

(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 9 月 10 日 (10.09.2020)



(10) 国际公布号
WO 2020/177547 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2020/076079

(22) 国际申请日: 2020 年 2 月 20 日 (20.02.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910163272.6 2019年3月5日 (05.03.2019) 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)。

(72) 发明人: 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)。 莫楠(MO, Nan); 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)。 陈宇杰(CHEN, Yujie); 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)。 陈宇(CHEN, 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)。 白兴强(BAI, Xingqiang); 中国广东省深圳市前海深港

(54) Title: BLOCKCHAIN SYSTEM AND TRANSACTION PROCESSING METHOD FOR BLOCKCHAIN SYSTEM

(54) 发明名称: 一种区块链系统及区块链系统的交易处理方法

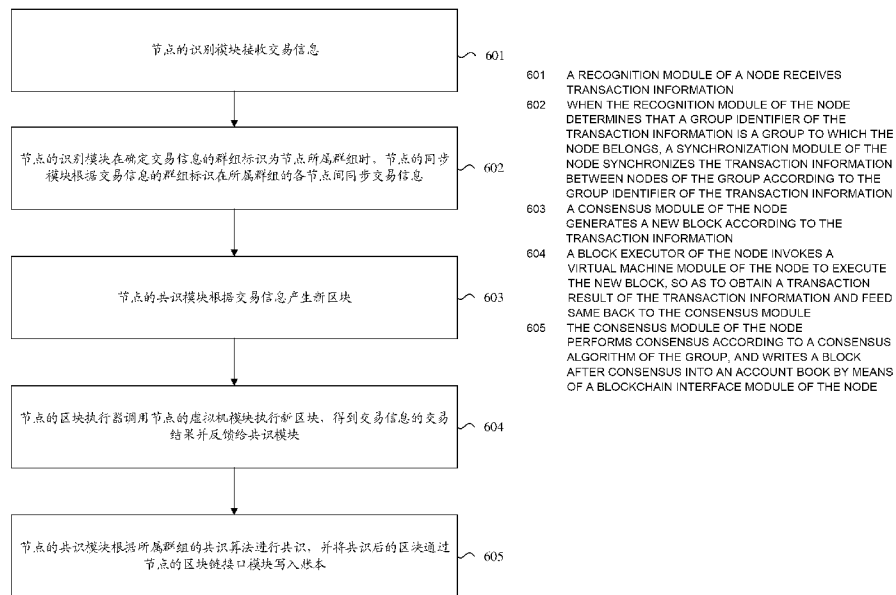


图 6

(57) Abstract: Disclosed are a blockchain system and a transaction processing method for a blockchain system. The method comprises: a node receiving transaction information; and when the node determines that a group identifier of the transaction information is a group to which the node belongs, processing the transaction information according to a consensus algorithm of the group. The technical solution is used for improving the security and privacy of a blockchain transaction.

(57) 摘要: 本发明公开了一种区块链系统及区块链系统的交易处理方法，该方法包括节点接收交易信息，节点在确定交易信息的群组标识为节点所属群组时，根据所属群组的共识算法处理交易信息。该技术方案用以提高区块链交易的安全性和隐私性。

合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 刘明臻(LIU, Mingzhen); 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)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区宝盛南路1号院20号楼8层101-01, Beijing 100192 (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))。

一种区块链系统及区块链系统的交易处理方法

相关申请的交叉引用

本申请要求在2019年03月05日提交中国专利局、申请号为201910163272.6、
申请名称为“一种区块链系统及区块链系统的交易处理方法”的中国专利申
5 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

本发明实施例属于金融科技（Fintech）领域，尤其涉及一种区块链（Block
chain）系统及区块链系统的交易处理方法。

背景技术

区块链系统是科技金融领域常用的一种分布式的系统架构，随着越来越
多企业级应用引入区块链技术，隐私性、可扩展性以及高性能逐渐成为区块
链技术的关键挑战。现有的公有链，如比特币、以太坊等，隐私性差；现有
15 的主流联盟链技术，如超级记账本（HyperLedger），引入多通道技术，可以很
好地支持私有交易，但 Order 节点仍然可以看到所有通道的交易，因此超级记
账本在隐私性方面同样存在瑕疵，且在技术实现上复杂度比较高。摩根的
Quorum 也是支持私有交易的联盟链之一，它是在以太坊基础上开发实现的，
可以方便地支持私有交易和私有合约，但不共识私有交易，仅将私有交易的
20 哈希写入公共账本进行共识，因此有被篡改的风险。

发明内容

本发明实施例提供一种区块链系统及区块链系统的交易处理方法，用以
提高区块链交易的安全性和隐私性。

25 本发明实施例提供的一种区块链系统，适用于联盟链，所述联盟链包括
多个群组，每个群组包括多个节点；

针对任一群组，所述群组设置有共识算法和账本，独立运行所述群组的交易信息；

针对任一节点，所述节点仅用于处理所属群组的交易信息从而实现群组间数据隔离。

5 上述技术方案中，区块链系统适用于联盟链，且该联盟链包括多个群组，每个群组包括多个节点，每个群组设置有共识算法和账本，进一步的，节点仅用于处理其所属群组的交易信息，从而实现每个群组独立运行群组内部的交易信息，做到各群组之间数据隔离，保障交易的隐私性。且各群组独立运行共识算法，从而保障群组内的交易的安全性。

10 可选的，所述节点属于多个不同的群组。

上述技术方案中，同一个节点可以属于多个不同的群组，即多个群组可以共用一个节点，降低联合组网的建链复杂度和运维复杂度。

可选的，所述各群组中至少有两个群组的共识算法不同。

15 上述技术方案中，根据业务性能和安全性能的需求，在不同群组运行不同的共识算法，针对不同群组对业务性能和安全性能需求的高低，可以采用不同的共识算法，在保障群组内交易的安全性和隐私性前提下，降低联合组网的建链复杂度和运维复杂度。

可选的，所述节点包括共识模块、区块执行器和虚拟机模块；

20 所述共识模块，用于针对所属群组的交易信息产生新区块并使用所述共识算法对所述新区块进行共识；

所述区块执行器，用于调用所述虚拟机模块执行所述新区块并将所述虚拟机模块执行的交易结果反馈给所述共识模块；

所述虚拟机模块，用于执行所述新区块的交易信息得到交易结果。

25 上述技术方案中，每个节点包括共识模块、区块执行器和虚拟机模块，共识模块用于针对所属群组的交易信息产生新区块以及对新区块进行共识，区块执行器用于执行新区块并将执行结果反馈至共识模块，虚拟机模块用于执行新区块的交易信息。将节点划分为多个模块，各模块具有对应的功能，

通过多个模块之间的交互实现区块链系统的易扩展性，便于运维人员的维护。
此外，可以通过共识模块，实现不同群组运行不同的共识算法。

可选的，所述共识模块包括打包线程模块和共识线程模块；

所述打包线程模块用于将所属群组的交易信息打包为新区块；

5 所述共识线程模块用于将所述新区块在所属群组内按照所述共识算法进行共识。

上述技术方案中，共识模块包括打包线程模块和共识线程模块，实现节点所属群组的交易信息的打包线程和共识线程的分离，从而达到共识模块的易扩展性。

10 可选的，所述节点还包括区块链接口模块；

所述区块链接口模块为所述账本的访问接口。

上述技术方案中，节点包括区块链接口模块，区块链接口模块用于访问账本，从而实现区块数据、区块信息、交易数据、交易信息以及交易执行结果的存取。

15 可选的，所述节点还包括同步模块；

所述同步模块用于在所属群组内进行交易信息的同步和账本的同步。

上述技术方案中，节点还包括同步模块，同步模块具有两种功能，分别是所属群组交易信息的同步和账本的同步，同步模块用于群组交易信息的同步，可以使该交易信息到达所属群组内所有的共识节点，保障出块节点基于最新交易产生新区块；同步模块用于群组账本的同步，可以使所属群组内节点的账本保持一致。

20 可选的，所述节点还包括：识别模块；

所述识别模块用于根据交易信息中的群组标识，确定所述交易信息为所属群组的交易信息。

25 上述技术方案中，节点在接收到交易信息后，节点的识别模块根据交易信息中的群组标识，确定该交易所属群组，从而使得该笔交易只在节点所属群组中进行，保障群组内交易的隐私性。

相应的，本发明实施例还提供了一种区块链系统的交易处理方法，适用于设置有多群组的联盟链；

所述方法包括：

节点接收交易信息；所述节点为群组中的节点；

5 所述节点在确定所述交易信息的群组标识为所述节点所属群组时，根据所属群组的共识算法处理所述交易信息。

10 上述技术方案中，节点在接收到交易信息后，先确定该交易信息对应的群组，并在确定该交易信息对应的群组为该节点所属群组后，根据该节点所属群组对应的共识算法，对该交易在所属群组内进行处理，从而实现群组内交易信息的隐私性，同时对该交易在所属群组内运行共识算法，从而实现区块链系统交易的安全性。

可选的，所述节点根据所属群组的共识算法处理所述交易信息，包括：

所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息。

15 上述技术方案中，节点的同步模块根据群组标识在所属群组的各节点间同步交易信息，可以使该交易信息到达所属群组内所有的共识节点，保障出块节点基于最新交易产生新区块，同时可以保障该交易信息的安全性。

可选的，所述节点为出块节点；

20 所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息之后，还包括：

所述节点的共识模块根据所述交易信息产生新区块；

所述节点的区块执行器调用所述节点的虚拟机模块执行所述新区块，得到所述交易信息的交易结果并反馈给所述共识模块；

25 所述节点的共识模块根据所属群组的共识算法进行共识，并将共识后的区块通过所述节点的区块链接口模块写入账本。

上述技术方案中，节点的共识模块根据交易信息产生新区块，节点的区块执行器调用节点的虚拟机模块执行新区块，并将交易信息的交易结果反馈

至共识模块，共识模块根据所属群组的共识算法进行共识，并将共识后的区块通过节点的区块链接口模块写入账本，节点通过不同模块实现交易信息的处理，各模块具有对应的功能，通过多个模块之间的交互实现区块链系统的易扩展性，便于运维人员的维护。此外，可以通过共识模块，实现不同群组运行不同的共识算法。

可选的，还包括：

所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间进行账本同步。

上述技术方案中，节点的同步模块根据交易信息的群组标识在所属群组的各节点间进行账本同步，以使所属群组内节点的账本保持一致，且账本同步不会同步至其他群组的节点，保障区块链交易的隐私性。

可选的，所述同步模块根据所述交易信息的群组标识在所属群组的各节点间进行账本同步，包括：

所述节点的同步模块向所属群组的不同节点发送不同的同步请求，从而完成所述节点的账本同步。

上述技术方案中，节点的同步模块在所属群组内与其他节点进行账本同步时，可以向不同的被请求节点发送不同的同步请求，不会出现该节点向该节点所属群组的一个被请求节点发送同步请求，造成被请求节点的同步压力过大，使得整个群组内节点的负载不均衡。

相应的，本发明实施例还提供了一种计算设备，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行上述区块链系统的交易处理方法。

相应的，本发明实施例还提供了一种计算机可读非易失性存储介质，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述区块链系统的交易处理方法。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，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，对于本领域的普通技术人员来讲，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他的附图。

图 1 为本发明实施例提供的一种区块链系统的示意图；

图 2 为本发明实施例提供的一种区块链系统适用于多机构联合组网的场景；

图 3 为本发明实施例提供的一种区块链系统适用于多链并行的场景；

图 4 为本发明实施例提供的一种区块链系统的节点的结构示意图；

图 5 为本发明实施例提供的一种区块链系统的交易处理方法的流程；

图 6 为本发明实施例提供的另一种区块链系统的交易处理方法的流程；

图 7 为本发明实施例提供的另一种区块链系统的交易处理方法的流程；

图 8 为本发明实施例提供的一种计算设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

图 1 示例性的示出了本发明实施例提供一种区块链系统，该区块链系统适用于联盟链，该联盟链包括多个群组，每个群组包括多个节点。针对任一群组，群组设置有共识算法和账本，独立运行群组的交易信息，针对任一节点，节点仅用于处理所属群组的交易信息从而实现群组间数据隔离。也就是说，群组内独立运行交易信息和共识算法，各群组之间数据相互隔离，保障群组内数据的隐私性。

根据业务性能和安全性能的需求，在不同群组运行不同的共识算法，各群组中至少有两个群组的共识算法不同，在保障群组内交易的安全性和隐私性前提下，降低联合组网的建链复杂度和运维复杂度。示例性的，安全性要求高的群组可使用 PBFT（Practical Byzantine Fault Tolerance，实用拜占庭容错）共识算法，性能要求高、安全性要求不高的群组可使用 Raft（Replication and Fault Tolerant，副本容错）共识算法。

需要说明的是，每个群组不仅可以包括多个节点，一个节点也可以属于多个不同的群组，即多个群组可以共用一个节点。节点可以理解为，区块链网络中的每一个参与者，节点参与区块链网络组建和数据交换，在区块链网络中，一个节点是指一个具有唯一身份的参与者，该节点具有一份完整的账本拷贝，具有参与区块链网络共识和账本维护的能力。

本发明实施例提供的一种区块链系统可以适用于多机构联合组网的场景，多机构联合组网建链是区块链系统中比较常见的场景之一，如联合贷、多机构联合签名等。具体的，参照图 2 举例说明，本区块链系统中设有 4 个机构，分别为机构 A、机构 B、机构 C、机构 D，其中，机构 B、机构 C、机构 D 中的节点分别与机构 A 中的节点组网，机构 A 启动三个群组，将机构 B 的节点 B1、节点 B2 加入至群组 1，将机构 C 的节点 C1、节点 C2、节点 C3 加入至群组 2，将机构 D 的节点 D1、节点 D2 加入至群组 3，即可完成多机构间联合组网。该技术方案中，机构 A 的运维人员只需要维护一套外网 IP（Internet Protocol，网络之间互连的协议）接口，大大降低了联合组网的建链复杂度和运维复杂度。此外，由于多群组架构中，群组间数据隔离，因此也保障了群组数据和交易的隐私性。

本发明实施例提供的一种区块链系统可以适用于多链并行的场景，具体的，参照图 3 举例说明，若企业内部有 N （ N 大于等于 2）个业务，企业的运维人员可以将 N 个业务部署在同一条链的不同群组中，由于群组间数据隔离，群组间多链并行，在降低运维成本的同时保证了群组间数据的隔离性。

可选的，节点包括共识（Consensus）模块、区块执行器（BlockVerifier）

和虚拟机模块。

其中，共识模块用于针对所属群组的交易信息产生新区块并使用共识算法对新区块进行共识，共识模块可以针对不同群组采用 PBFT、Raft 等多种共识算法，且每个群组可运行不同的共识算法，群组间的共识不相互影响。区块执行器用于调用虚拟机模块执行新区块并将虚拟机模块执行的交易结果反馈给共识模块。虚拟机模块用于执行新区块的交易信息得到交易结果。

具体的，共识模块可以分为打包（Sealer）线程模块和共识（Engine）线程模块，打包线程模块用于将所属群组的交易信息打包为新区块，共识线程模块用于将新区块在所属群组内按照共识算法进行共识。

本发明实施例中，节点还可以包括区块链接口模块，区块链接口模块为账本的访问接口，用于实现区块数据、区块信息、交易数据、交易信息以及交易执行结果的存取。

节点还包括同步模块，同步模块用于在所属群组内进行交易信息的同步和账本的同步。同步模块用于交易信息的同步，将节点接收到的交易信息广播到该节点所在群组的其他共识节点，从而保证切换出块节点时，新的出块节点能基于最新交易产生新区块；同步模块用于账本的同步，用来解决性能不同机器间区块高度不一致的问题，同步模块维护着同一个群组内所有节点的区块高度信息，当本节点区块高度落后于其他节点时，会主动发起区块下载请求，从而保证本节点区块高度与其他节点一致。

节点还包括识别模块，识别模块用于根据交易信息中的群组标识，确定交易信息为所属群组的交易信息。节点在接收到交易信息后，节点的识别模块根据交易信息中的群组标识，确定该交易所属群组，从而使得该笔交易只在节点所属群组中进行，保障群组内交易的隐私性。

上述区块链系统中，针对每个节点，可以将该节点划分为两层，即：网络层和群组层，网络层主要负责接收和发送数据，群组层主要负责处理群组的交易，并将交易执行结果上链。如图 4 所示，网络层包括识别模块，群组层包括存储模块、虚拟机模块、交易池（TxPool）、区块链接口模块、区块执

行器、同步模块和共识模块。

结合图 4 所示的节点，对节点中各模块做具体说明：

一、网络层

识别模块主要用于接收交易信息，并将交易信息发送至群组层，以使群组层对该交易信息进行处理。结合图 2 举例来说，节点 A1 同属于群组 1 和群组 2，节点 A1 接收客户端发送的交易信息，并根据接收到的交易信息确定该交易信息中的群组标识，若该交易信息中的群组标识为群组 1，则节点 A1 可以确定该交易信息需要在群组 1 中进行处理。处理方式在下述实施例中详细阐述。

二、群组层

此处，为了方便运维人员管理以及提高区块链系统的扩展性能，可以将群组层划分为核心层、接口层和调度层。

(1) 核心层包括存储模块和虚拟机模块。

存储模块可以包括 storage 和 state 两部分，storage 采用表式存储结构，如 AMDB、LevelDB，主要用来存储区块信息、系统表等；state 主要存储交易执行结果，包括 mpt state 和 storage state，mpt state 是一棵世界状态树，可追溯任何一笔交易的历史信息，storage state 存储交易执行后的当前状态，不保存历史信息。需要说明的是，存储模块存储有本节点的账本白名单，该账本白名单包括本节点所属群组中的所有节点信息，用于在节点之间交易信息同步或账本同步时，只在群组内通信，保障了各群组通信的隐私性。

虚拟机模块主要用于执行交易。其中，虚拟机模块可以为以太坊虚拟机。

(2) 接口层包括交易池、区块链接口模块和区块执行器。

交易池主要用于从客户端或其他节点接收交易信息，并将验证合法的交易存放到交易池队列中，供调度层打包区块时使用。

区块链接口模块是调度层访问核心层的统一接口，区块数据、区块信息、交易数据、交易信息以及交易执行结果的存取均是通过区块链接口模块完成的。

区块执行器用于调用虚拟机模块执行新区块并将虚拟机模块执行的交易结果反馈给共识模块。

(3) 调度层主要包括同步模块和共识模块。

同步模块主要负责交易信息同步和区块同步，区块同步即账本同步。其中，交易信息同步会将节点接收到的所有的交易信息广播到节点所属群组的其他共识节点，从而保证切换出块节点时，新的出块节点能基于最新交易产生新区块；区块同步则用来解决性能不同机器间区块高度不一致的问题，同步模块维护着所有节点的区块高度信息，当本节点区块高度落后于其他节点时，会主动发起区块下载请求，从而保证本节点区块高度与其他节点一致。

共识模块分为打包线程模块和共识线程模块，打包线程模块负责从交易池中取出交易，打包成区块；共识线程模块负责执行新区块、运行共识算法，将所有达成共识的区块通过区块链接口模块写入存储模块进行存储。

上述技术方案中，区块链系统适用于联盟链，且该联盟链包括多个群组，每个群组包括多个节点，每个群组设置有共识算法和账本，进一步的，节点仅用于处理其所属群组的交易信息，从而实现每个群组独立运行群组内部的交易信息，做到各群组之间数据隔离，保障交易的隐私性。且各群组独立运行共识算法，从而保障群组内的交易的安全性。

基于上述描述，图 5 示例性的示出了本发明实施例提供的一种区块链系统的交易处理方法的流程，该流程适用于设置有多群组的联盟链。

如图 5 所示，该流程具体包括：

步骤 501，节点接收交易信息。

节点和客户端通过链上链下协议连接，节点可以接收客户端的交易信息，此处，节点可以为上述区块链系统群组中的节点。具体的，可以为节点的识别模块接收客户端发送的交易信息。

步骤 502，所述节点在确定所述交易信息的群组标识为所述节点所属群组时，根据所属群组的共识算法处理所述交易信息。

本发明实施例中，节点的识别模块在接收到交易信息后，对交易信息进

行解析，可以解析出如下信息：

群组标识：群组编号，如 1-127，用于标识客户端所要访问的群组。

调用接口：标识客户端访问的节点接口名称，如：执行交易、获取区块高度、获取指定交易回执等。

5 参数信息：发送给调用接口的对应参数，如：获取交易信息时，参数信息包括交易哈希；获取指定区块时，参数信息包括区块高度等；执行交易时，参数信息包括交易的具体内容。

10 其中，节点可以包含于多个群组，节点识别模块可以根据群组标识确定出节点接收到的交易信息应在哪一个群组中进行处理。结合图 2 举例来说，节点 A1 同属于群组 1 和群组 2，节点 A1 接收客户端发送的交易信息，并根据接收到的交易信息确定该交易信息中的群组标识，若该交易信息中的群组标识为群组 1，则节点 A1 可以确定该交易信息需要在群组 1 中进行处理。

15 节点的识别模块根据解析出的信息，确定在群组中对交易信息进行处理，具体的，节点的识别模块可以在对交易信息验证合法后，将交易信息存储在节点的交易池中。

20 验证交易信息的合法性可以如以下参数：（1）节点的交易池中的交易队列是否已满，若交易队列已满，则确定该交易信息未通过验证。（2）交易信息是否重复，客户端发送的交易哈希不能与交易池内已有哈希相同，也不能与区块链上已有交易哈希相同，若重复，则确定该交易信息未通过验证。（3）交易签名必须有效，若交易签名无效，则确定该交易信息未通过验证。

25 上述例子中，节点 A1 可以确定该交易信息需要在群组 1 中进行处理，则节点 A1 将交易信息存储在节点 A1 的交易池中。为保障切换出块节点时，新的出块节点能基于最新交易产生新区块，则需要节点的同步模块根据交易信息的群组标识在所属群组的各节点间同步该交易信息，也就是节点 A1 的同步模块根据交易信息的群组标识在群组 1 的各节点间同步该交易信息。

需要说明的是，每个节点的存储模块中都存储有本节点的账本白名单，该账本白名单包括本节点所属群组中的所有节点信息，用于在节点之间交易

信息同步或账本同步时，只在群组内通信，保障了各群组通信的隐私性。图 2 示出的架构图中，节点 A1 将交易信息存储在节点 A1 的交易池中，节点 A1 获取本节点存储的关于群组 1 的账本白名单，根据该账本白名单可以确定出节点 A1 的同步模块可以将交易池中的交易信息同步给节点 A3、节点 B1、节点 B2。也就是说，节点 A1 的同步模块不会将交易信息同步给群组 2 或群组 3 中的节点。

节点的同步模块根据交易信息的群组标识在所属群组的各节点间同步交易信息之后，节点所属群组内的所有节点的交易池中都有该交易信息，节点的共识模块将交易信息打包为新区块。此处，接收交易信息的节点和将交易信息打包为新区块的节点可以为同一个，也可以不为同一个。进一步的，可以将上述将交易信息打包为新区块的节点理解为出块节点。

节点的区块执行器调用节点的虚拟机模块执行新区块，得到交易信息的交易结果并反馈给节点的共识模块，节点的共识模块根据所属群组的共识算法进行共识，并将共识后的区块通过节点的区块链接口模块写入账本。

本发明实施例中，节点的共识模块包括节点的打包线程模块和节点的共识线程模块，节点的打包线程模块会尝试从节点的交易池内加载交易，并打包成新区块，节点的打包线程模块的主要工作包括：

产生新空块：通过区块链接口模块获取当前最高块，并基于最高块产生新空块，具体的，将新区块父哈希置为最高块哈希，时间戳置为当前时间，区块交易清空；

取出交易信息：从节点的交易池内取出交易信息，并将取到的交易信息插入到上述新区块中；

组装新区块：节点的打包线程模块打包到交易后，将新区块的打包者置为出块节点索引，并根据打包到的交易计算所有交易的 TransactionRoot。

节点的打包线程模块将打包到的新区块发送至节点的共识线程模块，节点的共识线程模块调用节点的区块执行器执行新区块，即节点的区块执行器调用节点的虚拟机模块执行新区块中的交易信息。节点的共识线程模块还会

将新区块广播给节点所属群组内所有其他共识节点，并基于从 P2P（Peer to Peer，对等）网络收到的共识消息包执行共识算法，若区块共识成功，则通过区块链接口模块将新区块写入账本。

本发明实施例提供一种具体的实现方式，可以如图 6 所示。

5 步骤 601，节点的识别模块接收交易信息。

步骤 602，节点的识别模块在确定交易信息的群组标识为节点所属群组时，节点的同步模块根据交易信息的群组标识在所属群组的各节点间同步交易信息。

步骤 603，节点的共识模块根据交易信息产生新区块。

10 步骤 604，节点的区块执行器调用节点的虚拟机模块执行新区块，得到交易信息的交易结果并反馈给共识模块。

步骤 605，节点的共识模块根据所属群组的共识算法进行共识，并将共识后的区块通过节点的区块链接口模块写入账本。

由于本实施例的具体实现方式已在其他实施例中描述，在此不作赘述。

15 本发明实施例中，节点的同步模块不仅用于根据交易信息的群组标识将交易池中的交易信息广播至所属群组的其他节点，还用于根据交易信息的群组标识在所属群组的各节点间进行账本同步。当本节点区块落后于所属群组的其他节点时，本节点的同步模块会主动向所属群组内其他节点下载落后的区块，并将其通过区块链接口模块写入本地数据库；当本节点收到所属群组
20 内其他节点的区块下载请求时，本节点通过区块链接口模块取出所属群组内其他节点请求下载的区块，并通过 P2P 网络发送给请求节点；此外，当本节点收到其他群组节点（非所属群组的节点）的区块下载请求时，不会执行任何操作，保障了群组数据的安全性。

进一步的，节点的同步模块向所属群组的不同节点发送不同的同步请求，
25 从而完成节点的账本同步。也就是说，当本节点区块落后于所属群组的其他节点时，可以同时向所属群组的其他节点发送下载区块的请求，做到负载均衡，不会出现本节点向该节点所属群组的一个被请求节点发送同步请求，造

成被请求节点的同步压力过大，使得整个群组内节点的负载不均衡。

示例性的，如图 2 所示的架构中，群组 3 中包括节点 A4、节点 A5、节点 D1、节点 D2，假设节点 A4 的存储模块中的区块为 500 个，节点 A5、节点 D1、节点 D2 的存储模块中的区块分别为 800 个，则节点 A4 的同步模块
5 分别向节点 A5、节点 D1、节点 D2 发送同步请求，示例性的，A4 的同步模块向节点 A5 获取 100 个区块，向节点 D1 获取 100 个区块，向节点 D2 获取 100 个区块，从而完成节点的账本同步。

为了更好的解释本发明实施例，下面将在具体的实施场景下描述该区块链系统的交易处理方法，如图 7 所示，具体如下：

10 客户端通过链上链下协议，与节点建立 SSL (Secure Sockets Layer, 安全套接层) 连接，并将向群组 i 发送的交易封装在数据包中发送给群组 i 中的节点，节点的监听服务器收到客户端的数据包后，解析数据包，并将其转发到远程调用模块，远程调用模块解析客户端发送的请求，此处，节点的监听服务器和节点的远程调用模块二者可以理解为节点的识别模块；远程调用模块
15 根据解析的群组信息、调用接口以及参数信息，调用节点相应接口，并将执行后的结果返回给客户端。群组内的交易执行具体如下。

远程调用模块接收到交易信息，根据交易信息中附带的群组标识(群组 i)，获取群组 i 的交易池实例，并在确定交易信息验证合法后，将交易信息插入交易池，节点将交易池中的交易信息进行广播，该交易信息只会广播给群组 i
20 的所有节点，保证客户端发送的交易可以到达所有共识节点的同时，保障了交易的隐私性。出块节点的共识模块的打包线程模块会尝试从交易池内加载交易，并打包成新区块，打包线程模块打包到的新区块将提供给共识模块的共识线程模块，共识线程模块调用区块执行器执行新区块，将新区块广播给所有其他共识节点，并基于从 P2P 网络收到的共识消息包执行共识算法，若
25 区块共识成功，则通过区块链接口模块将新区块写入区块链。

上述技术方案中，节点在接收到交易信息后，先确定该交易信息对应的群组，并在确定该交易信息对应的群组为该节点所属群组后，根据该节点所

属群组对应的共识算法，对该交易在所属群组内进行处理，从而实现群组内交易信息的隐私性，同时对该交易在所属群组内运行共识算法，从而实现区块链系统交易的安全性。

基于同一发明构思，本发明实施例还提供了一种计算设备，如图 8 所示，
5 包括：

包括处理器 801、存储器 802、收发机 803、总线接口 804，其中处理器 801、存储器 802 与收发机 803 之间通过总线接口 804 连接；

收发机 803，用于在处理器 801 的控制下接收交易信息；

10 处理器 801，用于读取存储器 802 中的程序，执行下列方法：在确定所述交易信息的群组标识为所述节点所属群组时，根据所属群组的共识算法处理所述交易信息；

存储器 802，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

804 总线接口，提供接口，处理器负责管理总线架构和通常的处理。

15 其中，在图 8 中，总线构架可以包括任意数量的互联的总线和桥，具体由处理器 801 代表的一个或多个处理器和存储器 802 代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。

20 处理器 801，还用于：根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息。

处理器 801，还用于：

根据所述交易信息产生新区块；

25 调用所述节点的虚拟机模块执行所述新区块，得到所述交易信息的交易结果并反馈给所述共识模块；

根据所属群组的共识算法进行共识，并将共识后的区块通过所述节点的区块链接口模块写入账本。

处理器 801，还用于：

根据所述交易信息的群组标识在所属群组的各节点间进行账本同步。

收发机 803，还用于：

5 在所述处理器的控制下向所属群组的不同节点发送不同的同步请求，从而完成所述节点的账本同步。

基于同一发明构思，本发明实施例还提供了一种计算机可读非易失性存储介质，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述区块链系统的交易处理方法。

10 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

15 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。

20 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。

25 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，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种区块链系统，其特征在于，适用于联盟链，所述联盟链包括多个群组，每个群组包括多个节点；

5 针对任一群组，所述群组设置有共识算法和账本，独立运行所述群组的交易信息；

针对任一节点，所述节点仅用于处理所属群组的交易信息从而实现群组间数据隔离。

2、如权利要求 1 所述的系统，其特征在于，所述节点属于多个不同的群组。

10 3、如权利要求 1 所述的系统，其特征在于，所述各群组中至少有两个群组的共识算法不同。

4、如权利要求 1 所述的系统，其特征在于，所述节点包括共识模块、区块执行器和虚拟机模块；

15 所述共识模块，用于针对所属群组的交易信息产生新区块并使用所述共识算法对所述新区块进行共识；

所述区块执行器，用于调用所述虚拟机模块执行所述新区块并将所述虚拟机模块执行的交易结果反馈给所述共识模块；

所述虚拟机模块，用于执行所述新区块的交易信息得到交易结果。

20 5、如权利要求 4 所述的系统，其特征在于，所述共识模块包括打包线程模块和共识线程模块；

所述打包线程模块用于将所属群组的交易信息打包为新区块；

所述共识线程模块用于将所述新区块在所属群组内按照所述共识算法进行共识。

25 6、如权利要求 4 所述的系统，其特征在于，所述节点还包括区块链接口模块；

所述区块链接口模块为所述账本的访问接口。

7、如权利要求 6 所述的系统，其特征在于，所述节点还包括同步模块；
所述同步模块用于在所属群组内进行交易信息的同步和账本的同步。

8、如权利要求 1 至 7 任一项所述的系统，其特征在于，所述节点还包括：
识别模块；

5 所述识别模块用于根据交易信息中的群组标识，确定所述交易信息为所属群组的交易信息。

9、一种区块链系统的交易处理方法，其特征在于，适用于设置有多群组的联盟链；

所述方法包括：

10 节点接收交易信息；所述节点为群组中的节点；

所述节点在确定所述交易信息的群组标识为所述节点所属群组时，根据所属群组的共识算法处理所述交易信息。

10、如权利要求 9 所述的方法，其特征在于，所述节点根据所属群组的共识算法处理所述交易信息，包括：

15 所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息。

11、如权利要求 10 所述的方法，其特征在于，所述节点为出块节点；

所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息之后，还包括：

20 所述节点的共识模块根据所述交易信息产生新区块；

所述节点的区块执行器调用所述节点的虚拟机模块执行所述新区块，得到所述交易信息的交易结果并反馈给所述共识模块；

所述节点的共识模块根据所属群组的共识算法进行共识，并将共识后的区块通过所述节点的区块链接口模块写入账本。

25 12、如权利要求 9 所述的方法，其特征在于，还包括：

所述节点的同步模块根据所述交易信息的群组标识在所属群组的各节点间进行账本同步。

13、如权利要求 12 所述的方法，其特征在于，所述同步模块根据所述交易信息的群组标识在所属群组的各节点间进行账本同步，包括：

所述节点的同步模块向所属群组的不同节点发送不同的同步请求，从而完成所述节点的账本同步。

5 14、一种计算设备，其特征在于，包括：

处理器、存储器、收发机、总线接口，其中处理器、存储器与收发机之间通过总线接口连接；

所述收发机，用于在所述处理器的控制下接收交易信息；

所述处理器，用于读取所述存储器中的程序，执行下列方法：

10 在确定所述交易信息的群组标识为所述节点所属群组时，根据所属群组的共识算法处理所述交易信息；

所述存储器，用于存储一个或多个可执行程序，可以存储所述处理器在执行操作时所使用的数据；

所述总线接口，用于提供接口。

15 15、如权利要求 14 所述的计算设备，其特征在于，所述处理器，还用于：根据所述交易信息的群组标识在所属群组的各节点间同步所述交易信息。

16、如权利要求 15 所述的计算设备，其特征在于，所述处理器，还用于：根据所述交易信息产生新区块；

20 调用所述节点的虚拟机模块执行所述新区块，得到所述交易信息的交易结果并反馈给所述共识模块；

根据所属群组的共识算法进行共识，并将共识后的区块通过所述节点的区块链接口模块写入账本。

17、如权利要求 14 所述的计算设备，其特征在于，所述处理器，还用于：根据所述交易信息的群组标识在所属群组的各节点间进行账本同步。

25 18、如权利要求 17 所述的计算设备，其特征在于，所述收发机，还用于：在所述处理器的控制下向所属群组的不同节点发送不同的同步请求，从而完成所述节点的账本同步。

19、一种计算机可读非易失性存储介质，其特征在于，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行如权利要求 9 至 13 任一项所述的方法。

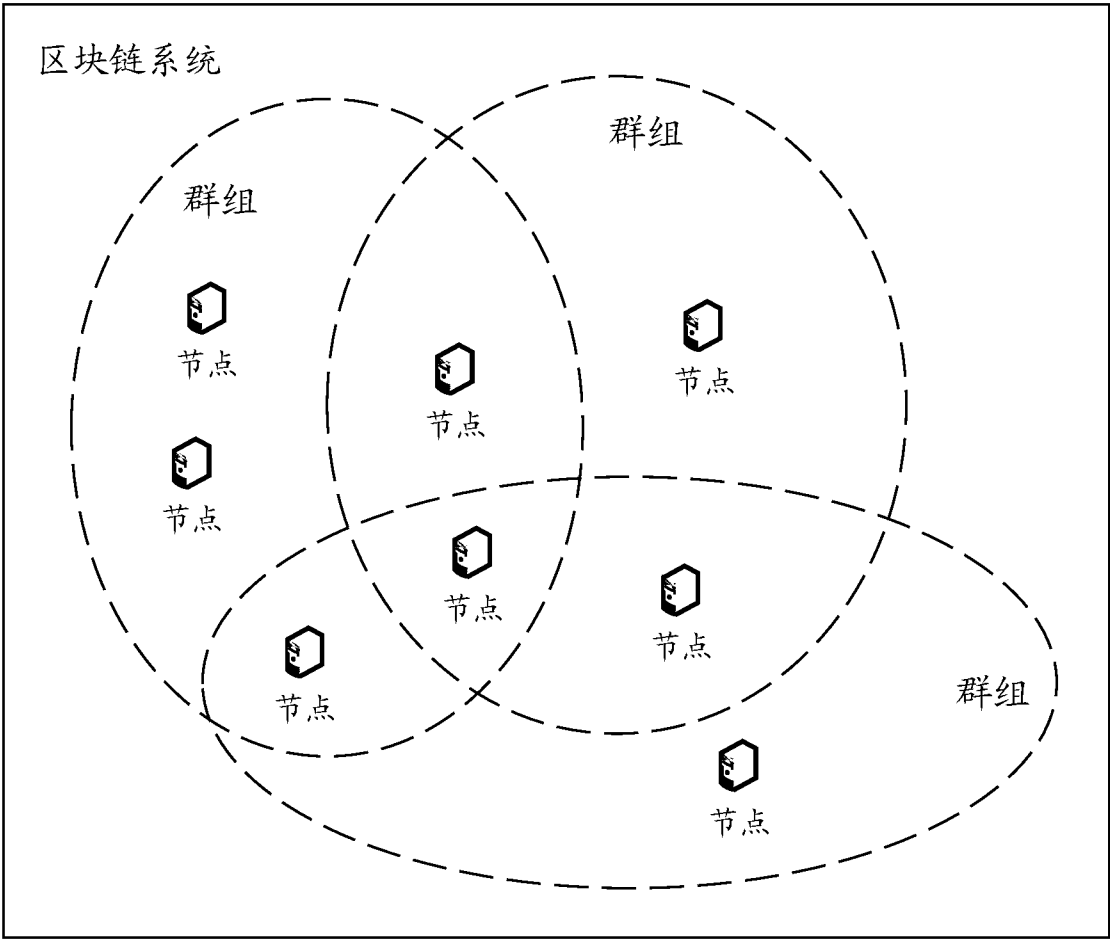


图 1

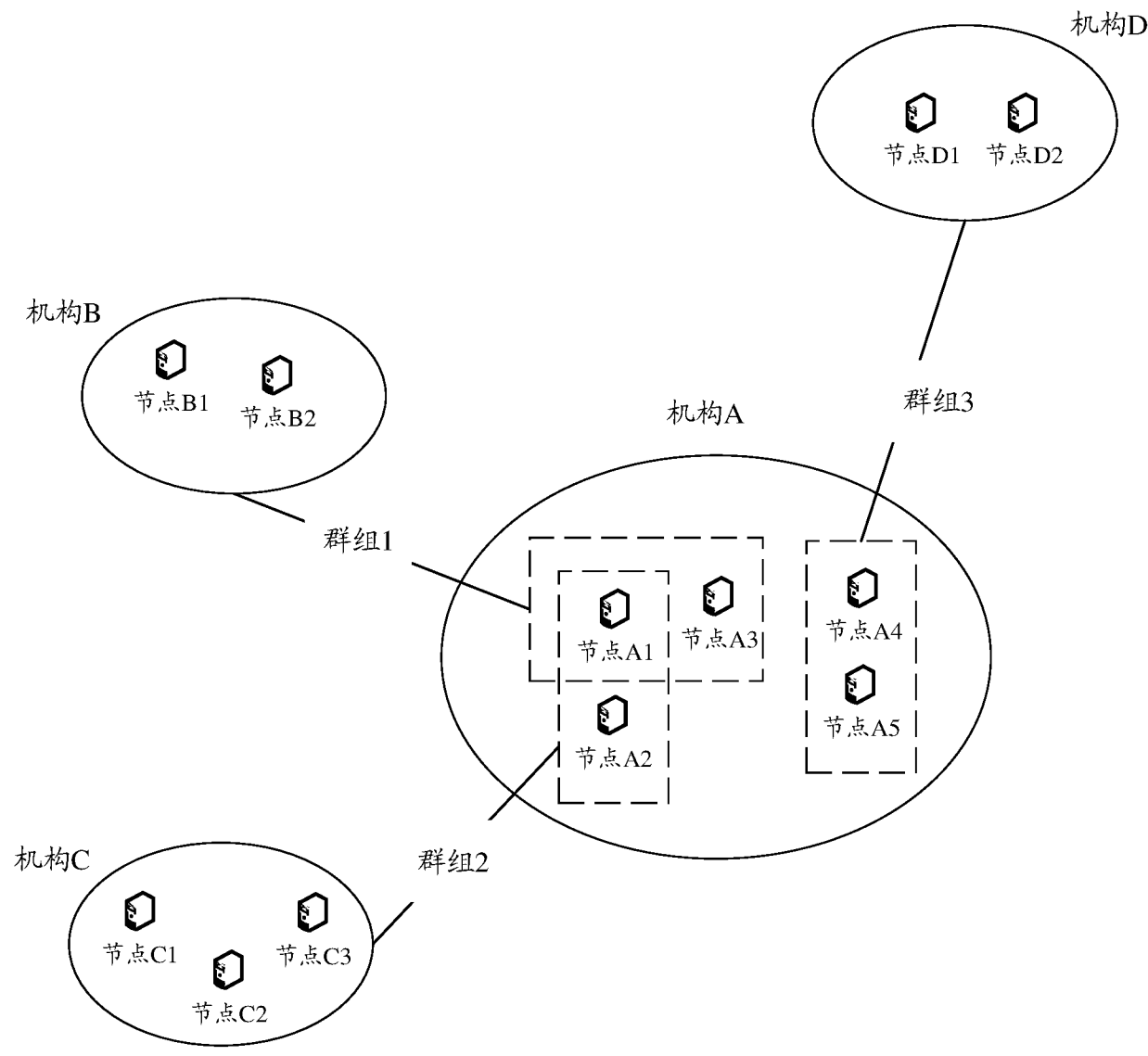


图 2

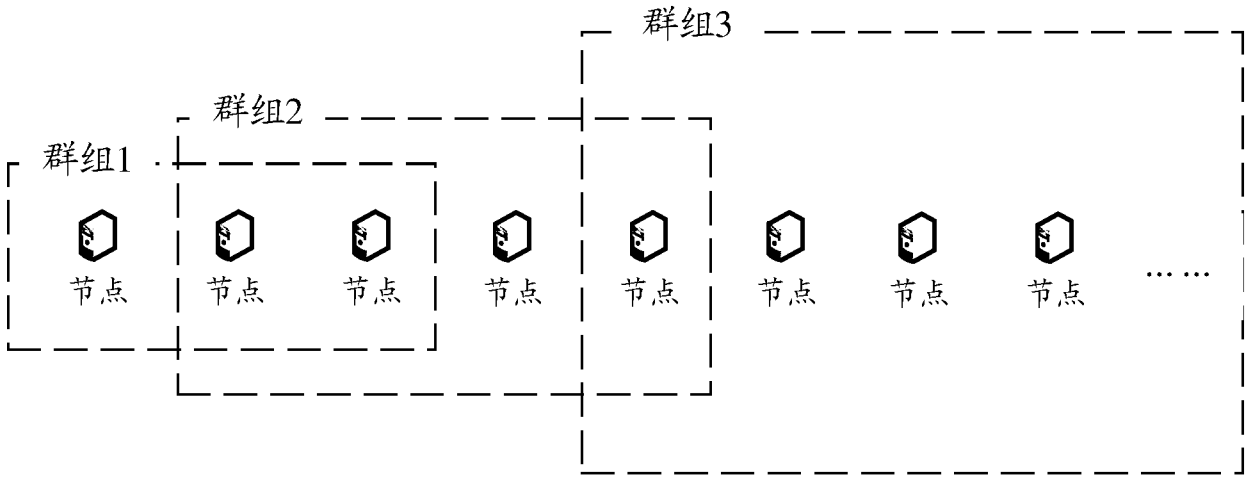


图 3

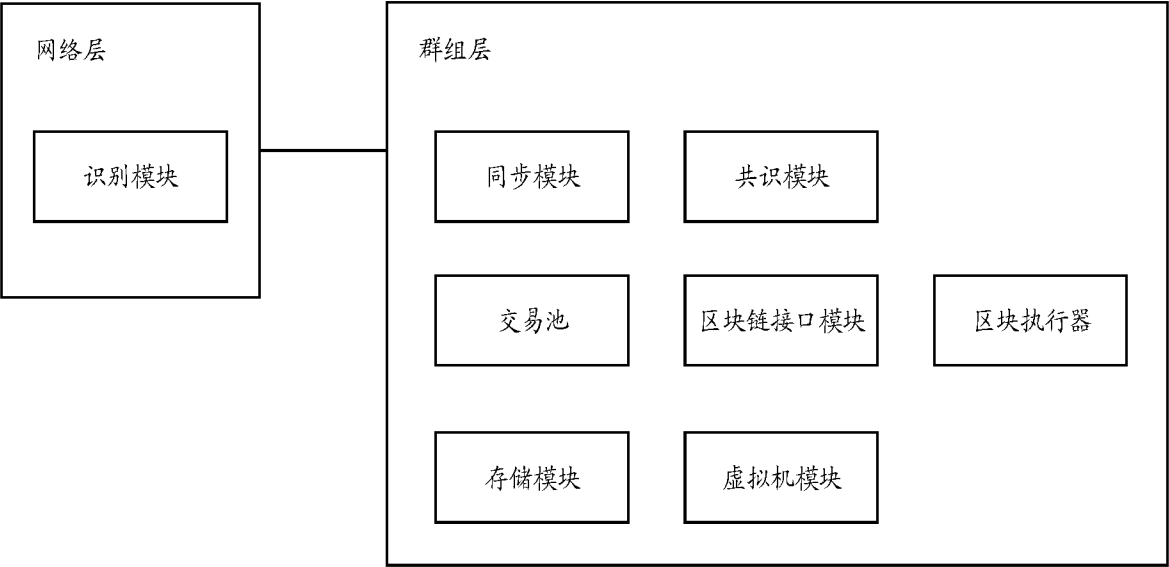


图 4

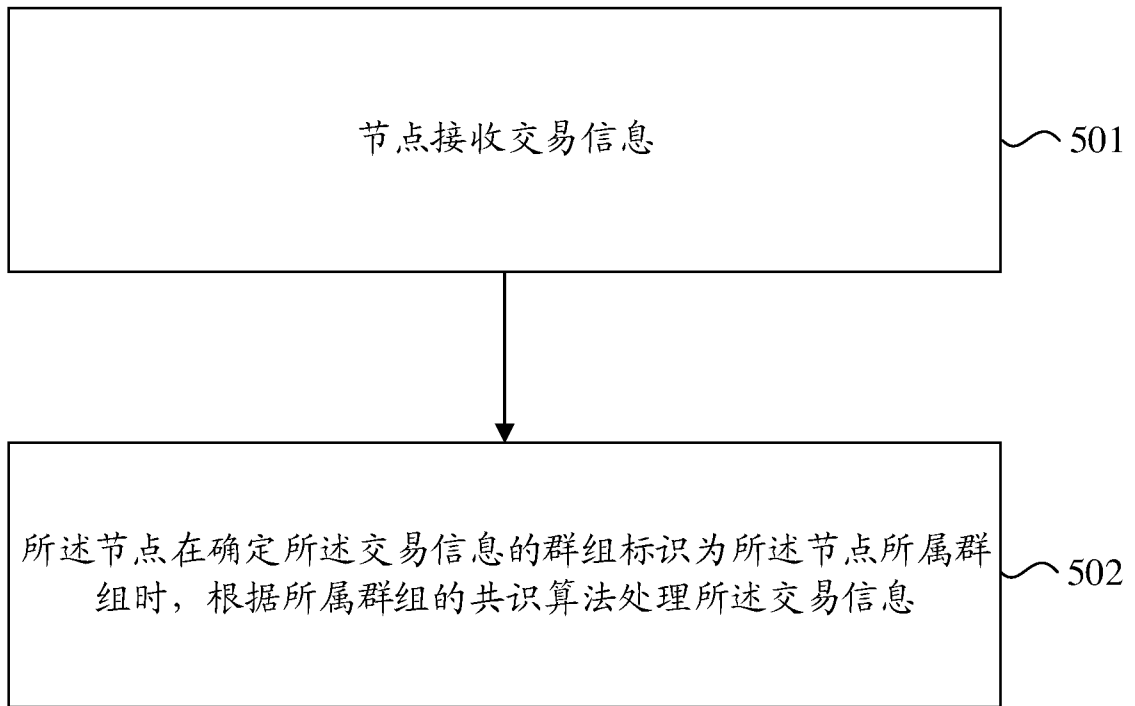


图 5

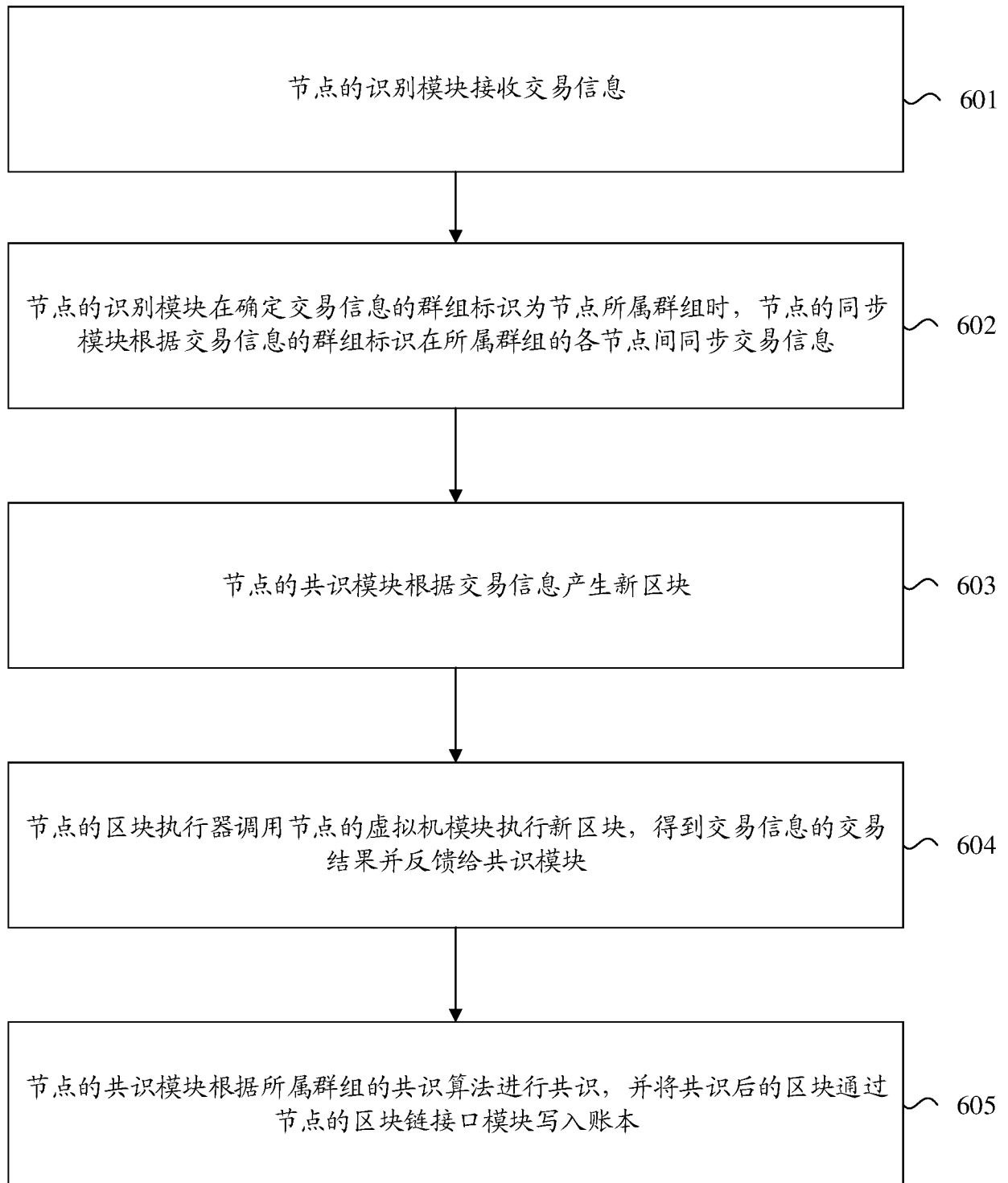


图 6

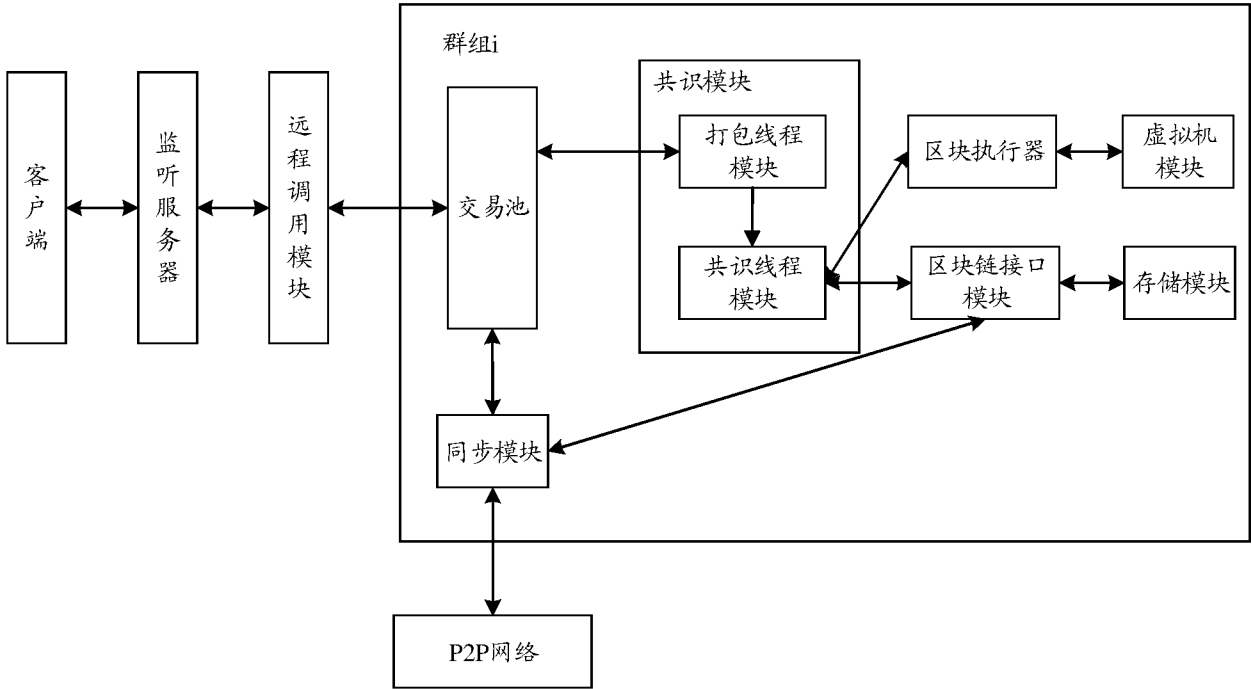


图 7

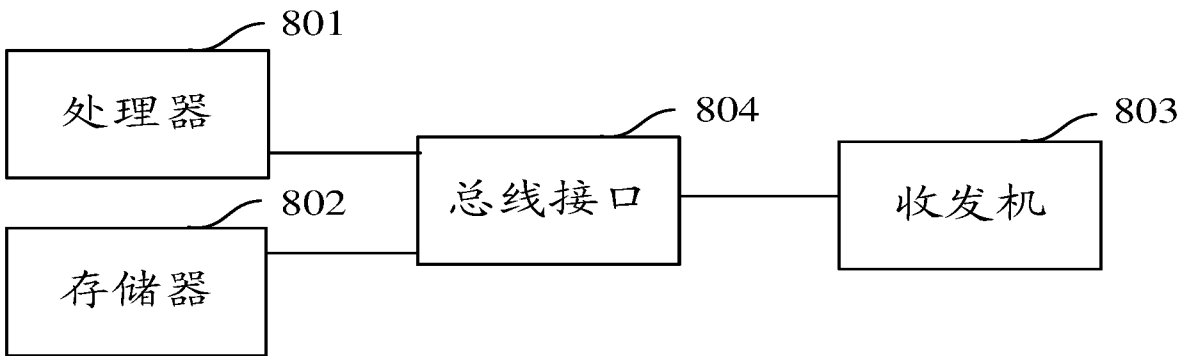


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/076079

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)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)

H04L,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: 联盟, 链, 区块链, 节点, 群, 组, 共识算法, 交易, 账本, 同步, 共享, 公共, 共识, 标识, block, chain, group, pbft, raft, consensus, account, synchronize, share, ID

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109995850 A (SHENZHEN QIANHAI WEIZHONG BANK CO., LTD.) 09 July 2019 (2019-07-09) claims 1-15 and description, paragraphs 130-134	1-19
Y	CN 107360248 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.) 17 November 2017 (2017-11-17) description, paragraphs 66-83	1-8, 11-13, 16-18
Y	CN 107766540 A (SHANGHAI DISTRIBUTION INFORMATION TECHNOLOGY CO., LTD.) 06 March 2018 (2018-03-06) description, paragraphs 65-89	1-8, 11-13, 16-18
X	CN 107360248 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.) 17 November 2017 (2017-11-17) description, paragraphs 66-83	9, 10, 14, 15, 19
A	CN 109327548 A (BEIJING RUI ZHUO XI TOU TECHNOLOGY DEVELOPMENT CO., LTD.) 12 February 2019 (2019-02-12) entire document	1-19
A	CN 109242483 A (ALIBABA GROUP HOLDING LIMITED) 18 January 2019 (2019-01-18) entire document	1-19

☒ 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

07 May 2020

Date of mailing of the international search report

19 May 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/CN2020/076079

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019033394 A1 (CLOUDMINDSCHENGDUTECHNOLOGIS CO., LTD.) 21 February 2019 (2019-02-21) entire document	1-19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/076079

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109995850	A	09 July 2019	None			
CN	107360248	A	17 November 2017	TW	201911837	A	16 March 2019
				SG	11201807918 P	A	28 March 2019
				AU	2018233013	A1	14 February 2019
				WO	2019024500	A1	07 February 2019
				JP	2019526945	A	19 September 2019
CN	107766540	A	06 March 2018	None			
CN	109327548	A	12 February 2019	None			
CN	109242483	A	18 January 2019	WO	2020029628	A1	13 February 2020
WO	2019033394	A1	21 February 2019	CN	108012582	A	08 May 2018

国际检索报告

国际申请号

PCT/CN2020/076079

A. 主题的分类 H04L 29/08 (2006.01) 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) H04L, 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: 联盟, 链, 区块链, 节点, 群, 组, 共识算法, 交易, 账本, 同步, 共享, 公共, 共识, 标识, block, chain, group, pbft, raft, consensus, account, synchronize, share, ID		
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 109995850 A (深圳前海微众银行股份有限公司) 2019年 7月 9日 (2019 - 07 - 09) 权利要求1-15, 说明书第130-134段	1-19
Y	CN 107360248 A (众安信息技术服务有限公司) 2017年 11月 17日 (2017 - 11 - 17) 说明书第66-83段	1-8, 11-13, 16-18
Y	CN 107766540 A (上海分布信息科技有限公司) 2018年 3月 6日 (2018 - 03 - 06) 说明书第65-89段	1-8, 11-13, 16-18
X	CN 107360248 A (众安信息技术服务有限公司) 2017年 11月 17日 (2017 - 11 - 17) 说明书第66-83段	9-10, 14-15, 19
A	CN 109327548 A (北京瑞卓喜投科技发展有限公司) 2019年 2月 12日 (2019 - 02 - 12) 全文	1-19
A	CN 109242483 A (阿里巴巴集团控股有限公司) 2019年 1月 18日 (2019 - 01 - 18) 全文	1-19
A	WO 2019033394 A1 (CLOUDMINDSCHENGDU TECHNOLOGIES CO., LTD.) 2019年 2月 21日 (2019 - 02 - 21) 全文	1-19
☐ 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 2020年 5月 7日		国际检索报告邮寄日期 2020年 5月 19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 赵新蕾 电话号码 86-(10)-53961623

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/076079

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	109995850	A	2019年 7月 9日	无	
CN	107360248	A	2017年 11月 17日	TW 201911837 A 2019年 3月 16日 SG 11201807918P A 2019年 3月 28日 AU 2018233013 A1 2019年 2月 14日 WO 2019024500 A1 2019年 2月 7日 JP 2019526945 A 2019年 9月 19日	
CN	107766540	A	2018年 3月 6日	无	
CN	109327548	A	2019年 2月 12日	无	
CN	109242483	A	2019年 1月 18日	WO 2020029628 A1 2020年 2月 13日	
WO	2019033394	A1	2019年 2月 21日	CN 108012582 A 2018年 5月 8日	