Optimizing Resilience and Availability in TEE-based BFT Protocols

Ines Messadi and Rüdiger Kapitza

Friedrich-Alexander University Erlangen-Nuremberg (FAU)

abstract

BFT protocols that leverage Trusted Execution Environments (TEEs) improve safety and prevent equivocation. One example is SplitBFT, a multi-compartment BFT protocol that relies on TEEs to improve safety. However, maintaining the availability and reliability of the system in the face of faulty TEE compartments remains a challenge. To tackle this, rejuvenation has been proposed to address issues such as memory leaks or problems that arise over time. But traditional methods, such as simply restarting enclaves, can result in downtime, impacting the system's availability and reliability. Our work offers two key contributions. Firstly, we critically examine existing approaches and identify their limitations. Secondly, we present a proactive recovery approach for BFT protocols that seamlessly switches between different TEEs in case of failure.