(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108665365 B
(45)授权公告日 2021.07.13

(21)申请号 201810468531.1
(22)申请日 2018.05.16
(65)同一申请的已公布的文献号
申请公布号 CN 108665365 A
(43)申请公布日 2018.10.16
(73)专利权人 四川大学
地址 610000 四川省成都市一环路南一段24号四川大学
(72)发明人 王运鹏 杨进
(74)专利代理机构 北京高沃律师事务所 11569
代理人 王戈
(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 107733855 A,2018.02.23
CN 107733855 A,2018.02.23
CN 107392611 A,2017.11.24
CN 107730277 A,2018.02.23
US 2017346833 A1,2017.11.30

审查员 高民芳

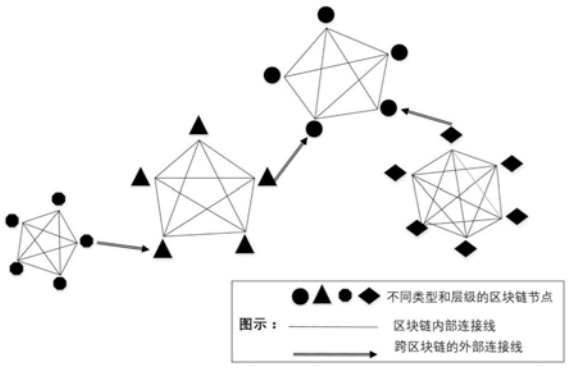
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种混合区块链架构系统、处理方法及处理系统

(57)摘要

本发明公开一种混合区块链架构系统、处理方法及处理系统。所述系统包括：上层区块链、当前区块链和下层区块链，所述当前区块链的输入端与所述下层区块链连接，所述当前区块链的输出端与所述上层区块链连接；所述当前区块链用于接收来自所述下层区块链的区块打包信息，同时用于向上层区块链打包所述当前区块链中的打包信息。采用本发明的架构系统能够使得区块链适应各种复杂的应用场景，从而提升信息化水平。



CN 108665365 B

1.一种混合区块链架构系统，其特征在于，所述系统包括：上层区块链、当前区块链和下层区块链，所述当前区块链的输入端与所述下层区块链连接，所述当前区块链的输出端与所述上层区块链连接；所述当前区块链用于接收来自所述下层区块链的区块打包信息，同时用于向上层区块链打包所述当前区块链中的打包信息；

不限层级的区块链实现：在不限层级的混合区块链架构中最大特点是区块链间的关系和存在是可以不限层级进行扩展的，一个区块链可以由一个或多个下层级的区块链，同时其也可能有一个或多个上层区块链，本层区块链为其下层区块链的打包区块提供验证和背书功能；同时其上层区块链则为其提供验证和背书功能；每层的区块链通过区块链的链接节点进行区块链的链接；

混合区块链架构：在区块链技术的使用上，提供一种混合的架构，即架构中的每个区块链可以采用不同的实现技术，但其交易需要继承混合区块链指定的基类，在基类的基础上，每一层级的区块链根据应用场景和所承载业务的不同，选择不同交易信息模型的区块链；

不同的共识机制管理：在区块链的关键技术共识机制上，混合区块链通过接口技术对常见的共识机制进行接口定义，不同层级的区块链继承此接口，实现区块链的初始化注册，但共识机制接口也实现了自我重载或定义的灵活性，可以使共识机制随着理论的发展，进行自定义扩展；同时在区块链技术的应用上是混合的，即不同的区块链；

下层链初始化：下层区块链初始化是不限层次混合区块链架构进行区块链扩展的手段，通过对一个区块链进行下层链的初始化，让该区块链拥有下层区块链；在初始化下层区块链时，可由本层区块链向下层区块链颁发创世区块的区块信息hash和创链时间，同时利用该功能与区块链注册功能结合使用，使新初始化的区块链可以在区块链注册中心进行查询；

区块链注册：对新初始化的区块链进行注册，在注册时会把新建区块链的上层区块链信息、新区块链的链标识、区块链共识机制、区块链节点等进行管理；区块链注册后，混合区块链架构中的其他区块链可以通过注册中心获取新区块链的相关信息、服务方式、交互方式等；

区块打包：混合区块链架构中各层级区块链的区块信息打包与单条区块链的信息打包不同，单层区链打包时只需要把本层区块链发生的交易进行运算打包，而混合区块链在各层级的区块链打包时，需要把其下层区块链的形成的区块信息hash作为交易进行打包；

当处于下层级区块链在打包完成一个区块后，需要把区块信息同本层区块链标识、上层区块链标识进行信息的hash，然后把信息hash构造信息上报交易，交易发起方为下层区块链，交易接收方为其对应的上层区块链，然后通过本层的链接者向上层区块链的接收者发送交易；

区块验证提供跨区块链间进行区块信息验证的功能，该功能可由本层区块链发起，也可以由下层区块链发起；当由区块链发起区块信息验证功能时，由该区块链的上层区块链的链接者根据区块链注册时的信息向待验证区块链发送需要验证区块的区块高度，然后待验证链根据区块高度向上层区块链发送其对应的区块信息，上层区块链再收到其区块信息后，对信息进行hash运算，运行完成后与自身存储的该下层区块链在该区块打包确认时发送的信息进行比较，如果一致，则区块验证通过，否则不通过。

2.根据权利要求1所述的混合区块链架构系统，其特征在于，所述当前区块链还用于接

收上层区块链的区块打包信息。

3.根据权利要求2所述的混合区块链架构系统，其特征在于，所述当前区块链在接收来自所述上/下层区块链的区块打包信息后，还用于进行交易确认。

4.根据权利要求1所述的混合区块链架构系统，其特征在于，所述当前区块链与一个或多个所述下层区块链连接，所述当前区块链与一个或多个所述上层区块链连接。

5.根据权利要求1所述的混合区块链架构系统，其特征在于，各所述区块链的连接方式包括：公有链连接，私有链连接、联盟链连接和多种链混合连接。

6.根据权利要求1所述的混合区块链架构系统，其特征在于，各所述区块链的内部节点是不同的。

7.根据权利要求1所述的混合区块链架构系统，其特征在于，各所述区块链的数据交易结构是不同的。

8.根据权利要求1所述的混合区块链架构系统，其特征在于，任意层级的区块链的交易信息包括：本层区块链的交易数据结构和下层区块链的链标识。

9.一种基于权利要求1所述的混合区块链架构系统的处理方法，其特征在于，所述处理方法包括：

发起交易；

将所述交易揽入当前区块链交易池；

所述当前区块链对交易池中的交易进行打包，得到打包交易；

判断所述当前区块链是否具有上层区块链，得到判断结果；

若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息；

若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

10.一种基于权利要求1所述的混合区块链架构系统的处理系统，其特征在于，所述处理系统包括：

交易发起模块，用于发起交易；

交易池模块，用于将所述交易揽入当前区块链交易池；

打包交易获取模块，用于根据所述当前区块链对交易池中的交易进行打包，得到打包交易；

判断模块，用于判断所述当前区块链是否具有上层区块链，得到判断结果；

第一判断结果模块，用于若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息；

第二判断结果模块，若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

一种混合区块链架构系统、处理方法及处理系统

技术领域

[0001] 本发明涉及区块链领域，特别是涉及一种混合区块链架构系统、处理方法及处理系统。

背景技术

[0002] 区块链在应用上比较成熟的领域主要是虚拟货币，其主要的代表由比特币、以太币、莱特币等虚拟货币，基本上都是运用区块链本质的去中心化软件架构在实现的，但是其核心的分布式公识算法则各不相同，有的运用工作量证明机制(Pow)，有的使用权益证明(POS)，有的使用股份授权证明机制(DPos)，也有实用拜占庭容错(PBFT)，授权拜占庭容错算法(delegatedBFT)等算法，这些共识机制在中心化程度、区块链治理能力、资源利用情况、共识周期长短等方面各有各的优势和劣势；同时在区块链在应用范围上划分出不同的区块链，如公有链、联盟链、私有链。这样针对某一单一的区块链来讲，将面临如下的挑战：

[0003] 信息化领域的复杂性：当前互联网技术的发展已经从PC互联网、移动互联网时间向万物互联的时代发展。同时信息化的应用领域越来越多：面向广大自然人的互联网应用如：社交、媒体、购物等应用，其参与的人数非常庞大，数据量也大的惊人，其对系统吞吐量和并发能力要求很高，需要在较短的时间内响应数量非常大的消费群体，其业务模型较简单，但对性能要求很高；信息化应用领域也应用于企业内部：如企业内部的电子产品研发设计类、企业资源规则类应用领域，涉及到的产品物料清单复杂，一个成品电子产品的数据量较大，业务处理也很复杂，其对性能的要求可能没有互联网应用那么高，但是其对数据准确率要求较高；在应用于跨企业间的信息化应用领域，如著名的环球同业银行金融电讯协会所使用的SWIFT系统，它由国际间的各大银行联盟进行金融数据报文交换的信息化系统规范，其需要快速、准确、简明、可靠的信息架构进行保障；同时如军事领域的信息化应用，需要能在较短的时间内进行组网、接入、高安全、高可靠的信息服务。总之，复杂的信息化应用领域对信息系统的架构要求也越来越高，对不同的应用领域也有其不同的架构要求；

[0004] 对区块链类型的融合应用需求：当今社会，任何一家面向广大消费者的企业在信息化应用方面基本上都有如下的应用场景：面向广大消费者的B2C、面向企业上下游关系的B2B，企业内部信息化这三个应用场景。在这三个场景中，面向广大消费者进行交易时因其应用场景是公开地面向外部，这样使用公有链显得较有优势；在企业联盟、产业联盟或有上下游业务关系的企业间进行信息化集成时，则使用联盟链更能提高交易的安全性和共识效率；而在企业内部的信息化需求的应用场合时，私有链的适应度则更高。

[0005] 对区块链共识机制定制化的应用需求：每一种信息化工作或手段其运用的场景和业务要求是不一样的，如面向广大互联网用户开发的站点或服务因其公开性，则会需要更安全、更可靠、可安全进出的的共识机制来实现；而对企业联盟内部，可信度较高，对加入区块链的节点也有较高的要求，则需要不安全公开，多中心化的共识机制来保障；在企业内网，网络环境相对较安全，数量交易量也较大，则需要效率较高，较容易达成共识的共识机制来支撑。

[0006] 总之，复杂的业务应用场景对区块链的应用需求差异较大，特定的区块链架构和区块链共识机制也不能满足大多数应用场景，这就需要一种混合的区块链架构来解决复杂的业务问题。

发明内容

[0007] 本发明的目的是提供一种混合区块链架构系统、处理方法及处理系统，从而满足大多数的应用场景。

[0008] 为实现上述目的，本发明提供了如下方案：

[0009] 一种混合区块链架构系统，所述系统包括：上层区块链、当前区块链和下层区块链，所述当前区块链的输入端与所述下层区块链连接，所述当前区块链的输出端与所述上层区块链连接；所述当前区块链用于接收来自所述下层区块链的区块打包信息，同时用于向上层区块链打包所述当前区块链中的打包信息。

[0010] 可选的，所述当前区块链还用于接收上层区块链的区块打包信息。

[0011] 可选的，所述当前区块链在接收来自所述上/下层区块链的区块打包信息后，还用于进行交易确认。

[0012] 可选的，所述当前区块链与一个或多个所述下层区块链连接，所述当前区块链与一个或多个所述上层区块链连接。

[0013] 可选的，各所述区块链的连接方式包括：公有链连接，私有链连接、联盟链连接和多种链混合连接。

[0014] 可选的，各所述区块链的内部节点是不同的。

[0015] 可选的，各所述区块链的数据交易结构是不同的。

[0016] 可选的，任意层级的区块链的交易信息包括：本层区块链的交易数据结构和下层区块链的链标识。

[0017] 为实现上述目的，本发明提供了如下方案：

[0018] 一种混合区块链架构系统的处理方法，所述处理方法包括：

[0019] 发起交易；

[0020] 将所述交易揽入当前区块链交易池；

[0021] 所述当前区块链对交易池中的交易进行打包，得到打包交易；

[0022] 判断所述当前区块链是否具有上层区块链，得到判断结果；

[0023] 若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息。

[0024] 若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

[0025] 为实现上述目的，本发明提供了如下方案：

[0026] 一种混合区块链架构系统的处理系统，所述处理系统包括：

[0027] 交易发起模块，用于发起交易；

[0028] 交易池模块，用于将所述交易揽入当前区块链交易池；

[0029] 打包交易获取模块，用于根据所述当前区块链对交易池中的交易进行打包，得到打包交易；

[0030] 判断模块，用于判断所述当前区块链是否具有上层区块链，得到判断结果；

[0031] 第一判断结果模块，用于若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息。

[0032] 第二判断结果模块，若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

[0033] 根据本发明提供的具体实施例，本发明公开了以下技术效果：

[0034] 本发明公开一种混合区块链架构系统、处理方法及处理系统。所述系统包括：上层区块链、当前区块链和下层区块链，所述当前区块链的输入端与所述下层区块链连接，所述当前区块链的输出端与所述上层区块链连接；所述当前区块链用于接收来自所述下层区块链的区块打包信息，同时用于向上层区块链打包所述当前区块链中的打包信息。本发明采用的不限层级的混合区块链架构在很大程度上扩展了区块链的应用范围和区块链在不同领域的可使用性，同时也使传统信息化应用领域在信息上的去分布式计算和存储、信息可追溯、信息防篡改等方面的能力得到较大的提高，具有良好的应用前景。

附图说明

[0035] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0036] 图1为本发明实施例混合区块链架构系统结构图；

[0037] 图2为本发明实施例混合区块链架构系统的处理方法流程图；

[0038] 图3为本发明实施例混合区块链架构系统的处理系统结构图。

具体实施方式

[0039] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，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他实施例，都属于本发明保护的范围。

[0040] 为使本发明的上述目的、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发明作进一步详细的说明。

[0041] 图1为本发明实施例混合区块链架构系统结构图。如图1所示，一种混合区块链架构系统，所述系统包括：上层区块链、当前区块链和下层区块链，所述当前区块链的输入端与所述下层区块链连接，所述当前区块链的输出端与所述上层区块链连接；所述当前区块链用于接收来自所述下层区块链的区块打包信息，同时用于向上层区块链打包所述当前区块链中的打包信息。

[0042] 所述当前区块链还用于接收上层区块链的区块打包信息。

[0043] 所述当前区块链在接收来自所述上/下层区块链的区块打包信息后，还用于进行交易确认。

[0044] 所述当前区块链与一个或多个所述下层区块链连接，所述当前区块链与一个或多个所述上层区块链连接。

[0045] 各所述区块链的连接方式包括：公有链连接，私有链连接、联盟链连接和多种链混合连接。

[0046] 各所述区块链的内部节点是不同的。

[0047] 各所述区块链的数据交易结构是不同的。

[0048] 任意层级的区块链的交易信息包括：本层区块链的交易数据结构和下层区块链的链标识。

[0049] 不限层级的区块链实现：在不限层级的混合区块链架构中最大特点是区块链间的关系和存在是可以不限层级进行扩展的，一个区块链可以由一个或多个下层级的区块链，同时其也可能有一个或多个上层区块链，本层区块链为其下层区块链的打包区块提供验证和背书功能；同时其上层区块链则为其提供验证和背书功能；每层的区块链通过区块链的链接节点进行区块链的链接；

[0050] 混合区块链架构：在区块链技术的实用上，本专利提供一种混合的架构，即架构中的每个区块链可以采用不同的实现技术，但其交易需要继承混合区块链指定的基类，在基类的基础上，每一层级的区块链根据应用场景和所承载业务的不同，选择不同交易信息模型的区块链；

[0051] 不同的共识机制管理：在区块链的关键技术共识机制上，混合区块链通过接口技术对常见的共识机制进行接口定义，不同层级的区块链继承此接口，实现区块链的初始化注册，但共识机制接口也实现了自我重载或定义的灵活性，可以使共识机制随着理论的发展，进行自定义扩展；同时在区块链技术的应用上是混合的，即不同的区块链；

[0052] 下层链初始化：下层区块链初始化是不限层次混合区块链架构进行区块链扩展的手段，通过对一个区块链进行下层链的初始化，让该区块链拥有下层区块链。在初始化下层区块链时，可由本层区块链向下层区块链颁发创世区块的区块信息hash和创链时间，同时利用该功能与区块链注册功能结合使用，使新初始化的区块链可以在区块链注册中心进行查询；

[0053] 区块链注册：对新初始化的区块链进行注册，在注册时会把新建区块链的上层区块链信息、新区块链的链标识、区块链共识机制、区块链节点等进行管理；区块链注册后，混合区块链架构中的其他区块链可以通过注册中心获取新区块链的相关信息、服务方式、交互方式等；

[0054] 区块打包：混合区块链架构中各层级区块链的区块信息打包与单条区块链的信息打包不同，单层区链打包时只需要把本层区块链发生的交易进行运算打包，而混合区块链在各层级的区块链打包时，需要把其下层区块链的形成的区块信息hash作为交易进行打包。

[0055] 当处于下层级区块链在打包完成一个区块后，需要把区块信息同本层区块链标识、上层区块链标识进行信息的hash，然后把信息hash构造信息上报交易，交易发起方为下层区块链，交易接收方为其对应的上层区块链，然后通过本层的链接者向上层区块链的接接者发送交易；

[0056] 区块验证提供跨区块链间进行区块信息验证的功能，该功能可由本层区块链发

起，也可以由下层区块链发起；当由区块链发起区块信息验证功能时，由该区块链的上层区块链的链接者根据区块链注册时的信息向待验证区块链发送需要验证区块的区块高度，然后待验证链根据区块高度向上层区块链发送其对应的区块信息，上层区块链再收到其区块信息后，对信息进行hash运算，运行完成后与自身存储的该下层区块链在该区块打包确认时发送的信息进行比较，如果一致，则区块验证通过，否则不通过。

[0057] 本发明采用的不限层级的混合区块链架构采用的不限扩展层级、混合区块链技术、自定义交易模型、自定义共识机制等机制在很大程度上扩展了区块链的应用范围和区块链在不同领域的可使用性，同时也使传统信息化应用领域在信息上的去分布式计算和存储、信息可追溯、信息防篡改等方面的能力得到较大的提高，具有良好的应用前景。

[0058] 图2为本发明实施例混合区块链架构系统的处理方法流程图。如图2所示，一种混合区块链架构系统的处理方法，所述处理方法包括：

[0059] 步骤201：发起交易；

[0060] 步骤202将所述交易揽入当前区块链交易池；

[0061] 步骤203：所述当前区块链对交易池中的交易进行打包，得到打包交易；

[0062] 步骤204：判断所述当前区块链是否具有上层区块链，得到判断结果；

[0063] 步骤205：若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息。

[0064] 步骤206：若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

[0065] 图3为本发明实施例混合区块链架构系统的处理系统结构图。如图3所示，一种混合区块链架构系统的处理系统，所述处理系统包括：

[0066] 交易发起模块301，用于发起交易；

[0067] 交易池模块302，用于将所述交易揽入当前区块链交易池；

[0068] 打包交易获取模块303，用于根据所述当前区块链对交易池中的交易进行打包，得到打包交易；

[0069] 判断模块304，用于判断所述当前区块链是否具有上层区块链，得到判断结果；

[0070] 第一判断结果模块305，用于若所述判断结果表示所述当前区块链具有上层区块链，则获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息。

[0071] 第二判断结果模块306，若所述当前区块链不具有上层区块链，则根据所述打包交易直接进行交易确认。

[0072] 本说明书中各个实施例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部分互相参见即可。对于实施例公开的系统而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0073] 本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处。综上所述，本说明书内容不

应理解为对本发明的限制。

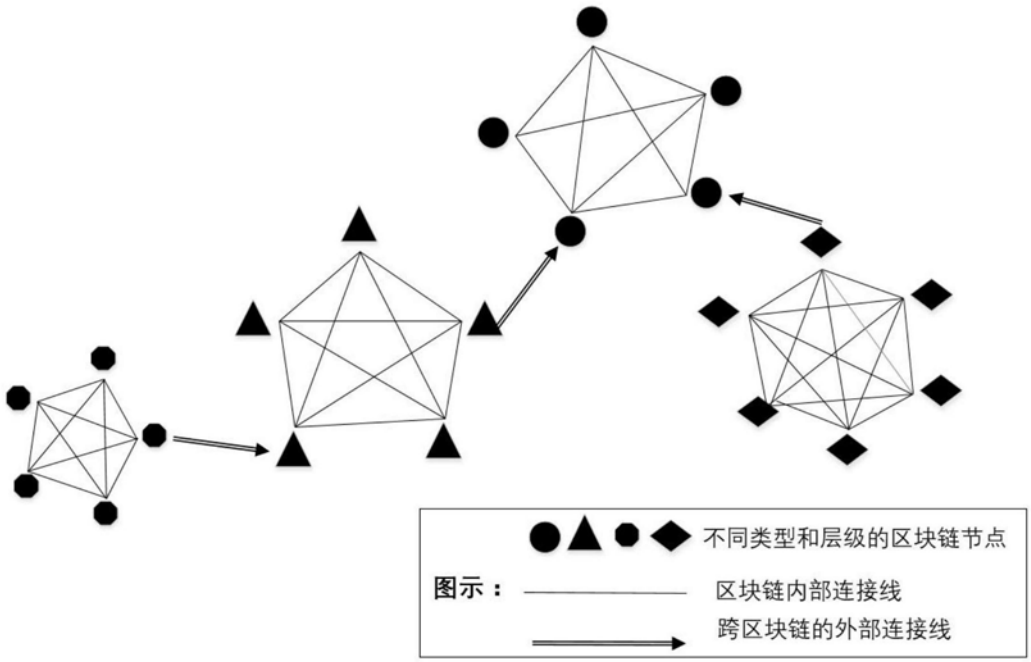


图1

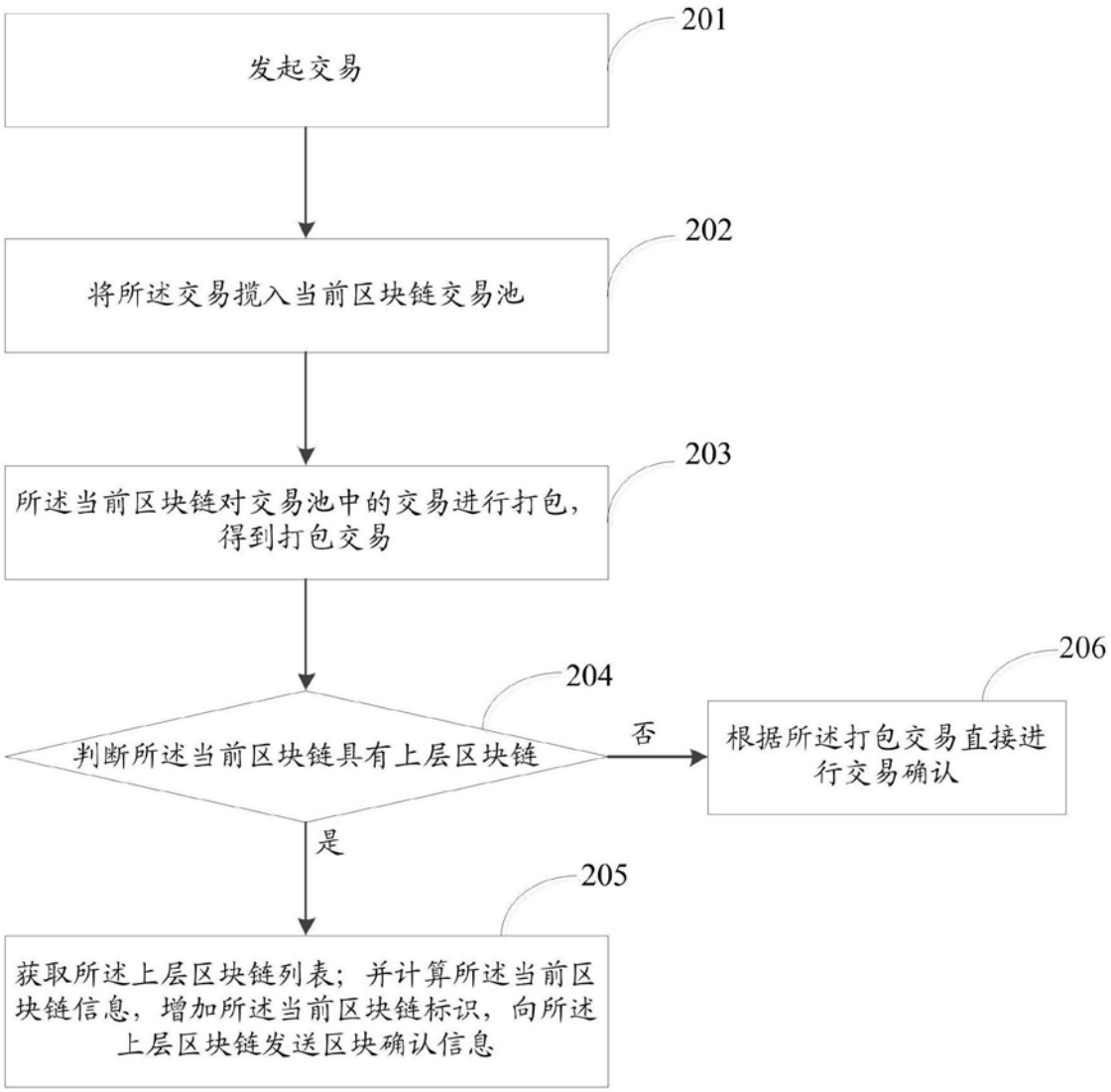

发起交易
201
将所述交易揽入当前区块链交易池
202
所述当前区块链对交易池中的交易进行打包，得到打包交易
203
判断所述当前区块链具有上层区块链
204
否
根据所述打包交易直接进行交易确认
206
是
获取所述上层区块链列表；并计算所述当前区块链信息，增加所述当前区块链标识，向所述上层区块链发送区块确认信息
205

图2

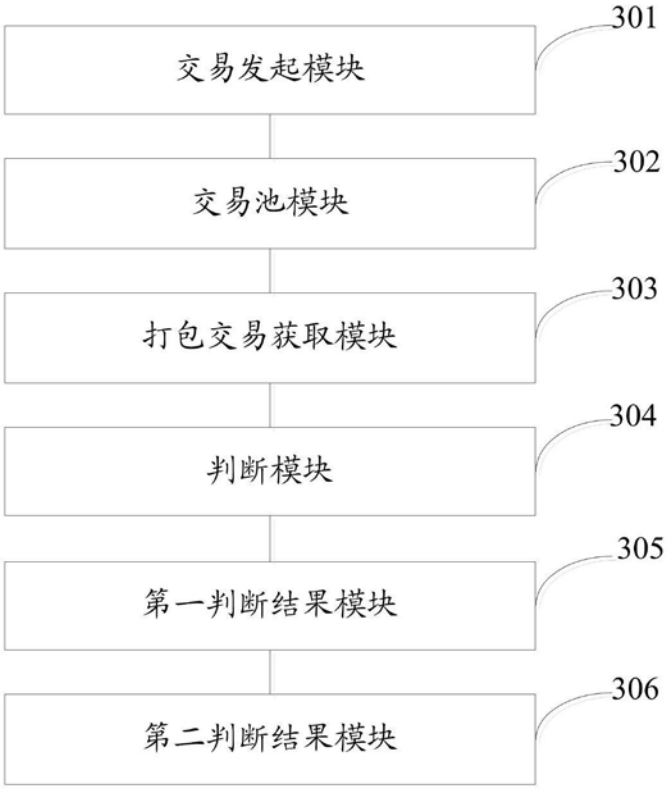

301
交易发起模块
302
交易池模块
303
打包交易获取模块
304
判断模块
305
第一判断结果模块
306
第二判断结果模块

图3