

一种云平台场景下的 CA-PBFT 算法 *

李婷婷

四川文轩职业学院 四川省成都市 611330

摘要: 针对区块链与云平台相结合的场景中, 传统的拜占庭容错算法 (practical byzantine fault tolerant, PBFT) 存在通信复杂度高、共识效率低、吞吐量较低等问题, 提出一种基于通信和模型的改进型拜占庭容错算法。该算法以多维度综合性评分模型和通信性能模型为基础, 评估节点的评分并将其划分为多级队列, 规范节点行为, 优化选主策略; 同时依据通信性能模型对于集群进行分簇, 簇内部执行动态调整的一致性协议, 分解共识任务, 提高共识效率。最后在模拟无线网络搭建的仿真环境中, CA-PBFT 共识算法在集群内部存在恶意节点与否的情况下, 相较于 PBFT 共识算法, 在吞吐量、网络负载和共识时延等性能方面表现更优。

关键词: 区块链; 共识算法; 实用拜占庭容错共识算法; 动态一致性协议

1 算法概述

PBFT 算法是由 Miguel Castro 和 Barbara Liskov 于 1999 年提出, 其大体组成可以分为一致性协议, 视图切换协议和检查点协议。

1.1 一致性协议

PBFT 算法的核心就是一致性协议, 其主要功能是保证区块链各个节点数据同步。该协议定义了两种类型的角色: 客户端节点 (Client) 和副本节点 (Replica), 其中副本节点又分为主节点和备份节点, PBFT 算法的一致性协议的执行过程如图 1 所示, 其五个过程分别是请求、预准备、准备、提交和响应。

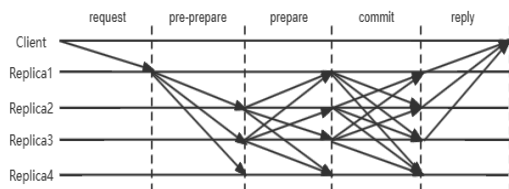


图 1 PBFT 算法一致性协议过程

(1)Request 阶段: 该阶段需要选取主节点、客户端发送请求到主节点。在该算法中选取主节点主要是按照依次轮换或者随机算法的方式。若采用的方式是依次轮换, 则其公式为:

$$i = v \bmod |N| \quad (1)$$

式中: N 为参与共识的节点总数量, i 为副本节点编号,

v 表示当前视图编号。主节点选取完毕之后, 客户端会向选出的主节点发送 Request 消息。

(2)Pre-prepare 阶段: 主节点接收客户端发送的消息, 若该消息为合理请求, 则会向备份节点广播发送 Pre-prepare 消息, 各备份节点会收到该消息。

(3)Prepare 阶段: 验证收到的 Pre-prepare 之后会广播 Prepare 消息到该集群中除自己之外的所有节点。而在相同时间会有很多节点在广播 Prepare 消息, 若如果收到至少 $2f$ 个 Prepare 消息, 则表明 Prepare 阶段结束。

(4)Commit 阶段: 节点会向除自己以外的所有节点广播 Commit 消息, 同 Prepare 阶段一样, 同时会有多个节点同时广播 Commit 消息, 若收到 $2f + 1$ 个 Commit 消息, 则表明此时达成了共识, 随后该节点就会运行具体的操作, 把请求消息写入本地。

(5)Reply 阶段: 各节点在把请求消息写入本地之后就会向客户端发送相关的响应消息。

1.2 视图切换协议

视图切换协议指的是上述阐述的共识过程中, 在某间隔时间内没有生成新区块, 主节点发生了错误或者故障, 这时候 PBFT 算法就需要将视图 v (view) 切换为视图 v , 并启用别的副本节点作为新的主节点, 如图 2 所示, 该协议主要包括以下三个过程:

(1) View-change 阶段: 如果备份节点发现主节点出现了问题, 那么就会向其余节点发送 View-change 消息。

(2) View-change-ack 阶段：如果新的主节点（即上文的备份节点）收到了包括自己在内的 $2f+1$ 个 View-change 消息就会进入 New-view 阶段。

(3) New-view 阶段：新的主节点会向其他所有节点发送 New-view 消息，其余的从节点会进行验证并且不会发送 New-view 消息。

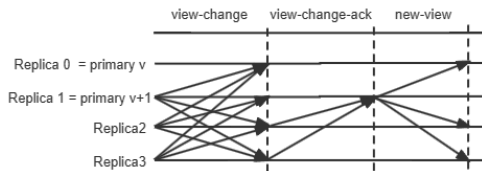


图 2 PBFT 算法视图切换协议过程

1.3 算法缺陷分析

通过分析上诉 PBFT 算法的一致性协议、视图切换协议和检查点协议流程，可以发现 PBFT 共识机制主要存在以下缺陷：

(1) 通信复杂度高且安全性与效率之间难以平衡。在一致性协议流程中，为了确保较高的安全性会使副本节点多次同时群发消息进行两两之间的通信，且会随着节点数量的增多群发消息的次数也会大大增加，其通信复杂度为 $O(n^2)$ ，这时候网络就会出现拥塞，网络性能和共识效率大幅下降，很明显这对于云平台场景下设备平均性能较低的状态是不能接受的。

(2) 节点作恶成本低。在上述提及的视图更换协议中，对于集群而言最后也只是简单的更换了主节点，但是原主节点却一直留在了集群中，这也对于共识效率产生了很大的隐患。

(3) 节点所处网络动态性低，且职责单一。在 PBFT 共识机制的网络中，节点数目是在共识过程中不会发生任何变化的，且所有节点都可以参与共识过程，然而云平台场景下多数设备节点受限于网络和自身性能原因，会导致共识阻塞。

2 CA-PBFT

2.1 多维度综合性模型

全面且完善的评分机制是对集群节点进行队列划分的重要依据，下面列举了本模型所考虑的评分因素，这些要素体现了节点的本轮共识表现以及历史共识表现，同时因为节点是云平台设备，所以加入设备安全度这一特殊因素来计算

评分。

1. 设备安全性：设备安全度指的是节点所对应的云平台设备本身的物理安全性，若节点设备本身安全性较低，就有被恶意节点或黑客攻击并篡改其共识信息的风险。其计算公式如下式所示：

$$I(i) = \begin{cases} \frac{I_i}{I_0} & I_i < I_0 \\ 1 & I_i \geq I_0 \end{cases} \quad (2)$$

式中 I_0 指的是对设备安全度参数的参考阈值， $I(i)$ 的值越大表示设备的物理安全性越高，同时不会高于 1。

2. 节点活跃率：节点活跃率指的是节点总在线时长占当前视图下的共识周期时长的比率，若节点在本周期内在线时间较长，那么节点状态则会更稳定。其计算公式如下式所示：

$$d = \frac{t}{T} \quad (3)$$

式中： T 指的是当前视图共识周期时长， t 指的是该节点的在线时长。

2.2 通信性能模型

云平台环境中，各设备之间的连通性，网络延迟等因素都会对共识结果产生影响，因此需要对一个节点的通信性能进行评估，以此作为划分多级队列、构建多中心的双层网络结构和主节点选取的重要依据，下面是该模型参考的因素。

(1) 接近中心性。通过引入网络流的特征，使用节点接近整个网络中其他节点的难易程度来定义节点的接近中心性。

$$CC_i = \frac{1}{d_i} = \frac{N}{\sum_{j=1}^N d_{ij}} \quad (4)$$

式中： d_i 表示网络中节点 i 到其他所有节点距离的平均值，节点到其他所有节点距离的平均值越小，意味着节点与其他节点越接近，因此利用 d_i 的倒数来定义节点的接近中心性。 d_{ij} 则是节点 i 和节点 j 之间的距离。

(2) 度中心性。在网络分析中，通常采用度中心性来描述节点的网络影响力。节点的度中心性越大，所关联的其他节点就越多，将其选作中继节点转发消息就越有可能使得消息更快到达目的节点。在包含 N 个节点的网络中，节点的度中心计算公式如下式所示：

$$DC_i = \frac{k_i}{N-1} \quad (5)$$

式中: k_i 是节点 i 连接的一跳邻居节点数目。

(3) 介数中心性。在实际网络中, 某个节点可能具有较小的度中心性 (即关联的节点很少), 但是该节点却对网络的联通性起到很大的作用。介数中心性描述了节点对网络中节点对之间沿着最短路径传递消息的控制能力。具体地, 节点在网络中的介数中心性可定义为:

$$BC_i = \sum_{s \neq i \neq t} \frac{n_{st}^i}{g_{st}} \quad (6)$$

式中: g_{st} 为从节点 s 到节点 t 的最短路径的数目。 n_{st}^i 为从节点 s 到节点 t 的 g_{st} 条最短路径中经过节点 i 的最短路径数目。

(4) 能量值。用来表示该云平台设备所具备的收发消息的能力, 如网络带宽, 设备物理性能等。

$$Z_i = \begin{cases} \frac{Z_z}{Z_0} & Z_z < Z_0 \\ 1 & Z_z \geq Z_0 \end{cases} \quad (7)$$

式中: Z_0 指的是对设备能量值参数的参考阈值, Z_i 的值越大表示设备的能量值越高, 且不会高于 1。

综上因素, 通信性能评分计算公式如下所示:

$$G_i = Z_i \cdot \frac{CC_i + DC_i + BC_i}{L_0} \quad (8)$$

式中: L_0 得是标准的中心性数值, 根据集群数值可以做出相应的调整。

3 结束语

为了解决传统 PBFT 算法通信复杂度高、节点作恶成本低、节点所处网络动态性低、指责单一的缺点, 本文提出了

CA-PBFT 共识算法。CA-PBFT 共识算法以多维度综合性评分模型和通信性能模型为基础, 评估节点的和通信能力, 将其划分为四种队列来规范节点行为, 并且在共识过程动态更新节点的评分和通信性能评分, 以达到对于云平台复杂网络的适应; 同时采用分簇机制和可动态调节的一致性协议, 分簇分解了共识任务, 降低了通信复杂度, 提升了共识效率, 而动态调节的一致性协议则进一步降低了通信消息的数量, 从而优化了通信效率。

但是, CA-PBFT 共识算法还有一些不足, 后续工作将进一步优化动态一致性协议, 使其可复用之前的状态, 避免重新进行共识, 以此来降低共识时延续和通信量。

参考文献:

[1] Zhou W, Jia Y, Peng A, et al. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.[J].IEEE Internet of Things Journal,2019,6(2):1606-1616.

[2] 李腾, 程哲, 贾东立, 等. 基于角色管理的实用拜占庭容错共识算法 [J]. 计算机工程与科学, 2022,44(02):237-243.

[3] 刘炜, 阮敏捷, 余维, 张志鸿, 田钊. 面向云平台的 PBFT 优化共识算法 [J]. 计算机科学, 2021,48(11):151-158.

[4] 方维维, 王子岳, 宋慧丽等. 一种面向区块链的优化 PBFT 共识算法 [J]. 北京交通大学学报, 2019,43(05):58-64.

作者简介: 李婷婷 (2000.01—), 女, 汉, 广西, 本科, 中级工程师, 研究方向: 一种云平台场景下的 CA-PBFT 算法。