

(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 12 月 24 日 (24.12.2020)



(10) 国际公布号
WO 2020/253476 A1

- (51) 国际专利分类号:
G06F 21/55 (2013.01) **G06Q 40/04** (2012.01)
G06F 21/57 (2013.01)
- (21) 国际申请号: PCT/CN2020/092174
- (22) 国际申请日: 2020 年 5 月 25 日 (25.05.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910541002.4 2019年6月21日 (21.06.2019) CN
- (71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。清华大学 (TSINGHUA UNIVERSITY) [CN/CN]; 中国北京市海淀区清华大学, Beijing 100084 (CN)。
- (72) 发明人: 马福辰 (MA, Fuchen); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室,

Guangdong 518027 (CN)。姜宇 (JIANG, Yu); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。傅滢 (FU, Ying); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。任萌 (REN, Meng); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。王明哲 (WANG, Mingzhe); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。范瑞彬 (FAN, Ruibin); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。张开翔 (ZHANG, Kaixiang); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。李辉忠 (LI, Huizhong); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。石翔 (SHI, Xiang); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。李成博 (LI,

(54) Title: METHOD AND DEVICE FOR MONITORING SMART CONTRACT IN BLOCKCHAIN

(54) 发明名称: 一种区块链中智能合约的监控方法及装置

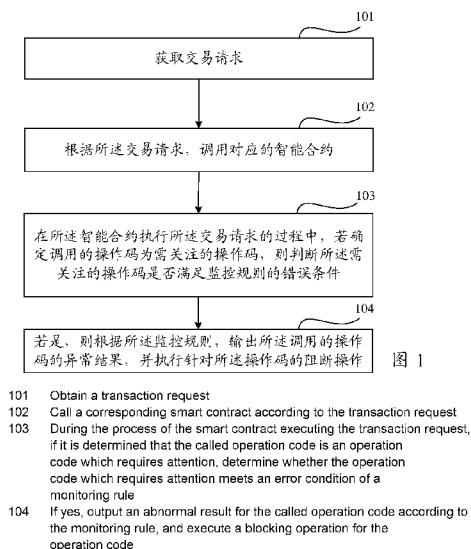


图 1

(57) Abstract: Provided are a method and device for monitoring a smart contract in a blockchain, relating to the field of financial technology (fintech), and used for improving the security of smart contracts. The method comprises: obtaining a transaction request (101); calling a corresponding smart contract according to the transaction request (102); during the process of the smart contract executing the transaction request, if it is determined that the called operation code is an operation code which requires attention, determining whether the operation code which requires attention meets an error condition of a monitoring rule (103); and if yes, outputting an abnormal result for the called operation code according to the monitoring rule, and executing a blocking operation for the operation code (104).

(57) 摘要: 一种区块链中智能合约的监控方法及装置, 涉及科技金融 (Fintech) 领域, 用以提高智能合约的安全性。所述方法包括: 获取交易请求 (101); 根据所述交易请求, 调用对应的智能合约 (102); 在所述智能合约执行所述交易请求的过程中, 若确定调用的操作码为需关注的操作码, 则判断所述需关注的操作码是否满足监控规则的错误条件 (103); 若是, 则根据所述监控规则, 输出所述调用的操作码的异常结果, 并执行针对所述操作码的阻断操作 (104)。

Chengbo); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (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, 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))。

一种区块链中智能合约的监控方法及装置

相关申请的交叉引用

本申请要求在2019年06月21日提交中国专利局、申请号为201910541002.4、
申请名称为“一种区块链中智能合约的监控方法及装置”的中国专利申请的
5 优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及科技金融（Fintech）领域，尤其涉及一种区块链中智能合约
的监控方法及装置。

背景技术

随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业
正在逐步向金融科技（fintech）转变，区块链（block chain）技术也不例外，
但由于金融行业的安全性、实时性要求，也对技术提出的更高的要求。

15 智能合约（smart contract）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，其执行过程以交易的形式在区块链上共识、确认。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。

目前，区块链系统的安全性受到越来越多人的关注，在智能合约的漏洞
检测上，目前还没有比较好的方案，以保证区块链系统的安全性。

发明内容

本申请提供一种区块链中智能合约的监控方法及装置，用以提高智能合
约的安全性。

25 本发明实施例提供的一种区块链中智能合约的监控方法，包括：获取交
易请求；根据所述交易请求，调用对应的智能合约；在所述智能合约执行所
述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述

需关注的操作码是否满足监控规则的错误条件；若是，则根据所述监控规则，输出所述调用的操作码的异常结果；所述异常结果包括针对所述操作码的阻断操作。

本发明实施例中，通过获取交易请求；根据所述交易请求，调用对应的智能合约；在所述智能合约执行所述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件；若是，则根据所述监控规则，输出所述调用的操作码的异常结果；所述异常结果包括针对所述操作码的阻断操作。可以实时检查运行状态，及时终止危险交易，有效提高智能合约的安全性。

一种可能的实现方式，所述需关注的操作码为时间戳操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：若确定所述交易请求的输入参数中的交易值大于预设常数值，则确定所述时间戳操作码为满足时间戳异常的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：若在所述智能合约执行所述交易请求的过程中，所述调用操作码为非首次的调用操作码，所述调用操作码的调用节点为所述交易的首次调用的操作码的执行节点，且所述调用操作码的输入参数中的交易值大于预设常数值，则确定所述调用操作码满足函数可重入的错误条件。

一种可能的实现方式，所述需关注的操作码为委托调用操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境；若是，则确定所述委托调用操作码为满足危险调用的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：输入的交易值大于第一预设阈值，交易上限大于第

二预设阈值，且所述调用操作码返回的结果为费用 gas 不足；则确定所述调用操作码满足费用不足的错误条件。

一种可能的实现方式，所述在所述智能合约执行所述交易请求之前，还包括：根据所述交易请求，建立存储所述至少一个操作码的监控信息的数据结构；将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

一种可能的实现方式，所述需关注的操作码为计算操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：若确定所述计算操作码的输出结果满足计算溢出的错误条件，则确定所述计算调用操作码为满足计算溢出的错误条件。

一种可能的实现方式，所述方法还包括：若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述操作码的操作。

本发明实施例还提供一种区块链中智能合约的监控装置，包括：

收发单元，用于获取交易请求；

处理单元，用于根据所述交易请求，调用对应的智能合约；在所述智能合约执行所述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件；若是，则根据所述监控规则，输出所述调用的操作码的异常结果；所述异常结果包括针对所述操作码的阻断操作。

一种可能的实现方式，所述需关注的操作码为时间戳操作码；所述处理单元，具体用于：若确定所述交易请求的输入参数中的交易值大于预设常数值，则确定所述时间戳操作码为满足时间戳异常的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述处理单元，具体用于：若在所述智能合约执行所述交易请求的过程中，所述调用操作码为非首次的调用操作码，且所述调用操作码的输入参数中的交易值大于预设常数值，则确定所述调用操作码满足函数可重入的错误条件。

一种可能的实现方式，所述需关注的操作码为委托调用操作码；所述处

理单元，具体用于：判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境；若是，则确定所述委托调用操作码为满足危险调用的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述处理单元，具体用于：输入的交易值大于第一预设阈值，交易上限大于第二预设阈值，且所述调用操作码返回的结果为费用 gas 不足，则确定所述调用操作码满足费用不足的错误条件。

一种可能的实现方式，所述需关注的操作码为计算操作码；所述处理单元，具体用于：若确定所述计算操作码的输出结果满足计算溢出的错误条件，则确定所述计算调用操作码为满足计算溢出的错误条件。

一种可能的实现方式，所述处理单元，还用于：根据所述交易请求，建立存储所述至少一个操作码的监控信息的数据结构；将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

一种可能的实现方式，所述处理单元，还用于：若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述调用的操作码的操作。

本发明实施例还提供一种电子设备，包括：

至少一个处理器；以及，与所述至少一个处理器通信连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行如上所述的方法。

本发明实施例还提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行如上所述的方法。

附图说明

图 1 为本发明实施例提供的一种区块链中智能合约的监控方法的流程示

意图；

图 2 为本发明实施例提供的一种智能合约的虚拟机架构示意图；

图 3 为本发明实施例提供的一种区块链中智能合约的监控方法的执行结果示意图；

5 图 4 为本发明实施例提供的一种区块链中智能合约的监控装置的结构示意图；

图 5 为本发明实施例提供的电子设备的结构示意图。

具体实施方式

10 为了便于理解，下面对本发明实施例中可能涉及的名词进行定义和解释。

区块链：是由一系列区块组成的一条链，每个块上除了记录本块的数据还会记录上一块的 Hash（哈希）值，通过这种方式组成一条链。区块链的核心理念有两个，一个是密码学技术，另一个是去中心化思想，基于这两个理念做到区块链上的历史信息无法被篡改。一个区块由块头和块体组成，其中
15 块头定义包括该区块高度 h，上一个区块的 Hash 值 prevHash 等重要字段，而块体主要存储交易数据。

智能合约：现有技术的智能合约中，以以太坊为例，在触发智能合约时，智能合约的执行可以包括：智能合约方，为执行智能合约的相关参与者，通过智能合约方的外部账户发送消息，触发智能合约；智能合约资源集合，为
20 智能合约执行涉及的参与者资源，比如各智能合约方账户、拥有的数字财产等；智能合约中的事务主要包含需要发送的数据；而智能合约中的事件则是对这些数据的描述信息。事务及事件信息被智能合约的执行节点接收后，智能合约资源集合中的资源状态会被更新，进而触发智能合约进行状态机判断。状态机，包括当前资源状态判断、下一步智能合约事务执行选择等；智能合
25 约系统若确定事件中包含的触发条件满足时，从智能合约的自动状态机自动发出预设的数据资源，以及包括触发条件的事件；智能合约事务集合，为智能合约的下一步动作或行为集合，控制着智能合约的资产并对接收到的信息

进行回应。

具体的，基于区块链的智能合约的执行可以包括：

步骤一、定期检查区块中的智能合约，逐条遍历每个智能合约内的状态机、事务以及触发条件；将条件满足的事务推送到待验证的队列中，等待共识；未满足触发条件的事务将继续存放在区块链上。

步骤二、进入最新轮验证的事务，会扩散到每一个验证节点，与普通区块链交易或事务一样，验证节点首先进行签名验证，确保事务的有效性；验证通过的事务会进入待共识集合，等大多数验证节点达成共识后，事务会成功执行并通知用户。各节点执行智能合约是相互独立的，当各节点执行智能合约完毕时，将彼此验证结果是否一致，验证通过后，将结果返回至用户。

步骤三、事务执行成功后，智能合约的状态机会判断所属智能合约的状态，当智能合约包括的所有事务都顺序执行完后，状态机会将智能合约的状态标记为完成，并从最新的区块中移除该智能合约；反之将标记为进行中，继续保存在最新的区块中等待下一轮处理，直到处理完毕；整个事务和状态的处理都由区块链底层内置的智能合约系统自动完成，全程透明、不可篡改。

智能合约中，存储了各智能合约方的账户信息，访问接口，以及访问各接口的方法。智能合约发布时，根据各方约定将访问接口分配给指定的合作方授权使用，各智能合约方通过访问接口可实现对智能合约内数据的存取。各智能合约方执行智能合约时需要通过数据访问接口轮询智能合约，并根据轮询结果来判断所需完成的任务，任务的执行结果通过智能合约的接口保存在智能合约当中。

共识：一种区块链各节点对某个交易的正确性达成一致的算法。

Solidity：一种智能合约高级语言，运行在以太坊虚拟机（ethereum virtual machine，EVM）之上。

以太坊是一个基于区块链技术的平台，在以太坊中，开发者可以开发自己的去中心化的应用。随着人们对区块链技术不断深入的探索 and 认识，以太坊平台已经成为世界第二大区块链公链网络，规模仅次于比特币平台。在以太坊

以太坊上开发的程序叫做智能合约，开发者利用一种图灵完备的语言，比如 Solidity 来编写智能合约，完成自己想要实现的功能。近些年来，在以太坊平台日益发展的同时，针对智能合约和平台本身的攻击也越来越多，造成的财产损失十分巨大。比如 2018 年 2 月，一个新的公链代币平台美链上线，在 4 月某攻击者利用一个 ERC-20 智能合约中的溢出漏洞攻击了美链平台，成功将美链中巨量的代币转入其他的两个账户地址，最终导致美链平台在一夜之间损失 64 亿人民币，相当于美链全部的市值。近些年像这样的例子层出不穷，区块链系统的安全性受到越来越多人的关注，以太坊平台作为第一个区块链开发生态环境，其安全性受到社会各界人士的关注。

为了解决这些安全性的问题，目前针对智能合约的安全保障工具使用的方法主要分为两种：模糊测试技术和符号执行技术。模糊测试是一种相对成熟的安全测试方法，它介于完全的手工测试和完全的自动化测试之间。针对智能合约的模糊测试工具比如 Echidna 和 ContractFuzzer 可以通过模拟交易执行以发现智能合约在设计上存在的漏洞。符号执行技术使用符号值来表示程序的输入，并将程序的运算过程逐指令，逐语句地转换为数学表达式，在控制流图的基础上生成符号执行树，并为每一条路径建立一系列以输入为变量的符号表达式。目前有一些面向智能合约的符号执行工具，它们可以触发关键路径并检测安全漏洞。但是，上述工具往往会遗漏某些漏洞。例如，利用 ContractFuzzer 运行一份已知存在时间戳错误的智能合约，经过两个小时的测试，ContractFuzzer 依然没有检测到该安全漏洞的存在。这说明只在智能合约的层次上关注安全问题是不全面的。

为了解决上述现有技术中的问题，本发明实施例提供了一种区块链中智能合约的监控方法，如图 1 所示，本发明实施例提供的区块链中智能合约的监控方法包括以下步骤：

步骤 101：获取交易请求；

其中，一笔交易可以调用多个操作码；一笔交易也可以调用多个智能合约，在此不做限定。

步骤 102: 根据所述交易请求, 调用对应的智能合约;

步骤 103: 在所述智能合约执行所述交易请求的过程中, 若确定调用的操作码为需关注的操作码, 则判断所述需关注的操作码是否满足监控规则的错误条件;

5 步骤 104: 若是, 则根据所述监控规则, 输出所述调用的操作码的异常结果, 并执行针对所述操作码的阻断操作。

本发明实施例, 针对现有技术的不足, 通过实时监测智能合约的操作码, 为以太坊虚拟机执行智能合约提供实时保障防护, 及时发现危险交易, 及时阻断问题交易的执行, 并提示用户该交易存在潜在危害, 有效的提高了智能
10 合约的安全性。

本发明实施例可以通过在 EVM 层面解决上述问题。本发明实施例所提供的区块链中智能合约的监控方法可以由以下功能模块组成, 如图 2 所示, 包括: 监控规则模块、操作码监控模块、虚拟机执行模块。其中, 监控规则模块中可以存储有需关注的操作码对应的错误条件; 例如, 根据监控规则确定
15 需关注的操作码和危险交易的阻断条件。具体的, 可以包括: 基于每种危险交易的类型确定监控规则, 筛选出与该类型相关的需关注的操作码, 定义其需要满足的错误条件和阻断交易需进行的操作。

针对不同的危险操作, 监控规则模块提供相关的错误条件去判定调用的操作符是否满足错误条件。如果条件满足, 监控规则模块或虚拟机执行模块
20 可以调用阻断机制, 对智能合约的执行进行阻断, 并回滚区块链系统的状态。

针对以上安全漏洞类型, 本发明实施例提供相应的策略进行实时监控。本发明实施例根据在交易的执行过程中, 导致交易失败的主要错误类型, 确定监控规则。针对不同的漏洞类型, 本发明实施例提供如下监控规则:

一种可能的实现方式, 所述需关注的操作码为计算操作码; 所述若确定
25 调用的操作码为需关注的操作码, 则判断所述需关注的操作码是否满足监控规则的错误条件, 包括:

若确定所述计算操作码的输出结果满足计算溢出的错误条件, 则确定所

述计算调用操作码为满足计算溢出的错误条件。

在执行计算操作时，出现溢出操作导致财产损失，为溢出错误。例如，ADD、SUB、MUL、ADDMOD、MULMOD 和 EXP 等。如果在执行上述操作码时，满足以下条错误条件中的任意一条，就证明发生了溢出错误：两个
5 正数执行加法运算，运算结果为负数；

两个负数执行加法运算，运算结果为正数；一个正数减去一个负数，运算结果为负数；

一个负数减去一个正数，运算结果为正数；两个正数执行乘法运算，运算结果为负数；

10 两个负数执行乘法运算，运算结果为负数；一个正数执行指数运算，运算结果为负数。

一种可能的实现方式，所述需关注的操作码为时间戳操作码；若确定所述交易请求的输入参数中的交易值大于预设常数值，则确定所述时间戳操作码为满足时间戳异常的错误条件。此处的预设常数值可以为 0，当然，还可以
15 根据实际需要进行设定，在此不做限定。

时间戳错误：在采用当前时间生成某种随机数的应用中，因为矿工控制时间戳而导致随机数的数值重复或泄露。例如，与时间戳错误相关的需关注的操作码为时间戳 TIMESTAMP，如果在一次交易执行的开端，调用 CALL 函数时传入的参数值大于零，或者 CALL 函数尝试向其他智能合约发送资源
20 时，出现了时间戳 TIMESTAMP 操作码，就可能发生了时间戳错误。

一种可能的实现方式，若在所述智能合约执行所述交易请求的过程中，所述调用操作码为非首次的调用操作码，所述调用操作码的调用节点为所述交易的首次调用的操作码的执行节点，且所述调用操作码的输入参数中的交易值大于预设常数值，则确定所述调用操作码满足函数可重入的错误条件。
25 此处的预设常数值可以为 0，当然，还可以根据实际需要进行设定，在此不做限定。

具体的，在调用其他函数的操作完成之前，被调用智能合约可能会被多

次执行，造成同一操作的反复执行，可能导致的费用损失。

例如，函数可重入错误关注的操作码为 CALL。当一个所述交易的首次调用的操作码的执行节点（即交易对应的调用链的起源调用者），在调用链中又调用了自己本身，同时这次调用过程中传递的交易值不为预设常数值，并且这次调用过程设置了足够多的费用上限，那么我们认为函数可重入错误可能出现。此处的预设常数值可以为 0，当然，还可以根据实际需要进行设定，在此不做限定。

一种可能的实现方式，所述需关注的操作码为非首次的调用操作码；若确定首次出现的调用操作码的输出未存在异常错误，且执行过程中的调用操作码的输出未异常错误，则确定所述调用操作码满足异常处理的错误条件。

具体的，当一个智能合约以不同的方式调用另一个智能合约时，Solidity 没有一个一致的方法来处理异常，导致调用智能合约无法获取被调用智能合约的异常信息。异常处理错误关注的操作码也只有 CALL。当一个调用链里面的首次调用的调用操作码的输出结果没有输出为异常，而调用链中的任意一次调用的调用操作码的输出结果为异常，则认为存在异常处理错误，可能的原因是一些异常结果并没有传递到根调用的调用操作码上，导致执行过程中出现错误。

一种可能的实现方式，若确定所述调用的操作码为委托调用操作码，则判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境；若是，则确定所述委托调用操作码为满足危险调用的错误条件。

具体的，调用 delegateCall 操作符时，若调用过程是获取调用的智能合约在本地执行，则被调用的智能合约中的函数的部分参数将会传递至调用方，使得智能合约中的 public 函数暴露，攻击者可以通过该操作，使得智能合约的拥有者向攻击者的账户或其他危险账户中传递资源。例如，危险调用错误关注的操作码是 DelegateCall。当一次 DelegateCall 调用的函数可以通过输入的参数值（比如 msg.data）完全掌控原始的智能合约，那么一次危险调用错误就会出现。

一种可能的实现方式，若所述调用的操作码为调用操作码，且输入的交易值大于第一预设阈值，交易上限大于第二预设阈值，且所述调用操作码返回的结果为费用 gas 不足；则确定所述调用操作码满足费用不足的错误条件。

具体的，当发送者调用 send 函数给接收者传递资源时，会调用接收智能合约的回调函数，以太坊中规定这个过程最多可消耗预设资源额度如 2300，如果接收智能合约的回调函数需要的调用的费用大于这个预设资源额度，就会发生费用不足错误，造成发送方额外的资源损失。

例如，费用不足错误关注的操作码为调用操作码 Call。当一次调用操作码 Call 调用的时候传递的值大于或等于预设常数，例如不为 0，并且设置的费用上限是预设资源额度，可以判定这次调用操作码 Call 是一次传递 send 操作。如果这次传递 send 操作返回的结果是 ErrOutOfGas，则确定所述调用操作码满足费用不足的错误条件。

虚拟机执行模块，可以通过在虚拟机的源代码的适当位置通过插桩，插入监控规则和中断机制，以实时获取智能合约的操作码的执行信息，对交易的执行过程进行动态实时监测，捕捉危险操作并及时阻断交易。

本发明实施例中，虚拟机对智能合约进行解释执行的过程中，可以包括以下步骤：

步骤一、判断操作码是不是需关注的操作码；

其中，需关注的操作码可以为危险操作码或起始操作码。

步骤二、根据判断结果决定是否将当前调用的操作码插入操作码的数据结构；

步骤三、在每一个操作码执行之前，对该交易对应的操作码的存储结构进行分析；

具体的，可以包括若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件。

步骤四、在遍历所有的监控规则之后，如果发现危险操作，立即停止执行；否则，执行步骤五；

步骤五、正常执行当前操作码，并返回操作码的执行结果。

一种可能的实现方式，若发现可能的漏洞威胁，虚拟机会立即输出异常警告，并对区块状态进行复原，终止交易的继续执行。本发明实施例中的虚拟机就可以实时检查运行状态，及时终止危险交易。

5 一种可能的实现方式，所述方法还包括：

若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述操作码的操作。

10 本发明实施例提供一种区块链中智能合约的监测方法，通过在虚拟机层进行监测，可以在执行智能合约的过程中实施诊断出一些危险行为，并及时阻断交易执行，并发出警报，有效提高智能合约的安全性。

15 本发明实施例中的虚拟机可以有效地发掘智能合约中的漏洞，对传统漏洞检测工具无法甄别出来的漏洞，也可以进行阻断和报警。本发明实施例中的虚拟机可以弥补智能合约检测工具的不足，针对难以被智能合约测试工具发现的危险交易，也可以通过虚拟机及时捕捉并终止，如图 3 所示，经过测试，本发明实施例中的虚拟机可以及时发现智能合约测试工具检测不到的潜在威胁，并 100% 阻断危险交易的执行。

一种可能的实现方式，为进一步提高监控效率，在步骤 202 之前，还可以包括：

20 根据所述交易请求，建立存储所述至少一个操作码的监控信息的数据结构；

将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

25 操作码结构是一种用户定义的数据结构，操作码结构存储了执行过程中涉及到的需关注的操作码，记录与危险行为分析相关的需关注的操作码和运行时信息，具体的，可以通过对操作码的操作码序列进行存储，以进行进一步的错误条件分析。

操作码监控模块包括一个用于存储的数据结构，用于存储操作码。存储

的数据结构的选择可以根据监控规则确定。如果监控规则关注操作码和它的操作数本身，可以采用一些线性结构对操作码进行存储。如果监控规则更关注操作码之间的关系，那么可以采用一些拓扑结构对操作码进行存储。新插入的操作码要根据监控规则，插入到数据结构的特定位置，以实现操作码结构。例如，数据结构为数据栈，根据操作码的执行顺序，存储操作码。

操作码结构的构建可以基于堆栈、队列、树等数据结构，实现方式的选择可以取决于监控规则的复杂性。例如，如果只考虑操作码之间的邻接关系，可以选择栈或队列；一种可能的实现方式，如果策略侧重于操作码之间更复杂的关系，则可以采用树结构。

在具体实施过程中，操作码结构的建立及操作可以包括三个部分：操作码结构的初始化、操作码的存储和操作码运行时的分析。

在每个调用过程中，首先对操作码结构进行初始化，本发明实施例以堆栈的数据结构为例进行说明，例如，为每笔交易建立一个新的操作码的栈结构。

操作码的存储过程包括：在执行每个操作码之前，将该操作码更新至操作码结构中。例如，将操作码压入所述栈结构中。

对所述操作码进行监控规则的分析，可以通过虚拟机执行模块，将监控规则和操作码结构通过插桩，插入到虚拟机的源码中，以通过所有监控规则对操作码结构进行分析，实现虚拟机执行智能合约的有效监测。例如，如果数据结构中的操作码的执行结果被认为是危险的，即满足监控规则中的任一错误条件，则所述操作码的执行过程将被中断。

在具体实施过程中，监控规则可以存储在虚拟机项目的目录下的一个新目录中，每种监控规则可以封装为一个返回值为布尔类型的函数，中断机制可以封装为一个抛出异常的操作。

一种可能的实现方式，对于操作码结构的执行过程，可以包括：

步骤一、若确定交易的初始调用的操作码为调用操作码 CALL，则建立一个名为 op_Stack 的新栈并进行初始化，将第一个操作码压入栈中；

其中，一种可能的实现方式，初始化操作被插入到 CALL 操作码所在位置之后。

针对交易过程中的每个操作码，执行以下监控步骤：

5 步骤二、若确定当前调用的操作码为需关注的操作码，则将所述调用的操作码压入栈，遍历所有监控规则对当前操作码结构进行测试，判断其状态是否安全。

步骤三、如果确认未存在异常结果则确认当前操作码为安全操作码，执行当前的操作码，并开启执行下一操作码的监控；否则，执行步骤四；

10 步骤四、调用中断机制阻断交易执行，同时向用户提示该交易存在潜在危害。

通过虚拟机执行模块，在虚拟机的源代码的适当位置通过插桩，插入监控规则、中断机制和操作码结构，来获取实时的智能合约的操作码的执行信息，对交易的执行过程进行动态实时监测，捕捉危险操作并及时阻断交易，有效提高了监测效率。

15 本发明实施例提供的虚拟机，支持基于不同语言编写的虚拟机，适用于多种应用场景。区块链平台的开发者可以将监控规则嵌入到本发明实施例提供的虚拟机中；例如，以太坊使用者可以使用封装好的本发明实施例中的虚拟机进行交易，在发生异常情况时及时阻断交易，避免不必要的损失。

20 基于相同的发明构思，本发明实施例还提供了一种区块链中智能合约的监控装置，如图 4 所示，包括：

收发单元 401，用于获取交易请求；

25 处理单元 402，用于根据所述交易请求，调用对应的智能合约；在所述智能合约执行所述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件；若是，则根据所述监控规则，输出所述调用的操作码的异常结果；所述异常结果包括针对所述操作码的阻断操作。

一种可能的实现方式，所述需关注的操作码为时间戳操作码；所述处理

单元 402，具体用于：

若确定所述交易请求的输入参数中的交易值大于预设常数值，则确定所述时间戳操作码为满足时间戳异常的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述处理单元 402，具体用于：

若在上述智能合约执行所述交易请求的过程中，所述调用操作码为非首次的调用操作码，且所述调用操作码的输入参数中的交易值大于预设常数值，则确定所述调用操作码满足函数可重入的错误条件。

一种可能的实现方式，所述需关注的操作码为委托调用操作码；所述处理单元 402，具体用于：

判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境；若是，则确定所述委托调用操作码为满足危险调用的错误条件。

一种可能的实现方式，所述需关注的操作码为调用操作码；所述处理单元，具体用于：

输入的交易值大于第一预设阈值，交易上限大于第二预设阈值，且所述调用操作码返回的结果为费用 gas 不足，则确定所述调用操作码满足费用不足的错误条件。

一种可能的实现方式，所述处理单元 402，还用于：

根据所述交易请求，建立存储所述至少一个操作码的监控信息的数据结构；

将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

一种可能的实现方式，所述处理单元，还用于：

若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述调用的操作码的操作。

基于相同的原理，本发明还提供一种电子设备，如图 5 所示，包括：

包括处理器 701、存储器 702、收发机 703、总线接口 704，其中处理器 701、存储器 702 与收发机 703 之间通过总线接口 704 连接；

所述处理器 701, 用于读取所述存储器 702 中的程序, 执行下列方法:

根据所述交易请求, 调用对应的智能合约; 在所述智能合约执行所述交易请求的过程中, 若确定调用的操作码为需关注的操作码, 则判断所述需关注的操作码是否满足监控规则的错误条件; 若是, 则根据所述监控规则, 输出所述调用的操作码的异常结果; 所述异常结果包括针对所述操作码的阻断操作。

一种可能的实现方式, 所述需关注的操作码为时间戳操作码; 所述处理器 701, 具体用于:

若确定所述交易请求的输入参数中的交易值大于预设常数值, 则确定所述时间戳操作码为满足时间戳异常的错误条件。

一种可能的实现方式, 所述需关注的操作码为调用操作码; 所述处理器 701, 具体用于:

若在所述智能合约执行所述交易请求的过程中, 所述调用操作码为非首次的调用操作码, 且所述调用操作码的输入参数中的交易值大于预设常数值, 则确定所述调用操作码满足函数可重入的错误条件。

一种可能的实现方式, 所述需关注的操作码为委托调用操作码; 所述处理器 701, 具体用于:

判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境; 若是, 则确定所述委托调用操作码为满足危险调用的错误条件。

一种可能的实现方式, 所述需关注的操作码为调用操作码; 所述处理器 701, 具体用于:

输入的交易值大于第一预设阈值, 交易上限大于第二预设阈值, 且所述调用操作码返回的结果为费用 gas 不足, 则确定所述调用操作码满足费用不足的错误条件。

一种可能的实现方式, 所述处理器 701, 还用于:

根据所述交易请求, 建立存储所述至少一个操作码的监控信息的数据结构;

将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

一种可能的实现方式，所述处理器 701，还用于：

若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述调用的操作码的操作。

5 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、
10 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

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

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图
20 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。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本
25 发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包括这些改动和变型在内。

权利要求

1、一种区块链中智能合约的监控方法，其特征在于，包括：

获取交易请求；

根据所述交易请求，调用对应的智能合约；

5 在所述智能合约执行所述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件；

若是，则根据所述监控规则，输出所述调用的操作码的异常结果，并执行针对所述操作码的阻断操作。

2、如权利要求 1 所述的方法，其特征在于，所述需关注的操作码为时间戳操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：

若确定所述交易请求的输入参数中的交易值大于预设常数值，则确定所述时间戳操作码为满足时间戳异常的错误条件。

3、如权利要求 1 所述的方法，其特征在于，所述需关注的操作码为调用操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：

若在上述智能合约执行所述交易请求的过程中，所述调用操作码为非首次的调用操作码，所述调用操作码的调用节点为所述交易的首次调用的操作码的执行节点，所述调用操作码的输入参数中的交易值大于预设常数值，则
20 确定所述调用操作码满足函数可重入的错误条件。

4、如权利要求 1 所述的方法，其特征在于，所述需关注的操作码为委托调用操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：

判断所述智能合约的操作环境是否为所述委托调用操作码的操作环境；
25 若是，则确定所述委托调用操作码为满足危险调用的错误条件。

5、如权利要求 1 所述的方法，其特征在于，所述需关注的操作码为调用

操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：

5 输入的交易值大于第一预设阈值，交易上限大于第二预设阈值，且所述调用操作码返回的结果为费用 gas 不足；则确定所述调用操作码满足费用不足的错误条件。

6、如权利要求 1 所述的方法，其特征在于，所述需关注的操作码为计算操作码；所述若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件，包括：

10 若确定所述计算操作码的输出结果满足计算溢出的错误条件，则确定所述计算调用操作码为满足计算溢出的错误条件。

7、如权利要求 1-6 任一项所述的方法，其特征在于，所述在所述智能合约执行所述交易请求之前，还包括：

根据所述交易请求，建立存储所述至少一个操作码的监控信息的数据结构；

15 将所述至少一个操作码的对应的至少一个监控规则，存储至所述数据结构中。

8、如权利要求 1-6 任一项所述的方法，其特征在于，所述方法还包括：

若确定所述需关注的操作码的运行结果中，未出现满足监控规则的错误条件，则执行所述操作码的操作。

20 9、一种区块链中智能合约的监控装置，其特征在于，包括：

收发单元，用于获取交易请求；

25 处理单元，用于根据所述交易请求，调用对应的智能合约；在所述智能合约执行所述交易请求的过程中，若确定调用的操作码为需关注的操作码，则判断所述需关注的操作码是否满足监控规则的错误条件；若是，则根据所述监控规则，输出所述调用的操作码的异常结果；所述异常结果包括针对所述操作码的阻断操作。

10、一种电子设备，其特征在于，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1-8 任一所述的方法。

5

11、一种非暂态计算机可读存储介质，其特征在于，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行权利要求 1~8 任一所述方法。

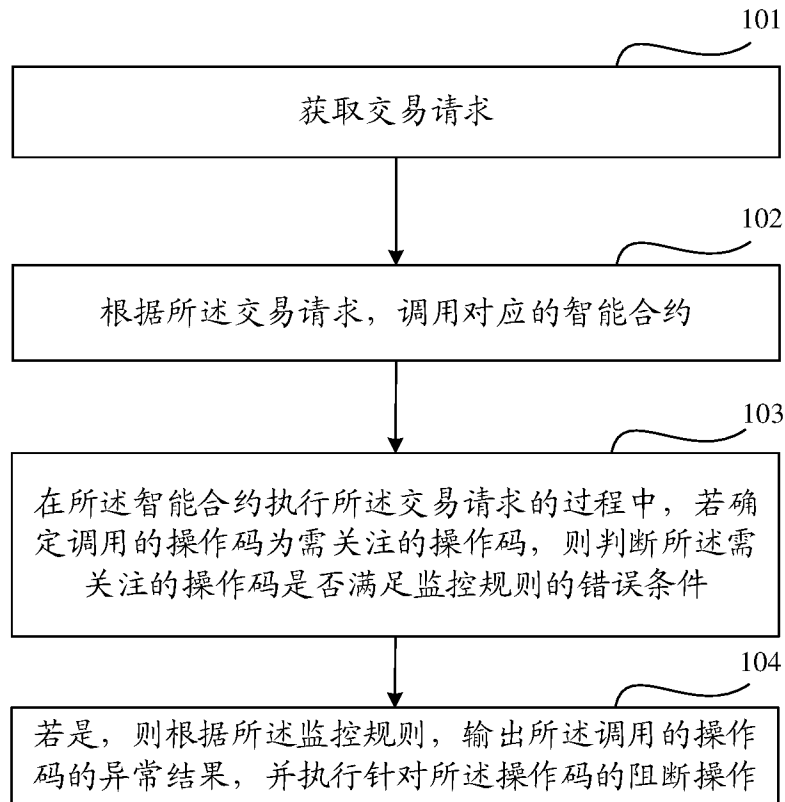


图 1

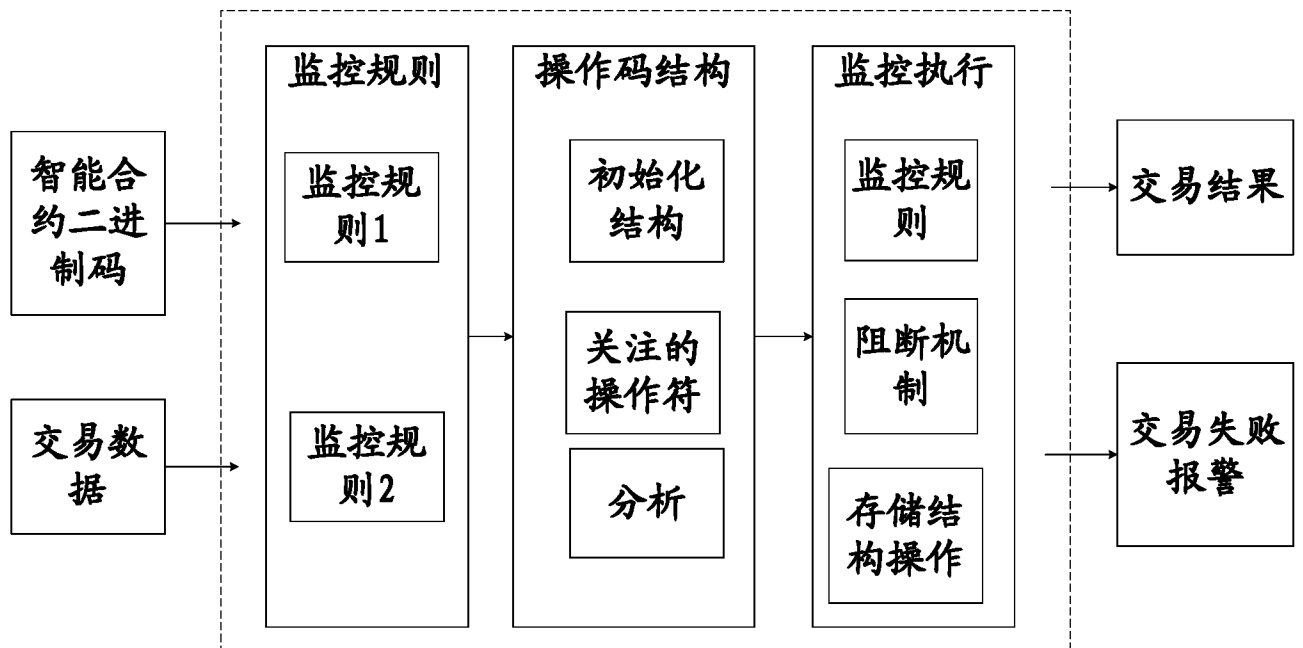


图 2

智能合约编号	智能合约测试工具检测情况	现有 EVM 执行情况	本发明 EVM 执行情况	错误类型
# 1	有危险	一直执行到结束	阻断交易	溢出
# 2	有危险	一直执行到结束	阻断交易	时间戳
# 3	正常	一直执行到结束	阻断交易	溢出
# 4	正常	一直执行到结束	阻断交易	溢出
# 5	正常	一直执行到结束	阻断交易	溢出
# 6	有危险	一直执行到结束	阻断交易	时间戳
# 7	有危险	一直执行到结束	阻断交易	时间戳
# 8	有危险	一直执行到结束	阻断交易	溢出
# 9	正常	一直执行到结束	阻断交易	溢出
# 10	正常	一直执行到结束	阻断交易	溢出

图 3

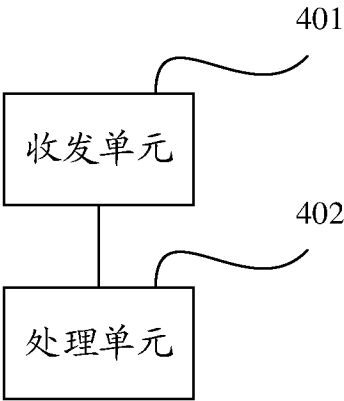


图 4

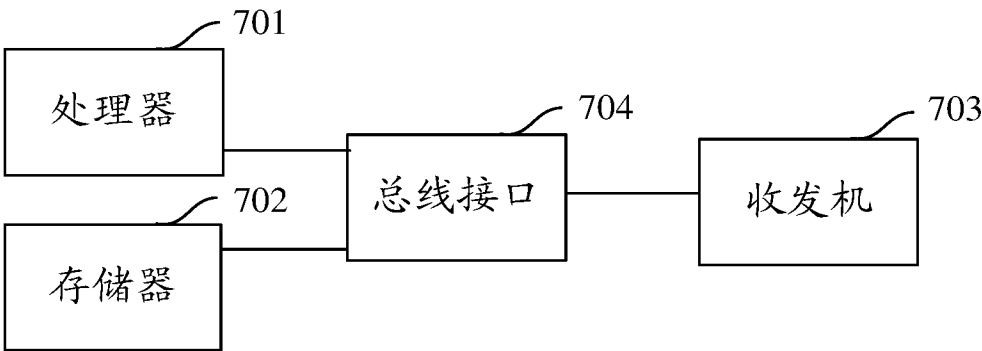


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/092174

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55(2013.01)i; G06F 21/57(2013.01)i; G06Q 40/04(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)

G06F; G06Q

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

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

EPODOC, WPI, CNPAT, CNKI, IEEE: 智能, 合约, 异常, 漏洞, 错误, 安全, 检测, 监测, 交易, 操作码, 参数, 调用, 触发, 中断, 阻断, 中止, 溢出, 时间戳, smart, contract, abnormal, bug, error, fault, safety, monitor, detect, transaction, opcode, parameter, call, trigger, interrupt, block, abort, overflow, time, stamp

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110263536 A (SHENZHEN QIANHAI WEBANK CO., LTD. et al.) 20 September 2019 (2019-09-20) claims 1-11	1-11
Y	CN 109493226 A (BEIJING WUZI UNIVERSITY) 19 March 2019 (2019-03-19) abstract, description, paragraphs 5-6 and 22-31, figure 1	1-11
Y	CN 109767329 A (BEIJING KINGSOFT SECURITY SOFTWARE CO., LTD.) 17 May 2019 (2019-05-17) description, paragraphs 3, 61-106	1-11
A	CN 107886000 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 06 April 2018 (2018-04-06) entire document	1-11
A	CN 108256337 A (BEIJING ARXAN FINTECH CO., LTD.) 06 July 2018 (2018-07-06) entire document	1-11
A	CN 109492402 A (HANGZHOU QULIAN TECHNOLOGY CO., LTD.) 19 March 2019 (2019-03-19) 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

05 August 2020

Date of mailing of the international search report

26 August 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

International application No.

PCT/CN2020/092174

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019070357 A1 (SIEMENS AKTIENGESELLSCHAFT et al.) 11 April 2019 (2019-04-11) entire document	1-11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/092174

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110263536	A	20 September 2019	None	
CN	109493226	A	19 March 2019	None	
CN	109767329	A	17 May 2019	None	
CN	107886000	A	06 April 2018	None	
CN	108256337	A	06 July 2018	None	
CN	109492402	A	19 March 2019	None	
WO	2019070357	A1	11 April 2019	None	

国际检索报告

国际申请号

PCT/CN2020/092174

A. 主题的分类 G06F 21/55(2013.01)i; G06F 21/57(2013.01)i; G06Q 40/04(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) G06F; G06Q 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) EPDOC, WPI, CNPAT, CNKI, IEEE: 智能, 合约, 异常, 漏洞, 错误, 安全, 检测, 监测, 交易, 操作码, 参数, 调用, 触发, 中断, 阻断, 中止, 溢出, 时间戳, smart, contract, abnormal, bug, error, fault, safety, monitor, detect, transaction, opcode, parameter, call, trigger, interrupt, block, abort, overflow, time, stamp																										
C. 相关文件 <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 110263536 A (深圳前海微众银行股份有限公司 等) 2019年 9月 20日 (2019 - 09 - 20) 权利要求1-11</td> <td>1-11</td> </tr> <tr> <td>Y</td> <td>CN 109493226 A (北京物资学院) 2019年 3月 19日 (2019 - 03 - 19) 摘要、说明书第5-6和22-31段、图1</td> <td>1-11</td> </tr> <tr> <td>Y</td> <td>CN 109767329 A (北京金山安全软件有限公司) 2019年 5月 17日 (2019 - 05 - 17) 说明书第3、61-106段</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 107886000 A (华中科技大学) 2018年 4月 6日 (2018 - 04 - 06) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 108256337 A (北京阿尔山金融科技有限公司) 2018年 7月 6日 (2018 - 07 - 06) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 109492402 A (杭州趣链科技有限公司) 2019年 3月 19日 (2019 - 03 - 19) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>WO 2019070357 A1 (SIEMENS AKTIENGESELLSCHAFT 等) 2019年 4月 11日 (2019 - 04 - 11) 全文</td> <td>1-11</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 110263536 A (深圳前海微众银行股份有限公司 等) 2019年 9月 20日 (2019 - 09 - 20) 权利要求1-11	1-11	Y	CN 109493226 A (北京物资学院) 2019年 3月 19日 (2019 - 03 - 19) 摘要、说明书第5-6和22-31段、图1	1-11	Y	CN 109767329 A (北京金山安全软件有限公司) 2019年 5月 17日 (2019 - 05 - 17) 说明书第3、61-106段	1-11	A	CN 107886000 A (华中科技大学) 2018年 4月 6日 (2018 - 04 - 06) 全文	1-11	A	CN 108256337 A (北京阿尔山金融科技有限公司) 2018年 7月 6日 (2018 - 07 - 06) 全文	1-11	A	CN 109492402 A (杭州趣链科技有限公司) 2019年 3月 19日 (2019 - 03 - 19) 全文	1-11	A	WO 2019070357 A1 (SIEMENS AKTIENGESELLSCHAFT 等) 2019年 4月 11日 (2019 - 04 - 11) 全文	1-11
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
PX	CN 110263536 A (深圳前海微众银行股份有限公司 等) 2019年 9月 20日 (2019 - 09 - 20) 权利要求1-11	1-11																								
Y	CN 109493226 A (北京物资学院) 2019年 3月 19日 (2019 - 03 - 19) 摘要、说明书第5-6和22-31段、图1	1-11																								
Y	CN 109767329 A (北京金山安全软件有限公司) 2019年 5月 17日 (2019 - 05 - 17) 说明书第3、61-106段	1-11																								
A	CN 107886000 A (华中科技大学) 2018年 4月 6日 (2018 - 04 - 06) 全文	1-11																								
A	CN 108256337 A (北京阿尔山金融科技有限公司) 2018年 7月 6日 (2018 - 07 - 06) 全文	1-11																								
A	CN 109492402 A (杭州趣链科技有限公司) 2019年 3月 19日 (2019 - 03 - 19) 全文	1-11																								
A	WO 2019070357 A1 (SIEMENS AKTIENGESELLSCHAFT 等) 2019年 4月 11日 (2019 - 04 - 11) 全文	1-11																								
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																										
<table border="0"> <tr> <td> * 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 </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 “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 </td> </tr> </table>			* 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																						
* 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 2020年 8月 5日		国际检索报告邮寄日期 2020年 8月 26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 姜晓庆 电话号码 86-(10)-53961427																								

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/092174

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	110263536	A	2019年 9月 20日	无	
CN	109493226	A	2019年 3月 19日	无	
CN	109767329	A	2019年 5月 17日	无	
CN	107886000	A	2018年 4月 6日	无	
CN	108256337	A	2018年 7月 6日	无	
CN	109492402	A	2019年 3月 19日	无	
WO	2019070357	A1	2019年 4月 11日	无	