数据进行赋值操作的若干目标参数, 以及若干目标参数各自进行赋值操作的操作频次 (103), 若干目标参数属于区块链的世界状态参数, 外部数据自外部输入智能合约; 根据若干目标参数各自对应的操作频次, 确定智能合约是否存在安全风险 (105)。

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))。

智能合约的安全检测方法及装置

5 本申请要求于 2021 年 7 月 1 日提交中国国家知识产权局、申请号为 202110749282.5、
申请名称为“智能合约的安全检测方法及装置”的中国专利申请的优先权，其全部内容通过
引用结合在本申请中。

技术领域

10 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及智能合约的安全检测方法
及装置。

背景技术

智能合约 (Smart contract) 是以数字形式定义的承诺 (Commitment)。其中可以由部
署智能合约的区块链系统，保障智能合约的存储、读取以及执行等过程可跟踪且不可篡改。
15 注册在区块链系统中的交易双方可以对智能合约进行部署或调用，实现通过透明且无
冲突的方式交换资源或其它业务目的。

经发明人研究发现，智能合约自身可能存在安全风险。例如，智能合约自身可能存在
被进行重排攻击的风险，入侵者可能通过对智能合约进行重排攻击，使用户发起的用于调
用智能合约的交易无法达到其预期的效果。

20 希望有一种新的技术方案，以期检测智能合约自身是否存在安全风险。

发明内容

本说明书一个或多个实施例中提供了一种智能合约的安全检测方法及装置，可以更加
高效的检测智能合约是否存在安全风险。

25 第一方面，提供了一种智能合约的安全检测方法，包括：确定智能合约对应的过程间
控制流图；在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，
以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链
的世界状态参数，外部数据自外部输入所述智能合约；根据所述若干目标参数各自对应的
操作频次，确定所述智能合约是否存在安全风险。

30 在一种可能的实施方式中，根据所述若干目标参数各自对应的操作频次，确定所述智
能合约是否存在安全风险，具体包括：当存在大于 1 的操作频次时，确定所述智能合约存
在安全风险。

在一种可能的实施方式中，所述智能合约包括存储于内存中的代码段和数据段，所述
数据段中包括所述若干目标参数，所述代码段中通过所述数据段在所述内存中的基地址和
35 所述目标参数对应的地址偏移量对所述目标参数进行标识。

在一种可能的实施方式中，所述在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，包括：在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程；在所述过程间控制流图中确定若干第二指令序列，所述第二指令序列用于表征世界状态参数被赋值的过程；根据所述若干第一指令序列和所述若干第二指令序列之间重合的赋值指令，确定所述若干目标参数。

在一种可能的实施方式中，在所述过程间控制流图中确定若干第一指令序列，包括：在所述过程间控制流图中，对外部数据对应的参数添加污点标记，沿着数据流向进行污点跟踪，将添加有污点标记的参数对应的指令归入所述第一指令序列。

在一种可能的实施方式中，在所述过程间控制流图中确定若干第二指令序列，包括：在所述过程间控制流图中确定世界状态参数；在所述过程间控制流图中，确定用于对世界状态参数进行赋值的赋值指令，并将该赋值指令归入所述第二指令序列。

在一种可能的实施方式中，在所述过程间控制流图中确定世界状态参数，包括：在所述过程间控制流图中，确定调用预定函数的若干函数调用指令；将所述函数调用指令请求更新的参数确定为世界状态参数。

在一种可能的实施方式中，根据所述若干第一指令序列和若干第二指令序列之间重合的赋值指令，确定所述若干目标参数，包括：将所述重合的赋值指令所指向的世界状态参数作为所述目标参数。

在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程用于指示未利用外部数据进行赋值。所述根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险，具体包括：确定所述若干目标参数中是否存在第一参数，其中所述第一参数对应的操作频次大于 1，所述第一参数被赋值的过程包括第一类赋值过程和第二类赋值过程；如果是，确定所述智能合约存在安全风险。

在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程指示未利用外部数据进行赋值。所述根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险，具体包括：确定所述若干目标参数中是否存在第二参数，其中所述第二参数对应的操作频次大于 1，所述第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程，所述第二参数的第一类赋值过程和第二类赋值过程，在所述过程间控制流图中对应不同的方法函数；如果是，确定所述智能合约存在安全风险。

在一种可能的实施方式中，所述智能合约是待部署到区块链中的智能合约；和/或，所

述安全风险具体包括被进行重排攻击的风险。

第二方面，提供了一种智能合约的安全检测装置，包括：解析处理单元，配置为确定智能合约对应的过程间控制流图；赋值检测单元，配置为在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约；风险确定单元，配置为根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

在一种可能的实施方式中，所述风险确定单元，配置为当存在大于 1 的操作频次时，确定所述智能合约存在安全风险。

在一种可能的实施方式中，所述智能合约包括存储于内存中的代码段和数据段，所述数据段中包括所述若干目标参数，所述代码段中通过所述数据段在所述内存中的基地址和所述目标参数对应的地址偏移量对所述目标参数进行标识。

在一种可能的实施方式中，所述赋值检测单元包括：第一确定子单元，配置为在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程；第二确定子单元，配置为在所述过程间控制流图中确定若干第二指令序列，所述第二指令序列用于表征世界状态参数被赋值的过程；赋值检测子单元，配置为根据所述若干第一指令序列和所述若干第二指令序列之间重合的赋值指令，确定所述若干目标参数。

在一种可能的实施方式中，所述第一确定子单元，配置为在所述过程间控制流图中，对外部数据对应的参数添加污点标记，沿着数据流向进行污点跟踪，将添加有污点标记的参数对应的指令归入所述第一指令序列。

在一种可能的实施方式中，所述第二确定子单元，配置为在所述过程间控制流图中确定世界状态参数；在所述过程间控制流图中，确定用于对世界状态参数进行赋值的赋值指令，并将该赋值指令归入所述第二指令序列。

在一种可能的实施方式中，所述第二确定子单元，具体配置为在所述过程间控制流图中，确定调用预定函数的若干函数调用指令；将所述函数调用指令请求更新的参数确定为世界状态参数。

在一种可能的实施方式中，所述赋值检测子单元，具体配置为将所述重合的赋值指令所指向的世界状态参数作为所述目标参数。

在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程用于指示未利用外部数据进行赋值。所述风险确定单元，具体配置为确定所述若干目标参数中是否存在第一参数，其中所述第一参数对应的操作频次大于 1，所述第一参数被赋值的过程包括第一类赋值过程和第二类赋值过程；如果是，确定所述智能合约存在安全风险。

在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程指示未利用外部数据进行赋值。所述风险确定单元，具体配置为确定所述若干目标参数中是否存在第二参数，其中所述第二参数对应的操作频次大于1，所述第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程，所述第二参数的第一类赋值过程和第二类赋值过程，在所述过程间控制流图中对应不同的方法函数；如果是，确定所述智能合约存在安全风险。

在一种可能的实施方式中，所述智能合约是待部署到区块链中的智能合约；和/或，所述安全风险具体包括被进行重排攻击的风险。

第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序/指令，当计算机程序/指令在计算设备中执行时，计算设备执行如第一方面中任一项所述的方法。

第四方面，提供了一种计算设备，包括存储器和处理器，存储器中存储有计算机程序/指令，处理器执行可计算机程序/指令时，实现如第一方面中任一项所述的方法。

通过本说明书一个或多个实施例中提供的方法及装置，可以通过确定出智能合约对应的过程间控制流图，然后基于过程间控制流图，确定智能合约中利用外部数据进行赋值操作的若干目标参数各自对应的操作频次，进而基于若干目标参数各自对应的操作频次，快速且高效的确定智能合约是否存在安全风险。

附图说明

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

图1为本说明书实施例中提供的一种智能合约的安全检测方法的流程图；

图2为本说明书实施例中确定利用外部数据进行赋值操作的目标参数的过程示意图；

图3为本说明书实施例中提供的示例性的过程间控制流图；

图4为本说明书实施例中提供的一种智能合约的安全检测装置的示意图。

具体实施方式

下面结合附图，对本说明书所提供的各个非限制性实施例进行详细描述。

经发明人研究发现，智能合约自身可能存在安全风险。例如，智能合约自身可能存在被进行重排攻击的风险，入侵者可能通过对智能合约进行重排攻击，使用于调用智能合约的交易无法达到预期的效果。又如，智能合约自身允许利用外部数据对世界状态参数进行赋值，入侵者可能通过调用智能合约中不同的方法函数，对世界状态参数进行恶意修改，

使用于调用智能合约的交易无法达到其预期的效果。

经发明人研究发现，确定智能合约的过程间控制流图（inter procedural control flow graph, ICFG）之后，可以通过对 ICFG 进行静态分析，获知智能合约中利用自外部输入智能合约的外部数据，对属于区块链的世界状态参数的若干目标参数分别进行赋值操作的频次。若干目标参数各自对应的操作频次，能够在某种程度上反映智能合约自身存在安全风险的可能性，其中该安全风险包括但不限于被进行重排攻击的风险。

与之相应的，为了实现快速且高效的检测智能合约是否存在安全风险，本说明书实施例中提供了一种智能合约的安全检测方法及装置。如图 1 所示，该方法至少可以包括：步骤 101，确定智能合约对应的过程间控制流图；步骤 103，在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约；步骤 105，根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

其中进行安全检测的智能合约可以是待部署到区块链的智能合约，或者还可以是已经部署到区块链的智能合约。鉴于智能合约部署到区块链之后，具有不可修改或者说是难以修改的特点，因此优选对待部署到区块链的智能合约进行安全检测；如此，当确定该智能合约存在安全风险的情况下，有利于于工作人员对智能合约快速且高效的进行修改，而且能够避免将存在安全风险的智能合约部署到区块链而为区块链带来其它安全问题。

下面对如图 1 所示实施例中的各方法步骤进行详细描述。

首先，在步骤 101，确定智能合约对应的过程间控制流图。

可以通过对加载到内存中的智能合约进行反汇编，首先基于反汇编的结果对智能合约中的每个函数分别构建其对应的控制流图（control flow graph, CFG）。其中，CFG 是以基本块为节点的有向图，单个基本块中包括需要顺序执行的多条汇编指令；CFG 中连接两个节点的有向边表征两个节点间存在控制转移，而且 CFG 中具有唯一的入口节点和出口节点。接着基于反汇编的结果确定智能合约中的函数调用关系，并根据函数调用关系利用每个函数分别对应的 CFG 构建 ICFG。其中，ICFG 是由智能合约中的每个函数各自对应的 CFG、若干 Call edges 和若干 Return edges 组成的有向图；Call edges 由主调函数对应的 CFG 中的函数调用指令，指向被调用函数对应的 CFG 中的入口节点；Return edges 由被调用函数对应的 CFG 中的 Ret 指令，指向主调函数对应的 CFG 中的函数调用指令的下一条指令。换言之，智能合约对应的 ICFG 由多条汇编指令组成，其至少表征了对应相同或不同函数的汇编指令的排列/执行顺序。

由汇编指令组成的 CFG 中通常并不直接包含被赋值的世界状态参数，而是通过内存地址或者指向内存地址的地址指针表征世界状态参数，通过在内存地址上写入数据来完成对世界状态参数的赋值。如需确保后续过程中能够基于 ICFG，发现利用外部数据对各世界状态参数进行赋值的全部赋值操作，则需要确保单个世界状态参数在内存中具有固定且唯

一的内存地址，即需要将内存地址作为世界状态参数的标识。鉴于以上需要，在一些实施例中，对于加载到内存中的被检测的智能合约，其包括存储于内存中的代码段和数据段，数据段中包括但不限于智能合约涉及的全部世界状态参数；对于单个世界状态参数而言，代码段中通过数据段在内存中的基地址，以及该世界状态参数对应的地址偏移量，对该世界状态参数进行标识。与之相应的是，由于 ICFG 实质上是对智能合约的代码段进行反汇编得到，因此在 ICFG 中由基地址和偏移量进行标识的内存地址或者指向该内存地址的地址指针，即可作为相应世界状态参数的标识。

接着，在步骤 103，在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约。

通过对 ICFG 进行分析，可以发现外部数据的传播过程和世界状态参数被赋值的过程，进而基于外部数据的传播过程和世界状态参数被赋值的过程，从智能合约涉及的全部世界状态参数中，确定利用外部数据进行赋值操作的目标参数。在一个较为具体的示例中，请参考图 2，可以通过如下步骤 1031-步骤 1035，在 ICFG 中确定利用外部数据进行赋值操作的若干目标参数。

步骤 1031，在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程。

通过在 ICFG 中对外部数据对应的参数添加污点标记，然后沿着数据流向进行污点跟踪，即可依次确定出添加有污点标记的参数所对应的多个指令，依次确定的多个指令即可组成用于表征外部数据的传播过程的第一指令序列。示例性的，请参考图 3 中示例并简化的 ICFG，智能合约中的方法函数 Function_A 和 Int Add (x, y) 各自对应的 CFG 由不同的指令序列组成，其中未图示 CFG 中由指令组成的基本块，未图示表征控制转移的有向边；直线箭头的方向指示 CFG 中指令的排列/执行顺序，折线箭头表征 Call edge 或者 Return edge；此外将对应外部数据的参数 a 和参数 b 的实例化参数/参数值，示例性的表述为“0Ah（即实例化参数/参数值 10）”和“14h（即实例化参数/参数值 20）”，在实际业务场景中显然可以为其它实例化参数/参数值。那么，通过对该 ICFG 进行分析以确定出参数 a 和参数 b 是对应外部数据的参数后，即可对参数 a 和参数 b 进行标记，即对“mov dword ptr[a], 0Ah”和“mov dword ptr[b], 14h”中的 ptr[a]和 ptr[b]进行污点标记，然后沿着数据流向进行污点跟踪，确定出起点为“mov dword ptr[a], 0Ah”并且终点为“mov dword ptr[c], eax”的第一指令序列。其中需要特别说明的是在该第一指令序列中，组成 Int Add (x, y) 对应的 CFG 的指令序列位于“call _Add”和“add esp, 8”之间。

步骤 1033，在所述过程间控制流图中确定若干第二指令序列，所述第二指令序列用于表征世界状态参数被赋值的过程。

首先，可以在 ICFG 中确定智能合约涉及的全部世界状态参数。在一个较为具体的示例中，首先在 ICFG 中确定调用预定函数的若干函数调用指令。其中，该预定函数可以用

于在非易失性存储介质中更新区块链的世界状态参数，例如该预定函数可以通过其自身或调用其它方法函数，实现将赋值后的世界状态参数写入非易失性存储介质；或者，该预定函数可以是区块链节点中用于实现预定业务的方法函数，例如该预定函数实现的预定业务是，其被智能合约调用时可以使区块链节点获知智能合约已经完成对某个世界状态参数进行赋值，从而使区块链节点可以按照相应的业务逻辑将完成赋值的世界状态参数写入到非易失性存储介质中。接着，对已确定的每个函数调用指令，以该函数调用指令为起点在 ICFG 中进行向上搜索，确定该函数调用指令请求更新的参数，并将该参数确定为世界状态参数。示例性的，请继续参考图 3，可以首先在 ICFG 中确定调用预定函数“_Rt”的函数调用指令“call _Rt”，然后以“call _Rt”为起点在 ICFG 中进行向上搜索，确定“call _Rt”请求更新的参数是由“mov eax, dword ptr[c]”和“push eax”加入函数栈中的参数 c，进而将参数 c 确定为世界状态参数，其中参数 c 在图 3 中通过地址指针 ptr[c]进行标识。

接着，由于 ICFG 中通过内存地址或者地址指针标识世界状态参数，因此对于已确定的每个世界状态参数而言，可以通过用于标识该世界状态参数的内存地址或者地址指针，在 ICFG 中确定用于对该世界状态参数进行赋值的全部赋值指令。示例性的，请继续参考图 3，可以基于已确定的用于标识世界状态参数 c 的地址指针 ptr[c]，在 ICFG 中确定出用于对 ptr[c]进行赋值的赋值指令“mov dword ptr[c], eax”。

最后，对于已确定的每个世界状态参数，可以将用于对该世界状态参数进行赋值的全部赋值指令分别归入不同的第二指令序列。具体地，针对用于对单个世界状态参数进行赋值的每个赋值指令，可以将该赋值指令作为起点在 ICFG 中进行向上搜索，直到搜索到该赋值指令直接或间接的使用的参数值的来源，进而确定用于表征该世界状态参数被赋值的过程的其中一个第二指令序列。示例性的，请继续参考图 3，当确定用于对 ptr[c]进行赋值的“mov dword ptr[c], eax”时，则可以在 ICFG 中以“mov dword ptr[c], eax”为起点进行向上搜索，直到搜索到“mov dword ptr[c], eax”间接使用的参数 a 和参数 b。其中“mov eax, dword ptr[b]”和“push eax”用于将参数 b 的实例化参数 ptr[b]加入函数栈，“mov ecx, dword ptr[a]”和“push ecx”用于将参数 a 的实例化参数 ptr[a]加入函数栈，因此可以将搜索到的这四条指令作为“mov dword ptr[c], eax”间接使用的参数值的来源；或者，前述四条指令用于将实例化参数 ptr[a]、ptr[b]加入函数栈，但是并未表明 ptr[a]和 ptr[b]在 ICFG 中如何被创建，因此可以在 ICFG 中继续进行向上搜索，直到搜索到用于在函数栈中创建 ptr[a]和 ptr[b]的“mov dword ptr[a], 0Ah”和“mov dword ptr[b], 14h”，然后将“mov dword ptr[a], 0Ah”和“mov dword ptr[b], 14h”作为“mov dword ptr[c], eax”间接使用的参数值的来源。与之相应的是，针对用于对世界状态参数 ptr[c]进行赋值的赋值指令“mov dword ptr[c], eax”，可以从 ICFG 中确定起点为“mov eax, dword ptr[b]”或者“mov dword ptr[a], 0Ah”、终点为“mov dword ptr[c], eax”的第二指令序列，该第二指令序列能够完整的表征世界状态参数 ptr[c]被赋值的过程。

需要特别说明的是，图 3 示例的 ICFG 中可以确定出 1 个用于表征 ptr[c]被赋值的过程

的第二指令序列，但是在实际业务场景中，智能合约对应的 ICFG 中可能确定出多个用于表征 ptr[c] 被赋值的过程的第二指令序列。示例性的，假设智能合约中除了包括前述的方法函数 Function_A 和 Int Add (x, y) 以外，还包括方法函数 Function_B，其中 Function_B 实现的功能为将外部数据直接赋值给世界状态参数 c，并通过调用预定函数 “_Rt”，使得区块链节点实现对非易失性存储介质中的世界状态参数 c 进行更新。那么，该智能合约对应的 ICFG 中，可以在图 3 示例的 ICFG 的基础上，还包括 Function_B 对应的 CFG，Function_B 对应的 CFG 中同样包括用于对 ptr[c] 进行赋值的赋值指令。与之相应的是，由于 Function_A 对应的 CFG 和 Function_B 对应的 CFG 中均包括用于对 ptr[c] 进行赋值的赋值指令，因此可以从 ICFG 中确定出 2 个用于表征世界状态参数 c 被赋值的过程的第二指令序列。

步骤 1035，根据所述若干第一指令序列和所述若干第二指令序列之间重合的赋值指令，确定所述若干目标参数。

参照前述示例不难发现，第二指令序列中的最后一条指令是用于对世界状态参数进行赋值的赋值指令，第一指令序列中的第一条指令用于在函数栈中创建外部数据或者将外部数据加入函数栈。因此，当第二指令序列中的最后一条指令和第一指令序列中的最后一条指令重合/相同时，则说明第二指令序列中可能直接或间接的使用了外部数据对世界状态参数进行赋值，因而可以将重合的赋值指令指向的参数确定为使用外部数据进行赋值的目标参数，即将重合的赋值指令请求赋值的参数确定为使用外部数据进行赋值的目标参数。在一个较为具体的示例中，对于智能合约涉及的每个世界状态参数，确定出用于表征该世界状态参数被赋值的过程的全部第二指令序列后，可以对该世界状态参数对应的每个第二指令序列，检测已确定的全部第一指令序列中是否存在目标指令序列，该目标指令序列中的最后一条指令与该第二指令序列中的最后一条指令相同；如果是则将该世界状态参数确定为利用外部数据进行赋值操作的目标参数。与之相应的是，对用于表征该世界状态参数被赋值的过程的每个第二指令序列均执行前述的处理，即可统计出该世界状态参数被确定为目标参数的累计次数，该累计次数即为该世界状态参数利用外部数据进行赋值操作的操作频次。

下面回到图 1，在步骤 105，根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

在一种可能的实施方式中，当若干目标参数各自对应的操作频次中存在大于 1 的操作频次时，即可确定智能合约存在安全风险。

在一些实施例，还可以将第二指令序列表征的世界状态参数被赋值的过程，划分为第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程指示未利用外部数据进行赋值。对于单个世界状态参数而言，在确定出表征该世界状态参数被赋值的过程的若干第二指令序列时，可以确定该若干第二指令

序列各自对应的赋值类型，进而统计出该世界状态参数对应的全部赋值类型。与之相应的，步骤 105 中具体可以确定若干目标参数中是否存在第一参数，该第一参数对应的操作频次大于 1，该第一参数被赋值的过程同时包括第一类赋值过程和第二类赋值过程两种赋值类型，即该第一参数对应的赋值类型同时包括第一类赋值过程和第二类赋值过程；如果若干目标参数中存在第一参数，则确定智能合约存在安全风险。如此，通过综合考虑世界状态参数利用外部数据进行赋值操作的操作频次，以及世界状态参数被赋值的过程所属的赋值类型，可以更加准确的确定智能合约是否存在安全风险。

示例性的，请继续参考图 3。以“mov dword ptr[a], 0Ah”为起点且以“mov dword ptr[c], eax”为终点的一个第二指令序列，表征世界状态参数 c 被赋值的过程。由于该第二指令序列指示了利用参数 a 和参数 b 各自对应的外部数据进行逻辑运算，并利用进行逻辑运算后得到的运算结果对世界状态参数 c 进行赋值，因此可以确定该第二指令序列所属的赋值类型为第二类赋值过程，即确定世界状态参数 c 的赋值过程包括第二类赋值过程，或者说确定世界状态参数 c 对应的赋值类型包括第二类赋值过程。

继续假设智能合约中还包括前述示例的方法函数 Function_B，那么基于 Function_B 对应的 CFG 中用于对世界状态参数 c 进行赋值的赋值指令，可以确定出用于表征世界状态参数 c 被赋值的过程的另一个第二指令序列，该第二指令序列由于使用外部数据对世界状态参数 c 进行直接赋值，因此可以确定该第二指令序列所属的赋值类型为第一类赋值过程，即确定世界状态参数 c 的赋值过程包括第一类赋值过程，或者说确定世界状态参数 c 对应的赋值类型包括第一类赋值过程。

继续假设智能合约中还包括方法函数 Function_C，其中 Function_C 实现的功能为将预设数值赋值给世界状态参数 c，并通过调用预定函数“_Rt”实现对非易失性存储介质中的世界状态参数 c 进行更新。那么智能合约对应的 ICFG 中可以包括 Function_C 对应的 CFG，Function_C 对应的 CFG 中包括用于对 ptr[c] 进行赋值的赋值指令。与之相应的，基于 Function_C 对应的 CFG 中用于对世界状态参数 c 进行赋值的赋值指令，可以确定出用于表征世界状态参数 c 被赋值的过程的又一个第二指令序列，该第二指令序列使用预设常数对世界状态参数 c 进行直接赋值，未利用外部数据对世界状态参数 c 进行赋值，因此可以确定该第二指令序列所属的赋值类型为第三类赋值过程，即确定世界状态参数 c 的赋值过程包括第三类赋值过程，或者说确定世界状态参数 c 对应的赋值类型包括第三类赋值过程。

在一些实施例中，对于单个世界状态参数而言，当确定出表征该世界状态参数被赋值的过程的若干第二指令序列时，还可以确定若干第二指令序列各自对应的方法函数，例如将单个第二指令序列中用于对该世界状态参数进行赋值的赋值指令所属的方法函数，确定为该第二指令序列对应的函数。与之相应的，步骤 105 中具体可以确定若干目标参数中是否存在第二参数，该第二参数对应的操作频次大于 1，该第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程，该第二参数包括的第一类赋值过程和第二类赋值过程在过程间控制流图中对应不同的方法函数；如果若干目标参数中存在第二参数，则确定智能合

约存在安全风险。如此，通过综合考虑世界状态参数利用外部数据进行赋值操作的操作频次，世界状态参数被赋值的过程所属的赋值类型，不同赋值类型的指令序列各自对应的方法函数，可以更加准确的确定智能合约是否存在安全风险。

示例性的，请继续参考图 3。假设智能合约中包括前述的方法函数 Function_A、Int Add

5 (x, y) 和方法函数 Function_B。那么，基于 Function_A 对应的 CFG 中用于对世界状态参数 c 进行赋值的赋值指令而确定的第二指令序列，其所属的赋值类型为第二类赋值过程，其对应的函数为 Function_A，即世界状态参数 c 包括的第二类赋值过程所对应的方法函数是 Function_A；基于 Function_B 对应的 CFG 中用于对世界状态参数 c 进行赋值的赋值指令而确定的第二指令序列，其所属的赋值类型为第一类赋值过程，其对应的函数包括
10 Function_B，即世界状态参数 c 的第一类赋值过程所对应的函数为 Function_B。此种情况下，世界状态参数 c 作为目标参数，其利用外部数据进行赋值操作的操作频次是 2 次，其被赋值的过程包括第一类赋值过程和第二类赋值过程，其包括的第一类赋值过程所对应的方法函数 Function_A，不同于其包括的第二类赋值过程所对应的方法函数 Function_B，因此世界状态参数 c 将会被确定为第二状态参数，进而可以确定智能合约存在安全风险。

15 需要说明的是，前述图 3 中示例并简化的 ICFG 仅用于辅助描述本说明书实施例中提供的技术方案，说明书中未详细描述图 3 中部分常用指令所需要实现的功能，但是这并不影响本领域技术人员对图 3 所示例的 ICFG 进行正确理解。在实际业务场景中，实现相同功能的指令可以具有不同的表达形式，可以通过更多或更少的指令来实现图 3 中的一个或多个指令所需要实现的功能。

20 与前述方法实施例基于相同的构思，本说明书实施例中还提供了一种智能合约的安全检测装置。如图 4 所示，该装置包括：解析处理单元 401，配置为确定智能合约对应的过程间控制流图；赋值检测单元 403，配置为在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约；风险
25 确定单元 405，配置为根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

在一种可能的实施方式中，所述风险确定单元 405，配置为当存在大于 1 的操作频次时，确定所述智能合约存在安全风险。

在一种可能的实施方式中，所述智能合约包括存储于内存中的代码段和数据段，所述
30 数据段中包括所述若干目标参数，所述代码段中通过所述数据段在所述内存中的基地址和所述目标参数对应的地址偏移量对所述目标参数进行标识。

在一种可能的实施方式中，所述赋值检测单元 403 包括：第一确定子单元，配置为在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程；第二确定子单元，配置为在所述过程间控制流图中确定若干第二指令序列，所述
35 第二指令序列用于表征世界状态参数被赋值的过程；赋值检测子单元，配置为根据所述若

干第一指令序列和所述若干第二指令序列之间重合的赋值指令，确定所述若干目标参数。

在一种可能的实施方式中，所述第一确定子单元，配置为在所述过程间控制流图中，对外部数据对应的参数添加污点标记，沿着数据流向进行污点跟踪，将添加有污点标记的参数对应的指令归入所述第一指令序列。

5 在一种可能的实施方式中，所述第二确定子单元，配置为在所述过程间控制流图中确定世界状态参数；在所述过程间控制流图中，确定用于对世界状态参数进行赋值的赋值指令，并将该赋值指令归入所述第二指令序列。

在一种可能的实施方式中，所述第二确定子单元，具体配置为在所述过程间控制流图中，确定调用预定函数的若干函数调用指令；将所述函数调用指令请求更新的参数确定为
10 世界状态参数。

在一种可能的实施方式中，所述赋值检测子单元，具体配置为将所述重合的赋值指令所指向的世界状态参数作为所述目标参数。

在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果
15 进行赋值，第三类赋值过程用于指示未利用外部数据进行赋值。所述风险确定单元 405，具体配置为确定所述若干目标参数中是否存在第一参数，其中所述第一参数对应的操作频次大于 1，所述第一参数被赋值的过程包括第一类赋值过程和第二类赋值过程；如果是，确定所述智能合约存在安全风险。

20 在一种可能的实施方式中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程指示未利用外部数据进行赋值。所述风险确定单元 405，具体配置为确定所述若干目标参数中是否存在第二参数，其中所述第二参数对应的操作频次大
25 于 1，所述第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程，所述第二参数的第一类赋值过程和第二类赋值过程，在所述过程间控制流图中对应不同的方法函数；如果是，确定所述智能合约存在安全风险。

在一种可能的实施方式中，所述智能合约是待部署到区块链中的智能合约；和/或，所述安全风险具体包括被进行重排攻击的风险。

30 本领域技术人员应该可以意识到，在上述一个或多个示例中，本说明书所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能所对应的计算机程序存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令/代码进行传输，以便这些功能所对应的计算机程序被计算机执行时，通过计算机实现本说明书任意一个实施例所述的方法。

35 本说明书实施例中还提供了一种计算机可读存储介质，其上存储有计算机程序/指令，

当所述计算机程序/指令在计算设备中执行时，计算设备执行本说明书任意一个实施例中提供的智能合约的安全检测方法。

- 5 本说明书实施例中还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有计算机程序/指令，所述处理器执行所述计算机程序/指令时，实现本说明书任意一个实施例中提供的智能合约的安全检测方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例中相同、相似的部分互相参见即可，每个实施例中重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

- 10 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。

- 15 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权 利 要 求 书

1. 一种智能合约的安全检测方法，包括：

确定智能合约对应的过程间控制流图；

在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约；

根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

2. 根据权利要求1所述的方法，其中，根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险，具体包括：当存在大于1的操作频次时，确定所述智能合约存在安全风险。

3. 根据权利要求1所述的方法，其中，所述智能合约包括存储于内存中的代码段和数据段，所述数据段中包括所述若干目标参数，所述代码段中通过所述数据段在所述内存中的基地址和所述目标参数对应的地址偏移量对所述目标参数进行标识。

4. 根据权利要求1所述的方法，其中，所述在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，包括：

在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程；

在所述过程间控制流图中确定若干第二指令序列，所述第二指令序列用于表征世界状态参数被赋值的过程；

根据所述若干第一指令序列和所述若干第二指令序列之间重合的赋值指令，确定所述若干目标参数。

5. 根据权利要求4所述的方法，其中，在所述过程间控制流图中确定若干第一指令序列，包括：在所述过程间控制流图中，对外部数据对应的参数添加污点标记，沿着数据流向进行污点跟踪，将添加有污点标记的参数对应的指令归入所述第一指令序列。

6. 根据权利要求4所述的方法，其中，在所述过程间控制流图中确定若干第二指令序列，包括：在所述过程间控制流图中确定世界状态参数；在所述过程间控制流图中，确定用于对世界状态参数进行赋值的赋值指令，并将该赋值指令归入所述第二指令序列。

7. 根据权利要求6所述的方法，其中，在所述过程间控制流图中确定世界状态参数，包括：在所述过程间控制流图中，确定调用预定函数的若干函数调用指令；将所述函数调用指令请求更新的参数确定为世界状态参数。

8. 根据权利要求4所述的方法，其中，根据所述若干第一指令序列和若干第二指令序列之间重合的赋值指令，确定所述若干目标参数，包括：将所述重合的赋值指令所指向的世界状态参数作为所述目标参数。

9. 根据权利要求4所述的方法，其中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类

赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程用于指示未利用外部数据进行赋值；

所述根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险，具体包括：

确定所述若干目标参数中是否存在第一参数，其中所述第一参数对应的操作频次大于1，所述第一参数被赋值的过程包括第一类赋值过程和第二类赋值过程；

如果是，确定所述智能合约存在安全风险。

10. 根据权利要求4所述的方法，其中，单个所述第二指令序列表征的世界状态参数被赋值的过程，属于第一类赋值过程、第二类赋值过程或者第三类赋值过程；其中第一类赋值过程指示利用外部数据进行直接赋值，第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值，第三类赋值过程指示未利用外部数据进行赋值；

所述根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险，具体包括：

确定所述若干目标参数中是否存在第二参数，其中所述第二参数对应的操作频次大于1，所述第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程，所述第二参数的第一类赋值过程和第二类赋值过程，在所述过程间控制流图中对应不同的方法函数；

如果是，确定所述智能合约存在安全风险。

11. 根据权利要求1-10中任一项所述的方法，其中，所述智能合约是待部署到区块链中的智能合约；和/或，所述安全风险具体包括被进行重排攻击的风险。

12. 一种智能合约的安全检测装置，包括：

解析处理单元，配置为确定智能合约对应的过程间控制流图；

赋值检测单元，配置为在所述过程间控制流图中，确定利用外部数据进行赋值操作的若干目标参数，以及所述若干目标参数各自进行所述赋值操作的操作频次，所述若干目标参数属于区块链的世界状态参数，外部数据自外部输入所述智能合约；

风险确定单元，配置为根据所述若干目标参数各自对应的操作频次，确定所述智能合约是否存在安全风险。

13. 根据权利要求12所述的装置，其中，所述风险确定单元，配置为当存在大于1的操作频次时，确定所述智能合约存在安全风险。

14. 根据权利要求12所述的装置，其中，所述智能合约包括存储于内存中的代码段和数据段，所述数据段中包括所述若干目标参数，所述代码段中通过所述数据段在所述内存中的基地址和所述目标参数对应的地址偏移量对所述目标参数进行标识。

15. 根据权利要求12所述的装置，其中，所述赋值检测单元包括：

第一确定子单元，配置为在所述过程间控制流图中确定若干第一指令序列，所述第一指令序列用于表征外部数据的传播过程；

第二确定子单元，配置为在所述过程间控制流图中确定若干第二指令序列，所述第二

指令序列用于表征世界状态参数被赋值的过程;

赋值检测子单元,配置为根据所述若干第一指令序列和所述若干第二指令序列之间重合的赋值指令,确定所述若干目标参数。

16. 根据权利要求 15 所述的装置,其中,所述第一确定子单元,配置为在所述过程间控制流图中,对外部数据对应的参数添加污点标记,沿着数据流向进行污点跟踪,将添加有污点标记的参数对应的指令归入所述第一指令序列。

17. 根据权利要求 15 所述的装置,其中,所述第二确定子单元,配置为在所述过程间控制流图中确定世界状态参数;在所述过程间控制流图中,确定用于对世界状态参数进行赋值的赋值指令,并将该赋值指令归入所述第二指令序列。

18. 根据权利要求 17 所述的装置,其中,所述第二确定子单元,具体配置为在所述过程间控制流图中,确定调用预定函数的若干函数调用指令;将所述函数调用指令请求更新的参数确定为世界状态参数。

19. 根据权利要求 15 所述的装置,其中,所述赋值检测子单元,具体配置为将所述重合的赋值指令所指向的世界状态参数作为所述目标参数。

20. 根据权利要求 15 所述的装置,其中,单个所述第二指令序列表征的世界状态参数被赋值的过程,属于第一类赋值过程、第二类赋值过程或者第三类赋值过程;其中第一类赋值过程指示利用外部数据进行直接赋值,第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值,第三类赋值过程用于指示未利用外部数据进行赋值;

所述风险确定单元,具体配置为确定所述若干目标参数中是否存在第一参数,其中所述第一参数对应的操作频次大于 1,所述第一参数被赋值的过程包括第一类赋值过程和第二类赋值过程;如果是,确定所述智能合约存在安全风险。

21. 根据权利要求 15 所述的装置,其中,单个所述第二指令序列表征的世界状态参数被赋值的过程,属于第一类赋值过程、第二类赋值过程或者第三类赋值过程;其中第一类赋值过程指示利用外部数据进行直接赋值,第二类赋值过程指示利用外部数据进行逻辑运算后的运算结果进行赋值,第三类赋值过程指示未利用外部数据进行赋值;

所述风险确定单元,具体配置为确定所述若干目标参数中是否存在第二参数,其中所述第二参数对应的操作频次大于 1,所述第二参数被赋值的过程包括第一类赋值过程和第二类赋值过程,所述第二参数的第一类赋值过程和第二类赋值过程,在所述过程间控制流图中对应不同的方法函数;如果是,确定所述智能合约存在安全风险。

22. 根据权利要求 12-21 中任一项所述的装置,其中,所述智能合约是待部署到区块链中的智能合约;和/或,所述安全风险具体包括被进行重排攻击的风险。

23. 一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算设备中执行时,计算设备执行权利要求 1-11 中任一项所述的方法。

24. 一种计算设备,包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器执行所述计算机程序时,实现权利要求 1-11 中任一项所述的方法。

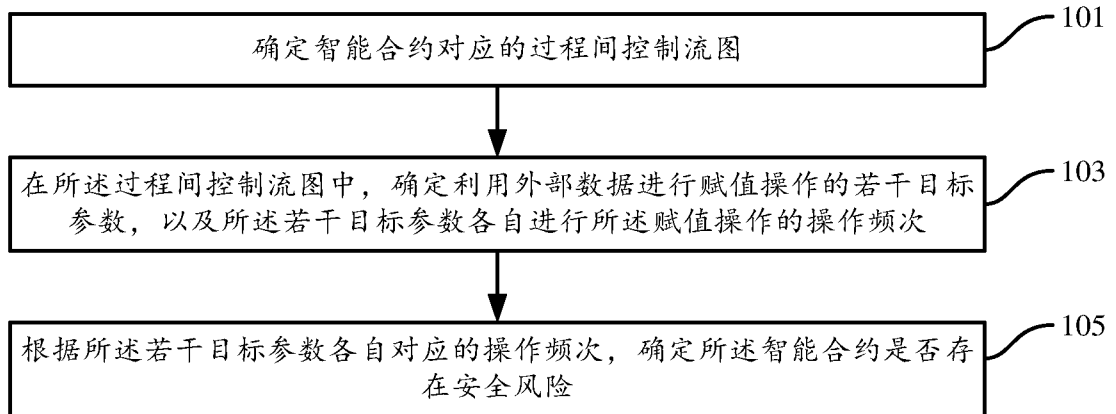


图 1

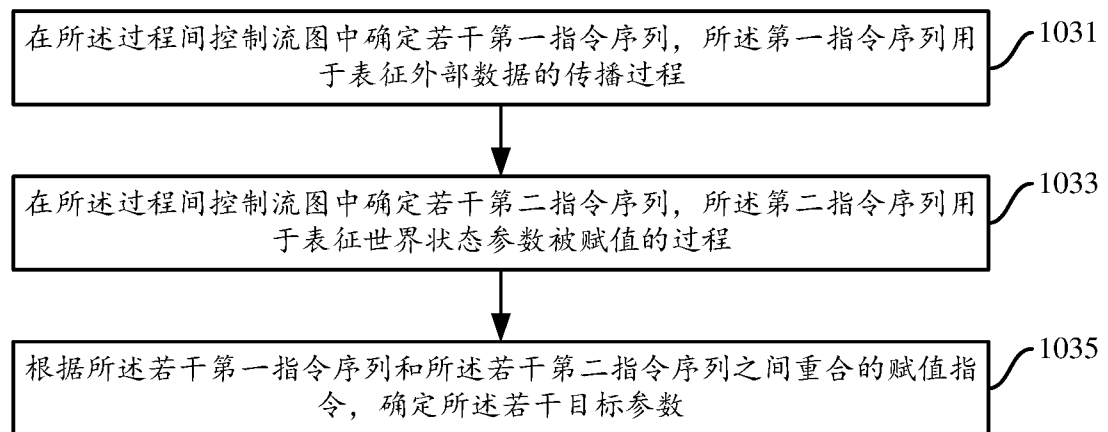


图 2

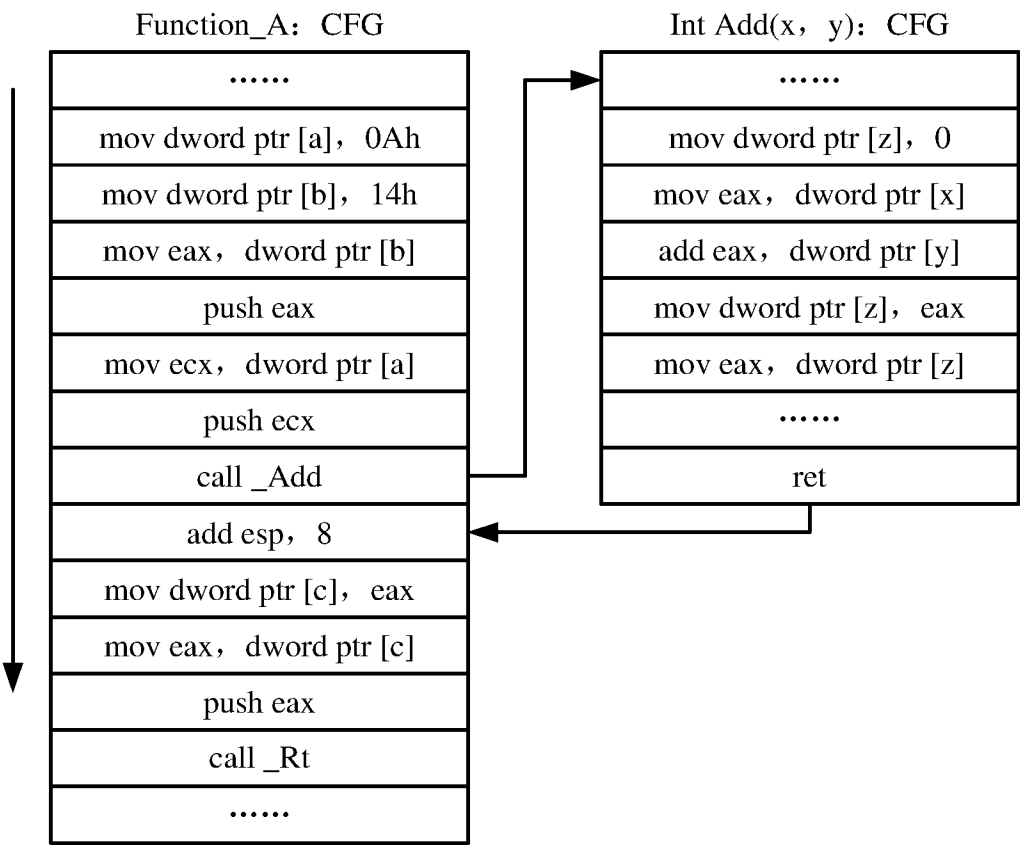


图 3

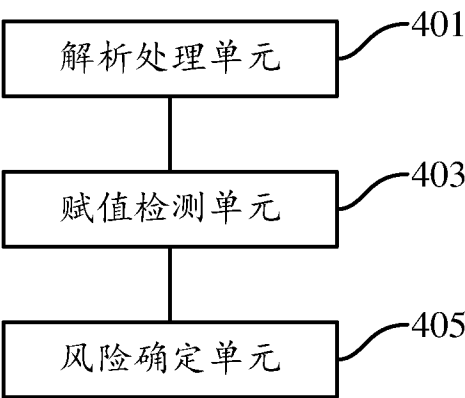


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/103305

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)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)

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: 智能合约, 检测, 过程, 流程图, 参数, 赋值, 频次, 区块链, 风险, smart S contract, detect, process, flow W diagram; , parameter, assignment, frequency, blockchain, risk

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113435893 A (ALIPAY (HANGZHOU) TECHNOLOGY CO., LTD. et al.) 24 September 2021 (2021-09-24) claims 1-24	1-24
A	CN 112711760 A (SOUTH CHINA NORMAL UNIVERSITY) 27 April 2021 (2021-04-27) description, paragraphs [0042]-[0059]	1-24
A	CN 112749389 A (SOUTH CHINA NORMAL UNIVERSITY) 04 May 2021 (2021-05-04) entire document	1-24
A	CN 112115472 A (BEIJING ZHIRONG YUNHE TECHNOLOGY CO., LTD.) 22 December 2020 (2020-12-22) entire document	1-24

☐ 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

30 August 2022

Date of mailing of the international search report

27 September 2022

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

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/103305

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	113435893	A	24 September 2021	None	
CN	112711760	A	27 April 2021	None	
CN	112749389	A	04 May 2021	None	
CN	112115472	A	22 December 2020	None	

国际检索报告

国际申请号

PCT/CN2022/103305

A. 主题的分类

G06Q 20/40(2012.01)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)

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))

CNPAT, WPI, EPDOC, CNKI, IEEE: 智能合约, 检测, 过程, 流程图, 参数, 赋值, 频次, 区块链, 风险, smart S contract, detect, process, flow W diagram; parameter, assignment, frequency, blockchain, risk

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 113435893 A (支付宝杭州信息技术有限公司 等) 2021年9月24日 (2021 - 09 - 24) 权利要求1-24	1-24
A	CN 112711760 A (华南师范大学) 2021年4月27日 (2021 - 04 - 27) 说明书第[0042]-[0059]段	1-24
A	CN 112749389 A (华南师范大学) 2021年5月4日 (2021 - 05 - 04) 全文	1-24
A	CN 112115472 A (北京智融云河科技有限公司) 2020年12月22日 (2020 - 12 - 22) 全文	1-24

☐ 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

2022年8月30日

国际检索报告邮寄日期

2022年9月27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

授权官员

李娜

电话号码 86-(10)-53961346

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/103305

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	113435893	A	2021年9月24日	无	
CN	112711760	A	2021年4月27日	无	
CN	112749389	A	2021年5月4日	无	
CN	112115472	A	2020年12月22日	无	