PBFT 算法

jask

2024-08-11

PBFT 算法

PBFT 算法是通过签名（或消息认证码 MAC）约束恶意节点的行为，也就是说，每个节点都可以通过验证消息签名确认消息的发送来源，一个节点无法伪造另外一个节点的消息。最终，基于大多数原则（2f + 1）实现共识的。

最终的共识是否达成，客户端是会做判断的，如果客户端在指定时间内未收到请求对应的 f + 1 相同响应，就认为集群出故障了，共识未达成，客户端会重新发送请求。

总结

不管口信消息型拜占庭问题之解，还是签名消息型拜占庭问题之解，都是非常理论化的，未考虑实际场景的需求，而且协商成本非常高，指数级的消息复杂度是很难在实际场景中落地，和解决实际场景问题的。

PBFT 算法是通过签名（或消息认证码 MAC）约束恶意节点的行为，采用三阶段协议，基于大多数原则达成共识的。另外，与口信消息型拜占庭问题之解（以及签名消息型拜占庭问题之解）不同的是，PBFT 算法实现的是一系列值的共识，而不是单值的共识。

相比 Raft 算法完全不适应有人作恶的场景，PBFT 算法能容忍 (n - 1)/3 个恶意节点(也可以是故障节点)。另外，相比 PoW 算法，PBFT 的优点是不消耗算力，所以在日常实践中，PBFT 比较适用于相对“可信”的场景中，比如联盟链。

需要你注意的是，PBFT 算法与 Raft 算法类似，也存在一个“领导者”（就是主节点），同样，集群的性能也受限于“领导者”。另外，O(n ^ 2) 的消息复杂度，以及随着消息数的增加，网络时延对系统运行的影响也会越大，这些都限制了运行 PBFT 算法的分布式系统的规模，也决定了 PBFT 算法适用于中小型分布式系统。