软件所等提出首个完全实用的异步共识算法“小飞象拜占庭容错算法”

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/12716.html

近日，中国科学院软件研究所研究员张振峰团队与美国新泽西理工学院（现悉尼大学副教授）唐强团队在区块链核心技术——拜占庭容错（BFT）共识研究中取得突破，提出首个完全实用的异步共识算法——小飞象拜占庭容错（DumboBFT）算法，研究成果以*Dumbo: Faster Asynchronous BFT Protocols*为题，发表于网络安全旗舰会议ACM CCS（第27届国际计算机与通信安全大会）。在异步BFT共识算法设计领域，我国此前未有重要研究成果在国际顶级会议上发表。

拜占庭容错（BFT）共识算法是区块链的核心技术，也是确保区块链安全可靠运行、提升区块链扩展能力和运行性能的核心算法。BFT共识算法具有运行性能高、资源消耗低、易于部署等特点，广泛应用于国内外区块链系统中。异步BFT算法能够容忍网络通信故障、抵抗拜占庭敌手恶意攻击，是保障区块链在互联网环境下健壮运行的理想共识技术。

如何设计高效的异步BFT共识算法，是密码学和分布式计算领域的著名难题。自上世纪80年代起，国内外学者先后对这一难题进行了探索。第一个接近实用的异步共识算法是在2016年提出的HoneyBadgerBFT算法，已被应用于蚂蚁链等区块链平台。为设计完全实用的异步共识算法，软件所于2015年开展小飞象拜占庭容错算法研究工作。该算法以独到视角对HoneyBadgerBFT算法进行分析，揭示其性能受限的根源是大量随机化子模块调用导致的运行时间增加，提出了全新的可证明可靠广播（provable reliable broadcast）原语，并给出了基于门限数字签名技术的高效构造方法，通过一种创新性的多值拜占庭共识应用，在容忍1/3的恶意节点的同时，突破了异步共识算法在性能上的设计挑战。

在遍布全球四大洲的100个共识节点的测试网络中，小飞象拜占庭容错算法DumboBFT的确认延迟时间为24秒、不到HoneyBadgerBFT算法的1/20，交易吞吐量为每秒近1.8万笔、是HoneyBadgerBFT算法的9倍多。此外，软件所特别研究助理路远等人进一步提出了小飞象多值共识算法（Dumbo-MVBA），在消息数量、通信代价和运行时间等关键性能指标上均达到了渐进理论最优，回答了国际密码界关于“如何提升异步共识算法的关键性能指标”这一问题。小飞象共识算法的创造性突破，解决了异步共识算法设计的理论难题，在性能上大幅提升并超越了当前工业界采用的HoneyBadgerBFT，成为国际首个完全实用的异步共识算法，可为我国区块链基础设施建设提供强安全、高性能、可扩展的新一代核心技术。

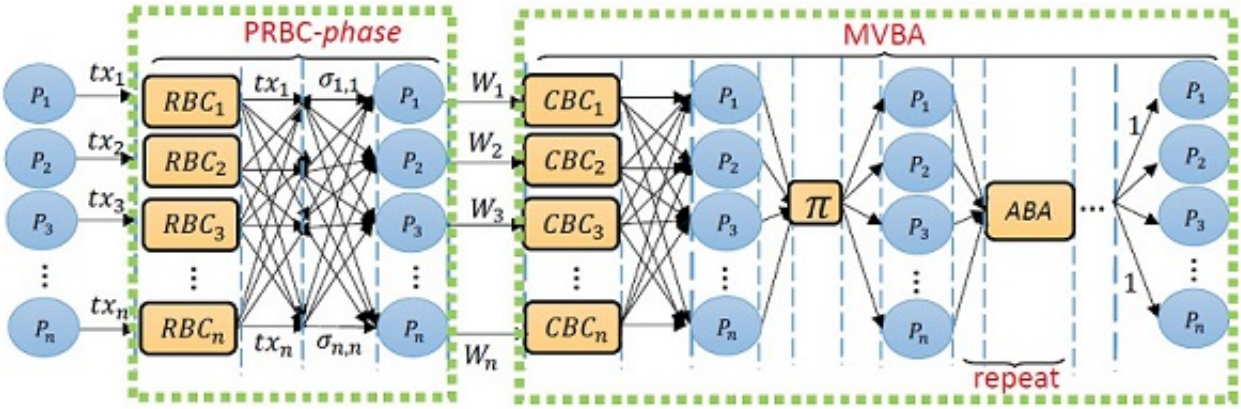

图1.Dumbo BFT协议执行流程

异步共识算法	64个全球节点		100个全球节点	
	确认延迟	交易吞吐量	确认延迟	交易吞吐量
HoneyBadgerBFT	240 秒	4453 笔/秒	491 秒	1934 笔/秒
DubmoBFT	14 秒 （延迟降低 94%）	18692 笔/秒 （吞吐量增长 320%）	24 秒 （延迟降低 95%）	17767 笔/秒 （吞吐量增长 819%）

图2.Dumbo BFT和HoneyBadger BFT在全球互联网中的实际性能对比

异步共识算法	系统规模为N个共识节点			
	随机化子模块数量	通信代价（比特）	运行时间	消息数量
HoneyBadgerBFT	O(N)	O(N)	O(logN)	$O(N^3)$
Dubmo-MVBA	O(1) （理论最优）	O(N) （理论最优）	O(1) （理论最优）	$O(N^2)$ （理论最优）

图3.Dumbo-MVBA协议和HoneyBadger BFT协议的渐近复杂度对比

研究团队单位：软件研究所