

(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



(10) 国际公布号

WO 2020/177508 A1

(43) 国际公布日

2020 年 9 月 10 日 (10.09.2020)

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 12/26 (2006.01)
- (21) 国际申请号: PCT/CN2020/074750
- (22) 国际申请日: 2020 年 2 月 11 日 (11.02.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910165256.0 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: 李昊轩 (LI, Haoxuan); 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)。王章 (WANG, Zhang); 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)。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)。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)。

(54) Title: BLOCK CHAIN CONSTRUCTION AND GROUP DIVISION METHOD AND APPARATUS

(54) 发明名称: 一种区块链的构建及群组划分方法与装置

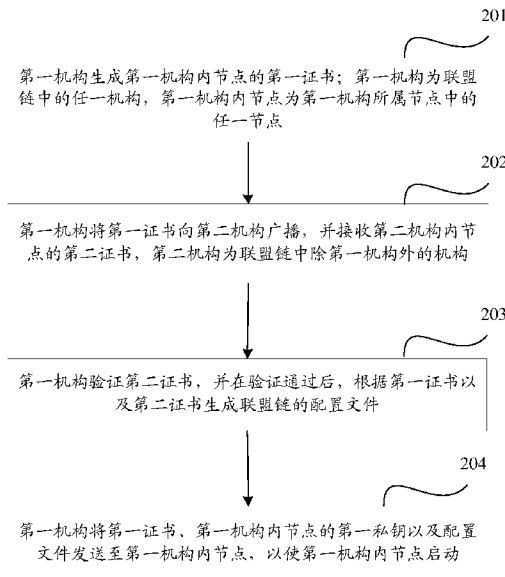


图 2

- 201 A first mechanism generates a first certificate of a node in the first mechanism, wherein the first mechanism is any mechanism in an alliance chain, and the node in the first mechanism is any node in nodes to which the first mechanism belongs
- 202 The first mechanism broadcasts the first certificate to a second mechanism, and receives a second certificate of a node in the second mechanism, wherein the second mechanism is a mechanism, other than the first mechanism, in the alliance chain
- 203 The first mechanism verifies the second certificate, and generates a configuration file of the alliance chain according to the first certificate and the second certificate after verification is passed
- 204 The first mechanism sends the first certificate, a first private key of the node in the first mechanism and the configuration file to the node in the first mechanism, so that the node in the first mechanism is started

(57) Abstract: The embodiments of the present invention relate to the technical field of Fintech, and in particular to a block chain construction and group division method and apparatus, for solving the problems of non-equivalence and low security of mechanisms in an alliance chain. The method comprises: a first mechanism generating a first certificate of a node in the first mechanism, wherein the first mechanism is any mechanism in an alliance chain, and the node in the first mechanism is any node in nodes to which the first mechanism belongs; the first mechanism broadcasting the first certificate to a second mechanism, and receiving a second certificate of a

(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))。

node in the second mechanism, wherein the second mechanism is a mechanism, other than the first mechanism, in the alliance chain; the first mechanism verifying the second certificate, and generating a configuration file of the alliance chain according to the first certificate and the second certificate after verification is passed; and the first mechanism sending the first certificate, a first private key of the node in the first mechanism and the configuration file to the node in the first mechanism, so that the node in the first mechanism is started.

(57) 摘要: 本发明实施例涉及金融科技(Fintech)技术领域, 尤其涉及一种区块链(Block chain)的构建及群组划分方法与装置, 用以解决联盟链中各机构不对等、安全性低的问题。其中方法包括: 第一机构生成第一机构内节点的第一证书; 第一机构为联盟链中的任一机构, 第一机构内节点为第一机构所属节点中的任一节点; 第一机构将第一证书向第二机构广播, 并接收第二机构内节点的第二证书, 第二机构为联盟链中除第一机构外的机构; 第一机构验证第二证书, 并在验证通过后, 根据第一证书以及第二证书生成联盟链的配置文件; 第一机构将第一证书、第一机构内节点的第一私钥以及配置文件发送至第一机构内节点, 以使第一机构内节点启动。

一种区块链的构建及群组划分方法与装置

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201910165256.0、申请名称为“一种区块链的构建及群组划分方法与装置”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

本发明涉及金融科技（Fintech）技术领域，尤其涉及一种区块链的构建及群组划分方法与装置。

背景技术

区块链（Block chain）技术是金融科技领域中一种全新的分布式基础架构与计算方式。在区块链技术中，根据区块链网络访问控制权限的不同，区块链可以分为公有链，私有链和联盟链。其中，公有链的节点是任何人都可以参与的，任何人都可以访问的一种区块链结构；私有链是仅仅对单独的个体开放（如公司，学校内部）的区块链结构；联盟链则是目前应用非常广泛的，非常普遍的一种区块链结构。在这种结构中，区块链由特定的某些组织维护，对某些个体开放，并且可以引入监管节点（比如银行监管机构、证券监管机构、央行等），让区块链在不可篡改的同时满足相应的监管需求。

目前，在联盟链初始化时无法满足联盟链的多个机构间地位对等的诉求。具体来说，联盟链在初始化时，各方需要协商创世区块中包含的节点信息。现有做法为其中一个机构生成自己的节点信息，启动区块链，再加入其它机构的节点，此时，该机构为加入的其它机构生成证书和私钥再发送给其它机构；或是由权威第三方机构直接生成所有机构内的节点信息，并将安装包发送给各机构。上述方法中，生成节点安装包的机构会拥有其它节点的所有信息，节点私钥的安全性低，不满足联盟链中各机构对等，安全的要求。

发明内容

本申请提供一种区块链的构建及群组划分方法与装置，用以解决联盟链中各机构不对等，安全性低的问题。

本发明实施例提供的一种区块链的构建及群组划分方法，包括：

5 第一机构生成第一机构内节点的第一证书；所述第一机构为联盟链中的任一机构，所述第一机构内节点为所述第一机构所属节点中的任一节点；

所述第一机构将所述第一证书向第二机构广播，并接收第二机构内节点的第二证书，所述第二机构为所述联盟链中除所述第一机构外的机构；

10 所述第一机构验证所述第二证书，并在验证通过后，根据所述第一证书以及所述第二证书生成联盟链的配置文件；

所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点，以使所述第一机构内节点启动。

一种可选的实施例中，所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点之后，还包括：

15 所述第一机构内节点利用所述第一私钥对所述第一证书进行验证，验证通过后所述第一机构内节点启动；

所述第一机构内节点启动后，还包括：

所述第一机构内节点根据所述配置文件向所述第二机构内节点发送第一心跳请求，并接收所述第二机构内节点的第二心跳请求；

20 所述第一机构内节点确定接收到的所述第二心跳请求的数量大于第一阈值后，生成所述联盟链的创世区块。

一种可选的实施例中，所述第一机构内节点确定接收到的所述第二心跳请求的数量大于阈值后，生成所述联盟链的创世区块之后，还包括：

25 所述第一机构从所述第一证书以及 N 个第二证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书，所述第一机构中包含属于所述群组的第一机构内节点；

所述第一机构根据所述第三证书生成群组配置项，所述群组配置项用于

指示所述第三节点的节点信息;

所述第一机构根据所述第三证书以及所述群组配置项,生成所述群组的群组配置文件;

5 所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点;

所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启,以使所述第一机构内节点具有群组属性。

一种可选的实施例中,所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启之后,还包括:

10 所述属于所述群组的第一机构内节点根据所述群组配置文件,向除所述第一机构内节点之外的第三节点发送第三心跳请求,并接收第四心跳请求;

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后,生成所述群组的群组创世区块。

15 一种可选的实施例中,所述第一机构根据所述第一证书以及所述第二证书生成联盟链的配置文件,包括:

所述第一机构分析所述第一证书以及所述第二证书中包含的公钥信息和证书指纹,生成所述配置文件,所述配置文件中包含 N 个第二节点的网络连接地址;

20 所述第一机构内节点根据所述配置文件向 N 个第二节点发送第一心跳请求,包括:

所述第一机构内节点根据所述 N 个第二节点的网络连接地址,向所述 N 个第二节点发送所述第一心跳请求。

本发明实施例还提供一种区块链的群组划分方法,包括:

25 第一机构从联盟链的所有证书中确定第三证书,所述第三证书为属于群组的第三节点对应的证书;所述第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构;

所述第一机构根据所述第三证书生成群组配置项,所述群组配置项用于

指示所述第三节点的节点信息;

所述第一机构根据所述群组配置项以及所述第三证书,生成所述群组的群组配置文件;

5 所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点,以使所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启,从而所述第一机构内节点具有群组属性。

一种可选的实施例中,所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启之后,还包括:

10 所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求,并接收第四心跳请求;

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后,生成所述群组的群组创世区块。

一种可选的实施例中,所述第一机构根据所述第三证书以及所述群组配置项,生成所述群组的群组配置文件,包括:

15 所述第一机构分析所述第三证书中包含的公钥信息和证书指纹,根据所述群组配置项,生成所述群组配置文件,所述群组配置文件中包含所述群组的群组序列号,以及所述第三节点的网络连接地址;

所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求,包括:

20 所述属于所述群组的第一机构内节点根据所述群组序列号以及所述第三节点的网络连接地址,向除所述第一机构内节点之外的第三节点发送所述第三心跳请求。

本发明实施例还提供一种区块链的构建装置,包括:

25 生成单元,用于生成第一机构内节点的第一证书;所述第一机构内节点为第一机构所属节点中的任一节点,所述第一机构为所述联盟链中的任一机构;

机构收发单元,用于将所述第一证书向第二机构广播,并接收第二机构

内节点的第二证书，所述第二机构为所述联盟链中除所述第一机构外的机构；

配置单元，用于验证所述第二证书，并在验证通过后，根据所述第一证书以及所述第二证书生成联盟链的配置文件；

5 所述机构收发单元，还用于将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点，以使所述第一机构内节点启动。

一种可选的实施例中，还包括：

启动单元，用于利用所述第一私钥对所述第一证书进行验证，验证通过后启动；

10 节点收发单元，用于根据所述配置文件向所述第二机构内节点发送第一心跳请求，并接收所述第二机构内节点的第二心跳请求；

共识单元，用于确定接收到的所述第二心跳请求的数量大于第一阈值后，生成所述联盟链的创世区块。

15 一种可选的实施例中，还包括确定单元，用于从所述第一证书以及 N 个第二证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书，所述第一机构中包含属于所述群组的第一机构内节点；

所述配置单元，还用于根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

20 所述配置单元，还用于根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件；

所述机构收发单元，还用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点；

所述启动单元，还用于根据所述群组配置文件进行重启，以使所述第一机构内节点具有群组属性。

25 一种可选的实施例中，所述节点收发单元，还用于根据所述群组配置文件，向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

所述共识单元，还用于确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

本发明实施例还提供一种区块链的群组划分装置，包括：

5 确定单元，用于从联盟链的所有证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书；所述确定单元所属的第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构；

生成单元，用于根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

10 所述生成单元，还用于根据所述群组配置项以及所述第三证书，生成所述群组的群组配置文件；

机构收发单元，用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点，以使所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，从而所述第一机构内节点具有群组属性。

一种可选的实施例中，还包括：

15 节点收发单元，用于根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

共识单元，用于确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

本发明实施例还提供一种电子设备，包括：

20 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。

25 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。

本发明实施例中，第一机构生成第一机构内节点的第一证书，第一机构

将生成的第一证书向第二机构广播，并接收第二机构内节点的第二证书，其中，第一机构为联盟链中的任一机构，第一机构内节点为第一机构所属节点中的任一节点，第二机构为联盟链中除第一机构外的机构。第一机构验证接收到的第二证书，并在验证通过后，根据第一证书以及第二证书生成联盟链
5 的配置文件，并将第一证书、第一机构内节点的第一私钥以及配置文件发送至第一机构内节点，以使第一机构内节点启动。本发明实施例中，机构间只需广播证书，节点的私钥由机构自己生成和维护，保证了机构内节点的私钥不出机构内网，确保了机构间节点的安全性。同时，联盟链的机构各自生成对应节点的证书和私钥，而不是由一个机构生成其余机构的证书和私钥，保
10 证了机构间的对等关系。

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
15 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性的前提下，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可能的系统构架的结构示意图；

图 2 为本发明实施例提供的一种区块链的构建方法的流程示意图；

图 3 为本发明具体实施例一提供的一种联盟链构建方法的流程示意图；

20 图 4 为本发明具体实施例二提供的一种联盟链的群组划分方法的流程示意图；

图 5 为本发明实施例提供的一种区块链的构建装置的结构示意图；

图 6 为本发明实施例提供的一种区块链的群组划分装置的结构示意图；

图 7 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

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份实施例，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。

5 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。然而在联盟链中，为单个机构生成所有机构内节点信息，无法满足去中心化思想的需求。

10 为了解决上述问题，本发明实施例提供了一种区块链的构建方法。该方法所适用的一种可能的系统构架，如图 1 所示，包括机构和节点。

其中，机构为通过联盟链委员会准入的主体，拥有机构证书 `agency.crt` 和机构私钥 `agency.key`。机构可以生成机构内节点。机构可以签发所属节点的节点证书 `node.crt` 并生成节点私钥 `node.key`。证书即数字证书，是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在互联网上验证通信实体身份的方式，数字证书不是数字身份证，而是身份认证机构盖在数字身份证上的一个章或印（或者说加在数字身份证上的一个签名）。它是由权威机构——证书授权（Certificate Authority, CA）机构中心发行的，人们可以在网上用它来识别对方的身份。

20 在区块链对等网络中，节点参与网络组建和数据交换。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，具有参与区块链对等网络共识和账本维护的能力。本发明实施例中，机构内节点即为联盟链中运行的节点，属于对应的机构，节点可能会处于一个或多个群组中。节点拥有节点证书 `node.crt` 和节点私钥 `node.key`。机构内节点会与所属群组的其他节点进行网络链接，并维护该群组。群组间数据隔离，每个群组独立运行各自的共识算法，不同群组可使用不同的共识算法。

25 本发明实施例支持多群组架构，群组间共享网络，通过网络准入模块实

现各账本间网络消息隔离。所有机构协商完成联盟链根证书，所有机构拥有各自对应机构内节点的节点证书 node.crt 和节点私钥 node.key。机构间地位对等，机构内节点只与所属群组的其他节点通信。机构间节点可以互相协商证书并新建群组。一个机构可以对应一个机构内节点，也可以对应多个机构内节点；同一个机构对应的机构内节点，可以属于同一个群组，也可以属于不同群组。

基于上述架构，本发明实施例提供了一种区块链的构建方法，如图 2 所示，本发明实施例提供的区块链的构建方法，包括以下步骤：

步骤 201、第一机构生成第一机构内节点的第一证书；第一机构为联盟链中的任一机构，第一机构内节点为第一机构所属节点中的任一节点。

步骤 202、第一机构将第一证书向第二机构广播，并接收第二机构内节点的第二证书，第二机构为联盟链中除第一机构外的机构。

步骤 203、第一机构验证第二证书，并在验证通过后，根据第一证书以及第二证书生成联盟链的配置文件。

步骤 204、第一机构将第一证书、第一机构内节点的第一私钥以及配置文件发送至第一机构内节点，以使第一机构内节点启动。

本发明实施例中，第一机构生成第一机构内节点的第一证书，第一机构将生成的第一证书向第二机构广播，并接收第二机构内节点的第二证书，其中，第一机构为联盟链中的任一机构，第一机构内节点为第一机构所属节点中的任一节点，第二机构为联盟链中除第一机构外的机构。第一机构验证接收到的第二证书，并在验证通过后，根据第一证书以及第二证书生成联盟链的配置文件，并将第一证书、第一机构内节点的第一私钥以及配置文件发送至第一机构内节点，以使第一机构内节点启动。本发明实施例中，机构间只需广播证书，节点的私钥由机构自己生成和维护，保证了机构内节点的私钥不出机构内网，确保了机构间节点的安全性。同时，联盟链的机构各自生成对应节点的证书和私钥，而不是由一个机构生成其余机构的证书和私钥，保证了机构间的对等关系。

具体来说，本发明实施例的联盟链中，各个机构分别为自身对应的机构内节点生成节点证书，多个机构之间采用对等协商的方法广播节点证书，并进行证书验证。机构可以根据所有节点的证书，生成联盟链节点启动时的配置文件，而节点私钥则存储在机构本地，不发送至其它机构，从而不会泄露节点私钥，保证了私钥的安全性。由于生成的配置文件不包含节点私钥，即使生成的配置文件泄露，非本机构也无法使用这些配置文件。

节点证书既可以由第一机构主动发送至联盟链中的其余机构，即第二机构；也可以由第二机构从第一机构中获取。各个机构收到其余机构广播的节点证书后，对证书的颁发者、使用者、有效期、密钥用法、证书中包含的公钥等信息进行验证，从而判断节点证书是否合法。若节点证书均合法，则节点证书协商成功，继续执行后续流程；若存在不合法的节点证书，则节点证书协商失败。

在节点证书协商成功后，联盟链中的每个机构生成对应机构内节点的配置文件，并将每个机构内节点的配置文件，连同该机构内节点的证书和私钥，发送给机构内节点，以使机构内节点启动。

相应地，所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点之后，还包括：

所述第一机构内节点利用所述第一私钥对所述第一证书进行验证，验证通过后所述第一机构内节点启动；

所述第一机构内节点启动后，还包括：

所述第一机构内节点根据所述配置文件向所述第二机构内节点发送第一心跳请求，并接收所述第二机构内节点的第二心跳请求；

所述第一机构内节点确定接收到的所述第二心跳请求的数量大于第一阈值后，生成所述联盟链的创世区块。

具体实施过程中，各机构将节点私钥配置至对应机构内节点的安装包，启动节点。目前支持两种配置方式，分别为 keycenter 类型的私钥加密方式和直接加载私钥至节点文件夹的方式。第一机构内节点接收到机构发送来的第

一证书、第一私钥和配置文件之后，可以利用第一私钥对第一证书进行验证，判断第一私钥与第一证书是否匹配，验证通过后第一机构内节点启动，否则，则结束联盟链的初始化过程。第一机构内节点启动后，根据接收到的配置文件，向联盟链中的其余节点，即第二机构内节点，发送第一心跳请求。第一机构内节点只有收集到足够数量的其他节点的心跳请求才会进行共识，即共同创建区块链。这样，保证了区块链创建的成功率。共识算法为区块链对等网络中的各个节点通过一种算法对一批交易进行确认，并确保所有节点对这

5 批数据具有一致的确认结果，这种算法就是区块链的共识算法。

举例来说，若协商的节点证书的数量为 n 个，则说明机构内节点的数量为 n 个，且已经完成证书协商、节点部署等操作。联盟链中各节点启动后，根据联盟链的配置文件与联盟链中其余的节点进行连接。不同共识方法中的第一阈值不同。如 PBFT (Practical Byzantine Fault Tolerance, 实用拜占庭容错算法) 方式中机构内节点只有收集到数量大于 $2n/3$ (向上取整) 的心跳请求后，才能生成联盟链的创世区块，进一步完成共识。RAFT (一种分布式一致性算法) 方式中只有收集到数量大于 $n/2$ (向上取整) 的心跳请求后，联盟链群组才能进行共识，完成部署。为了保证联盟链的共识效率，PBFT 中节点证书的数量 n 不建议超过 40，RAFT 中节点证书的数量 n 不建议超过 100。

10 15

进一步地，所述第一机构根据所述第一证书以及所述第二证书生成联盟链的配置文件，包括：

所述第一机构分析所述第一证书以及所述第二证书中包含的公钥信息和证书指纹，生成所述配置文件，所述配置文件中包含 N 个第二节点的网络连接地址。

20

所述第一机构内节点根据所述配置文件向所述 N 个第二节点发送第一心跳请求，包括：

所述第一机构内节点根据所述 N 个第二节点的网络连接地址，向所述 N 个第二节点发送所述第一心跳请求。

25

具体实施过程中，第一机构根据联盟链中所有的节点证书生成配置文件。

具体为分析证书中包含的公钥信息和证书指纹，生成联盟链的序列号，后续节点生成创世区块时，会将序列号信息放入创世区块中。同时，第一机构生成区块链启动所需的群组容量与网络连接地址等配置文件。这样，第一机构内节点需要发送第一心跳请求时，可以根据每个第二节点的网络连接地址，
5 向第二节点发送第一心跳请求。

联盟链初始化完成后，机构间需要根据不同业务划分不同群组。每个群组中含有多个节点，同一个机构所属的节点可以分属于不同的群组，也可以属于同一个群组。

所述第一机构内节点确定接收到的所述第二心跳请求的数量大于阈值
10 后，生成所述联盟链的创世区块之后，还包括：

所述第一机构从所述第一证书以及所述 N 个第二证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书，所述第一机构中包含属于所述群组的第一机构内节点；

所述第一机构根据所述第三证书生成群组配置项，所述群组配置项用于
15 指示所述第三节点的节点信息；

所述第一机构根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件；

所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点；

20 所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，以使所述第一机构内节点具有群组属性。

具体来说，联盟链初始化后划分群组，由于各机构已获得联盟链中的所有节点证书，因此，无需再次执行获取节点证书和验证的过程，由于第一机构中包含属于所述群组的第一机构内节点，第一机构可以直接从所有节点证书中确定出属于群组的第三节点对应的第三证书。根据第三证书生成群组配置项。群组配置项中可以包含群组中每个节点的证书、节点的 IP、端口号等
25 数据，可以指示群组中的第三节点具体为哪些节点。第一机构根据群组配置

项以及该群组中的节点证书，分析证书包含的公钥信息和证书指纹，生成该群组启动时的群组序列号。后续节点生成群组创世区块时，会将群组序列号信息放入群组创世区块中。同时，第一机构生成划分群组时所需的群组容量与群组内节点的网络连接地址等配置文件。各机构生成群组配置文件后，将

5 群组配置文件发送至属于该群组的机构内节点中，将群组配置文件导入节点安装包后，重启节点。这样，属于该群组的机构内节点根据群组配置文件进行重启后，会具有群组属性。

与联盟链初始化时类似，所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启之后，还包括：

10 所述属于所述群组的第一机构内节点根据所述群组配置文件，向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

也就是说，第一机构内节点只有收集到群组内足够数量的其他节点的心跳请求才会进行共识，即创建群组创世区块。这样，保证了群组划分的成功率。

15

进一步，本发明实施例中，节点还具有检测功能。具体为节点启动时，会生成对应的节点证书，节点配置项中包含节点 IP、端口号、节点所属群组等信息，确保生成节点可用。

20 进一步，本发明实施例还设计有监控功能。可以配置相应的监控服务，如默认配置将监控结果上报至使用者微信。本发明实施例可以通过机构向机构内节点发起 RPC（Remote Procedure Call，远程过程调用）请求，得到机构内节点运行时的相关参数，同时通过分析机构内节点运行时的 log 信息，对机构内节点进行监控，并将监控结果上报至用户配置的服务中。例如，默认配置

25 置监控服务，支持上报至微信、个人网址，支持专用服务设置，可上报至企业微信等。

此外，本发明实施例还提供一种联盟链的群组划分方法，用于无论利用

任何方式初始化的联盟链中，进行对等的群组划分。本发明实施例中联盟链的群组划分方法包括以下步骤：

第一机构从联盟链的所有证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书；所述第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构。

所述第一机构根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息。

所述第一机构根据所述群组配置项以及所述第三证书，生成所述群组的群组配置文件。

所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点。

所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，以使所述第一机构内节点具有群组属性。

所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求。

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

本发明实施例中，无论联盟链的初始化方式如何，对于节点的群组划分，每个属于群组的节点所属机构均根据群组内的所有证书生成群组配置文件，并配置至对应的节点安装包，从而维护了群组划分的对等性。同时，无需在机构间传输节点私钥，保证了私钥的安全性。

进一步地，所述第一机构根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件，包括：

所述第一机构分析所述第三证书中包含的公钥信息和证书指纹，根据所述群组配置项，生成所述群组配置文件，所述群组配置文件中包含所述群组的群组序列号，以及所述第三节点的网络连接地址；

所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第

一机构内节点之外的第三节点发送第三心跳请求，包括：

所述属于所述群组的第一机构内节点根据所述群组序列号以及所述第三节点的网络连接地址，向除所述第一机构内节点之外的第三节点发送所述第三心跳请求。

5 具体实施过程中，第一机构分析第三证书中包含的公钥信息和证书指纹，生成群组序列号，后续群组的节点生成群组创世区块时，会将群组序列号信息放入群组创世区块中。同时，第一机构生成区块链启动所需的群组容量与群组内节点的网络连接地址等群组配置文件。这样，第一机构内节点需要向群组内其它节点发送心跳请求时，可以根据节点的群组网络连接地址，向群
10 组内其它节点发送心跳请求。

为了更清楚地理解本发明，下面以具体实施例对上述流程进行详细描述，实施例一为联盟链的初始化过程，具体场景为，联盟链中包含节点 11、节点 12、... 节点 19 共 9 个节点，属于机构 1 至机构 4 共 4 个机构，其中，节点 11 与节点 15 为机构 1 的机构内节点，节点 11 属于第一群组，节点 15 属于第
15 二群组，具体实施例的步骤如图 3 所示，包括：

步骤 301: 机构 1 生成节点 11 的节点证书 110 和节点 15 的节点证书 150。

步骤 302: 机构 1 将节点证书 110 和节点证书 150 进行广播，即向机构 2、机构 3、机构 4 发送节点 11 与节点 15 的节点证书，并接收机构 2、机构 3、机构 4 发送的节点证书。

20 步骤 303: 机构 1 对接收到的节点证书进行验证，若验证通过，则执行步骤 304，否则执行步骤 311。

步骤 304: 机构 1 根据节点证书 110 至节点证书 190，生成联盟链的配置文件。

25 步骤 305: 机构 1 将配置文件发送至节点 11 与节点 15，并将节点证书 110 与对应的私钥发送至节点 11，将节点证书 150 与对应的私钥发送至节点 15。

步骤 306: 节点 11 利用接收到的私钥对节点证书 110 进行验证，若验证通过，则执行步骤 307，否则执行步骤 311。

步骤 307: 节点 11 启动。

步骤 308: 节点 11 根据配置文件, 向节点 12 至节点 19 发送第一心跳请求, 并接收第二心跳请求。

5 步骤 309: 节点 11 判断接收到的第二心跳请求的数量, 若大于阈值 5, 则执行步骤 310, 否则执行步骤 309。

步骤 310: 节点 11 进行共识。

步骤 311: 联盟链初始化失败。

具体实施例二为联盟链的群组划分过程, 仍沿用实施例一中的场景, 具体实施例的步骤如图 4 所示, 包括:

10 步骤 401: 机构 1 从节点证书 110 至节点证书 190 中确定, 节点 11 至节点 14 为第一群组, 节点 15 至节点 19 为第二群组。

步骤 402: 机构 1 根据节点证书 110 至节点证书 140, 生成第一群组的群组配置项, 进一步生成第一群组的群组配置文件。

步骤 403: 机构 1 将第一群组的群组配置文件向节点 11 发送。

15 步骤 404: 节点 11 利用私钥对群组配置文件进行验证, 若验证通过, 则执行步骤 405, 否则执行步骤 401。

步骤 405: 节点 11 根据第一群组的群组配置文件进行重启。

步骤 406: 节点 11 向节点 12、节点 13 和节点 14 发送第三心跳请求, 并接收第四心跳请求。

20 步骤 407: 节点 11 确定第四心跳请求的数量是否大于 2, 若是, 则执行步骤 408, 否则执行步骤 407。

步骤 408: 节点 11 进行共识。

本发明实施例还提供了一种区块链的构建装置, 如图 5 所示, 包括:

25 生成单元 501, 用于生成第一机构内节点的第一证书; 所述第一机构内节点为第一机构所属节点中的任一节点, 所述第一机构为所述联盟链中的任一机构;

机构收发单元 502, 用于将所述第一证书向第二机构广播, 并接收第二机

构内节点的第二证书, 所述第二机构为所述联盟链中除所述第一机构外的机构;

配置单元 503, 用于验证所述第二证书, 并在验证通过后, 根据所述第一证书以及所述第二证书生成联盟链的配置文件;

5 所述机构收发单元 502, 还用于将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点, 以使所述第一机构内节点启动。

进一步, 还包括:

10 启动单元 504, 用于利用所述第一私钥对所述第一证书进行验证, 验证通过后启动;

节点收发单元 505, 用于根据所述配置文件向所述第二机构内节点发送第一心跳请求, 并接收所述第二机构内节点的第二心跳请求;

共识单元 506, 用于确定接收到的所述第二心跳请求的数量大于第一阈值后, 生成所述联盟链的创世区块。

15 进一步, 还包括确定单元 507, 用于从所述第一证书以及所述 N 个第二证书中确定第三证书, 所述第三证书为属于群组的第三节点对应的证书, 所述第一机构中包含属于所述群组的第一机构内节点;

所述配置单元 503, 还用于根据所述第三证书生成群组配置项, 所述群组配置项用于指示所述第三节点的节点信息;

20 所述配置单元 503, 还用于根据所述第三证书以及所述群组配置项, 生成所述群组的群组配置文件;

所述机构收发单元 502, 还用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点;

25 所述启动单元 504, 还用于根据所述群组配置文件进行重启, 以使所述第一机构内节点具有群组属性。

进一步, 所述节点收发单元 505, 还用于根据所述群组配置文件, 向除所述第一机构内节点之外的第三节点发送第三心跳请求, 并接收第四心跳请求;

所述共识单元 506, 还用于确定接收到的所述第四心跳请求的数量大于第二阈值后, 生成所述群组的群组创世区块。

本发明实施例还提供一种区块链的群组划分装置, 如图 6 所示, 包括:

5 确定单元 601, 用于从联盟链的所有证书中确定第三证书, 所述第三证书为属于群组的第三节点对应的证书; 所述确定单元所属的第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构;

生成单元 602, 用于根据所述第三证书生成群组配置项, 所述群组配置项用于指示所述第三节点的节点信息;

10 所述生成单元 602, 还用于根据所述群组配置项以及所述第三证书, 生成所述群组的群组配置文件;

机构收发单元 603, 用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点, 以使所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启, 从而所述第一机构内节点具有群组属性。

进一步, 还包括:

15 节点收发单元 604, 用于根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求, 并接收第四心跳请求;

共识单元 605, 用于确定接收到的所述第四心跳请求的数量大于第二阈值后, 生成所述群组的群组创世区块。

基于相同的原理, 本发明还提供一种电子设备, 如图 7 所示, 包括:

20 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:

第一机构生成第一机构内节点的第一证书; 所述第一机构为联盟链中的任一机构, 所述第一机构内节点为所述第一机构所属节点中的任一节点;

25 所述第一机构将所述第一证书向第二机构广播, 并接收第二机构内节点的第二证书, 所述第二机构为所述联盟链中除所述第一机构外的机构;

所述第一机构验证所述第二证书, 并在验证通过后, 根据所述第一证书

以及所述第二证书生成联盟链的配置文件；

所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点，以使所述第一机构内节点启动。

5 基于相同的原理，本发明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图 2 至图 4 中任一所述的方法。

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，则本发明也意图包括这些改动和变型在内。

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。

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。

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。

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，则本发明也意图包括这些改动和变型在内。

权利要求

1、一种区块链的构建方法，其特征在于，包括：

第一机构生成第一机构内节点的第一证书；所述第一机构为联盟链中的任一机构，所述第一机构内节点为所述第一机构所属节点中的任一节点；

5 所述第一机构将所述第一证书向第二机构广播，并接收第二机构内节点的第二证书，所述第二机构为所述联盟链中除所述第一机构外的机构；

所述第一机构验证所述第二证书，并在验证通过后，根据所述第一证书以及所述第二证书生成所述联盟链的配置文件；

10 所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点，以使所述第一机构内节点启动。

2、如权利要求 1 所述的方法，其特征在于，所述第一机构将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点之后，还包括：

15 所述第一机构内节点利用所述第一私钥对所述第一证书进行验证，验证通过后所述第一机构内节点启动；

所述第一机构内节点启动后，还包括：

所述第一机构内节点根据所述配置文件向所述第二机构内节点发送第一心跳请求，并接收所述第二机构内节点的第二心跳请求；

20 所述第一机构内节点确定接收到的所述第二心跳请求的数量大于第一阈值后，生成所述联盟链的创世区块。

3、如权利要求 2 所述的方法，其特征在于，所述第一机构内节点确定接收到的所述第二心跳请求的数量大于阈值后，生成所述联盟链的创世区块之后，还包括：

25 所述第一机构从所述第一证书以及 N 个第二证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书，所述第一机构中包含属于所述群组的第一机构内节点；

所述第一机构根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

所述第一机构根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件；

5 所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点；

所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，以使所述第一机构内节点具有群组属性。

10 4、如权利要求 3 所述的方法，其特征在于，所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启之后，还包括：

所述属于所述群组的第一机构内节点根据所述群组配置文件，向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

15 5、如权利要求 2 所述的方法，其特征在于，所述第一机构根据所述第一证书以及所述第二证书生成联盟链的配置文件，包括：

所述第一机构分析所述第一证书以及所述第二证书中包含的公钥信息和证书指纹，生成所述配置文件，所述配置文件中包含 N 个第二节点的网络连接地址；

20 所述第一机构内节点根据所述配置文件向 N 个第二节点发送第一心跳请求，包括：

所述第一机构内节点根据所述 N 个第二节点的网络连接地址，向所述 N 个第二节点发送所述第一心跳请求。

6、一种区块链的群组划分方法，其特征在于，包括：

25 第一机构从联盟链的所有证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书；所述第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构；

所述第一机构根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

所述第一机构根据所述群组配置项以及所述第三证书，生成所述群组的群组配置文件；

5 所述第一机构将所述群组配置文件发送至所述属于所述群组的第一机构内节点，以使所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，从而所述第一机构内节点具有群组属性。

7、如权利要求6所述的方法，其特征在于，所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启之后，还包括：

10 所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

所述属于所述群组的第一机构内节点确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

15 8、如权利要求7所述的方法，其特征在于，所述第一机构根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件，包括：

所述第一机构分析所述第三证书中包含的公钥信息和证书指纹，根据所述群组配置项，生成所述群组配置文件，所述群组配置文件中包含所述群组的群组序列号，以及所述第三节点的网络连接地址；

20 所述属于所述群组的第一机构内节点根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求，包括：

所述属于所述群组的第一机构内节点根据所述群组序列号以及所述第三节点的网络连接地址，向除所述第一机构内节点之外的第三节点发送所述第三心跳请求。

9、一种区块链的构建装置，其特征在于，包括：

25 生成单元，用于生成第一机构内节点的第一证书；所述第一机构内节点为第一机构所属节点中的任一节点，所述第一机构为所述联盟链中的任一机构；

机构收发单元，用于将所述第一证书向第二机构广播，并接收第二机构内节点的第二证书，所述第二机构为所述联盟链中除所述第一机构外的机构；

配置单元，用于验证所述第二证书，并在验证通过后，根据所述第一证书以及所述第二证书生成联盟链的配置文件；

5 所述机构收发单元，还用于将所述第一证书、所述第一机构内节点的第一私钥以及所述配置文件发送至所述第一机构内节点，以使所述第一机构内节点启动。

10、如权利要求 9 所述的装置，其特征在于，还包括：

10 启动单元，用于利用所述第一私钥对所述第一证书进行验证，验证通过后启动；

节点收发单元，用于根据所述配置文件向所述第二机构内节点发送第一心跳请求，并接收所述第二机构内节点的第二心跳请求；

共识单元，用于确定接收到的所述第二心跳请求的数量大于第一阈值后，生成所述联盟链的创世区块。

15 11、如权利要求 10 所述的装置，其特征在于，

还包括确定单元，用于从所述第一证书以及 N 个第二证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书，所述第一机构中包含属于所述群组的第一机构内节点；

20 所述配置单元，还用于根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

所述配置单元，还用于根据所述第三证书以及所述群组配置项，生成所述群组的群组配置文件；

所述机构收发单元，还用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点；

25 所述启动单元，还用于根据所述群组配置文件进行重启，以使所述第一机构内节点具有群组属性。

12、如权利要求 11 所述的装置，其特征在于，

所述节点收发单元，还用于根据所述群组配置文件，向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

所述共识单元，还用于确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

5 13、一种区块链的群组划分装置，其特征在于，包括：

确定单元，用于从联盟链的所有证书中确定第三证书，所述第三证书为属于群组的第三节点对应的证书；所述确定单元所属的第一机构为所述联盟链中包含属于所述群组的第一机构内节点的任一机构；

10 生成单元，用于根据所述第三证书生成群组配置项，所述群组配置项用于指示所述第三节点的节点信息；

所述生成单元，还用于根据所述群组配置项以及所述第三证书，生成所述群组的群组配置文件；

15 机构收发单元，用于将所述群组配置文件发送至所述属于所述群组的第一机构内节点，以使所述属于所述群组的第一机构内节点根据所述群组配置文件进行重启，从而所述第一机构内节点具有群组属性。

14、如权利要求 13 所述的装置，其特征在于，还包括：

节点收发单元，用于根据所述群组配置文件向除所述第一机构内节点之外的第三节点发送第三心跳请求，并接收第四心跳请求；

20 共识单元，用于确定接收到的所述第四心跳请求的数量大于第二阈值后，生成所述群组的群组创世区块。

15、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，

25 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 1-5 任一所述的方法。

16、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 1~5 任一所述的方法。

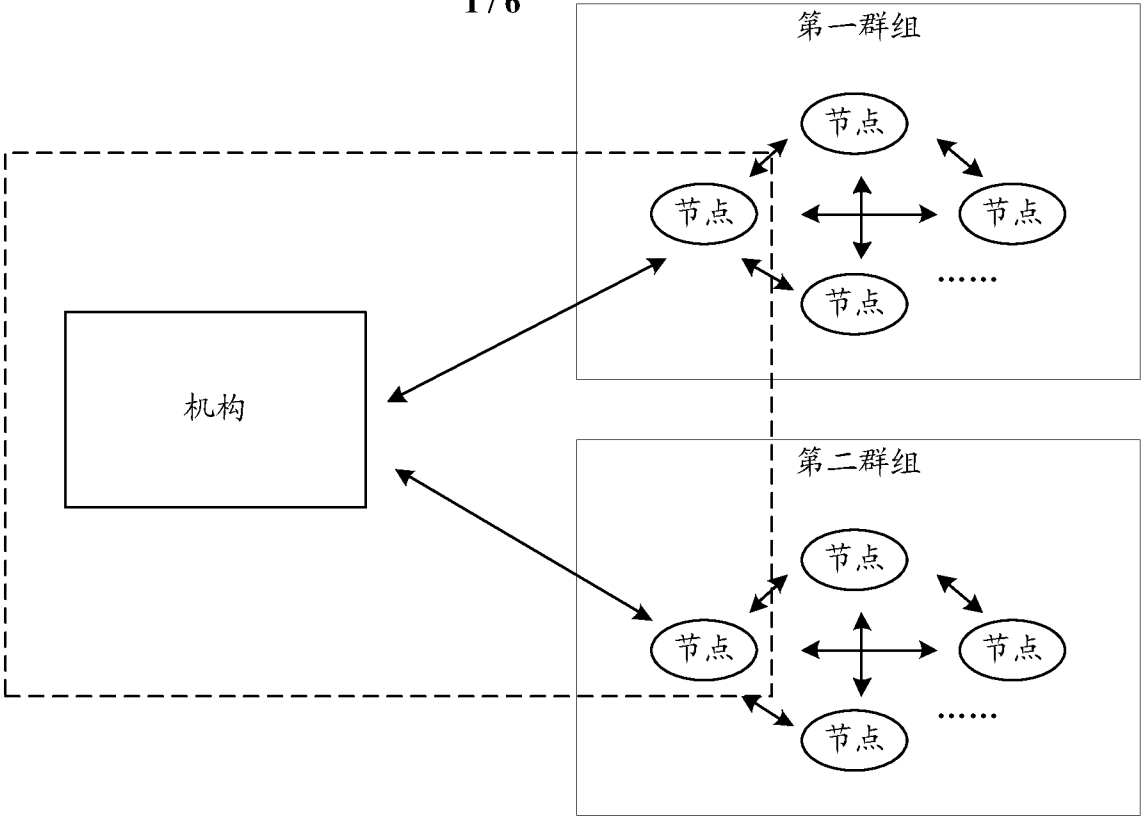


图 1

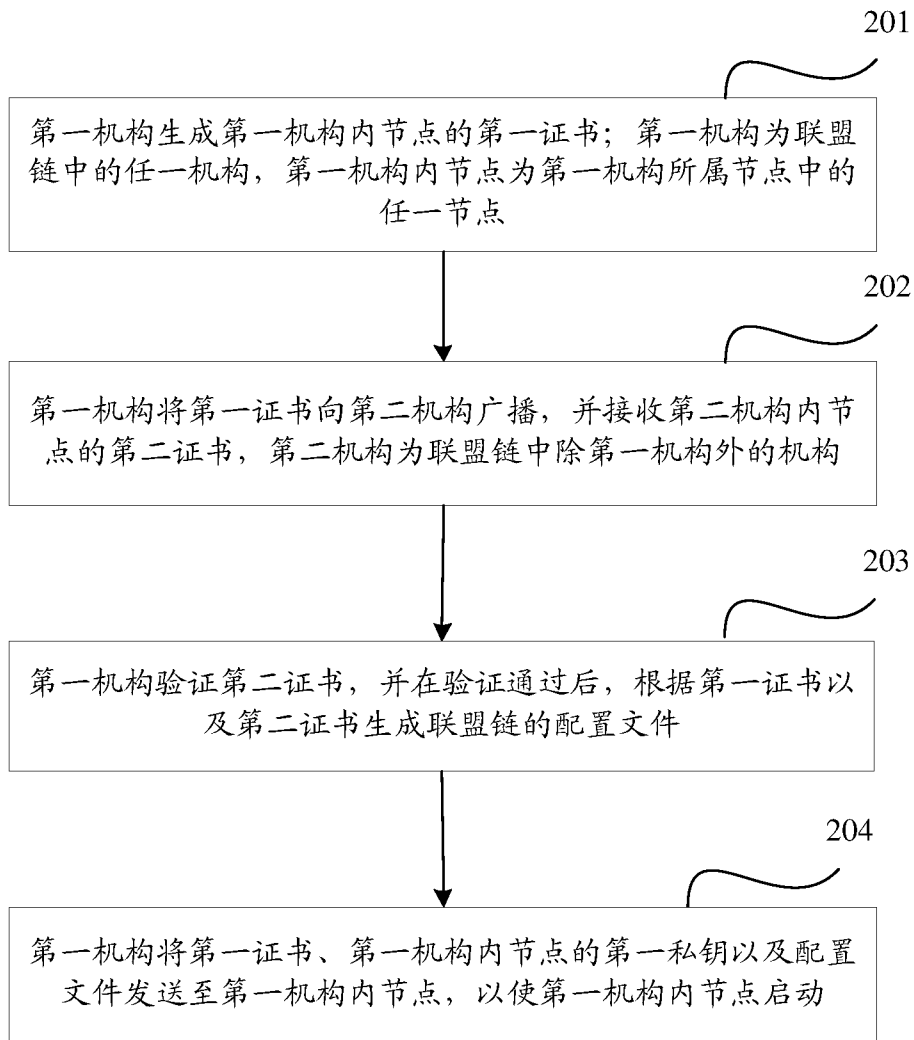


图 2

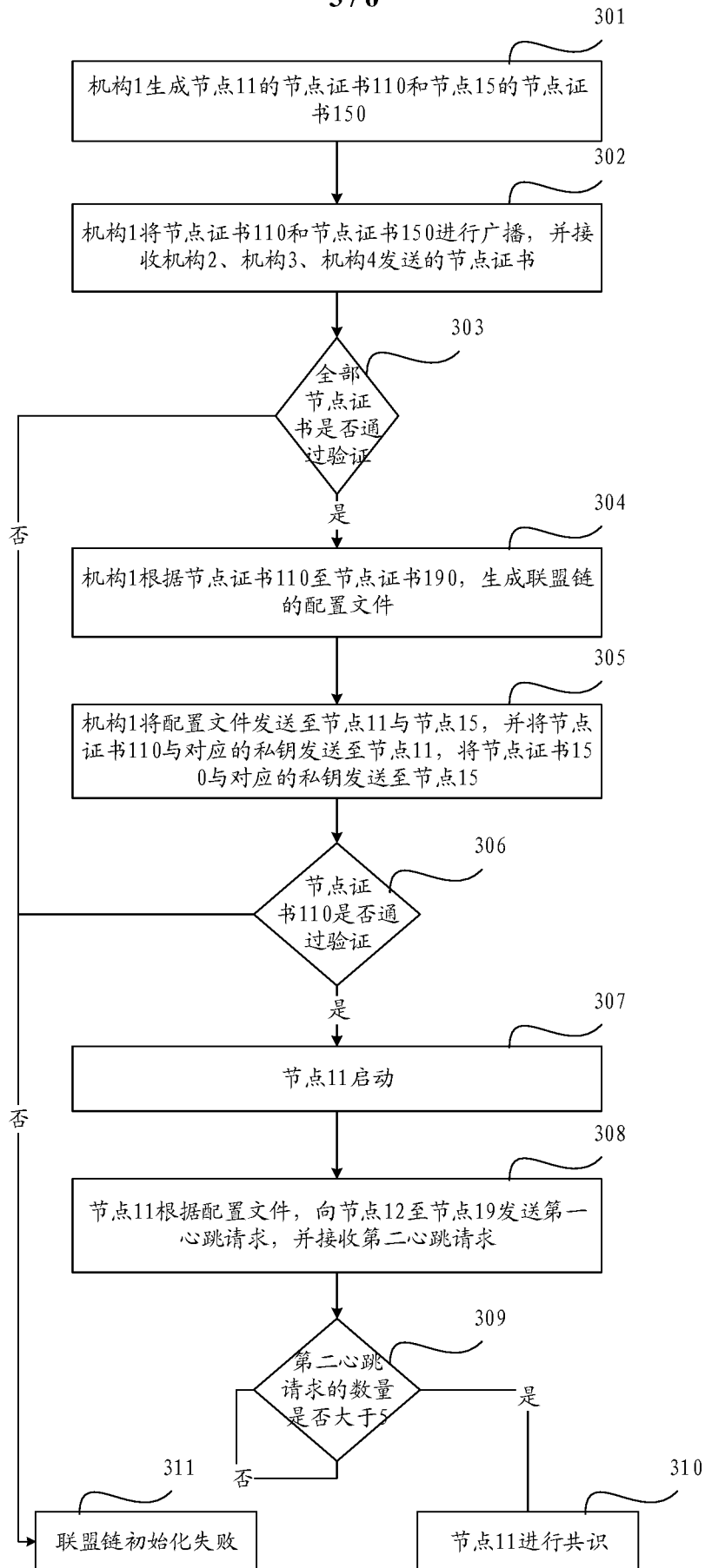


图 3

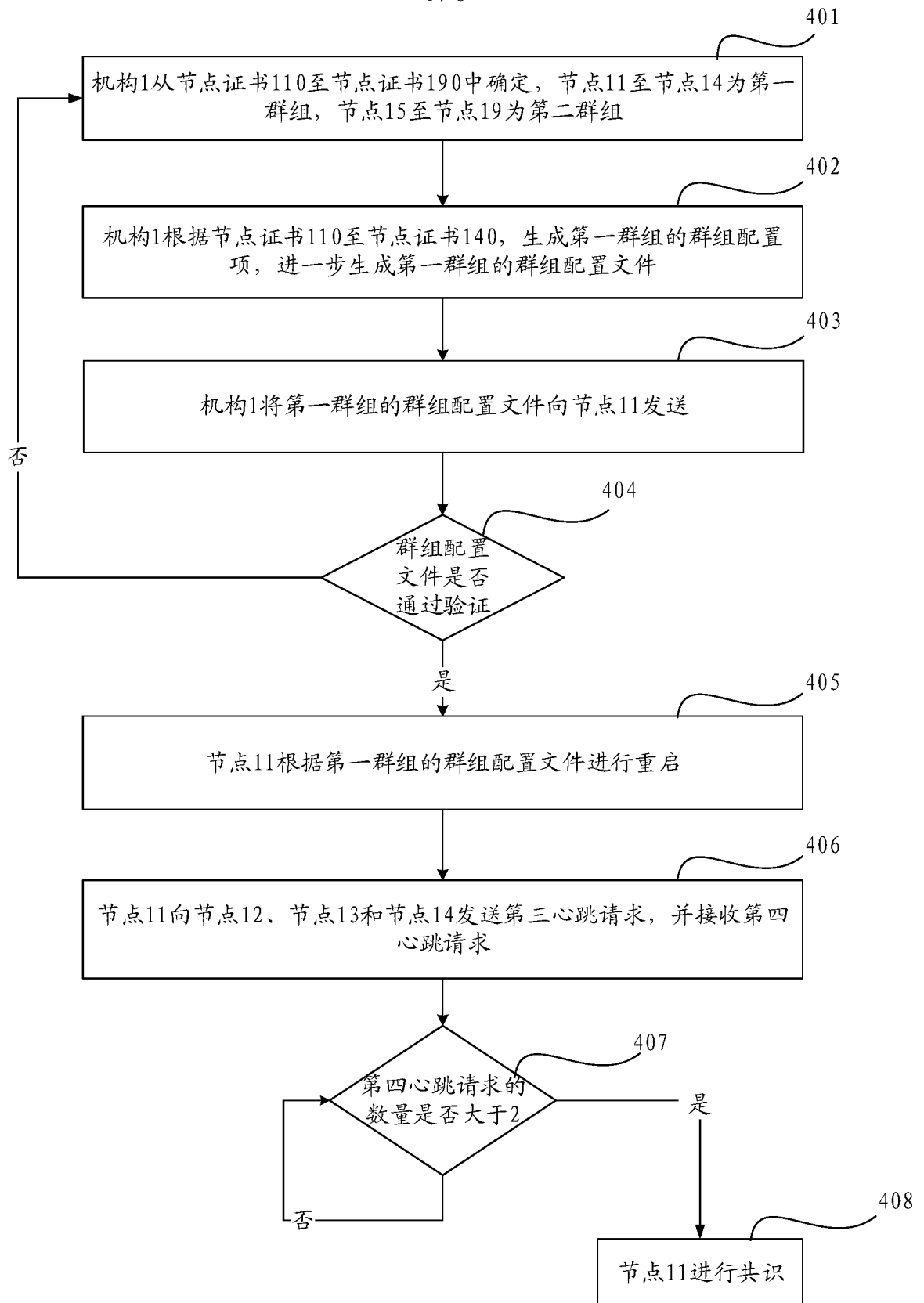


图 4

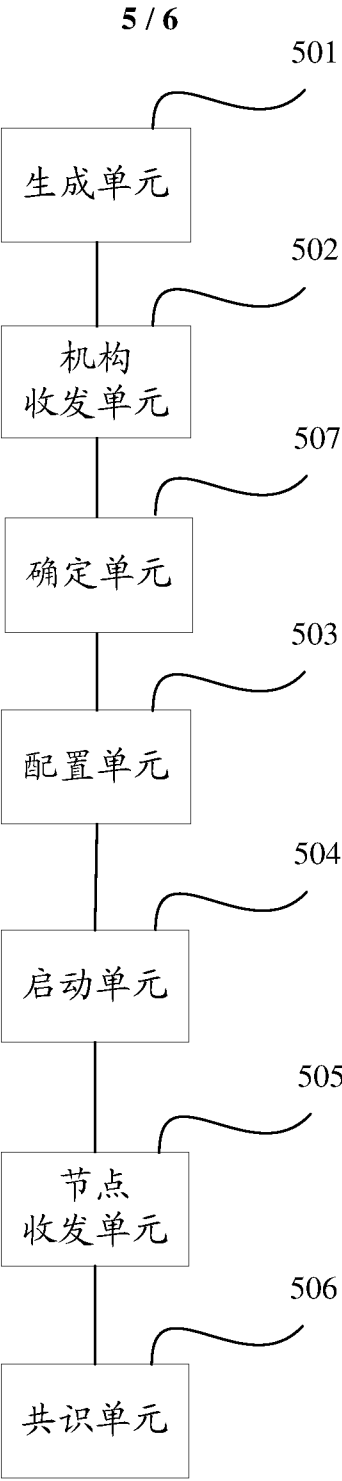


图 5

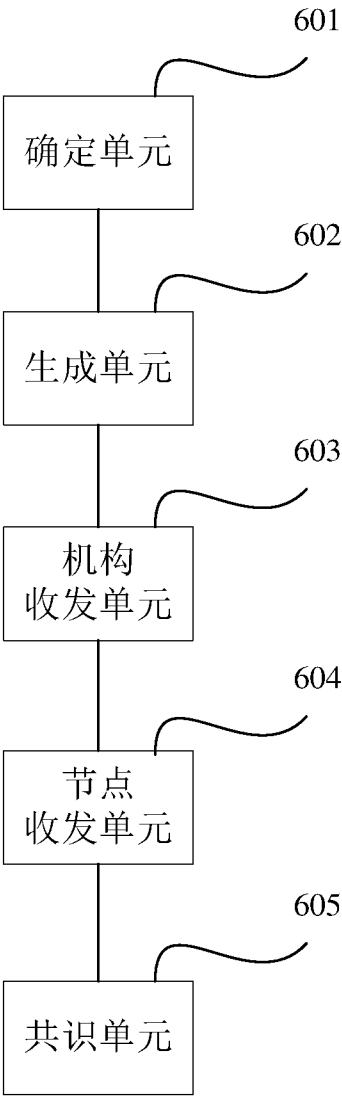


图 6

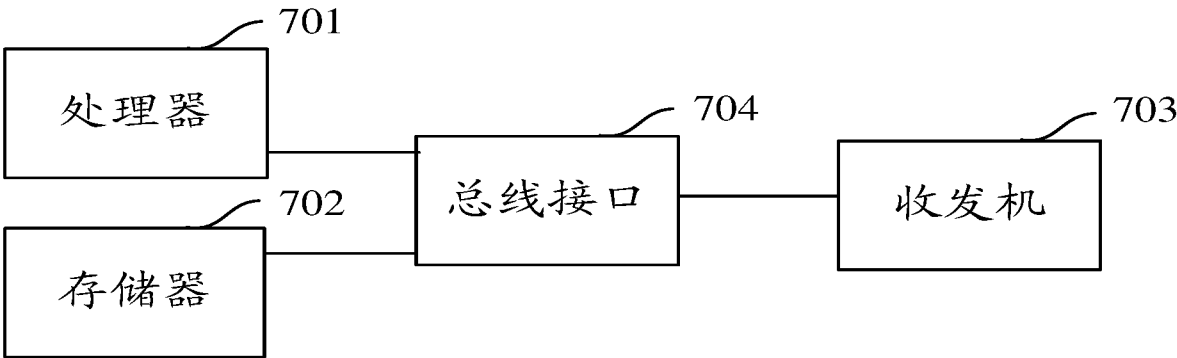


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/074750

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 12/26(2006.01)n

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; G06F

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

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

CNKI, CNPAT, WPI, EPODOC: 机构, 组织, 公司, 区块链, 联盟, 证书, 配置, 私钥, 群组, 集群, 组, 群, 广播, 激活, 启动, 集群, 验证, organization, group, union, blockchain, block chain, cluster, broadcast, active, startup, start, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110035059 A (SHENZHEN QIANHAI WEIZHONG BANK CO., LTD.) 19 July 2019 (2019-07-19) claims 1-16, and description, paragraphs [0079]-[0191]	1-16
X	CN 109040279 A (BEIJING JD FINANCE TECHNOLOGY HOLDING CO., LTD.) 18 December 2018 (2018-12-18) description, paragraphs [0034]-[0098] and [0153]-[0157]	1, 2, 5, 9, 10, 15, 16
A	CN 109040279 A (BEIJING JD FINANCE TECHNOLOGY HOLDING CO LTD.) 18 December 2018 (2018-12-18) description, paragraphs [0034]-[0098] and [0153]-[0157]	3, 4, 6-8, 11-14
A	CN 109242467 A (KINGDEE SOFTWARE (CHINA) CO., LTD.) 18 January 2019 (2019-01-18) description, paragraphs [0058]-[0067]	1-16
A	CN 108683630 A (ALIBABA GROUP HOLDING LIMITED) 19 October 2018 (2018-10-19) entire document	1-16
A	WO 2017127564 A1 (PRIV8PAY, INC.) 27 July 2017 (2017-07-27) 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

“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

28 April 2020

Date of mailing of the international search report

15 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/CN2020/074750

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109167771 A (BEIJING JD FINANCE TECHNOLOGY HOLDING CO., LTD.) 08 January 2019 (2019-01-08) entire document	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/074750

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110035059	A	19 July 2019	None			
CN	109040279	A	18 December 2018	None			
CN	109242467	A	18 January 2019	None			
CN	108683630	A	19 October 2018	US	2019305958	A1	03 October 2019
				WO	2019195108	A1	10 October 2019
				TW	201943250	A	01 November 2019
				HK	1262431	A0	17 January 2020
WO	2017127564	A1	27 July 2017	US	2018137512	A1	17 May 2018
				EP	3405862	A1	28 November 2018
CN	109167771	A	08 January 2019	WO	2020038361	A1	27 February 2020

国际检索报告

国际申请号

PCT/CN2020/074750

A. 主题的分类 H04L 29/06 (2006.01)i; H04L 12/26 (2006.01)n 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; G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNPAT, WPI, EPDOC: 机构, 组织, 公司, 区块链, 联盟, 证书, 配置, 私钥, 群组, 集群, 组, 群, 广播, 激活, 启动, 集群, 验证, organization, group, union, blockchain, block chain, cluster, broadcast, active, startup, start, validate		
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 110035059 A (深圳前海微众银行股份有限公司) 2019年 7月 19日 (2019 - 07 - 19) 权利要求1-16, 说明书第[0079]-[0191]段	1-16
X	CN 109040279 A (北京京东金融科技控股有限公司) 2018年 12月 18日 (2018 - 12 - 18) 说明书第[0034]-[0098]、[0153]-[0157]段	1-2, 5, 9-10, 15, 16
A	CN 109040279 A (北京京东金融科技控股有限公司) 2018年 12月 18日 (2018 - 12 - 18) 说明书第[0034]-[0098]、[0153]-[0157]段	3-4, 6-8, 11-14
A	CN 109242467 A (金蝶软件中国有限公司) 2019年 1月 18日 (2019 - 01 - 18) 说明书第[0058]-[0067]段	1-16
A	CN 108683630 A (阿里巴巴集团控股有限公司) 2018年 10月 19日 (2018 - 10 - 19) 全文	1-16
A	WO 2017127564 A1 (PRIV8PAY, INC.) 2017年 7月 27日 (2017 - 07 - 27) 全文	1-16
A	CN 109167771 A (北京京东金融科技控股有限公司) 2019年 1月 8日 (2019 - 01 - 08) 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 “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 4月 28日		国际检索报告邮寄日期 2020年 5月 15日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 李晓利 电话号码 86-(10)-53961772

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/074750

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	110035059	A	2019年 7月 19日	无			
CN	109040279	A	2018年 12月 18日	无			
CN	109242467	A	2019年 1月 18日	无			
CN	108683630	A	2018年 10月 19日	US	2019305958	A1	2019年 10月 3日
				WO	2019195108	A1	2019年 10月 10日
				TW	201943250	A	2019年 11月 1日
				HK	1262431	A0	2020年 1月 17日
WO	2017127564	A1	2017年 7月 27日	US	2018137512	A1	2018年 5月 17日
				EP	3405862	A1	2018年 11月 28日
CN	109167771	A	2019年 1月 8日	WO	2020038361	A1	2020年 2月 27日