



从 PBFT 至今: 拜占庭容错共识协议深入解读

冯了了^{1,2}, 傅翔^{1,2*}, 王怀民^{1,2*}, 王科铭¹, 史佩昌^{1,2}, 姜枫^{1,2}, 林墨恒^{1,2}

1. 国防科技大学计算机学院, 长沙 410073

2. 复杂关键软件环境全国重点实验室, 长沙 410073

* 通信作者. E-mail: fuxiang13@nudt.edu.cn, hmwang@nudt.edu.cn

比特币的巨大成功导致其底层技术区块链备受关注, 当前已经被广泛应用于各种场景, 促使人们不断追求更高效、节能和安全的区块链共识协议. 拜占庭容错 (Byzantine fault tolerance, BFT) 共识是一种有效的区块链共识解决方案. 自 1999 年第一个实用的 BFT 协议 PBFT 提出至今, 基于该协议的众多复杂变体协议被提出, 导致区块链行业的相关人员对 BFT 协议的评估和选择变得愈加困难, 更不用说为特定的区块链应用场景定制高效的共识协议. 为了更好地理解、评估、选择和定制区块链共识协议, 有必要对各类 BFT 变体进行系统性的梳理与评估. 通过给出不同优化思路在正确性 (安全性和活性) 上的直观解释, 帮助新入门的研究者快速把握共识协议的核心设计理念, 也便于从业者根据具体应用场景选择适合共识协议.

SCIENCE CHINA Information Sciences 2026 年第 1 期出版了王怀民院士团队的评述文章 “From PBFT to the present: a thorough overview of blockchain consensus protocols”, 系统回顾并分析了 PBFT 共识协议及其变体, 旨在全面梳理 BFT 共识协议的设计思路, 提出一种快速分析区块链 BFT 共识协议的技术框架. 本文将现有区块链 BFT 共识协议的设计理念分为两大类: 基于 PBFT 协议基础共识流程的重设计 (redesign of fundamental consensus processes, RFCP) 和不影响共识基础流程的可叠加优化机制 (addition of supplementary optimization mechanisms, ASOM). 对于 RFCP, 本文以 PBFT 的共识流程为基准, 分析了区块链 BFT 共识协议的重要设计要素, 例如提交阶段数、副本数和视图更改协议. 这些结构元素相互作用, 影响协议的基本原理

和正确性. 对于 ASOM, 本文概述了若干优化措施, 例如基于委员的共识、乐观机制和流水线技术, 这些优化措施可以在不影响基本共识流程的情况下进行叠加. 最后, 提出了一个快速共识分析与生成框架, 用于评估或设计特定的区块链 BFT 共识协议.

首先, 本文明确了研究的背景意义与选题范围, 对比了与当前工作的异同. 虽然已有许多研究对拜占庭容错共识协议进行了深入分析, 但鲜少从基本流程的角度对其核心设计思路进行系统性探讨. 此外, 协议中不同结构组件之间的相互作用, 以及优化机制的可堆叠性, 仍未得到充分探索. Amiri 等^[1] 提出了一个共识协议生成平台, 对 13 种已知协议的优化思路进行梳理, 总结其演化关系, 并最终仅捕获了两类新的共识协议. 然而, 该方案未讨论这些优化策略对协议正确性的影响, 也未分析不同优化策略叠加时的合法性. Sui 等^[2] 对 BFT 的基本参数 (提交阶段数、副本数、视图更改协议等) 进行数学建模, 通过组合并生成新的协议, 并给出了严格的正确性证明. 该方法共得到 23 个候选协议, 但其生成的协议与典型优化思路之间的映射关系不够直观, 其证明过程也相对晦涩, 初学者较难迅速理解. 相比之下, 本文工作系统分析了每类优化策略对 BFT 协议基本流程的影响, 并进一步探索不同优化策略的合法叠加关系. 本文捕获的协议集合并非 Sui 等工作的子集, 但二者存在交集. 对于这些交集, 读者可从两种互补的视角进行理解: Sui 等的方案更为严谨和形式化, 而本文的方法更直观, 易于把握优化思路及系统设计逻辑.

其次, 本文以 PBFT 为基准提出了共识流程的重设计思路 (RFCP), 将 BFT 类共识流程解构为 3 个核

英文原文: Feng L L, Fu X, Wang H M, et al. From PBFT to the present: a thorough overview of blockchain consensus protocols. *Sci China Inf Sci*, 2026, 69: 111102, <https://doi.org/10.1007/s11432-024-4431-y>

心组件: 提交阶段数、副本数和视图更改协议. 系统地探索了这些元素之间的相互作用, 识别了影响提交阶段数变化的因素, 并剖析了视图更改协议的消息结构. 实现共识的正确性需要对相关组件进行协调修改, 对这些组件之间的相互依赖性进行了建模与描述. 本文梳理了可叠加优化机制 (ASOM), 这些机制独立于基础共识流程运行. 具体而言, 分析了包括基于委员的共识、乐观机制和流水线技术等在内的 5 种机制, 这些机制可以叠加在核心共识流程之上, 以在不改变其基本结构的情况下提升协议性能.

最后, 本文提出了一个区块链共识协议的快速分析与生成框架. 该框架将影响基本共识流程的设计 (RFCP) 进行原子拆分, 并量化展示其影响. 通过排列组合和过滤, 本方案生成了可行的共识协议变体及其相

关的性能指标, 如表 1 所示. 基于本框架捕获了 26 种协议: 其中 22 种具有正确性保证, 9 种对应现有协议, 17 种为新的优化设计. 将表 1 中的协议变体与可叠加优化机制 (ASOM) 结合, 可进一步衍生出数百种共识协议变体. 该框架不仅支持对现有协议的高效分析, 也为面向特定应用场景的协议定制提供了有力技术支撑.

参考文献

- 1 Amiri M J, Wu C, Agrawal D, et al. The bedrock of Byzantine fault tolerance: a unified platform for BFT protocols analysis, implementation, and experimentation. In: Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation, 2024. 371–400
- 2 Sui X, Duan S, Zhang H. BG: a modular treatment of BFT consensus toward a unified theory of BFT replication. IEEE Trans Inform Forensic Secur, 2023, 19: 44–58

表 1 使用本文共识生成框架捕获的区块链共识协议.

Table 1 Blockchain BFT protocols generated using our framework.

Protocol	Phase	Replicas	Message complexity		Authenticator complexity		Captured protocols or similar protocols
			Commitment	View-change	Commitment	View-change	
BD[0,0,0,0]	3	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^3)/O(n^3)$	= PBFT
BD[1,0,0,0]	2	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n^2)$	= FlexiBFT
BD[2,0,0,0]	2	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n)$	•
BD[3,0,0,0]	2	$2f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n^2)$	•
BD[4,0,0,0]	2	$2f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n)$	•
BD[0,1,0,0]	2	$5f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n^2)$	= FaB
BD[0,0,1,0]	3(5)	$3f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n^2)$	• $\approx$ Fast-Hotstuff without locking mechanism
BD[0,0,2,0]	3	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n^2)$	•
BD[0,0,0,1]	4	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^3)/O(n)$	• $\approx$ Tendermint with view-change protocol and more commitment phases
BD[1,0,1,0]	2(3)	$3f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n^2)$	• $\approx$ FlexiBFT with linearization
BD[2,0,1,0]	2(3)	$3f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	•
BD[3,0,1,0]	2(3)	$2f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n^2)$	•
BD[4,0,1,0]	2(3)	$2f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	• $\approx$ TBFT with fewer phases of commitment and view-change protocols
BD[1,0,0,1]	3	$3f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n)$	•
BD[3,0,0,1]	3	$2f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n)$	•
BD[0,1,1,0]	2(3)	$5f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n^2)$	• $\approx$ Zyzzyva5 (slow path)
BD[0,1,0,1]	3	$5f + 1$	$O(n^2)$	$O(n^2)/O(n)$	$O(n^2)$	$O(n^2)/O(n)$	• $\approx$ BG[1,1,2] with DP1 without linearization
BD[0,0,1,1]	4(7)	$3f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	= Hotstuff
BD[0,0,2,1]	4	$3f + 1$	$O(n^2)$	$O(n)/O(n)$	$O(n^2)$	$O(n)/O(n)$	• $\approx$ The Hotstuff without linearization
BD[1,0,1,1]	3(5)	$3f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	•
BD[3,0,1,1]	3(5)	$2f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	•
BD[0,1,1,1]	3(5)	$5f + 1$	$O(n)$	$O(n)/O(n)$	$O(n)$	$O(n)/O(n)$	= BG[1,1,2] with DP1
The following are some protocols that have correctness defects or are not optimal solutions							
V[1]	3	$3f + 1$	$O(n^2)$	—	$O(n^2)$	—	= Tendermint
III[1]+V[2]	2(3)	$3f + 1$	$O(n)$	$O(n^2)/O(n^2)$ $/O(n)$	$O(n)$	$O(n^2)/O(n^3)$ $/O(n^3)$	= Zyzzyva (slow path), incomplete linearization
II[1]+V[3]	2	$7f + 1$	$O(n^2)$	$O(n^2)/O(n^2)$	$O(n^2)$	$O(n^2)/O(n^2)$	= Bosco
III[1]+V[2]+V[3]	2(3)	$5f + 1$	$O(n)$	$O(n^2)/O(n^2)$ $/O(n)$	$O(n)$	$O(n^2)/O(n^3)$ $/O(n^3)$	= Zyzzyva5 (slow path), incomplete linearization