Holden Rohrer, Holden Watson, and Nithya Jayakumar
2019 Oct 21
Applied Combinatorics–Math 3012
Livshyts

Part 2: Progress Report

Topic: Distributed Systems Integrity and Correctness

1 Overview

There's a famous problem in computer science called the Two Generals' Problem. It follows two Roman camps on opposite sides of a valley, claimed by enemies. Each can send a scout to the other to decide when to attack—which is necessary because if either attacks alone he is guaranteed to lose—but there is no guarantee the scout will arrive. Clearly, one message cannot guarantee consensus between the two. But neither can thirty—or a billion.

This is global consensus in a distributed system, and is still an unsolved problem so far as such a problem can be "solved." This is because it is intimately intertwined with novel technologies, starting with the internet and routing paths (even though it's about 50 years old), torrent software, the TOR network, server redundancy in commercial applications, and the almighty cryptocurrency.

We want to review existing literature on the topic as well as practical applications of those principles (e.g. Bitcoin's consensus algorithm and its failures),[1] so

2 Products

[1] *https://bitcointalk.org/index.php?topic=702755.0*