(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112910965 B
(45)授权公告日 2022.12.06

(21)申请号 202110063950.9
(22)申请日 2021.01.18
(65)同一申请的已公布的文献号
申请公布号 CN 112910965 A
(43)申请公布日 2021.06.04
(73)专利权人 香港理工大学深圳研究院
地址 518057 广东省深圳市南山区粤海街道高新技术产业园南区粤兴一道18号香港理工大学产学研大楼205室
(72)发明人 郭嵩 洪梓聪 谢鑫
(74)专利代理机构 深圳市君胜知识产权代理事务所(普通合伙) 44268
专利代理师 朱阳波
(51)Int.Cl.
H04L 67/1097(2022.01)
G06Q 20/40(2012.01)
G06Q 40/04(2012.01)
(56)对比文件
CN 111736963 A,2020.10.02
US 2016260169 A1,2016.09.08
审查员 王鹏飞

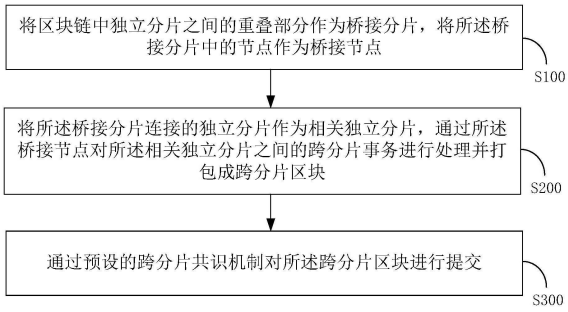
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种提交分片型区块链下跨分片事务的方法及系统

(57)摘要

本发明公开了一种提交分片型区块链下跨分片事务的方法及系统,通过将区块链中独立分片之间的重叠部分作为桥接分片,将所述桥接分片中的节点作为桥接节点;将所述桥接分片连接的独立分片作为相关独立分片,通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块;通过预设的跨分片共识机制对所述跨分片区块进行提交。本发明解决了现有区块链分片系统将各个跨分片事务拆分成若干个子事务来处理,大大降低了系统事务吞吐量和确认延时等性能指标的问题。



CN 112910965 B

1.一种提交分片型区块链下跨分片事务的方法,其特征在于,所述区块链中的独立分片之间有重叠,所述方法包括:

将区块链中独立分片之间的重叠部分作为桥接分片,将所述桥接分片中的节点作为桥接节点;

将所述桥接分片连接的独立分片作为相关独立分片,通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块;

通过预设的跨分片共识机制对所述跨分片区块进行提交;

所述通过预设的跨分片共识机制对所述跨分片区块进行提交包括:

建立跨分片共识机制;

通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息;

基于所述集体签名和所述提交信息完成对所述跨分片区块的提交;

所述通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息包括:

获取所述桥接分片中的节点对所述跨分片区块进行验证后生成的桥接集合签名;

将所述跨分片区块以及所述桥接集合签名发送至所述相关独立分片;

获取所述相关独立分片基于所述跨分片区块以及所述桥接集合签名进行签名并生成的独立集合签名;

获取基于所述独立集合签名生成的集体签名以及提交信息。

2.根据权利要求1所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述将区块链中独立分片之间的重叠部分作为桥接分片,将所述桥接分片中的节点作为桥接节点包括:

获取各分片的属性信息,根据各分片的属性信息确定桥接分片;所述桥接分片为区块链中独立分片之间的重叠部分;

将区块链中的节点随机分配至各分片中;

获取所述桥接分片中的节点,将所述桥接分片中的节点作为桥接节点。

3.根据权利要求1所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述将所述桥接分片连接的独立分片作为相关独立分片,通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块包括:

将所述桥接分片连接的独立分片作为相关独立分片;

通过所述桥接节点存储的账户信息对所述相关独立分片之间的转账交易信息进行验证;

将所述相关独立分片之间的转账交易信息以及验证结果打包成跨分片区块。

4.根据权利要求3所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述通过所述桥接节点存储的账户信息对所述相关独立分片之间的转账交易信息进行验证包括:

通过所述桥接节点存储的账户信息对检查转账交易中发送者的账户余额进行检查;

通过所述桥接节点存储的账户信息对检查转账交易中接收者的账户余额进行检查;

当所述发送者的账户余额正确减少以及所述接收者的账户余额正确增加时,所述相关

独立分片之间的转账交易的验证结果为正确。

5.根据权利要求1所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述获取所述桥接分片中的节点对所述跨分片区块进行验证后生成的桥接集合签名包括:

从所述桥接节点中选择一个节点作为领导节点,并将除所述领导节点之外的节点作为组员节点;

通过所述领导节点将所述跨分片区块发送至所述组员节点,使所述组员节点对所述跨分片区块进行验证并进行集体签名;

获取基于所述组员节点对所述跨分片区块进行签名生成的桥接集合签名。

6.根据权利要求1所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述获取基于所述独立集合签名生成的集体签名以及提交信息包括:

将所述独立集合签名发送至所述桥接分片;

获取所述桥接分片基于所述独立集合签名生成的集体签名以及提交信息。

7.根据权利要求1所述的一种提交分片型区块链下跨分片事务的方法,其特征在于,所述跨分片区块包括区块头和区块体;所述区块头包括所述相关独立分片的父区块哈希值及所述区块体的默克尔树根;所述区块体包括所述跨分片区块对应的跨分片事务以及所述相关独立分片中账户的状态信息。

8.一种区块链系统,其特征在于,所述区块链系统中的独立分片之间有重叠,所述区块链系统包括:

桥接分片,区块链中独立分片之间的重叠部分;

桥接节点,所述桥接分片中的节点;

相关独立分片,所述桥接分片连接的独立分片;

提交模块,用于通过所述桥接节点对所述相关独立分片之间的跨分片事务进行验证并打包成跨分片区块;

处理模块,用于通过预设的跨分片共识机制对所述跨分片区块进行提交;

所述通过预设的跨分片共识机制对所述跨分片区块进行提交包括:

建立跨分片共识机制;

通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息;

基于所述集体签名和所述提交信息完成对所述跨分片区块的提交;

所述通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息包括:

获取所述桥接分片中的节点对所述跨分片区块进行验证后生成的桥接集合签名;

将所述跨分片区块以及所述桥接集合签名发送至所述相关独立分片;

获取所述相关独立分片基于所述跨分片区块以及所述桥接集合签名进行签名并生成的独立集合签名;

获取基于所述独立集合签名生成的集体签名以及提交信息。

一种提交分片型区块链下跨分片事务的方法及系统

技术领域

[0001] 本发明涉及区块链领域，尤其涉及的是一种提交分片型区块链下跨分片事务的方法及系统。

背景技术

[0002] 目前，为了提高传统的区块链的可扩展性，设计出了完全分片系统。如图3所示，区块链完全分片系统中的节点划分为多个称为分片的组，这些组可以并行处理事务，各自维护一条区块链，达到提升区块链可扩展性的目的。但是分片系统中会出现跨分片事务，如一个分片中的账户往另外一个分片中的账户转账，这个事务的提交需要两个分片协同验证、共识，现有的完全分片协议通常采取将各个跨分片事务拆分成若干个子事务来处理的方法，这大大降低了系统事务吞吐量和确认延时等性能指标。

[0003] 因此，现有技术还有待改进和发展。

发明内容

[0004] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种提交分片型区块链下跨分片事务的方法及系统，旨在解决现有区块链的完全分片系统需要将各个跨分片事务拆分成若干个子事务来处理，大大降低了系统事务吞吐量和确认延时等性能指标的问题。

[0005] 本发明解决问题所采用的技术方案如下：

[0006] 第一方面，本发明实施例提供一种提交分片型区块链下跨分片事务的方法，其中，所述区块链中的独立分片之间有重叠，所述方法包括：

[0007] 将区块链中独立分片之间的重叠部分作为桥接分片，将所述桥接分片中的节点作为桥接节点；

[0008] 将所述桥接分片连接的独立分片作为相关独立分片，通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块；

[0009] 通过预设的跨分片共识机制对所述跨分片区块进行提交。

[0010] 在一种实施方式中，所述将区块链中独立分片之间的重叠部分作为桥接分片，将所述桥接分片中的节点作为桥接节点包括：

[0011] 获取各分片的属性信息，根据各分片的属性信息确定桥接分片；所述桥接分片为区块链中独立分片之间的重叠部分；

[0012] 将区块链中的节点随机分配至各分片中；

[0013] 获取所述桥接分片中的节点，将所述桥接分片中的节点作为桥接节点。

[0014] 在一种实施方式中，所述将所述桥接分片连接的独立分片作为相关独立分片，通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块包括：

[0015] 将所述桥接分片连接的独立分片作为相关独立分片；

[0016] 通过所述桥接节点存储的账户信息对所述相关独立分片之间的转账交易信息进行验证；

[0017] 将所述相关独立分片之间的转账交易信息以及验证结果打包成跨分片区块。

[0018] 在一种实施方式中，所述通过所述桥接节点存储的账户信息对所述相关独立分片之间的转账交易信息进行验证包括：

[0019] 通过所述桥接节点存储的账户信息对检查转账交易中发送者的账户余额进行检查；

[0020] 通过所述桥接节点存储的账户信息对检查转账交易中接收者的账户余额进行检查；

[0021] 当所述发送者的账户余额正确减少以及所述接收者的账户余额正确增加时，所述相关独立分片之间的转账交易的验证结果为正确。

[0022] 在一种实施方式中，所述通过预设的跨分片共识机制对所述跨分片区块进行提交包括：

[0023] 建立跨分片共识机制；

[0024] 通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息；

[0025] 基于所述集体签名和所述提交信息完成对所述跨分片区块的提交。

[0026] 在一种实施方式中，所述通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息包括：

[0027] 获取所述桥接分片中的节点对所述跨分片区块进行验证后生成的桥接集合签名；

[0028] 将所述跨分片区块以及所述桥接集合签名发送至所述相关独立分片；

[0029] 获取所述相关独立分片基于所述跨分片区块以及所述桥接集合签名进行签名并生成的独立集合签名；

[0030] 获取基于所述独立集合签名生成的集体签名以及提交信息。

[0031] 在一种实施方式中，所述获取所述桥接分片中的节点对所述跨分片区块进行验证后生成的桥接集合签名包括：

[0032] 从所述桥接节点中选择一个节点作为领导节点，并将除所述领导节点之外的节点作为组员节点；

[0033] 通过所述领导节点将所述跨分片区块发送至所述组员节点，使所述组员节点对所述跨分片区块进行验证并进行集体签名；

[0034] 获取基于所述组员节点对所述跨分片区块进行签名生成的桥接集合签名。

[0035] 在一种实施方式中，所述获取基于所述独立集合签名生成的集体签名以及提交信息包括：

[0036] 将所述独立集合签名发送至所述桥接分片；

[0037] 获取所述桥接分片基于所述独立集合签名生成的集体签名以及提交信息。

[0038] 在一种实施方式中，所述跨分片区块包括区块头和区块体；所述区块头包括所述相关独立分片的父区块哈希值及所述区块体的默克尔树根；所述区块体包括所述跨分片区块对应的跨分片事务以及所述相关独立分片中账户的状态信息。

[0039] 第二方面，本发明实施例还提供一种区块链系统，其中，所述区块链系统中的独立

分片之间有重叠，所述区块链系统包括：

[0040] 桥接分片，区块链中独立分片之间的重叠部分；

[0041] 桥接节点，所述桥接分片中的节点；

[0042] 相关独立分片，所述桥接分片连接的独立分片；

[0043] 提交模块，用于通过所述桥接节点对所述相关独立分片之间的跨分片事务进行验证并打包成跨分片区块；

[0044] 处理模块，用于通过预设的跨分片共识机制对所述跨分片区块进行提交。

[0045] 本发明的有益效果：本发明通过允许区块链中的分片重叠，将重叠部分作为桥接分片，使得桥接分片可存储多个其他分片的区块，充当分片之间的桥梁。并基于跨分片共识机制，桥接分片可以在保证安全、不冲突条件下，对跨分片事务直接进行验证、处理及共识，打包为跨分片区块，从而避免将跨分片事务拆分成多个子事务来处理，解决了现有区块链分片系统将各个跨分片事务拆分成若干个子事务来处理，大大降低了系统事务吞吐量和确认延时等性能指标的问题。

附图说明

[0046] 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，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0047] 图1是本发明实施例提供的一种提交分片型区块链下跨分片事务的方法的流程示意图。

[0048] 图2是本发明实施例提供的现有区块链系统中不分片系统的示意图。

[0049] 图3是本发明实施例提供的现有区块链系统中完全分片系统的示意图。

[0050] 图4是本发明实施例提供的本发明的桥接分片的示意图。

[0051] 图5是本发明实施例提供的桥接分片与独立分片之间的关系示意图。

[0052] 图6是本发明实施例提供的跨分片区块的组成示意图。

[0053] 图7是本发明实施例提供的跨分片共识机制的参考图。

[0054] 图8是本发明实施例提供的区块链系统的内部结构图。

[0055] 图9是本发明实施例提供的服务器的原理框图。

具体实施方式

[0056] 为使本发明的目的、技术方案及优点更加清楚、明确，以下参照附图并举实施例对本发明进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0057] 需要说明，若本发明实施例中有涉及方向性指示(诸如上、下、左、右、前、后……)，则该方向性指示仅用于解释在某一特定姿态(如附图所示)下各部件之间的相对位置关系、运动情况等，如果该特定姿态发生改变时，则该方向性指示也相应地随之改变。

[0058] 目前，区块链是信息技术领域中的一个热点。从本质上讲，区块链是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”、“全程留痕”、“可以追溯”、“公开透明”、“集

体维护”等特征，基于这些特征，区块链技术具有广阔的运用前景。

[0059] 分片技术最早是在传统的数据库领域里面提出的，主要用于大型商业数据库的优化。其概念就是将大型数据库中的数据划分成很多数据分片，再将这些数据分片分别存放在不同的服务器中，以减小每个服务器的数据访问压力，从而提高整个数据库系统的性能。简单来说，分而治之是分片技术的核心思想。而把分片技术运用到区块链网络中的思想是通过将系统节点分成多个分片，每个分片可并行处理区块链事务，从而在事务吞吐量和容纳节点数量的方面显著提高区块链的可扩展性。

[0060] 目前，传统的区块链包括不分片系统和完全分片系统。如图2所示，不分片系统中所有节点共同维护一条区块链，但由于每一轮的共识协议需要涉及到区块链网络中的所有节点，导致其可扩展性差。如图3所示，区块链完全分片系统中的节点划分为多个称为分片的组，这些组可以并行处理事务，各自维护一条区块链，达到提升区块链可扩展性的目的。但是分片系统中会出现跨分片事务，如一个分片中的账户往另外一个分片中的账户转账，这个事务的提交需要两个分片协同验证、共识，现有的完全分片协议通常采取将各个跨分片事务拆分成若干个子事务来处理，这大大降低了系统事务吞吐量和确认延时等性能指标。

[0061] 为了使现有的区块链系统在具备高可扩展性的同时，还能够避免由于跨分片事务导致系统事务吞吐量和确认延时等性能指标下降的问题，本发明提供一种提交分片型区块链下跨分片事务的方法。简单来说，本发明通过允许区块链中的独立分片重叠，将重叠部分作为桥接分片，使得桥接分片可存储多个其他独立分片的区块，充当独立分片之间的桥梁。并基于跨分片共识机制，桥接分片可以在保证安全、不冲突条件下，对跨分片事务直接进行验证、处理及共识，打包为跨分片区块，从而避免将跨分片事务拆分成多个子事务来处理，提升了区块链分片系统的性能。

[0062] 如图1所示，本实施例提供一种处理区块链中跨分片事务的方法，所述区块链中的独立分片之间有重叠，所述方法包括如下：

[0063] 步骤S100、将区块链中独立分片之间的重叠部分作为桥接分片，将所述桥接分片中的节点作为桥接节点。

[0064] 鉴于目前区块链的分片系统中会出现跨分片事务，例如一个分片中的账户往另外一个分片中的账户转账，这个事务的提交需要两个分片协同验证、共识，即为跨分片事务。因此本实施例中允许区块链中的独立分片之间有重叠，如图4所示，分片A、B之间的重叠部分即为分片AB。将重叠部分作为桥接分片，使得桥接分片可以存储多个独立分片的区块信息，从而实现通过桥接分片对其所桥接的独立分片之间的跨分片事务进行验证、处理及共识，并打包为跨分片区块。换言之，本实施例中的区块链系统包含两种分片，第一类是独立分片，只负责处理分片内部的事务；第二类是桥接分片，存储所桥接的分片的区块，并负责处理分片之间的跨分片事务。需要说明的是，桥接分片也能像独立分片一样处理内部事务。

[0065] 在一种实现方式中，所述步骤S100具体包括如下步骤：

[0066] 步骤S110、获取各分片的属性信息，根据各分片的属性信息确定桥接分片；所述桥接分片为区块链中独立分片之间的重叠部分；

[0067] 步骤S120、将区块链中的节点随机分配至各分片中；

[0068] 步骤S130、获取所述桥接分片中的节点，将所述桥接分片中的节点作为桥接节点。

[0069] 本实施例首先需要确定区块链系统中的桥接分片中包含的节点，即桥接节点，因为这些桥接节点将会存储多个分片的区块，可以直接验证以及处理相关的跨分片事务。具体地，系统启动时会设置分片数量以及各个分片的属性信息，每个分片的属性信息用于指示该分片是独立分片还是桥接分片，以及如果是桥接分片的话，分别桥接哪些独立分片。然后将区块链系统中的节点随机分配到各个分片中。在一种实现方式中，可以为区块链系统中的每个节点分配一个独有的节点ID，每个分片也分配一个独有的分片ID，然后系统会随机给每个节点ID分配一个分片ID，从而完成节点的随机分配。然后将桥接分片中的节点作为桥接节点，由于这些桥接节点存储多个分片的信息，因此它们可以直接对跨分片事务进行验证和打包成跨分片区块。

[0070] 为了处理分片之间的跨分片事务，如图1所示，所述方法还包括如下步骤：

[0071] 步骤S200、将所述桥接分片连接的独立分片作为相关独立分片，通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块。

[0072] 具体地，本实施例中将所述桥接分片所桥接的多个独立分片作为该桥接分片对应的相关独立分片，由于这些桥接节点存储多个分片的信息，因此它们可以直接对跨分片事务进行处理并打包成跨分片区块。举例说明，如图5所示，有三个分片在区块链系统中，其中桥接分片C所桥接的是独立分片A和B。因此在本实施例中，桥接分片C的相关独立分片就是独立分片A和独立分片B，桥接分片C中的桥接节点负责处理独立分片A和B之间的跨分片事务，并打包成跨分片区块。

[0073] 在一种实现方式中，所述步骤S200具体包括如下步骤：

[0074] 步骤S210、将所述桥接分片连接的独立分片作为相关独立分片；

[0075] 步骤S220、通过所述桥接节点存储的账户信息对所述相关独立分片之间的转账交易信息进行验证；

[0076] 步骤S230、将所述相关独立分片之间的转账交易信息以及验证结果打包成跨分片区块。

[0077] 具体地，本实施例中独立分片之间的跨分片事务指的是独立分片中账户间的转账交易，这些事务由于同时涉及到不同分片的账户信息，仅由单一的独立分片无法进行验证。而桥接节点由于存储着相关独立分片的区块，所以拥有相关独立分片的账户信息，可以对相关独立分片之间的跨分片事务进行验证。

[0078] 在一种实现方式中，对相关独立分片之间的跨分片事务进行验证的过程具体为：通过所述桥接节点存储的账户信息对检查转账交易中发送者的账户余额进行检查，以及通过所述桥接节点存储的账户信息对检查转账交易中接收者的账户余额进行检查。当所述发送者的账户余额正确减少以及所述接收者的账户余额正确增加时，所述相关独立分片之间的转账交易的验证结果为正确，反之，验证结果为错误。然后将所述相关独立分片之间的转账交易信息以及验证结果打包成跨分片区块。在一种实现方式中，如图6所示，跨分片区块包括区块头和区块体，所述区块头包括所述相关独立分片的父区块哈希值及所述区块体的默克尔树根，所述区块体包括所述跨分片区块对应的跨分片事务以及所述相关独立分片中账户的状态信息，其中跨分片事务和账户的状态信息可以以列表的形式呈现。

[0079] 打包成跨分片区块以后，还需要桥接分片以及独立分片中的节点同意该跨分片区块，如图1所示，所述方法还包括如下步骤：

[0080] 步骤S300、通过预设的跨分片共识机制对所述跨分片区块进行提交。

[0081] 具体地，当打包完毕跨分片区块以后，为了保证该跨分片区块在桥接分片以及独立分片之间的一致性，需要利用预设的跨分片共识机制对该跨分片区块进行提交。

[0082] 在一种实现方式中，所述步骤S300具体包括如下步骤：

[0083] 步骤S310、建立跨分片共识机制；

[0084] 步骤S320、通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息；

[0085] 步骤S330、基于所述集体签名和所述提交信息完成对所述跨分片区块的提交。

[0086] 传统分片系统中的共识机制只在分片内部进行共识，即只有单个分片内部的节点会参与共识。而本实施例中预先设置的跨分片共识既包含分片内部的共识，也包含多个分片之间的互相协作。本实施例首先建立一个跨分片共识机制，然后通过所述跨分片共识机制获取所述桥接节点以及所述相关独立分片对所述跨分片区块进行验证后生成的集体签名和提交信息。

[0087] 在一种实现方式中，为了生成的集体签名和提交信息，本实施例首先获取所述桥接节点对所述跨分片区块进行验证后生成的桥接集合签名。为了生成桥接集合签名，本实施例首先从所有桥接节点中选择一个节点作为领导节点(可以随机选择)，并将除所述领导节点之外的节点作为组员节点，然后通过所述领导节点将所述跨分片区块发送至所述组员节点，使所述组员节点对所述跨分片区块进行验证并进行集体签名，然后获取基于所述组员节点对所述跨分片区块进行签名生成的桥接集合签名。

[0088] 获取到桥接集合签名以后，将所述跨分片区块以及所述桥接集合签名发送至所述相关独立分片，再获取所述相关独立分片基于所述跨分片区块以及所述桥接集合签名进行签名并生成的独立集合签名，获取到独立集合签名以后，需要将所述独立集合签名回传至桥接分片，然后所述桥接分片基于所述独立集合签名生成的集体签名以及提交信息。最后，基于所述集体签名和所述提交信息完成对所述跨分片区块的提交。

[0089] 简单来说，如图7所示，可以将本实施例中通过预设的跨分片共识机制对所述跨分片区块进行提交的过程抽象为三个阶段：预准备阶段、准备阶段、提交阶段。首先，在预准备阶段，从桥接分片的节点中随机选择一个领导者，通过该领导者提出一个跨分片区块，然后将其发送至其余桥接节点进行验证并进行集体签名，当大部分桥接节点同意对该跨分片区块进行签名时，将会为该跨分片区块生成一个集合签名，为了区分不同类型的节点对应的集合签名，本实施例中将桥接节点的集合签名命名为桥接集合签名。由于桥接节点拥有多个独立分片的账户信息，所以可以生成一个合法的跨分片区块。然而，因为桥接分片所桥接的独立分片还未收到这个跨分片区块及账本状态仍未更新，因此该跨分片区块仍不能被提交。因此在准备阶段，该跨分片区块和桥接集合签名会被发送至所述桥接分片所桥接的独立分片，即相关独立分片。所述相关独立分片中的节点接收以后，会对该跨分片区块进行集体签名，并生成一个集合签名，本实施例中将相关独立分片中的节点的集合签名命名为独立集合签名，表示该跨分片区块已经被所述相关独立分片接收，然后将所述独立集合签名回传至所述桥接分片。最后，在提交阶段，如果桥接分片接收到所有相关独立分片的集合签名，则它会基于所有相关独立分片的集合签名进行一次集体签名，并生成提交信息声明该跨分片区块可以被提交，然后发送给相关独立分片，从而完成该跨分片区块的提交。

[0090] 本发明提供的一种提交分片型区块链下跨分片事务的方法在现时及/或将来皆可用来提高区块链的系统性能，拓宽区块链的应用范围，为车联网、智慧工厂、智慧城市等设备高异构性的场景提供高性能区块链系统。

[0091] 典型案例如：当区块链应用于智慧城市时，由于设备具有高异构性，使得区块链节点可以是各种物联网设备或边缘/云服务器，可以将具有不同能力的异构区块链节点分配给层级分片中不同分片中，能力较强的节点可以分配在桥接更多分片的桥接分片中，更充分的利用设备的能力以及提升区块链系统的性能。

[0092] 基于上述实施例，本发明实施例还提供一种区块链系统，所述区块链系统中的独立分片之间有重叠，如图8所示，所述区块链系统中包括：

[0093] 桥接分片01，区块链中独立分片之间的重叠部分；

[0094] 桥接节点02，所述桥接分片中的节点；

[0095] 相关独立分片03，所述桥接分片连接的独立分片；

[0096] 打包模块04，用于通过所述桥接节点对所述相关独立分片之间的跨分片事务进行验证并打包成跨分片区块；

[0097] 提交模块05，用于通过预设的跨分片共识机制对所述跨分片区块进行提交。

[0098] 基于上述实施例，本发明还提供了一种服务器，其原理框图可以如图9所示。该服务器包括通过系统总线连接的处理器、存储器、网络接口、显示屏。其中，该服务器的处理器用于提供计算和控制能力。该服务器的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该服务器的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种提交分片型区块链下跨分片事务的方法。该服务器的显示屏可以是液晶显示屏或者电子墨水显示屏。

[0099] 本领域技术人员可以理解，图9中示出的原理框图，仅仅是与本发明方案相关的部分结构的框图，并不构成对本发明方案所应用于其上的服务器的限定，具体的服务器可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0100] 在一种实现方式中，所述服务器的存储器中存储有一个或者一个以上的程序，且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于进行提交分片型区块链下跨分片事务的方法的指令。

[0101] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本发明所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0102] 综上所述，本发明公开了一种提交分片型区块链下跨分片事务的方法即区块链系

统，通过将区块链中独立分片之间的重叠部分作为桥接分片，将所述桥接分片中的节点作为桥接节点；将所述桥接分片连接的独立分片作为相关独立分片，通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块；通过预设的跨分片共识机制对所述跨分片区块进行提交。本发明通过允许区块链中的分片重叠，将重叠部分作为桥接分片，使得桥接分片可存储多个其他分片的区块，充当分片之间的桥梁。并基于跨分片共识机制，桥接分片可以在保证安全、不冲突条件下，对跨分片事务直接进行验证、处理及共识，打包为跨分片区块，从而避免将跨分片事务拆分成多个子事务来处理，解决了现有区块链的完全分片系统需要将各个跨分片事务拆分成若干个子事务来处理，大大降低了系统事务吞吐量和确认延时等性能指标的问题。

[0103] 应当理解的是，本发明的应用不限于上述的举例，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，所有这些改进和变换都应属于本发明所附权利要求的保护范围。

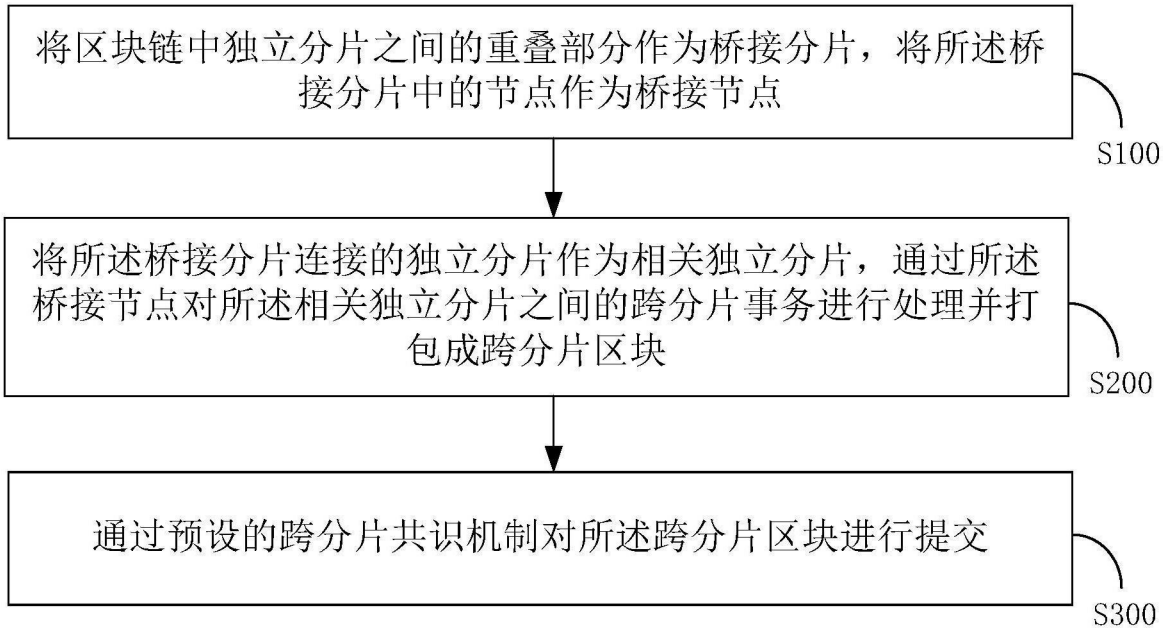

将区块链中独立分片之间的重叠部分作为桥接分片，将所述桥接分片中的节点作为桥接节点
S100
将所述桥接分片连接的独立分片作为相关独立分片，通过所述桥接节点对所述相关独立分片之间的跨分片事务进行处理并打包成跨分片区块
S200
通过预设的跨分片共识机制对所述跨分片区块进行提交
S300

图1

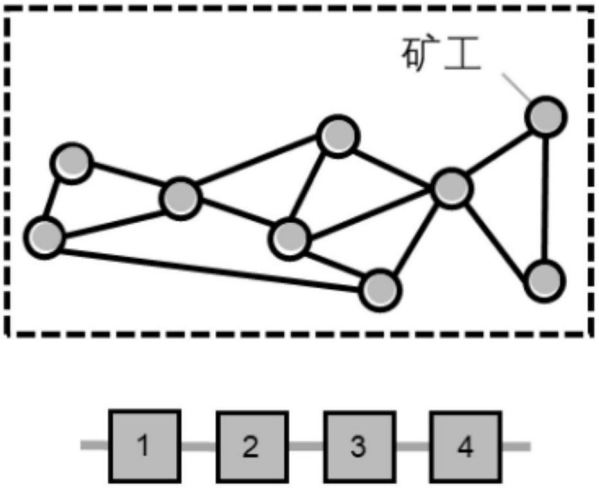

矿工
1
2
3
4

图2

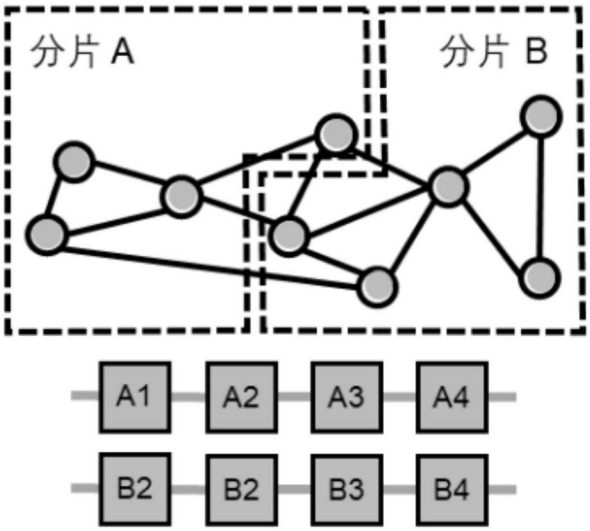

分片 A
分片 B
A1
A2
A3
A4
B2
B2
B3
B4

图3

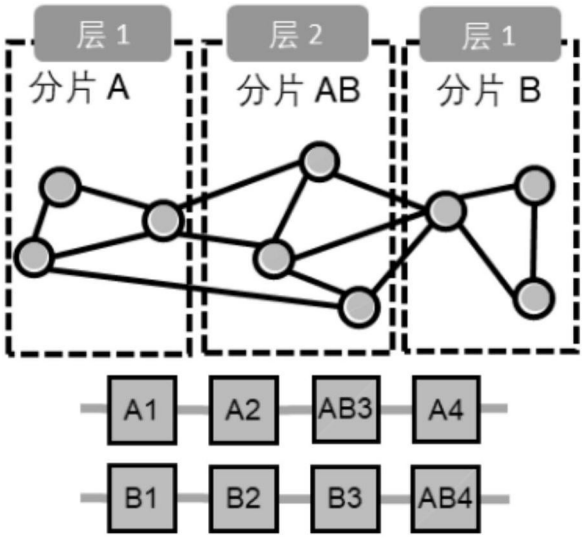

层 1
层 2
层 1
分片 A
分片 AB
分片 B
A1
A2
AB3
A4
B1
B2
B3
AB4

图4

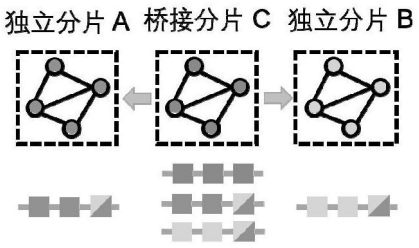

独立分片 A
桥接分片 C
独立分片 B

图5

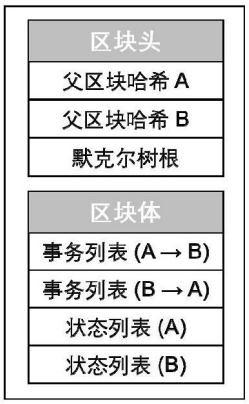

区块头
父区块哈希 A
父区块哈希 B
默克尔树根
区块体
事务列表 (A → B)
事务列表 (B → A)
状态列表 (A)
状态列表 (B)

图6

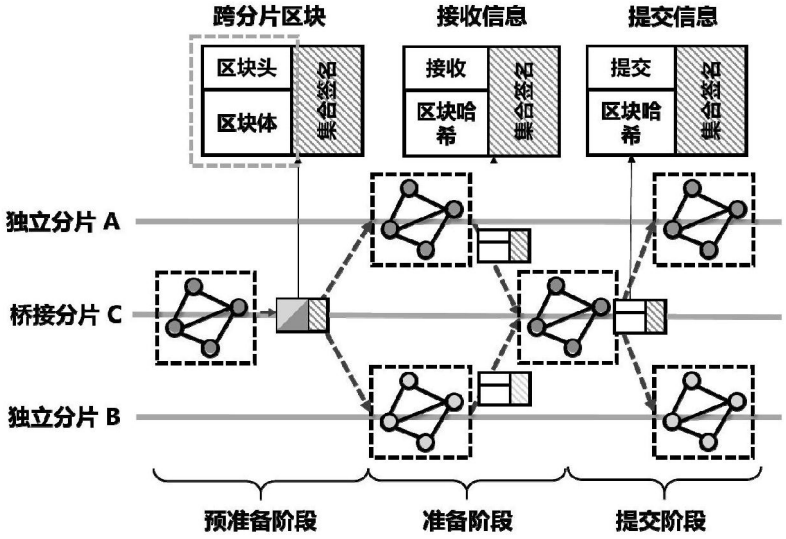

跨分片区块
区块头
区块体
默克尔树
接收信息
接收
区块哈希
默克尔树
提交信息
提交
区块哈希
默克尔树
独立分片 A
桥接分片 C
独立分片 B
预准备阶段
准备阶段
提交阶段

图7

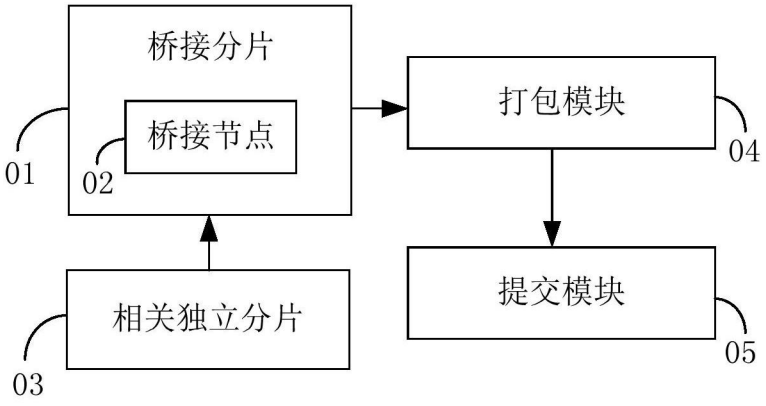

桥接分片
桥接节点
01
02
打包模块
04
相关独立分片
03
提交模块
05

图8

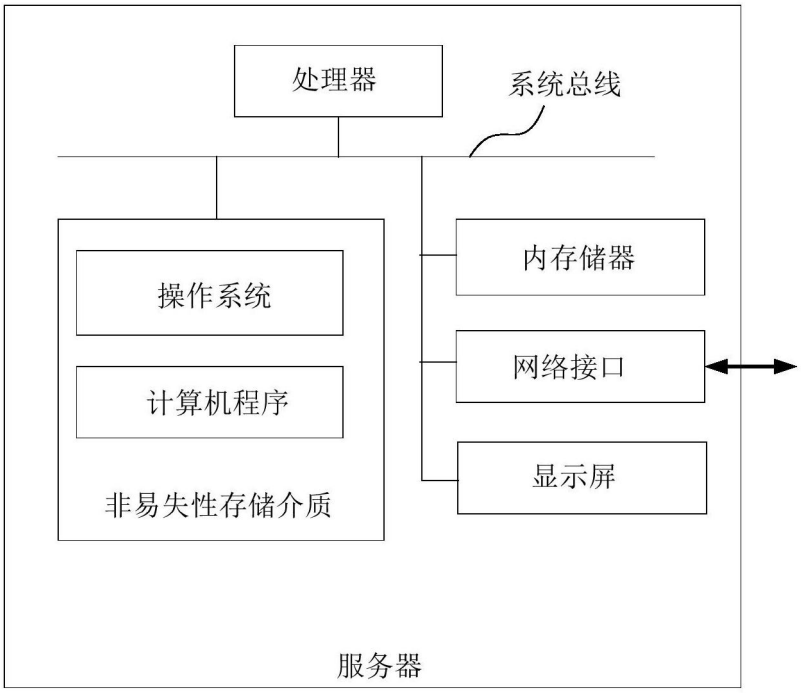


图9