(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108564470 A
(43)申请公布日 2018.09.21

(21)申请号 201810341423.8

(22)申请日 2018.04.17

(71)申请人 北京天德科技有限公司
地址 100089 北京市海淀区苏州街18号长远天地大厦B1座601

(72)发明人 蔡维德

(51)Int.Cl.
G06Q 40/04(2012.01)

权利要求书2页 说明书4页 附图2页

(54)发明名称

一种区块链中并行建块的交易分发方法

(57)摘要

本发明涉及到一种区块链并行建块的交易分发方法，其特征在于，包含以下几个步骤：(1)每个区块链节点内多个建块流程并行建块，同时处理交易，通过共识后存储在区块链上；(2)每个区块链节点有一个统一的交易分发模块，负责接收所有的外部交易，并负责交易向不同建块流程的分发；(3)同一个交易在不同的区块链节点中必须被分发到同一个建块流程中；(4)若不同交易之间存在着依赖关系，则分发时必须按照依赖顺序进行处理分发，被依赖的交易通过共识存储完毕后，依赖的交易才可以被分发。本发明设计了一种交易分发的机制，使得现有的区块链单链系统可以同时并行的运行多个链来处理数据，大大提升了区块链的处理速度，并针对实际应用中可能会存在的交易依赖问题，提供了通用的解决方案，保证了各个节点交易执行结果的正确性和执行顺序的一致性。

CN 108564470 A

1.一种区块链并行建块的交易分发方法，其特征在于，包含以下几个步骤：

(1)每个区块链节点内多个建块流程并行建块，同时处理交易，通过共识后存储在区块链上；

(2)每个区块链节点有一个统一的交易分发模块，负责接收所有的外部交易，并负责交易向不同建块流程的分发；

(3)同一个交易在不同的区块链节点中必须被分发到同一个建块流程中；

(4)若不同交易之间存在着依赖关系，则分发时必须按照依赖顺序进行处理分发，被依赖的交易通过共识存储完毕后，依赖的交易才可以被分发。

2.根据权利要求1所述的一种区块链中并行建块的分发方法，其特征在于：所述步骤(1)具体为：

步骤1.1 每个区块链节点内多个建块流程逻辑完全一致，同时处理交易，互不影响，每个建块流程根据一定规则生成标识号；

步骤1.2 各个区块链节点之间标识号相同的建块流程进行通信与共识，通过投票得到最终的结果。

3.根据权利要求1所述的一种区块链中并行建块的分发方法，其特征在于：所述步骤(2)具体为：

步骤2.1 各个区块链节点接收交易，并将交易送入交易分发模块；

步骤2.2 交易分发模块根据交易具体的业务特征获取交易的依赖规则和依赖特征值；

步骤2.3 根据交易依赖规则查找依赖的交易，如果依赖的交易没有被分发，则当前交易不会被分发，没有依赖的交易或依赖的交易已经被分发并存到了区块链上，则当前交易进入分发流程；

步骤2.4 交易分发模块的分发流程使用依赖特征值根据一定的算法得到交易对应的分发通道标号，对应区块链节点中建块流程的标号；

步骤2.5 交易根据步骤2.4中得到的标号分发到不同的建块流程中进行共识。

4.根据权利要求1所述的一种区块链中并行建块的分发方法，其特征在于：所述步骤(3)具体为：

步骤3.1 所有节点使用相同逻辑的交易分发模块；

步骤3.2 分发算法和具体的节点信息等无关，只和交易本身数据有关；

步骤3.3 必须保证相同的交易通过计算后得到相同的标号，被分发到同一个建块流程中。

5.根据权利要求1所述的一种区块链中并行建块的分发方法，其特征在于：所述步骤(4)具体为：

步骤4.1 交易间存在业务依赖的应用，依赖关系会影响交易的分发顺序；

步骤4.2 如果当前交易依赖一个或多个交易，依赖的交易处于分发阶段、共识阶段都会影响当前交易的分发，只有依赖的交易通过共识存入区块链后当前交易才可以进入分发阶段，依赖交易未处理完毕，则当前交易暂时退回，留待下次再进行分发处理；

步骤4.3 交易的依赖关系可以是多种类型的，根据实际应用的业务规则通过一定方法标注在交易上，即依赖规则；

步骤4.4 交易的依赖规则必须可以在交易数据上找到对应的特征值，用于计算分发的

建块流程标号；

步骤4.5 分发算法必须保证相同的特征值计算得到相同的结果。

一种区块链中并行建块的交易分发方法

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种私有区块链并行建块的交易分发方法。

背景技术

[0002] 在区块链系统中，多个节点维护一个相同的区块链，各个区块链节点的数据一致。现有的区块链系统每个节点同时只运行一条区块链，这个链上运行的仅有的一个建块流程对交易进行共识处理。当交易量较大时，只有一条链的区块链系统运行速度会大大降低，且无法通过有效的扩容手段来增加区块链吞吐量。

发明内容

[0003] 针对目前区块链系统的单链结构，本发明提出一种区块链中并行建块的交易分发方法，通过实现高效的交易分发模块，将多条区块链并行连接到一起，使得区块链系统能够有多个建块流程同时进行，在高并发交易数据的场景下，能够提升区块链的整体吞吐量，提高节点的处理性能，并且易于扩容。

[0004] 本发明提出一种区块链中并行建块时分发方法方案，包含以下特征：

(1)每个区块链节点内多个建块流程并行建块，同时处理交易，通过共识后存储在区块链上；

(2)每个区块链节点有一个统一的交易分发模块，负责接收所有的外部交易，并负责交易向不同建块流程的分发；

(3)同一个交易在不同的区块链节点中必须被分发到同一个建块流程中；

(4)若不同交易之间存在着依赖关系，则分发时必须按照依赖顺序进行处理分发，被依赖的交易通过共识存储完毕后，依赖的交易才可以被分发。

[0005] 进一步地，对于步骤(1)，具体为：

步骤1.1 每个区块链节点内多个建块流程逻辑完全一致，同时处理交易，互不影响，每个建块流程根据一定规则生成标识号；

步骤1.2 各个区块链节点之间标识号相同的建块流程进行通信与共识，通过投票得到最终的结果。

[0006] 进一步地，对于步骤(2)，具体为：

步骤2.1 各个区块链节点接收交易，并将交易送入交易分发模块，交易分发模块会收取所有的交易信息，并将新收到的交易信息放入一个节点内全局统一的一个缓存队列中，新的交易会被放置在队列的尾部。；

步骤2.2 交易分发模块根据交易具体的业务特征获取交易的依赖规则和依赖特征值；

步骤2.3 根据交易依赖规则查找依赖的交易，如果依赖的交易没有被分发，则当前交易不会被分发，没有依赖的交易或依赖的交易已经被分发并存到了区块链上，则当前交易进入分发流程；

步骤2.4 交易分发模块的分发流程使用依赖特征值根据一定的算法得到交易对应的分发通道标号，对应区块链节点中建块流程的标号；

步骤2.5 交易根据步骤2.4中得到的标号分发到不同的建块流程中进行共识。

[0007] 交易分发模块会不断地重复步骤(2)中的操作进行交易的分发。不断地将新的交易分发到各个建块流程中去。各个建块流程按照正常的区块链共识步骤对交易进行建块投票，最终存入区块链。

[0008] 进一步地，对于步骤(3)，具体为：

步骤3.1 所有节点使用相同逻辑的交易分发模块；

步骤3.2 分发算法和具体的节点信息等无关，只和交易本身数据有关；

步骤3.3 必须保证相同的交易通过计算后得到相同的标号，被分发到同一个建块流程中。

[0009] 进一步地，对于步骤(4)，具体为：

步骤4.1 交易间存在业务依赖的应用，依赖关系会影响交易的分发顺序；

步骤4.2 如果当前交易依赖一个或多个交易，依赖的交易处于分发阶段、共识阶段都会影响当前交易的分发，只有依赖的交易通过共识存入区块链后当前交易才可以进入分发阶段，依赖交易未处理完毕，则当前交易暂时退回，留待下次再进行分发处理；

步骤4.3 交易的依赖关系可以是多种类型的，根据实际应用的业务规则通过一定方法标注在交易上，即依赖规则；

步骤4.4 交易的依赖规则必须可以在交易数据上找到对应的特征值，用于计算分发的建块流程标号；

步骤4.5 分发算法必须保证相同的特征值计算得到相同的结果。

[0010] 进一步地，本发明需要注意的是：

无论交易分发模块使用怎样的算法进行分发，相同的交易在不同的节点应该得到同样的分发结果，且分发算法不应受外部的时间、节点等信息影响，而仅受制于交易数据本身或应用业务规则本身。交易的依赖关系可以是单一字段的，比如交易某一个字段为相同的值的所有交易必须按照时间戳进行处理；可以是一对一的依赖，比如交易A必须在交易B存入区块链后才能处理；也可以是一对多的，比如交易A必须在交易B、C、D等存入区块链后才能处理；也可以是其他业务规则描述的依赖关系等等。依赖规则不管通过怎样的方式描述，必须可通过一定方法找到依赖的交易对象，以进行依赖判断。

[0011] 本发明提供了一种区块链并行建块的交易分发方法，使得通过实现交易分发模块，将区块链进行横向扩展，并行连接在一起，在确保区块链数据的一致性和完整性的前提下，大大提升了大并发交易数据量下区块链的处理速度和吞吐量。并且，仅需要修改交易本身的依赖关系和依赖特征值，或替换具体的分发算法，本设计就可应用于大部分的应用场景，可复用性较高。

附图说明

[0012] 下文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。示例中相同的图例标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。本发明的目标及特征考虑到如下结合附图的描述将更加明显，

附图中：

附图1：交易分发处理流程模型；

附图2：判断交易依赖关系示意图；

附图3：交易分发泳道示意图。

具体实施方式

[0013] 在以下的叙述中，为了使本发明的目的、技术方案和优点更加清楚，下面结合附图将对本发明的实施作进一步的详细描述。

[0014] 具体的流程可参考如下：假设区块链系统中有4个节点，分别为节点A、节点B、节点C、节点D。案例中将建块流程称为泳道，即每个区块链节点包含多个泳道，交易通过分发进入不同的泳道进行共识。分发逻辑使用特征值模(%)泳道数量得到分发的标号。

[0015] (1)某个区块链的客户端构建了一批交易，并将这些交易广播到区块链A、B、C、D四个节点中去。

[0016] (2)节点A、节点B、节点C、节点D中都有各自的交易接收模块，这些交易接收模块将新收到的交易放入各自的全局缓存队列中去，例如存放在Redis中，A、B、C、D四个节点各自的全局缓存队列分别为QueueA、QueueB、 QueueC、 QueueD。

[0017] (3)A、B、C、D四个节点的交易分发模块会不断从各自的队列QueueA、QueueB、QueueC、QueueD中拿出一批交易进行处理。

[0018] 这里以节点A为例进行说明。A的交易分发模块从队列QueueA中拿出1000条交易逐条处理。交易处理的示意图如图1所示。针对每条交易，首先会判断该条交易(以交易T为例)是否有前置依赖的交易，判断过程如图2所示。判断依赖关系会取出该条交易的依赖字段(内容用D表示)，同时分别记录每个泳道中待处理交易和正在处理的交易的两个哈希表，分别称为H1和H2，这时会判断D是否作为key出现在了H1或H2中，如果出现在了H1或H2中任何一个哈希表中，则表示该交易T存在前置依赖的交易还未处理完，这时交易T就不能被分发。A的交易分发模块会将交易T记录下来，接着处理下一条交易。如果D作为key没有出现在H1或H2任何一个哈希表中，则表示该交易T不存在依赖的交易，这时会将交易T进行哈希，得到哈希值hashT，并计算hashT%泳道数量n，将得到的结果分发到不同泳道的交易处理流程中去，如计算得到3，则表示需要将交易T分发到标号为3的泳道中，如图2示意图所示。交易分发后会将交易T记录到上文中提到的H1哈希表中。就这样逐个处理完了这1000条交易，没有依赖的交易都被分到了不同的泳道中去，而那些存在依赖的交易会被重新放入节点A的缓存队列QueueA中去。其他节点的处理流程与此一致。

[0019] (4)A、B、C、D四个节点的建块模块分别从各自交易队列中获取交易，然后针对这些交易进行后续的拜占庭建块流程。

[0020] 再次以A为例，A的某个泳道如A1，获取了A1队列中的2000条交易进行建块。这时A1会将这2000条交易以依赖字段为key从H1哈希表中删除，并放入表示正在处理中交易的H2哈希队列中去。假设其中的1900条处理完成了共识，被记录到了区块链的账本上，A1会以这1900条交易的依赖字段为key，将这些交易从上文中提到的H2哈希队列中删除。剩下的100条未处理的交易会接着放回泳道A1的交易队列中去，并以这100条交易的依赖字段为key，将这些交易再次写回H1哈希表中。

[0021] 本发明说明书中未作详细描述的内容属本领域技术人员的公知技术。

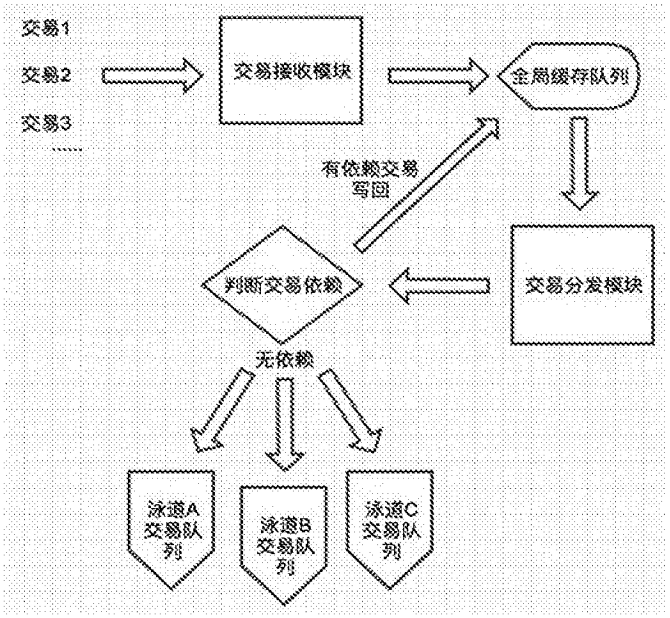
交易1
交易2
交易3
交易接收模块
全局缓存队列
有依赖交易
写回
判断交易依赖
交易分发模块
无依赖
泳道A
交易队
列
泳道B
交易队
列
泳道C
交易队
列

图1

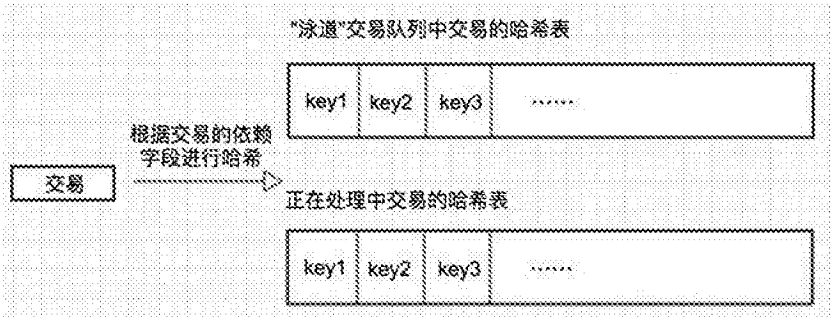
"泳道"交易队列中交易的哈希表
key1
key2
key3
……
根据交易的依赖
字段进行哈希
交易
正在处理中交易的哈希表
key1
key2
key3
……

图2

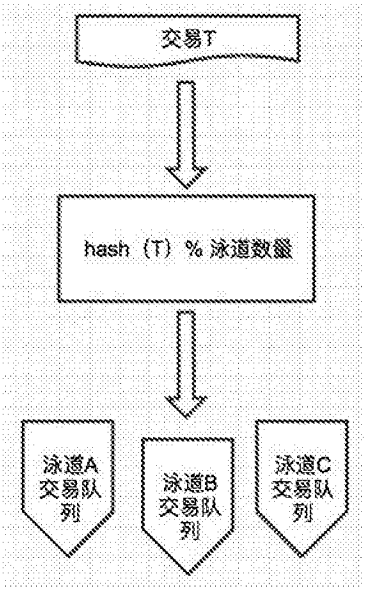

图3