Flexible BFT: Separating BFT Protocol Design from the Fault Model

Dahlia Malkhi
VMWare
https://dahliamalkhi.wordpress.com/

Abstract

Byzantine Fault Tolerant (BFT) protocols designed for building replicated services collapse if deployed under settings that differ from the fault model they are designed for. For example, in a partial-synchrony model, a known lower bound for BFT is 1/3. Optimal-resilience solutions completely break if the fraction of Byzantine faults exceeds 1/3. The only way we know to achieve $> 1/3$ resilience is by assuming synchrony, but this requires the protocol to be designed with that assumption. Flexible BFT is a new approach to BFT protocol design that separates between the fault model and the solution. Clients in Flexible BFT specify (i) the adversarial threshold they need to tolerate, and (ii) whether they believe in synchrony (and the presumed bound on transmission delays). We present a Flexible BFT solution that simultaneously supports different clients, who differ simply by the number of messages and/or time the clients are willing to wait for. At an even finer grain, Flexible BFT supports under the same solution high-value and low-value transactions, each tolerating a different threat model.

2012 ACM Subject Classification Theory of computation → Distributed algorithms

Keywords and phrases Byzantine fault-tolerance, blockchains

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2019.2

Category Keynote Lecture

Bio. Dahlia Malkhi carries applied and foundation research in broad aspects of reliability and security in distributed systems since the early nineties. In 2014, after the closing of the Microsoft Research Silicon Valley lab, she co-founded VMware Research and became a Principal Researcher at VMware. From 2004-2014, she was a principal researcher at Microsoft Research, Silicon Valley. From 1999-2007, she was a tenured associate professor at the Hebrew University of Jerusalem. In 2004, leaving for a brief sabbatical at Microsoft Research, she was bitten by the Silicon Valley bug and stayed there. Dr. Malkhi was elected ACM fellow in 2011, received the IBM Faculty award in 2003 and 2004, and the German-Israeli Foundation (G.I.F.) Young Scientist career award 2002. She currently co-leads the VMware blockchain research project. In the past decade, she founded and led the Corfu project, a database-less database. The Corfu data platform currently drives VMware's NSX-T distributed control plane.

International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019).
Editors: Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci-Piergiovanni;
Article No. 2; pp. 2:1–2:1

OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany