蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

PBFT与蜜罐共识算法

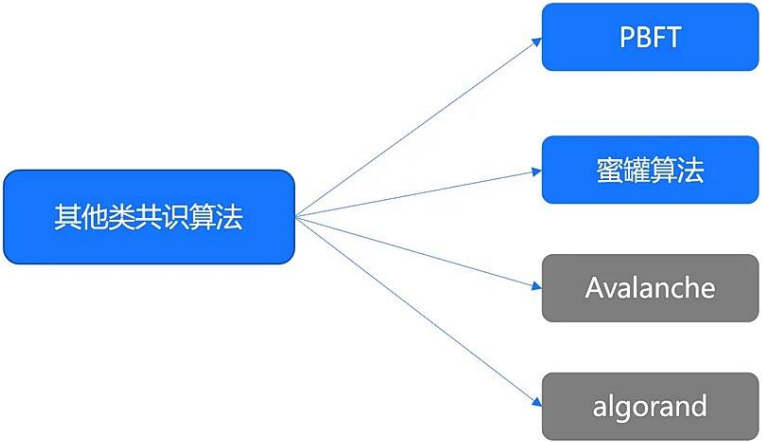
- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

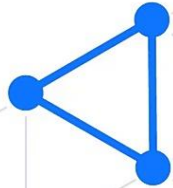
- 了解PBFT、蜜罐共识算法机制

其他类共识

除了我们前面介绍的两大类共识算法，还无法严格分类到上述两种类型当中去很多算法。



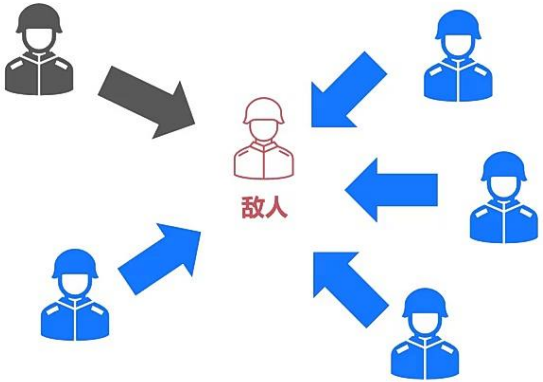
02 PBFT机制



拜占庭将军问题

拜占庭将军们如何才能保证有多于3支军队在同一时间一起发起进攻，从而赢取战斗？

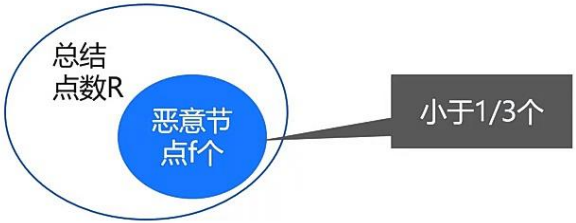
叛徒：扰乱进攻决策



实用拜占庭容错算法（Practical Byzantine Fault Tolerance，简称PBFT）。

PBFT简介

PBFT，实现了在有限个节点的情况下的拜占庭问题，算法经过三个阶段达成一致性，分别是有3f+1的容错性，即PBFT算法可以容忍小于1/3个无效或者恶意节点，并同时保证一定的性能。

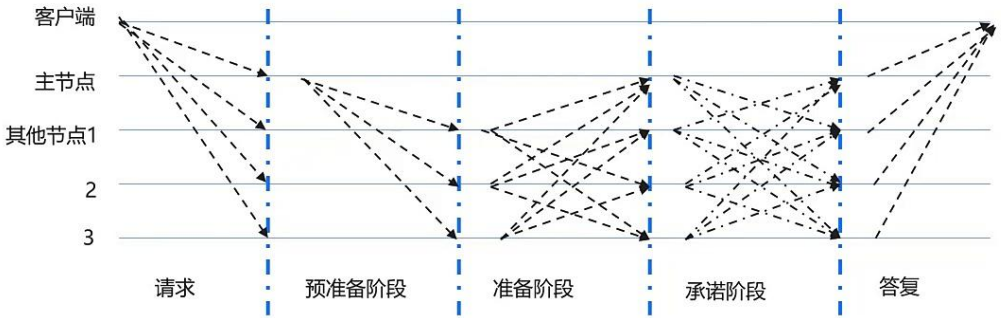


PBFT核心基本和原则——少数服从多数的原则

PBFT算法过程

为什么是3f+1的容错性?

PBFT达成共识的过程——三阶段过程（预准备阶段、准备阶段、承诺阶段）



POW与PBFT协议比较

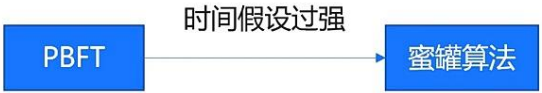
	PBFT	POW机制
优点	• 允许33%的容错； • 可以快速结算和快速担保交易。	• 不需要知道参与网络的所有节点； • 任何节点都可以在任何时间点离开或加入；可以扩展到分布在全世界的大量节点和参与者。
缺点	• 无法扩展到1000个节点以上	• 处理速度非常慢； • 吞吐量非常有限； • 消耗了大量的能量。

03 蜜罐算法概述

蜜罐算法简介

蜜罐算法（Honey Badger），是我们科学家与其他国家合作提出的一种拜占庭共识算法。

时间假设，指的是对于共识节点而言，他们期望对端节点在一个特定时间之内（特定时间长度不会变化）能够给出响应。



04 总结

总结

■ **除证明类、选举类共识还存在很多其他共识算法，并不断在发展**

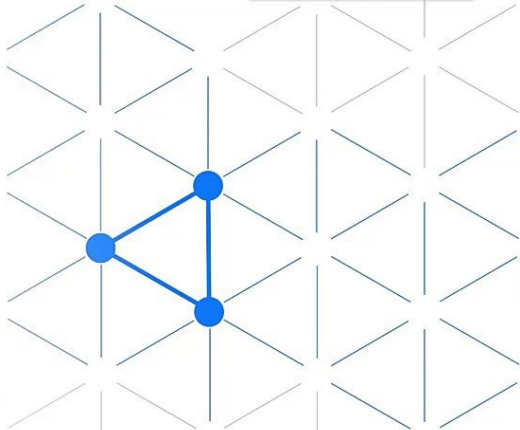
■ **PBFT共识算法是一种用于联盟链共识算法，具有3f+1的容错性**

- 节点可以通过轮流等方式进行确定
- 达成共识的过程包括预准备阶段、准备阶段、承诺阶段

■ **蜜獾算法是一种异步共识算**

- 删除了需要响应时间的要求
- 包括整体的算法分为步骤随机选择交易打包，加密生成、交易进行广播、解密交易，生成区块

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN