Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M23-153P
Published: 1/19/2024

Inventors

Rida Bazzi

Sara Tucci-Piergiovanni

Contact

Physical Sciences Team

Asynchronous Quorum System for Executing Payment Transactions in Parallel

Background

Existing cryptocurrencies solve the consensus problem to maintain a shared ledger of all transactions, but it has been shown in recent years that maintaining a shared ledger is not always strictly needed to support exchanging funds. In an asynchronous permissioned system where at most 1/3 of servers are subject to Byzantine failures, Byzantine quorums can be used to allow different parties to exchange funds through the system (asset transfer task).

In recent years, it has been found that solving consensus is not needed for asset transfer when the asset has a single owner. Consensus-less solutions have the ability to achieve higher throughput and reduced transaction latency. However, the transaction process is still fundamentally sequential even with the increased efficiency of the consensus-less approach. This requires every request to be processed by a full quorum so that any two quorums have at least f+1 servers in common, where f is an upper bound on the number of faulty servers.

Invention Description

Researchers at Arizona State University have developed a novel asynchronous quorum system for executing payment transactions in parallel. This system is a (k1, k2)-quorum system, where up to k1 transactions can be validated concurrently and asynchronously but prevent more than k2 transactions from being validated. This system provides a method in which a payer can execute multiple partial spending transactions to spend a portion of its initial balance with less than a full quorum validation. The remaining funds can then be reclaimed using one fully validated transaction, called a settlement transaction.

Potential Applications

- Distributed systems security
- Secure payment transaction system

Benefits and Advantages

- Asynchronous (no timing assumptions)
- Can prevent adversarial transactions from being validated
- Smaller validation quorums
- Higher throughput (consensus-less)

Related Publication: Breaking the f+1 barrier: Executing Payment Transactions in Parallel with Less than f+1 validations