

(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
2024 年 1 月 4 日 (04.01.2024)



(10) 国际公布号
WO 2024/001024 A1

- (51) 国际专利分类号:
G06F 16/27 (2019.01) **G06Q 40/04** (2012.01)
- (21) 国际申请号: PCT/CN2022/135304
- (22) 国际申请日: 2022 年 11 月 30 日 (30.11.2022)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202210750970.8 2022年6月29日 (29.06.2022) CN
- (71) 申请人: 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: 王江(**WANG, Jiang**); 中国上海市黄浦区外
马路618号8层803室, Shanghai 200010 (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,
CV, 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, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,

(54) **Title:** METHOD FOR EXECUTING TRANSACTION IN BLOCKCHAIN SYSTEM, AND BLOCKCHAIN SYSTEM AND
NODES

(54) 发明名称: 在区块链系统中执行交易的方法、区块链系统和节点

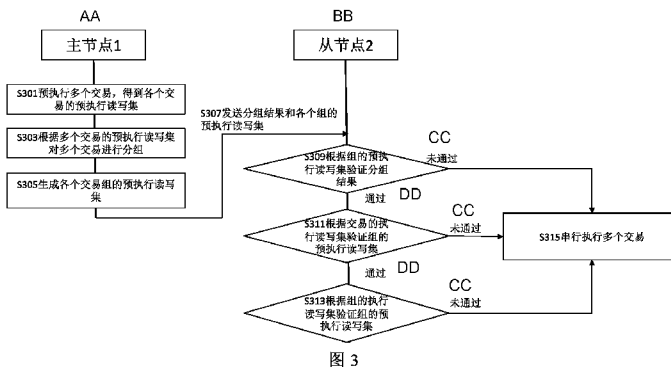


图 3

- S301 Pre-execute a plurality of transactions to obtain pre-execution read-write sets of the respective transactions
- S303 Group the plurality of transactions according to the pre-execution read-write sets of the plurality of transactions
- S305 Generate pre-execution read-write sets of the respective transaction groups
- S307 Send a grouping result and the pre-execution read-write sets of the respective groups
- S309 Verify the grouping result according to the pre-execution read-write sets of the groups
- S311 Verify the pre-execution read-write sets of the groups according to the execution read-write sets of the transactions
- S313 Verify the pre-execution read-write sets of the groups according to the execution read-write sets of the groups
- S315 Execute the plurality of transactions in series
- AA Master node
- BB Slave node
- CC Not passed
- DD Passed

(57) **Abstract:** A method for executing a transaction in a blockchain system, and a blockchain system and nodes. The blockchain system comprises a master node and a slave node. The method comprises: a master node pre-executing a plurality of transactions to obtain pre-execution read-write sets of the respective transactions; grouping the plurality of transactions according to the pre-execution read-write sets of the plurality of transactions, so as to obtain a plurality of transaction groups, and generating pre-execution read-write sets of the respective transaction groups; sending a grouping result and the pre-execution read-write sets of the respective transaction

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

groups to a slave node; the slave node verifying the grouping result according to the pre-execution read-write sets of the plurality of transaction groups; and when verification is passed, executing the plurality of transactions in parallel according to the grouping result, so as to obtain execution read-write sets of transactions, which are comprised in each transaction group, and verifying the pre-execution read-write set of the transaction group on the basis of the execution read-write sets of the transactions, which are comprised in the transaction group.

(57) 摘要: 一种在区块链中执行交易的方法、区块链系统和节点, 所述区块链系统包括主节点和从节点, 所述方法包括: 所述主节点预执行多个交易, 得到各个交易的预执行读写集; 根据多个交易的预执行读写集对多个交易进行分组, 得到多个交易组, 生成各个交易组的预执行读写集; 将分组结果和各个交易组的预执行读写集发送给从节点; 所述从节点根据所述多个交易组的预执行读写集对分组结果进行验证; 在验证通过的情况下根据分组结果并行执行所述多个交易, 得到每个交易组包括的交易的执行读写集, 基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

在区块链系统中执行交易的方法、区块链系统和节点

本申请要求于2022年6月29日提交中国国家知识产权局、申请号为202210750970.8、

- 5 申请名称为“在区块链系统中执行交易的方法、区块链系统和节点”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 本说明书实施例属于区块链技术领域，尤其涉及一种在区块链系统中执行交易的
方法、区块链系统和节点。

背景技术

- 15 区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等
计算机技术的新型应用模式。区块链系统中按照时间顺序将数据区块以顺序相连的方
式组合成链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。
由于区块链具有去中心化、信息不可篡改、自治性等特性，区块链也受到人们越来越
多的重视和应用。区块链节点在执行区块中的多个交易时，可通过并行执行交易加快
交易执行速度。

发明内容

本发明的目的在于提供一种在区块链中执行交易的方案，可以有效验证主节点是
否作恶。

本说明书第一方面提供一种在区块链中执行交易的方法，所述区块链包括主节点
和从节点，所述方法包括：

- 25 所述主节点预执行多个交易，得到各个交易的预执行读写集；根据多个交易的预
执行读写集对多个交易进行分组，得到多个交易组，生成各个交易组的预执行读写集；
将分组结果和各个交易组的预执行读写集发送给从节点；

- 所述从节点根据所述多个交易组的预执行读写集对分组结果进行验证；在验证通
过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行
30 读写集，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行
验证。

本说明书第二方面提供一种在区块链中执行交易的方法，所述区块链包括主节点和从节点，所述方法由所述从节点执行，包括：

从所述主节点接收对多个交易进行分组得到的分组结果和各个交易组的预执行读写集，其中，所述交易组的预执行读写集基于所述交易组中包括的各个交易的预执行读写集生成；

根据所述多个交易组的预执行读写集对分组结果进行验证；

在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集；

基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

本说明书第三方面提供一种区块链的从节点，包括：

接收单元，用于从所述区块链的主节点接收对多个交易进行分组得到的分组结果和各个交易组的预执行读写集，其中，所述交易组的预执行读写集基于所述交易组中包括的各个交易的预执行读写集生成；

验证单元，用于根据所述多个交易组的预执行读写集对分组结果进行验证；

执行单元，用于在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集；

所述验证单元还用于，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

本说明书第四方面提供一种区块链，包括主节点和从节点，

所述主节点用于：预执行多个交易，得到各个交易的预执行读写集；根据多个交易的预执行读写集对多个交易进行分组，得到多个交易组，生成各个交易组的预执行读写集；将分组结果和各个交易组的预执行读写集发送给从节点；

所述从节点用于：根据所述多个交易组的预执行读写集对分组结果进行验证；在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

本说明书第五方面提供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机中执行时，令计算机执行第二方面所述的方法。

本说明书第六方面提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第二方面所述的方法。

通过本说明书实施例提供的方案，从节点可以快速验证主节点是否作恶，并尽可能优化存在的耗时步骤，并确保即使存在主节点作恶的情况中，仍能维持区块链数据的正确性和一致性。

5 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说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

- 10 图1是本说明书实施例中的区块链架构图；
图2示出了本说明书实施例中的区块链结构图；
图3为本说明书实施例中的执行交易的方法流程图；
图4为本说明书实施例中的一种区块链的从节点的架构图。

15 具体实施方式

- 为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实
20 施例，都应当属于本说明书保护的范围。

- 图 1 示出本说明书实施例中的区块链架构图。如图 1 中，区块链中例如包含主节点 1、从节点 2～从节点 5 共 6 个节点。节点之间的连线示意性的表示 P2P(Peer to Peer，点对点) 连接。这些节点上都存储全量的账本，即存储全部区块和全部账户的状态。其中，区块链中的每个节点通过执行相同的交易而产生区块链中的相同的状态，区块
25 链中的每个节点存储相同的状态数据库。所不同的是，主节点 1 可负责从客户端接收交易，并向各个从节点发起共识提议，该共识提议中例如包括将要成块的区块（例如区块 B1）中的多个交易及各个交易的提交顺序等信息。在区块链中的节点对共识提议共识成功之后，各个节点可根据共识提议中的提交顺序执行该多个交易，从而生成区块 B1。

- 30 可以理解，图 1 所示的区块链仅仅是示例性的，本说明书实施例不限于应用于图

1 所示的区块链，例如还可以应用于包括分片的区块链系统中。

另外，图 1 中虽然示出了区块链中包括 6 个节点，本说明书实施例不限于此，而是可以包括其他数目的节点。具体是，区块链中包含的节点可以满足拜占庭容错

(Byzantine Fault Tolerance, BFT) 要求。所述的拜占庭容错要求可以理解为在区块链内部可以存在拜占庭节点，而区块链对外不体现拜占庭行为。一般的，一些拜占庭容错算法中要求节点个数大于 $3f+1$ ， f 为拜占庭节点个数，例如实用拜占庭容错算法 PBFT (Practical Byzantine Fault Tolerance)。

在相关技术中，为了提高区块链中的每秒执行交易 (TPS) 指标，需要加快交易的执行速度。为此，区块链节点中可通过并行执行交易来加快交易的执行速度。在一种实施方式中，区块链节点可通过单机中的多个进程并行执行交易，在另一种实施方式中，区块链节点可部署在服务器集群中，通过多台服务器并行执行交易。通常，对于转账交易，区块链节点首先根据交易访问的账户将多个交易划分为多个交易组，各个交易组之间不访问相同的账户，从而可并行执行各个交易组。然而，当交易中调用智能合约时，在执行该交易之前不能预知该交易中访问的变量，从而无法对多个交易进行有效的分组，也就无法对并行执行交易。

在一种相关技术中，在包括主节点和多个从节点的区块链中，可以由主节点预执行多个交易，得到多个交易各自的预执行读写集，并根据该预执行读写集将多个交易分为多个组，从而各个从节点可按照多个组并行执行多个交易。然而，在该方案中，可能存在主节点故意作恶的情况，比如向从节点提供错误的分组。

本说明书实施例提供了一种在图1所示区块链中并行执行交易的方案，可由从节点有效地检查主节点是否作恶，从而提高了区块链的系统效率。

图 2 示出了本说明书实施例提供的区块链的主节点 1 和从节点 (例如从节点 2) 的结构图。如图 2 所示，主节点 1 中包括预执行模块 11、冲突检测模块 12 和共识模块 13，从节点 2 中包括共识模块 22 和计算模块 23。主节点 1 例如可以与客户端连接，从而可以从客户端接收到多个交易。主节点 1 在接收到每个交易之后，预执行模块 11 预执行该交易，得到该交易的预执行读写集。其中，预执行读写集包括预执行读集和预执行写集，预执行读集具体可以为在预执行交易的过程中生成的读取的变量的键值对，预执行写集具体可以为在预执行交易的过程中生成的写入的变量的键值对。主节点 1 中可维护预执行状态集，预执行模块 11 在预执行交易时，可从预执行状态集或者状态数据库中读取变量的状态值。预执行模块 11 在预执行交易之后，可根据交易的预

执行读写集更新预执行状态集。

如图 2 中所示，预执行模块 11 中可包括多个预执行子模块，例如预执行子模块 111 和预执行子模块 112，这两个预执行子模块可并行预执行交易。冲突检测模块 12 中包括预执行状态集和预执行交易集合，其中，主节点 1 例如在内存中存储所述预执行状态集和预执行交易集合，以供冲突检测模块 12 使用。冲突检测模块 12 串行地对各个交易进行预执行冲突检测。具体是，冲突检测模块 12 检测该交易的预执行读集与已经预执行的交易的写集是否存在冲突，如果该交易的预执行读集中的某个变量的值与预执行状态集中的该变量的值不同，则可确定存在冲突。如果确定不存在冲突，冲突检测模块 12 将该交易的预执行写集中的状态更新到预执行状态集中，并将该交易顺序排列到预执行交易集合中。

共识模块 13 从预执行交易集合中获取在先记录的顺序排列的多个交易，共识模块 13 中包括分组子模块 131，分组子模块 131 根据该多个交易各自的预执行读写集对该多个交易进行分组，得到多个交易组，各个交易组之间不存在冲突交易。其中，两个交易组之间存在冲突交易的情况通常包括如下种情况：第一交易组中的交易读取第一变量（即第一交易组读取第一变量），第二交易组写入第一变量；第一交易组写入第一变量，第二交易组写入第一变量；第一交易组读取第一变量且写入第一变量，第二交易组写入第一变量；第一交易组读取第一变量且写入第一变量，第二交易组读取第一变量且写入第一变量。其中，如果两个交易组读取相同的变量也可以认为是不存在冲突交易。通常，为了简化方案，分组子模块 131 可按照各个交易组之间不访问相同的变量的要求来对多个交易进行分组。

另外，共识模块 13 还根据所述多个交易的预执行读写集生成各个交易组的预执行读写集。之后，主节点 1 向各个从节点的共识模块（例如共识模块 22）发起共识提议，其中，该共识提议中包括所述多个交易、所述多个交易在所述预执行交易集合中的排列顺序、所述多个交易的分组结果、以及各个交易组的预执行读写集。可以理解，主节点也可以向从节点广播所述多个交易，从而在共识提议中可以不包括所述多个交易。

在区块链中的多个共识节点共识成功之后，共识模块 22 中的分组验证子模块 221 可以根据各个组的组读写集验证各个组之间是否存在冲突，即验证各个组之间是否访问相同的变量或账户。

在分组验证子模块 221 的验证通过的情况中，从节点中的计算模块 23 可以按照分组开始并行执行所述多个交易。其中，从节点 2 的计算模块 23 中包括多个执行子模块

(图中示意示出执行子模块 232、执行子模块 233 和执行子模块 234)。每个执行子模块在执行交易的过程中可以根据得到的交易的执行读写集来验证分组的正确性。

通过如上所述的过程，主节点 1 通过将各个交易组的预执行读写集发送给各个从节点，从节点可以有效验证主节点是否作恶，提高了系统效率。

5 下文将参考图3所示的执行交易的方法流程图详细描述上述过程。在图3中仅示出了主节点1和从节点2执行的流程，可以理解，区块链中的其他从节点与从节点2执行相同的流程。

参考图3，首先，在步骤S301，主节点1预执行多个交易，得到各个交易的预执行读写集。

10 主节点 1 可以在每接收到一个交易之后，就立即对该交易进行预执行。

在一种实施方式中，主节点 1 可串行执行接收的多个交易。主节点 1 在预执行交易时，当从图 2 中的预执行状态集或者状态数据库中读取任意变量的值时，在内存中设置的该交易的读缓存中记录该读取的变量的键值对，在写入任意变量的值时，在该交易的写缓存中记录该写入的变量的键值对，并在预执行结束之后，可基于该交易的读缓存和写缓存获取该交易的预执行读写集。

具体是，主节点 1 在预执行该交易的过程中读取变量（例如变量 A）时，主节点 1 首先确定该交易的写缓存中是否存储有变量 A 的值，如果存储了变量 A 的值，可直接从写缓存中读取变量 A 的值。在确定所述写缓存中未存储变量 A 的值情况中，确定该交易的读缓存中是否存储有变量 A 的值，如果存储了变量 A 的值，可从读缓存中读取变量 A 的值。在确定所述读缓存中未存储变量 A 的值情况中，确定所述预执行状态集中是否存储变量 A 的值，如果存储了变量 A 的值，可从预执行状态集中读取变量 A 的值。在确定预执行状态集中未存储变量 A 的值的值的情况中，可从状态数据库读取变量 A 的值。也就是说，主节点 1 在预执行交易的过程中，读取变量的优先度为：交易的写缓存>交易的读缓存>预执行状态集>状态数据库，通过如此可保证预执行过程中读取的变量的值为该变量最新的值。

主节点 1 在如上所述预执行每个交易之后，得到各个交易的预执行读写集。在一种实施方式中，该预执行读写集中包括读集和写集，其中，读集包括预执行该交易时读取的变量的键值对（key-value），写集包括预执行该交易时写入的变量的键值对。在另一种实施方式中，该预执行读写集的读集中可包括预执行该交易时读取的变量的版本号，写集中可包括写入的变量的版本号，其中，在状态数据库中例如存储了变量

的各个写入值及各个写入值对应的版本号，从而通过在读写集中包括变量的版本号即可以确定交易读取和写入的值。

在交易中调用合约的情况中，区块链节点在执行该交易调用的合约的过程中，有可能根据读取的变量的值来对不同的变量进行写入。例如，当读取的变量的值为1时，对变量a写入10，当读取的变量的值为2时，对变量b写入20等等。因此，对于调用合约的交易，区块链节点必须通过执行该交易，才能确定该交易读取的变量和写入的变量，从而得到该交易的读写集。为此，主节点1通过预执行多个交易中的每个交易，得到每个交易的预执行读写集，该预执行的过程与执行交易的过程基本相同，不同在于，该对交易的预执行是在共识之前进行的执行过程，而对交易的执行是在共识之后进行的执行过程。并且预执行交易的预执行结果仅用于更新预执行状态集，而不用于更新世界状态，而执行交易的执行结果用于更新世界状态。

在一种实施方式中，参考图2，主节点1可通过多个预执行子模块对同时接收的多个交易并行进行预执行。为了防止多个预执行子模块并行更新预执行状态集导致冲突，主节点1在预执行各个交易之后，串行地对各个交易进行预执行冲突检测。

具体是，主节点1在对所述多个交易中的交易Tx1预执行冲突检测时，首先确定预执行状态集中是否包括交易Tx1的预执行读集中的变量（例如变量A）。如果没有，再类似地确定预执行状态集中是否包括交易Tx1的预执行读集中的其他变量。如果预执行状态集中不包括交易Tx1的预执行读集中的全部变量，也就是说，之前经过预执行冲突检测的交易还未对该交易访问的变量进行读写，则可确定交易Tx1的预执行读集与预执行状态集没有冲突，也即确定该交易Tx1的预执行与之前经过预执行冲突检测的交易不存在冲突。

如果主节点1确定预执行状态集中包括变量A的值，则确定预执行读集中的变量A的值与预执行状态集中的变量A的值是否一致，如果一致，说明该交易读取的变量A的值为预执行过程中变量A的最新状态。当主节点1对于交易Tx1预执行读集中的每个变量都确定所读取的值为预执行过程中的最新状态之后，可确定该交易Tx1的预执行读集与预执行状态集不存在冲突。

如果主节点1确定交易Tx1的预执行读集中的变量A的值与预执行状态集中的变量A的值不一致，说明该交易Tx1读取的变量A的值不是预执行过程中的最新状态，因此，可确定交易Tx1的预执行读集与预执行状态集存在冲突。在确定存在冲突的情况下，主节点1可对该交易Tx1重新进行预执行。

主节点 1 在确定交易的预执行读集与预执行状态集不存在冲突的情况中，基于该交易的预执行读写集更新预执行状态集和预执行交易集合。

具体是，例如，主节点1确定所述多个交易中的交易Tx2的预执行读集与预执行状态集不存在冲突，主节点1将交易Tx2的预执行读写集中读取或者写入的变量的值更新到预执行状态集中，从而使得该预执行状态集中记录各个变量在预执行过程中的最新状态。同时，主节点1将该交易顺序记录到预执行交易集合中，例如将该交易记录到预执行交易集合的末尾位置（即最后一个位置）。也就是说，预执行交易集合中记录的交易顺序体现了各个交易的冲突检测的顺序，并且所记录的各个交易与之前记录的交易不存在冲突。其中，所述预执行交易集合例如为顺序表的形式，或者为队列的形式。

在步骤 S303, 主节点 1 根据多个交易的预执行读写集对多个交易进行分组。

主节点1中可通过分组子模块131基于各个交易的预执行读写集中包括的读取的变量的键（key）和写入的变量key，对多个交易进行分组。如上文所述，该分组可使得不同交易组中的交易不访问相同的变量，该访问包括读操作和写操作，在达到该分组条件的情况下，各个交易组之间不会存在冲突交易，因此，各个交易组可以并行执行。

在步骤S305，主节点1生成各个交易组的预执行读写集。

分组子模块131还可以基于各个交易组中包括的各个交易的预执行读写集生成各个交易组的预执行读写集。具体是，分组子模块131可基于各个交易的预执行读集生成交易组的预执行读集，该预执行读集包括该交易组中的全部交易读取的变量的键(key)。例如，一个交易组中包括交易Tx1、交易Tx2、交易Tx3，其中，交易Tx1的预执行读集中包括变量a和变量b的键值对，交易Tx2的预执行读集中包括变量c和变量b的键值对，交易Tx3的预执行读集中包括变量a和变量c的键值对，则该交易组的预执行读集为{a, b, c}。

分组子模块131可基于各个交易的预执行写集生成交易组的预执行写集，与上述生成交易组的预执行读集类似的，该预执行写集中包括交易组中全部交易写入的变量的key。

主节点1在完成对多个交易的预执行之后，由于如上文所述，上述共识过程使得交易的预执行读写集与执行读写集一致，因此，主节点1可以直接将多个交易的预执行结果用作该交易的执行结果。根据该多个交易的预执行读写集更新状态数据库，并生成区块。该区块包括区块头和区块体。其中，区块体中例如包括所述多个交易各自的

交易体、收据等数据。区块头中可以包括状态根、收据根、交易根等数据。

在步骤S307，主节点1将多个交易的分组结果、各个交易组的预执行读写集、所述多个交易在预执行交易集合中的排列顺序发送给从节点（包括从节点2）。

具体是，主节点1可生成共识提议，该共识提议中可包括多个交易的分组结果、各个交易组的预执行读写集、所述多个交易在预执行交易集合中的排列顺序，并将该共识提议发送给各个从节点，从而与各个从节点达成共识，即将该多个交易作为即将生成的区块中的多个交易，并且该多个交易基于所述多个交易在预执行交易集合中的排列顺序执行。其中，从节点可另外从主节点或者客户端接收到所述多个交易，或者，在共识提议中还可以包括该多个交易。

通过如此，主节点1在进行预执行时排除了交易之间的冲突，并且各个节点在执行交易时按照预执行交易集合中的排列顺序执行各个交易，使得在主节点不作恶的情况下执行交易得到的读写集与该交易的预执行读写集必然是一致的。

在步骤S309，从节点根据各个交易组的预执行读写集验证分组结果。

具体是，从节点2可根据各个交易组的预执行读写集确定各个分组是否访问相同的变量，如果多个分组中至少两个分组之间访问相同的变量，说明该至少两个分组应分到一个交易组中，因此可确定分组结果是错误的，从而可确定主节点存在作恶的行为，即提供了错误的分组，因此该验证未通过，从节点2可执行步骤S315，按照共识提议中的顺序串行执行多个交易，即各个从节点不再信任主节点的分组结果，而是通过串行执行多个交易达到一致的执行结果。

当在步骤S309中的验证通过的情况下，从节点2执行步骤S311，在每个交易的执行过程中，根据交易的执行读写集验证组的预执行读写集。

从节点2在对分组结果的验证通过之后，可通过图2中示出的多个执行子模块并行执行多个交易，例如，每个执行子模块可从共识模块22接收一个或多个交易组，以串行执行每个交易组中的多个交易。其中，执行子模块在执行每个交易的过程中，生成该交易的执行读集和执行写集，其中，执行读集中包括该交易在执行过程中读取的变量的键值对，执行写集包括该交易在执行过程中写入的变量的键值对。

执行子模块在执行交易的中间，即未结束对交易的执行时，在每次读取一个变量时，可确定该交易所属的交易组的预执行读集中是否包括该变量，以对交易组的预执行读集进行验证。如果交易组的预执行读集中不包括该变量，说明主节点提供了错误的预执行读集，因此基于该预执行读集进行分组得到的分组结果也就是错误的结果，

因此，步骤S311中的验证未通过，从节点2可类似地执行步骤S315。反之，如果交易在执行过程中写入的全部变量都出现在交易组的预执行写集中，则可以继续进行对该组中其他交易的执行。

类似地，执行子模块在执行交易的过程中，还可以对交易组的预执行写集进行验证，类似地，可验证交易在执行过程中写入的变量是否出现在交易组的预执行写集中，如果未出现，则步骤S311中的验证未通过，从节点可执行步骤S315。反之，如果交易在执行过程中写入的全部变量都出现在交易组的预执行写集中，则可以继续进行对该组中其他交易的执行。

在步骤S311中的验证通过时，从节点可继续执行图3中的步骤S313。

10 在步骤S313，从节点根据交易组的执行读写集验证组的执行读写集。

从节点2在并行执行完成多个交易之后，可根据各个组中包括的交易的执行读写集生成各个交易组的执行读写集，该过程可参考上文中对生成交易组的预执行读写集的描述，在此不再赘述。

15 然后，从节点2可验证每个交易组的执行读写集是否与该交易组的预执行读写集一致，具体是，验证每个交易组的执行读集是否与该交易组的预执行读集一致，以及验证每个交易组的执行写集是否与该交易组的预执行写集一致。如果一致，则验证通过，从节点2可基于该多个交易的执行结果更新世界状态，生成区块。如果每个交易组的执行读写集与该交易组的预执行读写集不一致，则从节点2可执行步骤S315。

20 各个从节点在验证不通过的情况下完成步骤S315之后，可触发重新选举主节点，从而避免当前的主节点再次作恶。

图4为本说明书实施例中的一种区块链的从节点的架构图，包括：

接收单元41，用于从所述区块链的主节点接收对多个交易进行分组得到的分组结果和各个交易组的预执行读写集，其中，所述交易组的预执行读写集基于所述交易组中包括的各个交易的预执行读写集生成；

25 验证单元42，用于根据所述多个交易组的预执行读写集对分组结果进行验证；

执行单元43，用于在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集；

所述验证单元42还用于，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

30 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。

5 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)”

10 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

15 Description Language）、Lava、Lola、MyHDL、PALASM、RHDH（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。

20 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

25 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。

30 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。

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服务器系统。当然，本申请不排除随着未来计算机技术的发展，实现上述实施例功能的计算机例如可以为个人计算机、膝上型计算机、车载人机交互设备、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。

虽然本说明书一个或多个实施例提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或终端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行（例如并行处理器或者多线程处理的环境，甚至为分布式数据处理环境）。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、产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、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。例如若使用到第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现等。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

本发明是参照根据本发明实施例的方法、装置（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。

5 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。

10 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。

15 在典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。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。

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，磁带磁磁盘存储、石墨烯存储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。

25 本领域技术人员应明白，本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例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，本说明书一个或多个实施例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。

30 本说明书一个或多个实施例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一个或多个实施例，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。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，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。在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本说明书的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。以上所述仅为本说明书一个或多个实施例的实施例而已，并不用于限制本说明书一个或多个实施例。对于本领域技术人员来说，本说明书一个或多个实施例可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在权利要求范围之内。

权 利 要 求 书

1. 一种在区块链系统中执行交易的方法，所述区块链系统包括主节点和从节点，所述方法包括：

所述主节点预执行多个交易，得到各个交易的预执行读写集；根据多个交易的预执行读写集对多个交易进行分组，得到多个交易组，生成各个交易组的预执行读写集；将分组结果和各个交易组的预执行读写集发送给从节点；

所述从节点根据所述多个交易组的预执行读写集对分组结果进行验证；在验证通过的情况下根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

2. 根据权利要求 1 所述的方法，所述基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证包括：在执行每个交易的过程中，使用交易的执行读写集对该交易所属的交易组的预执行读写集进行验证。

3. 根据权利要求 1 或 2 所述的方法，所述基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证包括：在完成对所述多个交易的并行执行之后，根据各个交易组中包括的交易的执行读写集生成各个交易组的执行读写集，基于各个交易组的执行读写集对各个交易组的预执行读写集进行验证。

4. 根据权利要求 1-3 任一项所述的方法，所述从节点根据所述多个交易组的预执行读写集对分组结果进行验证包括：所述从节点根据所述多个交易组的预执行读写集验证所述多个交易组中的交易组之间是否访问相同变量。

5. 根据权利要求 1-3 任一项所述的方法，所述主节点预执行多个交易包括：所述主节点基于预执行状态集预执行所述多个交易，所述方法还包括：所述主节点在预执行完每个交易之后，串行地对每个交易进行如下处理：确定所述交易的预执行读写集是否与所述预执行状态集存在冲突，其中，在对于预执行完的第一交易确定不存在冲突的情况下，基于所述第一交易的预执行读写集更新所述预执行状态集，将所述第一交易顺序记录到预执行交易集合中；其中，各个交易组中的交易排列顺序基于各个交易组中的交易在所述预执行交易集合中的排列顺序确定。

6. 根据权利要求 5 所述的方法，还包括：所述主节点将所述多个交易在所述预执行交易集合中的排列顺序发送给所述从节点，所述从节点在验证不通过的情况下，根据所述多个交易在所述预执行交易集合中的排列顺序串行执行所述多个交易。

7. 根据权利要求 5 或 6 所述的方法，其中，所述主节点基于预执行状态集预执行所述多个交易包括，所述主节点在预执行任一交易中读取第一变量时，确定所述预执行状态集中是否存储有所述第一变量的值，在确定所述预执行状态集中未存储所述第一变量的值的情况下，从状态数据库读取所述第一变量的值。

8. 根据权利要求 5 或 6 所述的方法，其中，所述确定所述交易的预执行读集是否与所述预执行状态集存在冲突包括，确定所述预执行状态集中是否包括所述交易的预执行读集中的第二变量，在确定所述预执行状态集中包括所述第二变量的情况下，确定所述预执行状态集中的第二变量的值与所述预执行读集中的第二变量的值是否一致，如果不一致，则确定所述交易的预执行读集与所述预执行状态集存在冲突。

9. 一种在区块链系统中执行交易的方法，所述区块链系统包括主节点和从节点，所述方法由所述从节点执行，包括：

从所述主节点接收对多个交易进行分组得到的分组结果和各个交易组的预执行读写集，其中，所述交易组的预执行读写集基于所述交易组中包括的各个交易的预执行读写集生成；

根据所述多个交易组的预执行读写集对分组结果进行验证；

在验证通过的情况下根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集；

基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

10. 根据权利要求 9 所述的方法，所述基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证包括：在执行每个交易的过程中，使用交易的执行读集对该交易所属的交易组的预执行读集进行验证。

11. 根据权利要求 10 所述的方法，所述基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证还包括：在完成对所述多个交易的并行执行之后，根据各个交易组中包括的交易的执行读写集得到各个交易组的执行写集，基于各个交易组的执行写集对各个交易组的预执行写集进行验证。

12. 根据权利要求 9-11 任一项所述的方法，所述根据所述多个交易组的预执行读写集对分组结果进行验证包括：根据所述多个交易组的预执行读写集验证所述多个交易组中的交易组之间是否访问相同变量。

13. 一种区块链系统的从节点，包括：

接收单元，用于从所述区块链系统的主节点接收对多个交易进行分组得到的分组

结果和各个交易组的预执行读写集，其中，所述交易组的预执行读写集基于所述交易组中包括的各个交易的预执行读写集生成；

验证单元，用于根据所述多个交易组的预执行读写集对分组结果进行验证；

执行单元，用于在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集；

所述验证单元还用于，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

14. 一种区块链系统，包括主节点和从节点，

所述主节点用于：预执行多个交易，得到各个交易的预执行读写集；根据多个交易的预执行读写集对多个交易进行分组，得到多个交易组，生成各个交易组的预执行读写集；将分组结果和各个交易组的预执行读写集发送给从节点；

所述从节点用于：根据所述多个交易组的预执行读写集对分组结果进行验证；在验证通过的情况中根据分组结果并行执行所述多个交易，得到每个交易组包括的交易的执行读写集，基于每个交易组包括的交易的执行读写集对所述交易组的预执行读写集进行验证。

15. 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机中执行时，令计算机执行权利要求 9-12 中任一项的所述的方法。

16. 一种区块链节点，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 9-12 中任一项所述的方法。

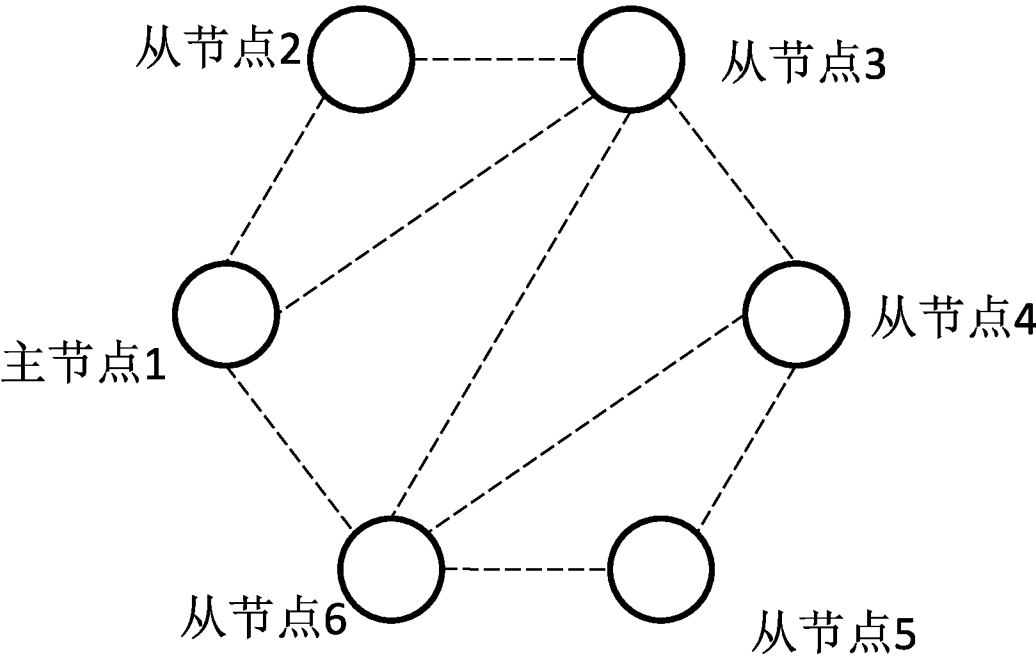


图 1

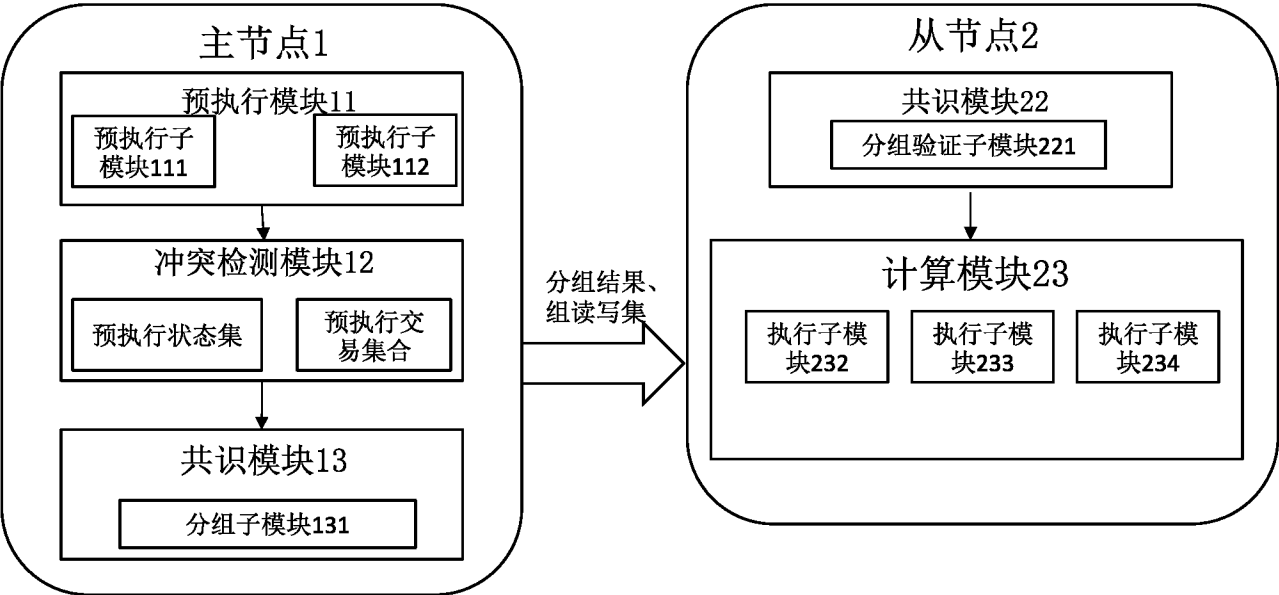


图 2

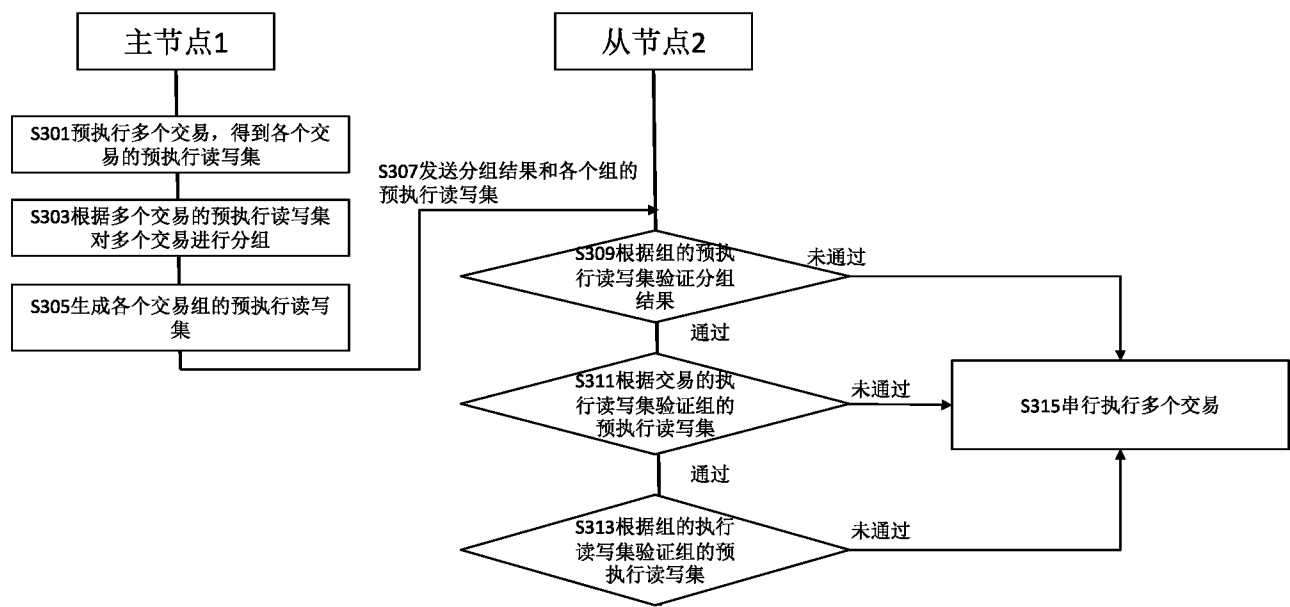


图 3

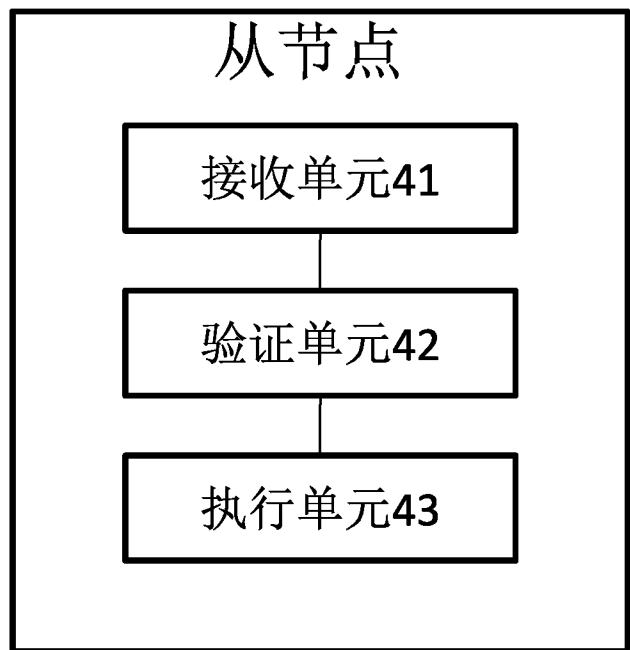


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/135304

A. CLASSIFICATION OF SUBJECT MATTER

G06F16/27(2019.01);G06Q40/04(2012.01)

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)

IPC: 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)

DWPI, ENTXTC, CNTXT, CNKI, IEEE: 区块链, 主节点, 从节点, 验证, 读写集, 预执行, 分组, 比较, 变量, 相同, 并行, 串行; blockchain, master node, slave node, verify, read-write set, pre-execute, packet, compar+, variable, same, parallel, serial

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115098594 A (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) 23 September 2022 (2022-09-23) claims 1-16	1-16
Y	CN 113743941 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 03 December 2021 (2021-12-03) claims 1-25, and description, paragraphs [0018]-[0082], and figures 1-7	1-16
Y	CN 113743949 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 03 December 2021 (2021-12-03) claims 1-25, and description, paragraphs [0017]-[0103], and figures 1-7	1-16
A	CN 113743950 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 03 December 2021 (2021-12-03) entire document	1-16
A	US 2019190719 A1 (KONINKLIJKE KPN N.V.) 20 June 2019 (2019-06-20) entire document	1-16



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

“D” document cited by the applicant in the international application

“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

10 March 2023

Date of mailing of the international search report

15 March 2023

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/135304

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115098594	A	23 September 2022	None			
CN	113743941	A	03 December 2021	None			
CN	113743949	A	03 December 2021	None			
CN	113743950	A	03 December 2021	None			
US	2019190719	A1	20 June 2019	EP	3499789	A1	19 June 2019
				EP	3499789	B1	30 June 2021
				US	11139979	B2	05 October 2021

国际检索报告

国际申请号

PCT/CN2022/135304

A. 主题的分类

G06F16/27(2019.01); G06Q40/04(2012.01);

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)

IPC: 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))

DWPI, ENTXT, CNTXT, CNKI, IEEE: 区块链, 主节点, 从节点, 验证, 读写集, 预执行, 分组, 比较, 变量, 相同, 并行, 串行; blockchain, master node, slave node, verify, read-write set, pre-execute, packet, compare, variable, same, parallel, serial

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 115098594 A (蚂蚁区块链科技(上海)有限公司) 2022年9月23日 (2022 - 09 - 23) 权利要求1-16	1-16
Y	CN 113743941 A (支付宝(杭州)信息技术有限公司) 2021年12月3日 (2021 - 12 - 03) 权利要求1-25, 说明书第[0018]-[0082]段, 图1-7	1-16
Y	CN 113743949 A (支付宝(杭州)信息技术有限公司) 2021年12月3日 (2021 - 12 - 03) 权利要求1-25, 说明书第[0017]-[0103]段, 图1-7	1-16
A	CN 113743950 A (支付宝(杭州)信息技术有限公司) 2021年12月3日 (2021 - 12 - 03) 全文	1-16
A	US 2019190719 A1 (KONINKLIJKE KPN N.V.) 2019年6月20日 (2019 - 06 - 20) 全文	1-16

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2023年3月10日

国际检索报告邮寄日期

2023年3月15日

ISA/CN的名称和邮寄地址

中国国家知识产权局

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

李敏

电话号码 (+86) 010-53961526

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/135304

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	115098594	A	2022年9月23日	无			
CN	113743941	A	2021年12月3日	无			
CN	113743949	A	2021年12月3日	无			
CN	113743950	A	2021年12月3日	无			
US	2019190719	A1	2019年6月20日	EP	3499789	A1	2019年6月19日
				EP	3499789	B1	2021年6月30日
				US	11139979	B2	2021年10月5日