

(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 2020/142907 A1

(43) 国际公布日

2020 年 7 月 16 日 (16.07.2020)

(51) 国际专利分类号:

G06Q 20/38 (2012.01)

(21) 国际申请号:

PCT/CN2019/070888

(22) 国际申请日:

2019 年 1 月 8 日 (08.01.2019)

(25) 申请语言:

中文

(26) 公布语言:

中文

(72) 发明人: 及

(71) 申请人: 张季恒(ZHANG, Jiheng) [CN/CN]; 中国香港特别行政区西贡区清水湾大学道1号香港科技大学工业工程与决策分析系, Hong Kong (CN)。

(72) 发明人: 何家豪(HE, Jiahao); 中国香港特别行政区西贡区清水湾大学道1号香港科技大学工业工程与决策分析系, Hong Kong (CN)。 王光举(WANG, Guangju); 中国香港特别行政区西

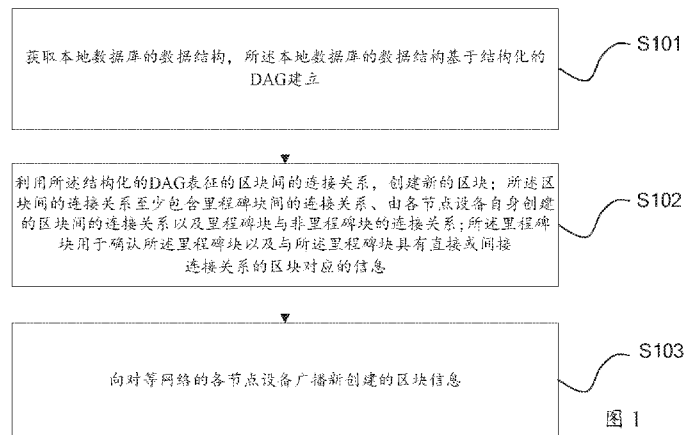
贡区清水湾大学道1号香港科技大学工业工程与决策分析系, Hong Kong (CN)。 张光远(ZHANG, Guangyuan); 中国香港特别行政区西贡区清水湾大学道1号香港科技大学工业工程与决策分析系, Hong Kong (CN)。

(74) 代理人: 北京恒都律师事务所(BEIJING HENGDU LAW FIRM); 中国北京市朝阳区建国门外大街1号国贸大厦3期B座50层, Beijing 100004 (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,

(54) Title: METHOD AND APPARATUS FOR CREATING AND ADDING BLOCK BASED ON STRUCTURED DIRECTED ACYCLIC GRAPH, AND METHOD AND APPARATUS FOR ESTABLISHING ACCOUNT BOOK

(54) 发明名称: 基于有向无环图的区块创建、添加、账本建立方法和装置



- S101 Obtain a data structure of a local database, said data structure being established on the basis of a structured DAG
- S102 Create a new block using an inter-block connection relationship represented by the structured DAG, said connection relationship comprising at least an inter-milestone-block connection relationship, an inter-block connection relationship created by each node device itself, and a connection relationship between a milestone block and a non-milestone block, the milestone block being used for confirming information corresponding to the milestone block and the blocks that have a direct or indirect connection relationship with the milestone block
- S103 Broadcast the information about the newly created block to each node device of a peer-to-peer network

图 1

(57) Abstract: A method and apparatus for creating and adding a block based on a structured directed acyclic graph, and a method and apparatus for establishing a distributed account book. A chain structure is extended to a DAG while a proof-of-work (PoW) mechanism and a Nakamoto consensus method are used, so as to achieve the technical effects of expanding the capacity, shortening the latency, and implementing mining hash rate decentralization, and increasing the processing opportunity of transactions with low fees without

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,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, 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))。

sacrificing security and decentralization.

(57) 摘要: 一种基于结构化有向无环图DAG的区块创建、添加、分布式账本建立方法和装置。在使用工作量证明机制PoW和中本聪共识方法的同时, 将链式结构扩展到DAG中, 以在不牺牲安全性和去中心化的前提下, 实现扩大容量、缩短延迟、挖矿算力去中心化、增加费用少的交易的处理机会的技术效果。

基于有向无环图的区块创建、添加、账本建立方法和装置

技术领域

本申请涉及计算机技术领域，特别地，涉及一种基于结构化有向无环图的区块创建、添加、分布式账本建立方法和装置。

背景技术

区块链（英文全称为 Block Chain）技术本质上是一种共识机制设计，该技术基于以分布式方式在对等网络上存储信息的链结构。以比特币为例，将一些交易组合在一起，并存储在一个小于 1 兆字节的区块中，所有区块都以链状结构连接。这可能不是存储信息的最有效方式。但是，在利用哈希算法、公开密钥、私有密钥等加密函数进行完整性检查和验证的基础上，基于链式结构提出的“中本聪共识”实现了安全性和去中心化。比特币和以太坊的出现和发展，证明了区块链技术取得巨大成功。这不仅是一个社会实验，证明了去中心化和安全的公开总账系统的可能性，而且对于金融市场也有很大影响，创建了一个具有可扩展服务和应用程序的全新生态系统。

分布式记账系统中出现的第一个问题就是谁有权通过形成一个区块来完成记账工作。这一问题是通过使用工作量证明机制(英文全称为 Proof of Work，英文简称为 PoW)来解决的，它要求所有参与者通过调整随机数来竞争解决加密难题，以便哈希结果显示某种所需模式。在特定期间内，可能只有一个矿工能够形成这样的区块，而这段时间足够在网络上传播指定大小的区块，这是一大难题。下一个问题是如何铸造历史，因为区块中的信息需要认证。矿工在创建未来区块的时候，可以选择不同意历史中某个区块的信息，他们只需在这个区块前进行分叉。基于大多数人群总是诚实的这一假设，所有诚实的矿工最终能够在有效区块链上达成一致，而在分支上的则是无效区块。因此，全部区块形成了一棵树，树中最长的链由所有诚实的矿工遵从工作量证明机制共同创造，被称为中本聪链，从而创造了历史。

随着区块链技术被越来越多的人所接受，它正面临着一个严重的瓶颈，那就是非常有限的容量，即每秒交易数量(英文全称为 transactions per second，英文

简称为 TPS)。消除这一瓶颈是推进区块链技术的重大突破, 并为其广泛应用开启了可能性。然而, 扩大容量不应在安全与去中心化上做出任何妥协。

受限于链式结构, 可以尝试增加区块大小, 等效地减少区块间的时间间隔, 或者两种方法的组合来增加每秒交易数量(TPS)。但是, 较大的块需要较长的时间来通过对等网络传送。即使在没有恶意矿工的情况下, 这种尝试也会增加分叉块的出现。因此, 需要超越链式结构进行探索, 以便将容量增加一个数量级。这自然引发了将链式区块(英文全称为 chain of blocks)扩展为区块的有向无环图(英文全称为 Directed Acyclic Graphs, 英文简称为 DAG)的想法。在现有的另一种区块创建方法中, 每个人都有权组建一个小区块, 而不需要运用工作量证明机制。区块的有效性是由直接或间接附加到它的未来块来证明的。然而, 这种方式很容易受到平衡攻击, 并需要“权重更新”来计算附加到它的区块数量, 计算成本昂贵。此外, 在当前的区块链系统中, 容量并不是唯一的问题。随着哈希算力(英文全称为 hashing power)不断提高, 加密难题变得越来越困难。期望具有一定哈希算力的矿工能够挖掘一定数量的区块, 从而获得相应的奖励。然而, 巨大的波动性迫使大多数矿工加入挖矿池以平稳收入, 导致哈希算力集中在少数几个大型矿池, 违背了分布式记账系统去中心化的初衷。另一个瓶颈是高延迟, 因为确认交易需要很长时间。此外, 出于自身利益考虑, 矿工希望将提供高交易费用的交易打包进区块, 以实现报酬最大化。因此, 交易费用很少或为零的交易几乎没有机会被处理。

因此, 需要一种区块创建和共识建立方法, 解决现有技术存在的容量有限、高延迟、算力集中的技术问题。

发明内容

本申请提供一种基于结构化有向无环图的区块创建、添加、分布式账本建立方法和装置, 用于解决现有技术存在容量有限、高延迟、算力集中的技术问题。

根据本申请实施例的第一方面, 公开了一种基于结构化有向无环图的区块创建方法, 应用于对等网络中的节点设备, 包括: 获取本地数据库的数据结构, 所述本地数据库的数据结构基于结构化的 DAG 建立; 利用所述结构化的 DAG 表征的区块间的连接关系, 创建新的区块; 所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑

块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息；向对等网络的各节点设备广播新创建的区块信息。

根据本申请实施例的第二方面，公开了一种基于结构化 DAG 的区块添加方法，应用于对等网络中的节点设备，包括：接收一节点设备发送的新区块信息；判断所述新区块信息是否满足设定条件；若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

根据本申请实施例的第三方面，公开了一种分布式账本建立方法，所述方法包括：获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

根据本申请实施例的第四方面，公开了一种基于结构化 DAG 的区块创建装置，包括：获取单元，用于获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立；创建单元，用于利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息；广播单元，用于向对等网络的各节点设备广播新创建的区块信息。

根据本申请实施例的第五方面，公开了一种基于结构化 DAG 的区块创建装置，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行如第一方面所述的基于结构化 DAG

的区块创建方法。

根据本申请实施例的第六方面，公开了一种存储介质，所述存储介质存储有用于执行如第一方面所述的基于结构化 DAG 的区块创建方法的程序。

根据本申请实施例的第七方面，公开了一种基于结构化 DAG 的区块添加装置，包括：接收单元，用于接收一节点设备发送的新区块信息；判断单元，用于判断所述新区块信息是否满足设定条件；添加单元，用于若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

根据本申请实施例的第八方面，公开了一种基于结构化 DAG 的区块添加装置，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行如第二方面所述的基于结构化 DAG 的区块添加方法。

根据本申请实施例的第九方面，公开了一种存储介质，所述存储介质存储有用于执行如第二方面所述的基于结构化 DAG 的区块添加方法的程序。

根据本申请实施例的第十方面，公开了一种分布式账本建立装置，包括：获取单元，用于获取新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块信息；更新单元，用于根据获取的所述新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

根据本申请实施例的第十一方面，公开了一种基于结构化 DAG 的区块添加装置，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行如第三方面所述的分布式账本建立方法。

根据本申请实施例的第十二方面，公开了一种存储介质，所述存储介质存储有用于执行如第三方面所述的分布式账本建立方法的程序。

根据本申请实施例的第十三方面，公开了一种基于 DAG 的区块数据处理装置，其中，所述装置包括：

创建模块，用于获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立；利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息；向对等网络的各节点设备广播新创建的区块信息；

添加模块，用于接收一节点设备发送的新区块信息；判断所述新区块信息是否满足设定条件；若满足，将所述新区块信息添加到所述节点设备的本地数据库中；

分布式账本建立模块，用于获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系。

与现有技术相比，本申请实施例具有以下优点：本申请基于结构化的 DAG，实现了节点设备区块的创建、添加、统一分布式账本的建立，提高了对等网络的容量、缩短了延迟、实现了算力的去中心化。

本申请实施例提供的基于结构化 DAG 的区块创建方法中，在节点设备创建区块时，获取基于结构化 DAG 建立的本地数据库的数据结构，利用该数据结构中结构化 DAG 表征的区块间的连接关系，创建新的区块，并向对等网络的各节点设备广播新创建的区块信息。由于在创建区块时，利用了区块间的连接关系，包括里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系，在增强区块间的连接性的同时，使用里程碑块的确认作用大规模地达成了共识并且交易很快能被处理和确认，在保证安全和去中心化的前提下，增加了网络容量、缩短了延迟、实现了算力的去中心化。

本申请实施例提供的基于结构化 DAG 的区块添加方法，在节点设备接收到

新区块信息时，首先判断所述新区块信息是否满足设定条件；若满足，将所述新区块信息添加到所述节点设备的本地数据库中。由于该本地数据库基于结构化的 DAG 创建，并能够表征区块间的连接关系，在增强区块间的连接性的同时，使得网络中的节点设备保持同样的数据结构，在保证安全和去中心化的前提下，增加了网络容量、缩短了延迟、实现了算力的去中心化。

本申请实施例提供的分布式账本建立方法，获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本。由于里程碑块的确认作用大规模地达成了共识并且交易很快能被处理和确认，在保证安全和去中心化的前提下，增加了网络容量、缩短了延迟、实现了算力的去中心化，并实现了统一分布式账本的建立。

附图说明

附图仅用于示出优选实施方式的目的，而并不认为是对本申请的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为本申请实施例基于结构化 DAG 的区块创建方法的流程图；

图 2 为本申请实施例提供的 DAG 示意图；

图 3 为本申请实施例基于结构化 DAG 区块添加方法的流程图；

图 4 为本申请实施例分布式账本建立方法的流程图；

图 5 为本申请基于结构化 DAG 的区块创建装置一实施例的结构示意图；

图 6 为本申请基于结构化 DAG 的区块创建装置一实施例的结构示意图；

图 7 为本申请基于结构化 DAG 的区块添加装置一实施例的结构示意图；

图 8 为本申请基于结构化 DAG 的区块添加装置一实施例的结构示意图；

图 9 为本申请分布式账本建立装置一实施例的结构示意图；

图 10 为本申请分布式账本建立装置一实施例的结构示意图；

图 11 为本申请基于 DAG 的区块数据处理装置一实施例的结构示意图。

具体实施方式

首先对本申请的思想进行阐述。本申请提供了一种基于结构化 DAG 的区块创建、添加、分布式账本建立方法，使得节点能够就工作量证明机制(PoW)在大范围内达成共识，并建立统一的分布式账本。此外，本申请还提供了一种基于

结构化有向无环图(DAG)的交易池交易分配方法,使得由多个矿工处理一笔交易的概率可以忽略不计。由此,在不牺牲安全性和去中心化的情况下,容量得到显著扩大。

在本申请实施例中,在使用工作量证明机制(PoW)和中本聪共识方法的同时,将链式结构扩展到有向无环图中,以在不牺牲安全性和去中心化的前提下,实现扩大容量、缩短延迟、挖矿算力去中心化、增加费用少的交易的处理机会的技术效果。

本申请实施例通过在结构化有向无环图(structured DAG)中嵌入中本聪链(Nakamoto chain),其具有强连接性和记录各个节点信息的功能。通过这种方式,方案的安全性得到了经证实的中本聪共识的保证。基于得到保障的安全性,本申请利用有向无环图结构中的强连接性来增加吞吐量并缩短延迟。有向无环图还提供交易排序,以便所有诚实的节点(矿工)一旦就有向无环图达成共识,就能够建立统一的分布式账本。

本申请实施例中,把大区块分成众多小区块。为了方便实施,本申请实施例实际上自始至终不断地将每笔交易打包进更小、更简单的区块内,而不是偶尔一次性广播一大批交易。如上所述,区块链的一个主要瓶颈是其线性结构,它禁止不同区块间的和区块大小与同步时间之间的权衡。使用小区块允许快速点对点传送和并行,从而显著提高吞吐量。为了安全和稳健性,本申请出于安全的目的在有向无环图中散置相对更难的区块,并称之为里程碑。本申请的有向无环图源自创世区块,该区块包含一组可信信息。创建区块的工作流程不管是否为里程碑,都是相同的。每个节点在准备其新区块时,是按照其最新的认知来准备三个不同的指针进行有效的交易。第一个指针指向节点的前一个区块,如果该节点没有前一个区块,则指向创世区块。根据这一需求,每个节点都将有一个节点链来表示该节点的状态,使得合并节点“标识”和哈希算力等信息成为可能。第二个指针指向上一个里程碑(milestone),若没有上一个的里程碑,则指向创世区块,如果有分叉的话,则遵循传统的最长链原则。这个指针是必需的,因为节点并不知道它是否会成为里程碑。如果这个区块被证明是里程碑,需要连接所有的里程碑来形成中本聪链。最后一个指针需指向另一个节点新近的常规区块,以增强节点链之间的连接性。需要注意的是,指向一个太旧的区

块对连接性的贡献很小，因此并不合乎需要。本申请中对奖励的设计机制有效的使节点没有动机进行此类行为。本申请的有向无环图结构如图2所示，其中突出显示了节点链和中本聪链。

在创建一个区块之后，节点就会通过调整随机数产生该区块的哈希值。如果哈希值显示了某种所需特征，例如前10位为0，那么这就是一个有效的块。如果运气好的话，哈希值具备了一个更难出现的特征，例如：前15位为0，那么它就是一个里程碑区块。无论区块为哪种类型，它都充当了交易的容器。

这些里程碑区块形成了中本聪链，在达成共识方面起到了关键作用。请注意，区块是否为里程碑只有在挖矿完成后才会显示，且仅由运气决定。没有节点能仅将其哈希算力用于里程碑区块，因为创建任何区块的工作流程都是相同的。

这样的设计不仅仅是扩大了容量，并且里程碑区块链是完全去中心化的，有助于以中本聪链一样的方式达成共识。因为一个区块会很快被一系列里程碑区块链所确认，所以延迟减少了。这里的“确认”是指，由里程碑区块到达其的路径由一系列上述三类指针构成。较小的区块虽然产生较少的回报，但并不需要进行较费力的哈希算法。这大大降低了矿工报酬的波动性，因此矿工不需要依赖加入矿池以平稳收入。

随着容量的扩大，一笔交易更有可能短时间内被多个节点处理。虽然这种冲突可以通过共识来解决，但多个区块包含相同一笔交易是对算力的浪费。因此，需要一种机制来避免这种冲突。其主要思路是根据节点的哈希算力将交易池中的所有交易“划分”给各节点。这就需要关于各个节点的状态和其对应的算力信息，这些信息由节点链提供。如果一笔交易与某个节点的最新区块的哈希值满足某个特征，例如，前若干位为0，那么这个交易可以被该节点处理。节点允许创建没有交易信息的“空”区块，并且只获得创建区块的奖励。如本申请的分析所示，通过仔细计算参数，这种方法有效地减少了一笔交易被多个矿工处理的机会。

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

在本申请实施例的描述中，需要理解的是，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的

数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者多个该特征。“多个”的含义是两个或两个以上，除非另有明确具体的限定。术语“包括”、“包含”及类似术语应该被理解为是开放性的术语，即“包括/包含但不限于”。术语“基于”是“至少部分地基于”。术语“一实施例”表示“至少一个实施例”；术语“另一实施例”表示“至少一个另外的实施例”。其他术语的相关定义将在下文描述中给出。

参考图 1，示出了本申请基于结构化有向无环图的区块创建方法一实施例的流程，执行主体为对等网络中的节点设备。本优选方法实施例包括以下步骤：

S101：节点设备获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立。

S102：节点设备利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系。所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

S103：节点设备向对等网络的各节点设备广播新创建的区块信息。

在本申请实施例中，对等网络的各节点设备（以下简称节点）在本地会以接收到的区块信息、基于结构化 DAG 建立本地数据库。所述本地数据库的数据结构基于结构化的 DAG 建立。如图 2 所示，为本申请实施例提供的结构化 DAG 示意图。

在本申请实施例中，所述结构化的 DAG 至少包含由各里程碑块连接而成的里程碑链以及由各节点设备自身创建的区块连接而成的对等节点链；所述对等节点链中的各区块至少指向一个里程碑块。其中，所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。所述区块对应的信息例如可以是区块对应的交易信息。在一些实施方式中，所述各节点设备的分布式账本包含的交易信息由所述里程碑块以及与所述里程碑块直接或间接连接的区块承载。在本申请各实施例中，将节点设备在本地维护的分布式账本又称之为本地分布式账本或者本地账本。在一些实施方式中，所述结构化的 DAG 表征的区块间的连接关系还包含非里程碑块与非里程碑块间的连接关系。所述对等节点链中的各区块还可以指向一个非里程碑块。在一种可能的实施方式中，所述利用所述结构化的 DAG 表征的区块间的连接关系，创建新

的区块包括:利用所述结构化的DAG表征的区块间的连接关系组建新区块信息,所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与所述结构化的DAG包含的区块的连接关系、随机数;调整所述新区块信息包含的随机数,直到所述新区块信息的哈希结果满足第一难度条件。其中,第一难度条件可以根据需要设置。其中,所述新区块信息还可以包括节点设备的信息,例如节点设备标识。进一步地,当调整所述新区块信息包含的随机数且确定所述新区块信息的哈希结果满足第二难度条件时,确认所述新区块为里程碑块。所述各节点设备的分布式账本包含的交易信息由所述里程碑块以及与所述里程碑块直接或间接连接的区块承载。其中,第二难度条件可以根据需要设置。

在一种可能的实施方式中,所述新区块与所述结构化的DAG包含的区块的连接关系至少包括:所述新区块指向所述结构化的DAG的最长里程碑链中最新生成的一个里程碑块的指针;所述新区块指向所述结构化的DAG中对等节点链中最新生成的一个区块的指针。进一步地,所述新区块与所述结构化的DAG包含的区块的连接关系还包括:所述新区块指向所述结构化的DAG中由其他节点创建的最近一个区块。需要说明的是,节点设备在从交易池中选择交易信息时,可以随机选取自己感兴趣的交易。当然,为了避免算力集中以及低费用交易不被处理的风险,可以依据一定的方式实现交易的分配。例如,可以根据各节点设备的算力信息分配交易池中的交易。

下面结合实例和附图对结构化的DAG以及本申请实施例提供的区块创建方法进行介绍。

在众多应用中,图形可以描述一个数据结构,每个“顶点”表示一个基本的信息单元,每个“边”表示两个单元之间的关系。本申请提出的结构化有向无环图描述了分布式账本的数据结构,所有节点都试图以分布式方式维护该数据结构。本申请实施例首先描述有向无环图中每个元素(即区块)的结构。

作为一个基本的信息单元,一个区块应该包含一条消息(message),这是一些基本数据如加密货币应用程序的交易信息,以及一些指向其他区块的指针,以便在有向无环图中对该区块定位。为了保证完整性,本申请实施例要求每个区块都遵循工作量证明机制。具体来说,假设存在一个随机哈希函数,它将任意长度的字符串映射成唯一标识。在实现时,本申请实施例将使用一个相当好的加密哈希函数,例如SHA-256,作为随机加密哈希函数,用于加密区块信息,记作 $H(B)$,以表示区块的标识。在进行区块完整性校验时,可以通过验证区块标

识是否与哈希计算结果匹配来进行区块校验。

在一种可能的实施方式中，组建新区块时，具体可以包括：选择当前数据库中，最长里程碑链的最近的一个区块的标识 ID，记录在新块中；选择本节点“节点链”最近的一个区块的标识 ID，记录在新块中；选择其他一个节点，选择其“节点链”的最近的一个区块的标识 ID，记录在新块中；选择当前交易池中一个交易，记录在新块中。之后，在新区块中不断尝试不同的随机数（nonce），直到新区块的哈希结果满足第一难度要求。

下面以一个实例进行说明。举例说明，对于区块 B 而言，可用公式 (1) 描述区块 B 的区块信息：

$$B = (id_{prev}, id_{ms}, id_{tip}, peer, nonce, message), \quad (1)$$

其中 $(id_{prev}, id_{ms}, id_{tip})$ 是有向无环图中各区块的唯一标识，节点（peer）是在这个区块上工作的节点，随机数(nouce)是一个加密难题的解决方案，message 用于表示交易信息。此外，本申请实施例将 genesis O 定义为包含某些可信准备资料的特殊区块，即创世区块。

在本申请实施例提供的方法中，还包含工作量证明机制。节点应该对随机数进行调整，直到 $H(B)$ 区块的哈希值显示某种模式。假设哈希值 $H(B)$ 是一个由 0、1 组成的字符串，“ $\cdot(H(B))$ ”将这个字符串转换为 $[0,1]$ 中的一个数字。由于哈希函数是随机的，对于任意区块的随机数值，“ $\cdot(H(B))$ ”在 $[0,1]$ 区间内为先验均匀分布。为了证明工作量，一个节点需要调整随机数的取值，使得区块的哈希符合普通区块的难度要求，例如使“ $\cdot(H(B)) < d$ ”，其中 d 称为难度值。 $H(B)$ 哈希值也用作区块 B 的标识。

在所有区块中，本申请实施例允许其中一部分为特殊类型，称其为里程碑。在一种可能的实施方式中，若当调整所述新区块信息包含的随机数且确定所述新区块信息的哈希结果满足第二难度条件时，确认所述新区块为里程碑块。举例说明，如果“ $\cdot(H(B)) < pd$ ”，则该区块为里程碑，其中 p 为里程碑占有所有区块的比例。需要注意的是，节点在进行哈希计算之前就必须明确区块的所有信息，包括三个指针，交易信息，创建节点，随机数；只有当其进行哈希计算后，才能知道这个区块是否会成为里程碑区块。换句话说，节点不能决定它们是针对里程碑还是非里程碑区块在工作。一个节点可能会在获得一个哈希值“ $\cdot(H(B)) \in [d \cdot d, d)$ ”继续工作，使其成为里程碑。然而，仅将节点的哈希算

力全部用于创建里程碑区块，并不会使其所能够创建的里程碑区块的期望值改变。因此，专门为里程碑区块而工作不能给节点带来经济上的好处。

为了描述本申请实施例提供的有向无环图中的结构，下面解释三个指针 $(id_{prev}, id_{ms}, id_{np})$ 。

在本申请实施例中，由各节点设备自身创建的区块连接而成的链称为对等节点链 (Peer Chain)，又可称为节点链。在区块信息中，指针 id_{prev} 被设计为指向由同一节点挖掘的最新区块，如果节点以前没有挖掘过任何区块，则指向创世区块。通过这种机制，同一节点挖掘出的区块被组成一个链，即节点链。节点链的设计目的是保持有向无环图的简洁结构，减轻延迟挖掘的影响。它还提供了有价值的信息，包括节点的哈希算力估计和挖矿历史记录。节点链头部为该节点链的最后一个区块，也表明了该节点的状态。

本申请实施例将介绍一个利用节点状态的交易方式。形式上，本申请实施例要求满足以下条件：

$$B.id_{prev} = H(B') \implies \{B'.peer = B.peer\} \text{ or } \{B' = 0\}. \quad (2)$$

从公式 (2) 可以看出，节点设备对应的节点链中的区块要么指向该节点设备自身创建的区块，要么指向创世区块。较佳地，指针 id_{prev} 指向由同一节点挖掘的最新区块。

需要注意的是，这种数学方面的要求不能防止恶意使用，例如分叉(不附加到节点最新挖掘的区块)和攻击(例如在另一个节点链上挖矿)。本申请实施例中，恶意节点的攻击只能浪费少量的系统容量，而不会影响共识，也不会使自己受益。

为了增强不同节点链之间的连接性，本申请实施例使用 id_{np} 指向另一个节点的非里程碑区块。当这样的区块不存在时，创世块 genesis 0 被设置为默认值。在形式上：

$$B.id_{np} = H(B_i) \implies \{B_i.peer \neq B.peer, H(B_i) \in [p \cdot d, d]\} \text{ or } \{B_i = 0\}. \quad (3)$$

需要说明的是， id_{np} 用于指向另一节点设备创建的普通块或者创世块，用于增强节点间的连接性。需要说明的是，在本申请具体实现时，可以在公式 (1) 中包含多个 id_{np} 。也就是说，可以定义新创建区块指向多个普通块的指针，以增强节点间的连接性。

有向边，即区块 B 指向 B_i ，起着确认之前区块的作用。区块间的连接更强导

确认速度就会更快。理论上,一个区块中可以有多条这样的边。然而,这些边必须被所有节点同步和存储,因此,更多的边会导致更高的间接费用。本申请实施例中,在 DAG 中嵌入里程碑区块链。其中,指针 id_{ms} 指向里程碑区块 B_m 或创世区块 genesis O,其中,里程碑块的哈希计算结果满足第二难度条件,即:

$$B.id_{ms} = H(B_m) \implies \{H(B_m) < p \cdot d\} \text{ or } \{B_m = O\}. \quad (4)$$

从本质上讲,对等网络能够高效地同步小而慢的消息。然而,加密货币系统必须具有高效的吞吐量。里程碑的设计充当了高吞吐量和稳定同步之间的桥梁。每一个里程碑都与一段不可逆转的历史联系在一起。因此,只要节点在所有的里程碑上达成共识,他们就能在历史上达成共识。为了实现这些目标,本申请实施例必须把所有的里程碑放在一个链中。但如前文所述,区块的类型是在挖矿之后确定的。因此,本申请实施例在所有区块上放置一个与里程碑相关的链接。

假设 $\mathcal{G}$ 为包含创世区块 genesis O 的区块集合,使每个非创世区块满足 (2)-(4),且:

$$\forall B \in \mathcal{G}, H(B') = B.id_{key}, key \in \{\text{prev}, \text{ms}, \text{tip}\} \implies B' \in \mathcal{G}. \quad (5)$$

换句话说,所有被 $B \in \mathcal{G}$ 所指向的区块也在 $\mathcal{G}$ 中。从本质上讲,如果本申请实施例把区块视为顶点,将指针指示视为定向边的话,那么 $\mathcal{G}$ 就是一个有向图。如果从区块 B 开始,可以沿着一系列方向一致的边到达区块 B' 。那么就认为存在一条从 B 到 B' 的路径。如果 $\mathcal{G}$ 中的任何区块 B 没有从 B 到其自身的有向通路,则称这种图为无环图。

如果区块的格式满足(1)且它的标识(id)与区块匹配,那么该区块在语法上是有效的。这可以称之为完整性检查,来验证区块头。如果有向无环图 $\mathcal{G}$ 中任何区块在语法上有效,非循环且满足(5),则该有向无环图 $\mathcal{G}$ 在语法上是有效的。如果 $\mathcal{G} \cup \{B\}$ 在语法上是有效的,那么区块 B 对于结构化有向无环图 $\mathcal{G}$ 在语法上有效。节点的第一项任务是确保其本地的有向无环图在语法上是有效。这样的检查可以避免系统被无效的区块淹没。

在本申请实施例的实施方式,里程碑区块树本质上就是有分叉的区块链中的树。同样,每个节点的区块也通过 id_{prev} 形成了一个链。这可以将本申请实施例的设计推广到基于信用的应用程序中。里程碑区块的“链”起着连接所有节点

“链”的作用。指针 id_{ip} 进一步增强了有向无环图的连接性。

参见图 2, 为本申请实施例提供的结构化 DAG 示意图。节点设备 1(peer 1)、节点设备 2(peer 2)、节点设备 3(peer 3)、节点设备 4(peer 4)、节点设备 5(peer 5) 为对等网络中的节点设备。每个节点设备均具有各自的对等节点链, 例如图 2 和图 3 中, 平行的几个链条分别对应各节点设备的节点链。其中, 黑色区块表示里程碑块, 由各里程碑块组成的链称为里程碑链。区块 0 为创世区块。

现在在结构化有向无环图中定义里程碑区块的高度。创世区块的高度为 $\eta(O) = 0$, 对于里程碑区块 B, 即: $H(B) < pd$, 高度定义为:

若满足: $H(B) < pd$ and $B.id_{ms} = B_m.id$

则有: $\eta(B) = \eta(B_m) + 1$

也就是说, 若满足了条件区块 B 指向了区块 B_m 且 $H(B) < pd$, B 的高度即为 B_m 的高度加 1. 其中, 区块 B 为里程碑块。

$\mathcal{G}$ 中创世区块和所有里程碑区块形成一棵树, 其中每个里程碑块的深度就是其的高度。全部里程碑区块的叶节点集合 (leaf set) 为

$$T_m(\mathcal{G}) = \{B_m \in \mathcal{G} : H(B_m) < pd \text{ and } \nexists B'_m \in \mathcal{G} \text{ s.t. } H(B'_m) < pd \text{ and } B'_m.id_{ms} = B_m.id\}. \quad (7)$$

对于叶节点集合 $\eta(B_m) = n$ 中的里程碑区块 B_m , 按照指针 id_{ms} , 可以找到这些区块的序列:

$$B_{m,n} = B_m, B_{m,n-1}, B_{m,n-2}, \dots, B_{m,1}, B_{m,0} = O, \quad (8)$$

对于 $H(B_{m,k}) < pd$ and $B_{m,k}.id_{ms} = B_{m,k-1}.id$, 其中 $k=1, 2, \dots, n$, 本申请实施例中, 将这种序列称为区块 B_m 的里程碑链。因此, 所有里程碑区块的叶节点集合中的每一个区块都代表一个里程碑链, 其长度就是该区块的高度。本申请实施例中, 将结构化有向无环图 $\mathcal{G}$ (sDAG $\mathcal{G}$) 的高度定义为最长链的长度。

$$\eta(\mathcal{G}) = \max\{\eta(B) : B \in T_m(\mathcal{G})\}. \quad (9)$$

需要注意的是, 可能存在多条最长链。要想选择最长的链, 本申请实施例中,

只需要选择叶节点集合中高度最高的区块。第 n 个里程碑区块 (The n th milestone) 则被定义为高度为 n 的最长里程碑链上的区块。

对于任何里程碑区块 $B_m \in \mathcal{G}$, 本申请实施例把由里程碑区块 B_m 确认的结构化有向无环图 (sDAG) 定义为:

$$C(B_m) = \{B \in \mathcal{G} : \text{there exists a path from } B \text{ to } B_m\} \cup \{B_m\}. \quad (10)$$

公式 (10) 定义了被里程碑块 B_m 确认过的块的集合, 该集合包含了这样的块, 即存在一条从 B_m 出发的路径能够到达的块。也就是说, 被里程碑块确认的块的集合, 包括该里程碑块、与里程碑块直接或者间接连接的块。

如果 $B'_m \in \mathcal{G}$ 是区块 B_m 紧随的里程碑区块或创世区块, 即: $B_m.\text{id}_{\text{msg}} = H(B'_m)$, 那么本申请实施例将水平集合定义为:

$$S(B_m, B'_m) = C(B_m) \setminus C(B'_m). \quad (11)$$

结构化有向无环图由遵循协议的对等网络上的所有节点以分布式方式共同创建和维护。遵循此协议的节点称为诚实节点, 而不遵循此协议的节点称为恶意节点。在去中心化系统中, 每个节点都有自己的局部或本地有向无环图 (Local DAG), 受网络同步延迟以及恶意攻击等影响, 可能与其他节点的本地结构化有向无环图 (local sDAG) 不同。但目标是所有诚实节点在结构化有向无环图 (sDAG) 达成共识, 从而各个节点维护的本地账本的信息也是相同的。

对于节点 p , 用 $\mathcal{G}_p$ 表示它的本地 DAG, 本地 DAG 随着该节点创建区块及接收其余节点广播的区块而不断演变。所有诚实的节点从创世区块开始它们的节点链。

下面对创建区块的一个具体实施例进行说明。

如果节点想要创建区块 B , 并使其被所有其他节点接受作为它们的有效本地 DAG 的一部分, 则操作如下。创建区块以包括消息, 即交易信息。因此, 节点需要做的第一件事就是找到一条消息, 其形式与 $\mathcal{G}_p$ 中的消息一致, 并设置:

$$B.\text{mes} = \text{message}$$

首先, 节点需要选择交易。为了与分布式账本构建功能兼容, 此交易的输入应该是 $C(B_m)$ 中的输出之一, B_m 是其有效本地 DAG 中的高度最大的里程碑块。

接下来，节点准备三个指针，以便区块在语法上有效。

1、在其有效的本地 DAG 中选取最高里程碑块 B_m 并设置：

$$B.id_{ms} = H(B_m)$$

通常， B_m 是它知道的最新里程碑区块（即在 G_P 中）。但是，由于网络同步， B_m 不一定是最近里程碑区块。

2、选取在 G_P 中由它自己创建的最新生成的区块 B' ，并设置：

$$B.id_{prev} = H(B_0)$$

如果不存在这样的 B' ，则设置 $B.id_{prev} = H(O)$ 。

注意，区块 B' 和 B 是由同一节点创建的连续区块。

3、将 tip 集定义为本地 DAG(G_P) 中、未由 G_P 中的任何区块指向并且不是由节点自己创建的常规区块的集合。从 tip 集中随机选取一个区块 B_t 并设置：

$$B.id_{tip} = H(B_t),$$

如果 tip 集是 $\{0\}$ 或空，则设置 $B.id_{tip} = H(O)$ 。

这意味着节点需要找到 B_t ，是由某个其他节点创建的常规区块。

最后，节点需要通过对等网络广播 B 。由图论中的经典结果可知，对每一个语义上正确的区块，将在期望为 $O(\log(n))$ 时间内到达所有诚实节点，如果每个诚实的节点在其验证该区块的正确性后立刻将其广播，其中 n 为诚实节点的数量。

参见图 3，为本申请实施例提供的一种基于结构化 DAG 的区块添加方法流程图，应用于对等网络中的节点设备，包括：

S301，节点设备接收一节点设备发送的新区块信息。

S302，节点设备判断所述新区块信息是否满足设定条件。

S303，若满足，节点设备将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系。所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

在一些实施方式中，所述新区块信息至少包括从交易池中选择的交易信息、

所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数。其中，所述新区块信息还可以包括节点设备的信息，例如节点设备标识。

在一些实施方式中，所述新区块与所述结构化的 DAG 包含的区块的连接关系至少包括：所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的指针。

在一些实施方式中，所述新区块与所述结构化的 DAG 包含的区块的连接关系还包括：所述新区块指向所述结构化的 DAG 中由其他节点创建的最近一个区块。

在一些实施方式中，所述判断所述新区块信息是否满足设定条件包括：判断所述新区块信息是否满足语法要求；若满足，判断所述新区块信息的哈希结果是否满足第一难度条件。其中，第一难度条件可以根据需要设定。

在一些实施方式中，所述方法还包括：判断所述新区块所指向的区块是否在本地数据库中；若否，向被所述新区块指向的所述区块的创建节点设备请求所述区块。

在一些实施方式中，所述方法还包括：若判断所述新区块信息包含的交易信息与本地交易池中的第一交易信息相同，在所述本地交易池中移除所述第一交易信息；其中，所述本地交易池中包含待处理的、未被区块承载的交易信息。第一交易信息为本地交易池中任意一个交易信息。

在一些实施方式中，所述方法还包括：判断所述新区块是否为里程碑块；若是，根据所述里程碑块以及与所述里程碑块具有直接或者间接连接的区块信息，更新本地分布式账本。

下面以一个实例进行说明。节点设备可以如下实例设置监听线程，当接收到新区块时，其可以包括以下处理：

A、验证新块是否满足难度要求，如不满足，跳过一下步骤，忽略该块。

具体实现步骤 A 时，节点设备通过监听线程收到的块可以理解为字符串。，节点设备接收新块时，先检查其是否语法有效，即符合块的定义；若其语法有效再对其进行哈希计算，检查其是否小于难度系数。语法无效的块没有进行哈希计算的必要。

B、新块指针所指块是否都在数据库中，如不在，向对等网络请求所缺块；

C、将新块添加到数据库，更新该块所属节点的节点链；

D、检查新块是否满足 milestone 难度要求：

E、若满足，将新块及所有被新块直接或者间接指向的块发送至线下验证算法，并更新数据中的 milestone 链。其中，线下验证算法可以由该节点设备执行。

F、将若新块包含的交易在交易池中，将该交易移出交易池。

举例说明，如果节点由于同步问题没有接收到 B 指向的区块，它应该从其对等节点中查询丢失的区块并执行验证，就像在这些区块之后接收到 B 一样。

在接收到新区块 B 时，节点首先检查 B 在语法上是否对 $\mathcal{G}$ 有效。如果是，通过下述方式进行更新：

$$\mathcal{G} := \mathcal{G} \cup \{B\}$$

也就是说，将新收到的块加入本地 DAG 中，并将其中继到对等节点；否则丢弃。

本申请实施例将交易池定义为保持要处理的所有待处理交易的缓冲区。如果 B 包含在节点的交易池中的交易，则节点从其交易池移除该交易。

无需进一步验证。唯一值得关注的是 B 是否是分叉的里程碑。换句话说，本申请实施例需要考虑它是什么类型的区块。如果 B 是非里程碑，则什么也不做。如果 B 是里程碑，本申请实施例需要将 $\mathcal{G}_p$ 的高度与 $\eta(B)$ 进行比较。若存在：

$$\eta(B) > \eta(\mathcal{G}_p),$$

则设置：

$$\mathcal{G}_p := C(B).$$

这意味着 $\mathcal{G}_p$ 的重大更新，因为节点需要从本地有效 DAG 中的当前里程碑链切换到本地 DAG 中的最长里程碑链。这里设置了出现里程碑块分叉时的解决方法。若分叉的部分比原有的里程碑链高度要大，节点设备将要自己的本地 DAG 更新为分叉的里程碑块所确认的所有块。

参见图 4，为本申请实施例提供的一种分布式账本建立方法流程图，所述方法可以应用于节点设备，所述方法包括：

S401，节点设备获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息：

S402, 节点设备根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息, 更新本地分布式账本。

其中, 所述本地分布式账本基于结构化的 DAG 建立, 所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系, 所述各区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系; 所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。所述各区块间的连接关系还包含非里程碑块与非里程碑块间的连接关系。

在一些实施方式中, 所述根据获取的所述新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块信息, 更新本地分布式账本包括: 从所述新的里程碑块出发, 遍历与所述里程碑块具有直接或间接连接的区块信息; 判断所述区块对应的交易信息是否与本地分布式账本冲突; 若不冲突, 将该交易信息添加至本地分布式账本; 若冲突, 忽略该交易信息。

在一些实施方式中, 从所述新的里程碑块出发, 遍历与所述里程碑块具有直接或间接连接的区块信息包括: 从所述新的里程碑块出发, 利用深度优先算法、广度优先算法或者其他能够唯一确定区块顺序的算法遍历与所述里程碑块具有直接或间接连接的区块信息。

在一些实施方式中, 所述方法还包括: 判断所述区块指向对等节点链区块的指针是否正确指向了该对等节点链的最新区块; 若是, 增加该节点设备的奖励值; 若否, 不更新该节点设备的奖励值。

具体实现时, 节点设备可以输入一个里程碑块 milestone 的信息、一组被该 milestone 所“确认”的区块 block 以及当前账本历史。里程碑块 Milestone 块“确认”一个普通块是指由 milestone 块出发, 可以沿着一条有向路径到达这个普通块。从 milestone 开始, 以“本节点链指针”“其他节点链指针”的顺序对所有 block 进行深度优先或者广度优先 (或者任意一种具有唯一排序性的算法) 的遍历, 对于每一个 block, 进行以下算法: 检查 block 中交易是否与当前账本冲突, 以及 block 的“本节点链指针”是否正确指向对应节点链的最新 block: (1) 如不冲突, 节点链正确, 将交易添加至账本历史, 当前节点奖励增加 (固定增量+ 交易费); (2) 如冲突, 节点链正确, 跳过该交易, 当前节点奖励增加 (固定增量); (3) 如不冲突, 节点链不正确, 将交易添加至账本历史, 不更新节点奖励; (4) 如冲突, 节点链不正确, 跳过该交易, 不更新节点奖励。其中, 判断

区块 block 的“本节点链指针”是否正确指向对应节点链的最新 block 的方法为，若此区块 block 的 id_{prev} 所指向的 block 已被其它 block 的 id_{prev} 指过，则不正确；否则，则指向正确。

下面将结合实例对本申请实施例的交易分配和如何构建分布式账本进行详细介绍。

在奖励计划中，本申请实施例的目标是激励节点选择连接最新的里程碑区块和连接另外一个节点最新的区块。本申请实施例的奖励计划如下。如果节点挖到常规区块，它将获得动态奖励和交易总和的 98%。如果节点挖到里程碑区块，它将获得固定奖励加上交易费，以及里程碑区块确认的所有区块的 2%。在分叉竞争中输掉的里程碑区块被视为常规区块。调整常规区块的动态奖励，使得每单位时间分配给常规区块的总奖励是固定的。本申请实施例在下表中总结了本申请实施例的奖励计划：

表 1 奖励计划

方案	区块	交易	奖励
1	常规，有效	有效	98% (动态+交易费)
2	常规，有效	无效	98% 动态
3	节点分叉	有效	无
4	节点分叉	无效	无
5	里程碑块	有效	固定+交易费+2% (总确认奖励)
6	里程碑块	无效	固定+2% (总确认奖励)
7	其他		无

不同于比特币，本申请实施例的奖励值基于结构化 DAG 来离线计算。这种机制使本申请实施例能够为常规区块和里程碑区块分配不同的奖励。如前所述，用户无法提前确定区块的类型。只有在区块已经发布时才会分配本申请实施例的奖励。为了使这个机制起作用，本申请实施例添加了一种特殊类型的交易：注册 Registration。Registration 首先通过将累积奖励放入输出中来声明累积奖励，然后提交从现在开始应该发送奖励的新地址。通过这样做，其他节点可以通过将所有其他节点链的头部保持为节点的状态来容易地检查另一节点是否在其节点链上进行挖掘。如果恶意节点违反协议并分叉它自己的节点链，则其他节点将注意到恶意节点正在尝试更新一个已经不是头部的区块。然后该区块被视为

无效。在拜占庭式攻击的情况下，恶意节点向不同的诚实节点发送不同的分叉，这种攻击造成的冲突由里程碑链解决。

现在本申请实施例讨论攻击节点链的可能性：向另一个节点的节点链添加分叉区块。假设 Alice 正试图在 Bob 的节点链上发布一个区块。Alice 无法发布 registration 区块，因为它需要 Bob 的私钥才能这样做。现在考虑一下当 Alice 在 Bob 的节点链上挖掘出一个常规区块的情况。如果 Alice 没有发布该区块，那么 Bob 很可能会挖掘一个区块并被下一个里程碑确认，这使得 Alice 的区块纯粹浪费了自己的哈希算力，无论内部的交易是否有效。事实上，本申请实施例唯一担心的是，Alice 通过让里程碑确认 Alice 在 Bob 的链上创建的分叉来减少 Bob 的奖励。值得注意的是，Alice 不会从攻击中受益。因为所有节点都会尝试尽可能多地包含其他区块从而提高自身的奖励，所以它们倾向于包括在 Bob 自己的链和 Alice 在 Bob 的链上创建的链之间包含更多奖励的链。总而言之，攻击是可能的，但不太可能成功，而且根本没有利润。

现在本申请实施例介绍如何构建分布式账本 Ledger。

现在考虑试图双花交易的恶意节点或用户。恶意节点发布尝试同时花费相同输出的交易 A 和交易 B。A 和 B 都可能进入 DAG。然后考虑一个恶意节点，它会将自己的节点链分叉，并尝试双倍声明其奖励。节点向一部分诚实节点发送一个分叉，而向其他的发送其他分叉。同样，根据本申请实施例的协议，两个分叉都可以进入 DAG。

两种情况都导致不合理的分布式账本的 DAG。因此，本申请实施例需要一种将 DAG 映射到合理的分布式账本的方法。这意味着，该方法需要消除分布式账本上的双花交易、双重声明和其他形式的攻击。本申请实施例通过定义一个合理的分布式账本来开始。

分布式账本是有序交易列表。另外，如果以下情况，则分布式账本是合理的：

1. 每个常规交易都基于其前面的交易历史记录有效，并且
2. 每个 registration 交易的输出量根据相应地址之前的交易与相应地址的奖励相匹配。

常规交易的有效性是不言而喻的。条件 2 有两个含义。首先，节点链分叉上的有效交易仍然有效。其次，不可以声称节点分叉上的奖励。

本申请实施例描述了一个分布式账本构建函数 $V: \mathcal{G} \rightarrow \mathcal{L}$ ，它将任何语法

上有效的结构化 DAG 映射到有效的交易分布式账本。分布式账本包含有序交易集，每个有序交易集基于由它前面的交易组成的分布式账本而有效。

本申请实施例的分布式账本构建函数 V 以最后的里程碑 $G_{\text{milestone}}$ 作为输入。然后从最早的里程碑开始， V 以 $\{id_{\text{prev}}, id_{\text{tip}}\}$ 顺序对区块 B 执行深度优先搜索。对于区块 B ， V 首先检查 B 中的交易 T_x 是否有效。如果 T_x （正常交易或注册交易）有效，则通过使 $\mathcal{L} \cup T_x \rightarrow \mathcal{L}$ 更新 $\mathcal{L}$ 并且通过使 $\mathcal{R}(T_x.address) + B.reward \rightarrow \mathcal{R}(T_x.address)$ 更新奖励 $\mathcal{R}$ 。另外，如果交易是有效登记交易，通过移除对应的奖励记录来更新 $\mathcal{R}$ 。显然本申请实施例的方法，建立了有效分布式账本。

对于前述的各方法实施例，为了描述简单，故将其都表述为一系列的动作组合，但是本领域的技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为根据本申请实施例，某些步骤可以采用其他顺序或同时执行；其次，本领域技术人员也应该知悉，上述方法实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请实施例所必须的。

通过前述实施例的描述，本申请实施例可以通过基于结构化 DAG 的区块创建、添加以及分布式账本建立方法，可以通过里程碑块大规模的达成共识。由于所有区块将由里程碑块确认，因此在保证安全性的前提下实现了大规模的达成共识，并增强了网络的连接性和网络容量。

此外，由于区块承载的交易能够很快被确认，因此缩短了延迟。在本申请实施例中，由于结构化 DAG 结构，相对于传统的区块链的线性结构，区块间的连接性更强，由此带来的一个技术效果是缩短了区块被确认的时间。

此外，在本申请实施例中，所有满足语法规则和交易分配的广播区块将记录在最终 DAG 中，并且交易池中的交易中的足够队列大小以不低于到达率的速率被处理，因此包含交易的区块的吞吐量的速率基本上仅受通信网络的物理状况的限制。本申请实施例提供的方法有效地增加了吞吐量。

本申请实施例还公开了一种在其上记录有用于执行上述方法的程序的存储介质。所述存储介质包括配置为以计算机（以计算机为例）可读的形式存储或传送信息的任何机制。例如，存储介质包括只读存储器（ROM）、随机存取存储器（RAM）、磁盘存储介质、光存储介质、闪速存储介质、电、光、声或其他形式的传播信号（例如，载波、红外信号、数字信号等）等。

参见图 5，为本申请基于结构化 DAG 的区块创建装置一实施例的结构示意图。所述装置 500 包括：

获取单元 501，用于获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立。

创建单元 502，用于利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系。所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

广播单元 503，用于向对等网络的各节点设备广播新创建的区块信息。

在一些实施方式中，所述获取单元获取的所述结构化的 DAG 至少包含由各里程碑块连接而成的里程碑链以及由各节点设备自身创建的区块连接而成的对等节点链；所述对等节点链中的各区块至少指向一个里程碑块。

在一些实施方式中，所述创建单元包括：

组建单元，用于利用所述结构化的 DAG 表征的区块间的连接关系组建新区块信息，所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数；

调整单元，用于调整所述新区块信息包含的随机数，直到所述新区块信息的哈希结果满足第一难度条件。

在一些实施方式中，所述组建单元具体用于下述信息组建新区块信息：所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的指针。

在一些实施方式中，所述组建单元具体还用于下述信息组建新区块信息：所述新区块指向所述结构化的 DAG 中未由其他区块指向且由其他节点创建的最近一个区块。

在一些实施方式中，所述装置还包括：

确认单元，用于当调整所述新区块信息包含的随机数且确定所述新区块信息的哈希结果满足第二难度条件时，确认所述新区块为里程碑块。

在一些实施方式中，所述各节点设备的分布式账本包含的交易信息由所述里程碑块以及与所述里程碑块直接或间接连接的区块承载。

参见图 6，为本申请基于结构化 DAG 的区块创建装置一实施例的结构示意图。一种基于结构化 DAG 的区块创建装置，包括至少一个处理器 601（例如 CPU），存储器 602 和至少一个通信总线 603，用于实现这些装置之间的连接通信。处理器 601 用于执行存储器 502 中存储的可执行模块，例如计算机程序。存储器 602 可能包含高速随机存取存储器（RAM：Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器 601 执行如图 1 所示的基于结构化 DAG 的区块创建方法。

参见图 7，为本申请基于结构化 DAG 的区块添加装置一实施例的结构示意图。其中，所述装置 700 包括：

接收单元 701，用于接收另一节点设备发送的新区块信息。

第一判断单元 702，用于判断所述新区块信息是否满足设定条件。

添加单元 703，用于若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

在一些实施方式中，所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数。

在一些实施方式中，所述新区块与所述结构化的 DAG 包含的区块的连接关系至少包括：

所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；

所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的指针。

在一些实施方式中，所述新区块与所述结构化的 DAG 包含的区块的连接关系还包括：

所述新区块指向所述结构化的 DAG 中未由其他区块指向且由其他节点创建的最近一个区块。

在一些实施方式中，所述第一判断单元具体用于：

判断所述新区块信息是否满足语法要求；若满足，判断所述新区块信息的哈希结果是否满足第一难度条件；若满足，确定所述新区块信息满足设定条件。

在一些实施方式中，所述装置还包括：

第二判断单元，用于判断所述新区块所指向的区块是否在本地数据库中；

请求单元，用于若否，向被所述新区块指向的所述区块的创建节点设备请求所述区块。

在一些实施方式中，所述装置还包括：

移除单元，用于若判断所述新区块信息包含的交易信息与本地交易池中的第一交易信息相同，在所述本地交易池中移除所述第一交易信息；其中，所述本地交易池中包含待处理的、未被区块承载的交易信息。

在一些实施方式中，所述装置还包括：

第三判断单元，用于判断所述新区块是否为里程碑块；

更新单元，用于若是，根据所述里程碑块以及与所述里程碑块具有直接或间接连接的区块信息，更新本地分布式账本。

参见图 8，为本申请基于结构化 DAG 的区块添加装置一实施例的结构示意图。一种基于结构化 DAG 的区块添加装置，包括至少一个处理器 801（例如 CPU），存储器 802 和至少一个通信总线 803，用于实现这些装置之间的连接通信。处理器 801 用于执行存储器 802 中存储的可执行模块，例如计算机程序。存储器 802 可能包含高速随机存取存储器（RAM：Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器 801 执行如图 3 所示的基于结构化 DAG 的区块添加方法。

参见图 9，为本申请分布式账本建立装置一实施例的结构示意图，所述装置 900 包括：

获取单元 901，用于获取新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块信息。

更新单元 902，用于根据获取的所述新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块间

的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

在一些实施方式中，所述更新单元 902 包括：

遍历单元，用于从所述新的里程碑块出发，遍历与所述里程碑块具有直接或间接连接的区块信息；

第一判断单元，用于判断所述区块对应的交易信息是否与本地分布式账本冲突；

交易添加单元，用于若不冲突，将该交易信息添加至本地分布式账本；若冲突，忽略该交易信息。

在一些实施方式中，所述遍历单元具体用于：

从所述新的里程碑块出发，利用深度优先算法或者广度优先算法遍历与所述里程碑块具有直接或间接连接的区块信息。

在一些实施方式中，所述装置还包括：

第二判断单元，用于判断所述区块指向对等节点链区块的指针是否正确指向了该对等节点链的最新区块；

奖励处理单元，用于若是，增加该节点设备的奖励值；若否，不更新该节点设备的奖励值。

参见图 10，为本申请分布式账本建立装置一实施例的结构示意图。一种分布式账本建立装置，包括至少一个处理器 1001（例如 CPU），存储器 1002 和至少一个通信总线 1003，用于实现这些装置之间的连接通信。处理器 1001 用于执行存储器 502 中存储的可执行模块，例如计算机程序。存储器 1002 可能包含高速随机存取存储器（RAM：Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器 1001 执行如图 4 所示的分布式账本建立方法。

参见图 11，为本申请基于 DAG 的区块数据处理装置一实施例的结构示意图。所述装置 1100 包括：

创建模块 1101，用于获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立；利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、

由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息；向对等网络的各节点设备广播新创建的区块信息。

添加模块 1102，用于接收一节点设备发送的新区块信息；判断所述新区块信息是否满足设定条件；若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

分布式账本建立模块 1103，用于获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

需要说明的是，上述装置实施例属于优选实施例，所涉及的单元和模块并不一定是本申请实施例所必须的。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于本申请实施例的装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例部分的说明即可。以上所描述的装置及装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，既可以位于一个地方或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

权 利 要 求 书

1、一种基于结构化有向无环图 DAG 的区块创建方法，其中，所述方法应用于对等网络中的节点设备，包括：

5 获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立；

利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息；

向对等网络的各节点设备广播新创建的区块信息。

2、根据权利要求 1 所述的方法，其中，所述结构化的 DAG 至少包含由各里程碑块连接而成的里程碑链以及由各节点设备自身创建的区块连接而成的对等节点链；所述对等节点链中的各区块至少指向一个里程碑块。

15 3、根据权利要求 1 或 2 所述的方法，其中，所述利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块包括：

利用所述结构化的 DAG 表征的区块间的连接关系组建新区块信息，所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数；

20 调整所述新区块信息包含的随机数，直到所述新区块信息的哈希结果满足第一难度条件。

4、根据权利要求 3 所述的方法，其中，所述新区块与所述结构化的 DAG 包含的区块的连接关系至少包括：

25 所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；

所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的指针。

5、根据权利要求 4 所述的方法，其中，所述新区块与所述结构化的 DAG 包含的区块的连接关系还包括：

30 所述新区块指向所述结构化的 DAG 中由其他节点创建的最近一个区块。

6、根据权利要求3所述的方法，其中，所述方法还包括：

当调整所述新区块信息包含的随机数且确定所述新区块信息的哈希结果满足第二难度条件时，确认所述新区块为里程碑块。

7、根据权利要求1所述的方法，其中，所述各节点设备的分布式账本包含
5 的交易信息由所述里程碑块以及与所述里程碑块直接或间接连接的区块承载。

8、一种基于结构化 DAG 的区块添加方法，其中，所述方法应用于对等网络中的节点设备，包括：

接收一节点设备发送的新区块信息；

判断所述新区块信息是否满足设定条件；

10 若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接
15 连接关系的区块对应的信息。

9、根据权利要求8所述的方法，其中，所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数。

10、根据权利要求8所述的方法，其中，所述新区块与所述结构化的 DAG
20 包含的区块的连接关系至少包括：

所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；

所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的指针。

25 11、根据权利要求8所述的方法，其中，所述新区块与所述结构化的 DAG 包含的区块的连接关系还包括：

所述新区块指向所述结构化的 DAG 中由其他节点创建的最近一个区块。

12、根据权利要求8所述的方法，其中，所述判断所述新区块信息是否满足设定条件包括：

30 判断所述新区块信息是否满足语法要求；

若满足，判断所述新区块信息的哈希结果是否满足第一难度条件；

若满足，确定所述新区块信息满足设定条件。

13、根据权利要求 10 或 12 所述的方法，其中，所述方法还包括：

判断所述新区块所指向的区块是否在本地数据库中；

若否，向被所述新区块指向的所述区块的创建节点设备请求所述区块。

5 14、根据权利要求 8 所述的方法，其中，所述方法还包括：

若判断所述新区块信息包含的交易信息与本地交易池中的第一交易信息相同，在所述本地交易池中移除所述第一交易信息；其中，所述本地交易池中包含待处理的、未被区块承载的交易信息。

15、根据权利要求 8 所述的方法，其中，所述方法还包括：

10 判断所述新区块是否为里程碑块；

若是，根据所述里程碑块以及与所述里程碑块具有直接或者间接连接的区块信息，更新本地分布式账本。

16、一种分布式账本建立方法，其中，所述方法包括：

15 获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；

根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块间的连接关系、
20 由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

17、根据权利要求 16 所述的方法，其中，所述根据获取的所述新的里程碑块信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本包括：
25

从所述新的里程碑块出发，遍历与所述里程碑块具有直接或间接连接的区块信息；

判断所述区块对应的交易信息是否与本地分布式账本冲突；

若不冲突，将该交易信息添加至本地分布式账本；

30 若冲突，忽略该交易信息。

18、根据权利要求 17 所述的方法，其中，从所述新的里程碑块出发，遍历

与所述里程碑块具有直接或间接连接的区块信息包括：

从所述新的里程碑块出发，利用深度优先算法或者广度优先算法遍历与所述里程碑块具有直接或间接连接的区块信息。

19、根据权利要求 17 所述的方法，其中，所述方法还包括：

5 判断所述区块指向对等节点链区块的指针是否正确指向了该对等节点链的
最新区块；

若是，增加该节点设备的奖励值；

若否，不更新该节点设备的奖励值。

20、一种基于结构化 DAG 的区块创建装置，其中，所述装置包括：

10 获取单元，用于获取本地数据库的数据结构，所述本地数据库的数据结构
基于结构化的 DAG 建立；

创建单元，用于利用所述结构化的 DAG 表征的区块间的连接关系，创建新
的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设
备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述
15 里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系
的区块对应的信息；

广播单元，用于向对等网络的各节点设备广播新创建的区块信息。

21、根据权利要求 20 所述的装置，其中，所述获取单元获取的所述结构化
的 DAG 至少包含由各里程碑块连接而成的里程碑链以及由各节点设备自身创建
20 的区块连接而成的对等节点链；所述对等节点链中的各区块至少指向一个里程
碑块。

22、根据权利要求 20 或 21 所述的装置，其中，所述创建单元包括：

组建单元，用于利用所述结构化的 DAG 表征的区块间的连接关系组建新区
块信息，所述新区块信息至少包括从交易池中选择的交易信息、所述新区块与
25 所述结构化的 DAG 包含的区块的连接关系、随机数；

调整单元，用于调整所述新区块信息包含的随机数，直到所述新区块信息
的哈希结果满足第一难度条件。

23、根据权利要求 22 所述的装置，其中，所述组建单元具体用于使用下述
信息组建新区块信息：所述新区块指向所述结构化的 DAG 的最长里程碑链中最
30 新生成的一个里程碑块的指针；所述新区块指向所述结构化的 DAG 中对等节点
链中最新生成的一个区块的指针。

24、根据权利要求 23 所述的装置，其中，所述组建单元具体还用于使用下述信息组建新区块信息：所述新区块指向所述结构化的 DAG 中由其他节点创建的最近一个区块。

25、根据权利要求 22 所述的装置，其中，所述装置还包括：

5 确认单元，用于当调整所述新区块信息包含的随机数且确定所述新区块信息的哈希结果满足第二难度条件时，确认所述新区块为里程碑块。

26、根据权利要求 20 所述的装置，其中，所述各节点设备的分布式账本包含的交易信息由所述里程碑块以及与所述里程碑块直接或间接连接的区块承载。

10 27、一种基于结构化 DAG 的区块创建装置，其中，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行如权利要求 1-7 所述的方法。

28、一种存储介质，其中，所述存储介质存储有用于执行权利要求 1~7 所述的方法的程序。

15 29、一种基于结构化 DAG 的区块添加装置，其中，所述装置包括：
接收单元，用于接收一节点设备发送的新区块信息；

第一判断单元，用于判断所述新区块信息是否满足设定条件；

添加单元，用于若满足，将所述新区块信息添加到所述节点设备的本地数据库中；所述本地数据库的数据结构基于结构化的 DAG 建立，所述结构化的
20 DAG 用于表征区块间的连接关系，所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

30、根据权利要求 29 所述的装置，其中，所述新区块信息至少包括从交易
25 池中选择的交易信息、所述新区块与所述结构化的 DAG 包含的区块的连接关系、随机数。

31、根据权利要求 29 所述的装置，其中，所述新区块与所述结构化的 DAG 包含的区块的连接关系至少包括：

所述新区块指向所述结构化的 DAG 的最长里程碑链中最新生成的一个里程碑块的指针；
30

所述新区块指向所述结构化的 DAG 中对等节点链中最新生成的一个区块的

指针。

32、根据权利要求 29 所述的装置，其中，所述新区块与所述结构化的 DAG 包含的区块的连接关系还包括：

所述新区块指向所述结构化的 DAG 中由其他节点创建的最近一个区块。

5 33、根据权利要求 29 所述的装置，其中，所述第一判断单元具体用于：

判断所述新区块信息是否满足语法要求；若满足，判断所述新区块信息的哈希结果是否满足第一难度条件；若满足，确定所述新区块信息满足设定条件。

34、根据权利要求 31 或 33 所述的装置，其中，所述装置还包括：

第二判断单元，用于判断所述新区块所指向的区块是否在本地数据库中；

10 请求单元，用于若否，向被所述新区块指向的所述区块的创建节点设备请求所述区块。

35、根据权利要求 29 所述的装置，其中，所述装置还包括：

15 移除单元，用于若判断所述新区块信息包含的交易信息与本地交易池中的第一交易信息相同，在所述本地交易池中移除所述第一交易信息；其中，所述本地交易池中包含待处理的、未被区块承载的交易信息。

36、根据权利要求 29 所述的装置，其中，所述装置还包括：

第三判断单元，用于判断所述新区块是否为里程碑块；

更新单元，用于若是，根据所述里程碑块以及与所述里程碑块具有直接或间接连接的区块信息，更新本地分布式账本。

20 37、一种基于结构化 DAG 的区块添加装置，其中，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行权利要求如 8-15 所述的方法。

38、一种存储介质，其中，所述存储介质存储有用于执行权利要求 8-15 所述的方法的程序。

25 39、一种分布式账本建立装置，其中，所述装置包括：

获取单元，用于获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；

30 更新单元，用于根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系，所述各区块间的连接关系至少包含里程碑块

间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接连接关系的区块对应的信息。

40、根据权利要求 39 所述的装置，其中，所述更新单元包括：

5 遍历单元，用于从所述新的里程碑块出发，遍历与所述里程碑块具有直接或间接连接的区块信息；

第一判断单元，用于判断所述区块对应的交易信息是否与本地分布式账本冲突；

10 交易添加单元，用于若不冲突，将该交易信息添加至本地分布式账本；若冲突，忽略该交易信息。

41、根据权利要求 40 所述的装置，其中，所述遍历单元具体用于：

从所述新的里程碑块出发，利用深度优先算法或者广度优先算法遍历与所述里程碑块具有直接或间接连接的区块信息。

42、根据权利要求 40 所述的装置，其中，所述装置还包括：

15 第二判断单元，用于判断所述区块指向对等节点链区块的指针是否正确指向了该对等节点链的最新区块；

奖励处理单元，用于若是，增加该节点设备的奖励值；若否，不更新该节点设备的奖励值。

20 43、一种分布式账本建立装置，其中，包括存储器和处理器，所述存储器用于存储机器可执行指令，所述处理器用于读取并执行所述机器可执行指令以执行如权利要求 16-19 所述的方法。

44、一种存储介质，其中，所述存储介质存储有用于执行权利要求 16-19 所述的方法的程序。

45、一种基于 DAG 的区块数据处理装置，其中，所述装置包括：

25 创建模块，用于获取本地数据库的数据结构，所述本地数据库的数据结构基于结构化的 DAG 建立；利用所述结构化的 DAG 表征的区块间的连接关系，创建新的区块；所述区块间的连接关系至少包含里程碑块间的连接关系、由各节点设备自身创建的区块间的连接关系以及里程碑块与非里程碑块的连接关系；所述里程碑块用于确认所述里程碑块以及与所述里程碑块具有直接或间接
30 连接关系的区块对应的信息；向对等网络的各节点设备广播新创建的区块信息；

添加模块，用于接收一节点设备发送的新区块信息；判断所述新区块信息

是否满足设定条件；若满足，将所述新区块信息添加到所述节点设备的本地数据库中；

5 分布式账本建立模块，用于获取新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息；根据获取的所述新的里程碑块的信息以及与所述里程碑块具有直接或间接连接的区块的信息，更新本地分布式账本；所述本地分布式账本基于结构化的 DAG 建立，所述结构化的 DAG 用于表征承载分布式账本中的交易信息的各区块间的连接关系。

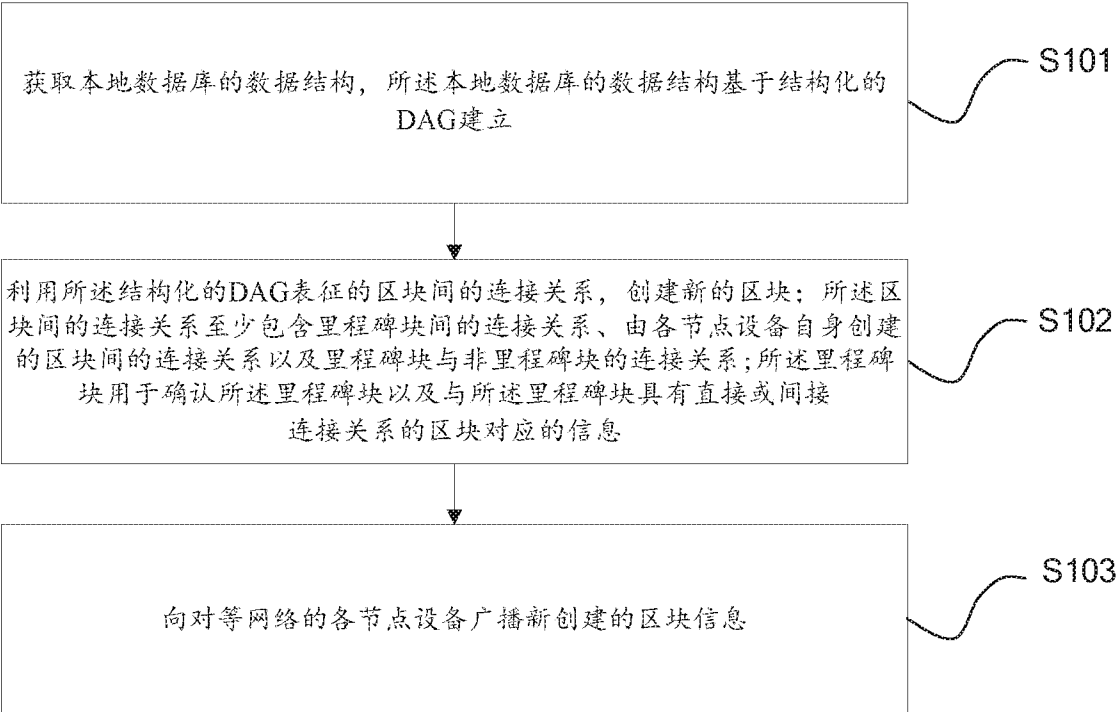


图 1

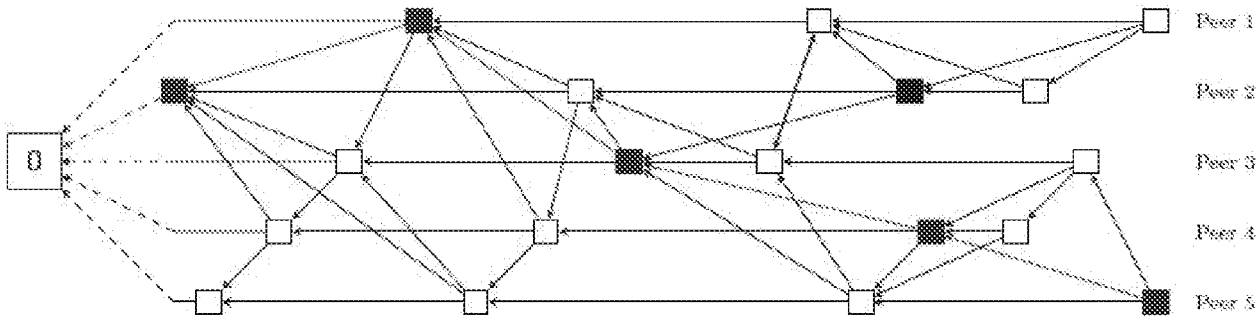


图 2

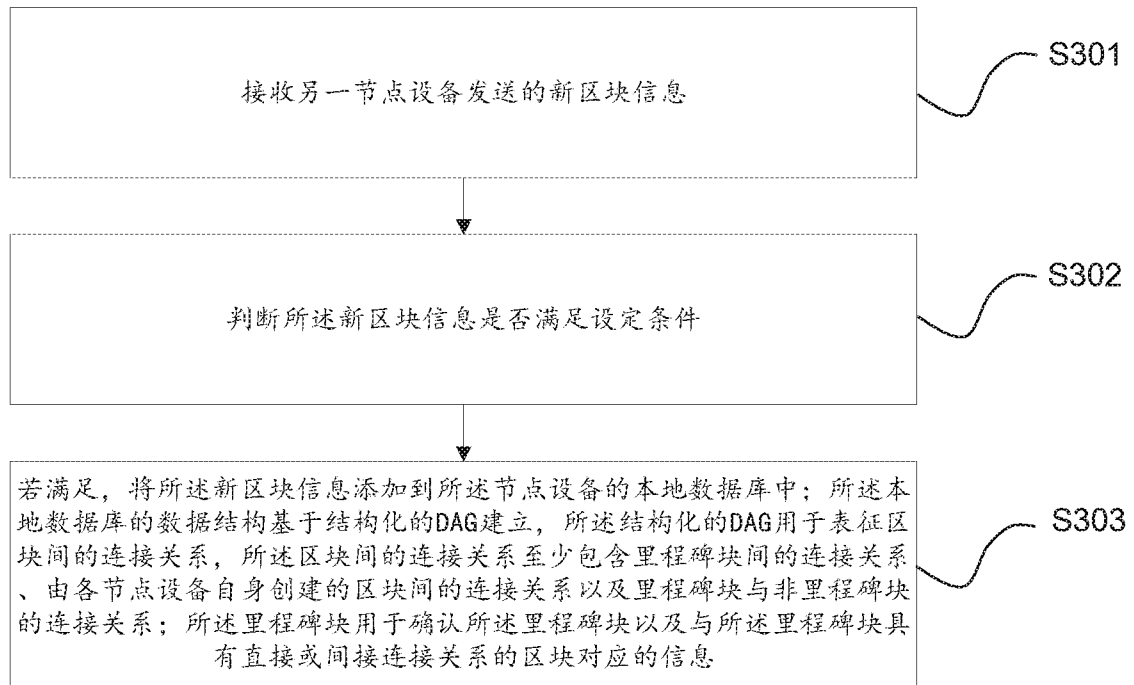


图 3

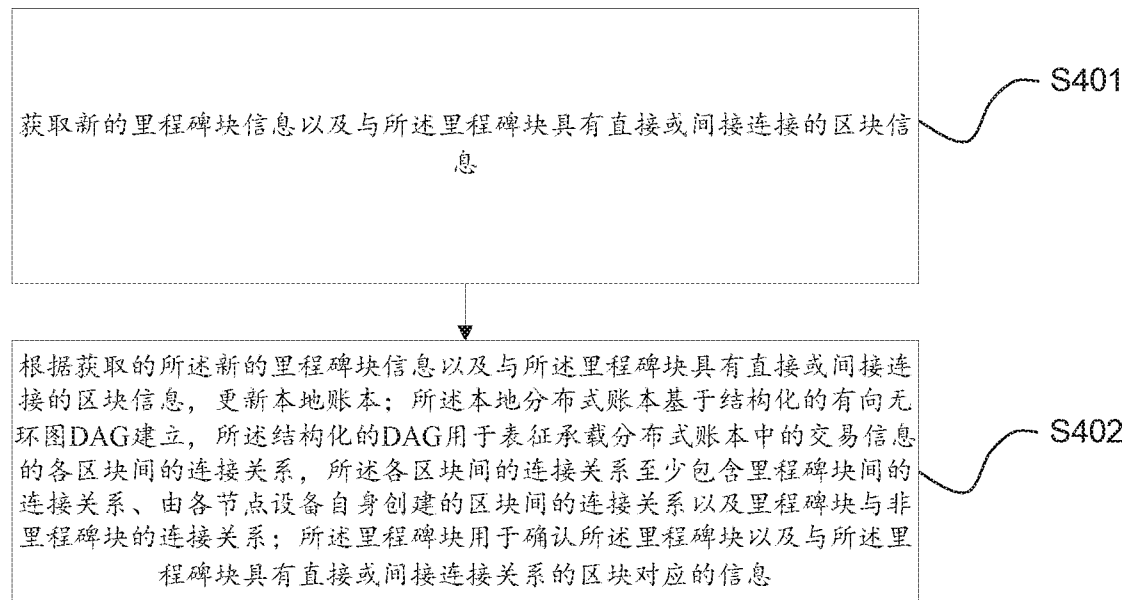


图 4

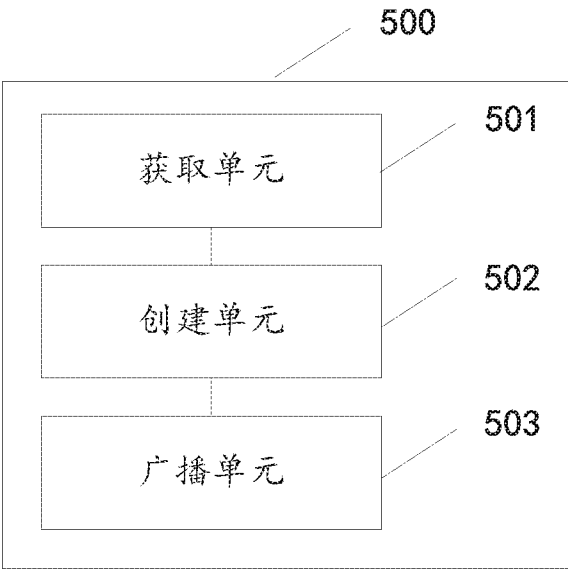


图 5

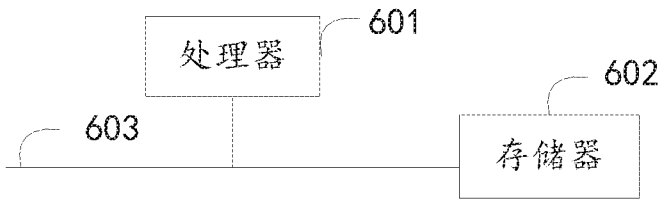


图 6

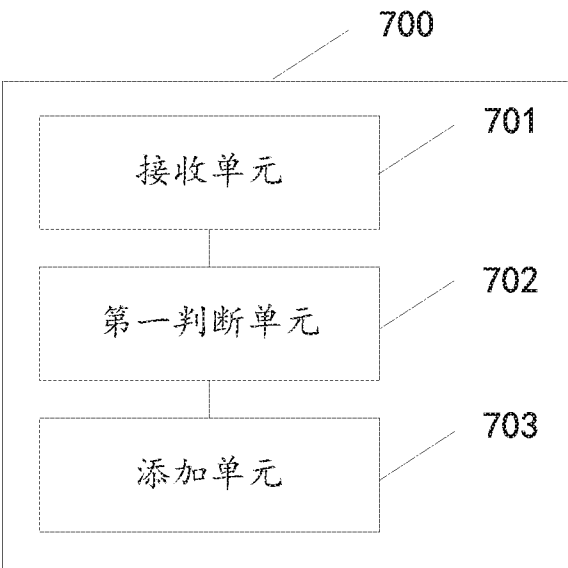


图 7

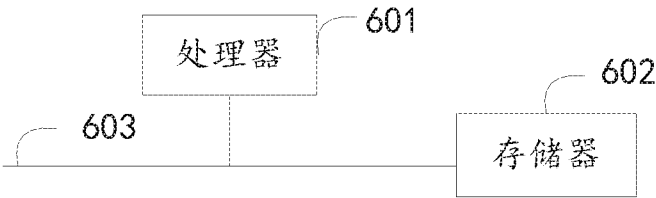


图 8

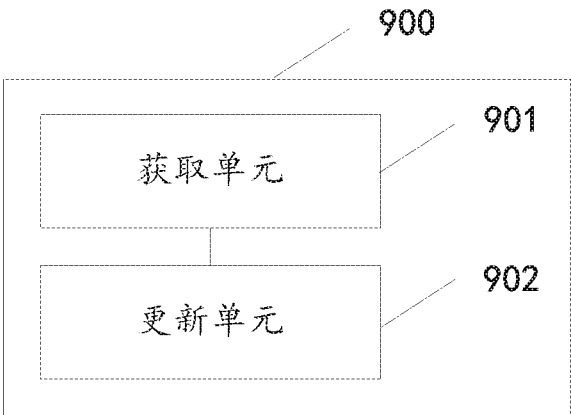


图 9

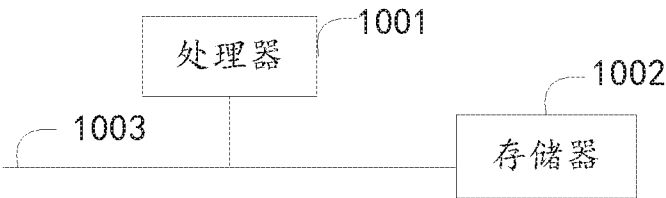


图 10

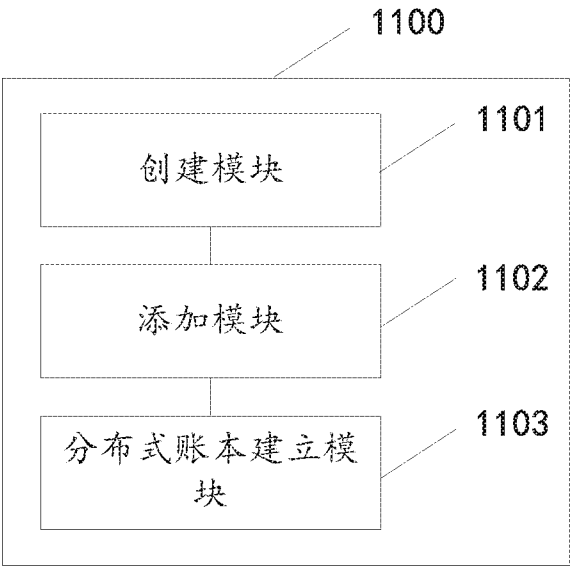


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/070888

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(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)

CNPAT, EPODOC, WPI, CNKI, IEEE: 有向无环图, 区块, 区块链, 里程碑块, 创建, 添加, 连接, 网络, 分布式, 扩容, 容量, 算力, 延迟, DAG, directed, acyclic, graphs, block chain, mileage, build, add, connect, joint, network, distributivity, dilatancy, capability, calculate, delay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106897351 A (BEIJING RUI JOSIE TECHNOLOGY DEVELOPMENT CO., LTD.) 27 June 2017 (2017-06-27) description, paragraphs [0002]-[0009] and [0025]-[0055], and abstract	1-45
A	CN 108985732 A (CHINA UNIVERSITY OF GEOSCIENCES, WUHAN) 11 December 2018 (2018-12-11) entire document	1-45
A	CN 108537543 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 14 September 2018 (2018-09-14) entire document	1-45
A	US 2017236120 A1 (ORACLE INTERNATIONAL CORPORATION) 17 August 2017 (2017-08-17) entire document	1-45
A	WO 2017109140 A1 (BIGCHAINDB GMBH) 29 June 2017 (2017-06-29) entire document	1-45



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

24 September 2019

Date of mailing of the international search report

11 October 2019

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
Information on patent family members

International application No.

PCT/CN2019/070888

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	106897351	A	27 June 2017	None	
CN	108985732	A	11 December 2018	None	
CN	108537543	A	14 September 2018	None	
US	2017236120	A1	17 August 2017	None	
WO	2017109140	A1	29 June 2017	None	

国际检索报告

国际申请号

PCT/CN2019/070888

A. 主题的分类 G06Q 20/38 (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)) CNPAT, EPDOC, WPI, CNKI, IEEE: 有向无环图, 区块, 区块链, 里程碑块, 创建, 添加, 连接, 网络, 分布式, 扩容, 容量, 算力, 延迟, DAG, directed, acyclic, graphs, block chain, mileage, build, add, connect, joint, network, distributivity, dilatancy, capability, calculate, delay																				
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>A</td> <td>CN 106897351 A (北京瑞卓喜投科技发展有限公司) 2017年 6月 27日 (2017 - 06 - 27) 说明书第[0002]-[0009], [0025]-[0055]段, 摘要</td> <td>1-45</td> </tr> <tr> <td>A</td> <td>CN 108985732 A (中国地质大学武汉) 2018年 12月 11日 (2018 - 12 - 11) 全文</td> <td>1-45</td> </tr> <tr> <td>A</td> <td>CN 108537543 A (百度在线网络技术北京有限公司) 2018年 9月 14日 (2018 - 09 - 14) 全文</td> <td>1-45</td> </tr> <tr> <td>A</td> <td>US 2017236120 A1 (ORACLE INTERNATIONAL CORPORATION) 2017年 8月 17日 (2017 - 08 - 17) 全文</td> <td>1-45</td> </tr> <tr> <td>A</td> <td>WO 2017109140 A1 (BIGCHAINDB GMBH) 2017年 6月 29日 (2017 - 06 - 29) 全文</td> <td>1-45</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	A	CN 106897351 A (北京瑞卓喜投科技发展有限公司) 2017年 6月 27日 (2017 - 06 - 27) 说明书第[0002]-[0009], [0025]-[0055]段, 摘要	1-45	A	CN 108985732 A (中国地质大学武汉) 2018年 12月 11日 (2018 - 12 - 11) 全文	1-45	A	CN 108537543 A (百度在线网络技术北京有限公司) 2018年 9月 14日 (2018 - 09 - 14) 全文	1-45	A	US 2017236120 A1 (ORACLE INTERNATIONAL CORPORATION) 2017年 8月 17日 (2017 - 08 - 17) 全文	1-45	A	WO 2017109140 A1 (BIGCHAINDB GMBH) 2017年 6月 29日 (2017 - 06 - 29) 全文	1-45
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
A	CN 106897351 A (北京瑞卓喜投科技发展有限公司) 2017年 6月 27日 (2017 - 06 - 27) 说明书第[0002]-[0009], [0025]-[0055]段, 摘要	1-45																		
A	CN 108985732 A (中国地质大学武汉) 2018年 12月 11日 (2018 - 12 - 11) 全文	1-45																		
A	CN 108537543 A (百度在线网络技术北京有限公司) 2018年 9月 14日 (2018 - 09 - 14) 全文	1-45																		
A	US 2017236120 A1 (ORACLE INTERNATIONAL CORPORATION) 2017年 8月 17日 (2017 - 08 - 17) 全文	1-45																		
A	WO 2017109140 A1 (BIGCHAINDB GMBH) 2017年 6月 29日 (2017 - 06 - 29) 全文	1-45																		
☐ 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 style="vertical-align: top;"> * 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 style="vertical-align: top;"> “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 2019年 9月 24日		国际检索报告邮寄日期 2019年 10月 11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 吴媛媛 电话号码 86-(10)-53961351																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/070888

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	106897351	A	2017年 6月 27日	无	
CN	108985732	A	2018年 12月 11日	无	
CN	108537543	A	2018年 9月 14日	无	
US	2017236120	A1	2017年 8月 17日	无	
WO	2017109140	A1	2017年 6月 29日	无	