Implementation of a SmartNIC-based HW Accelerator for Algorand Relay Nodes to broadcast Blockchain Messages
The Algorand protocol is an environmentally friendly Blockchain technology based on the Proof-of-Stake (POS) consensus mechanism. It represents a new platform for smart contracts trying to solve the blockchain trilemma consisting of scalability, decentralization and security. As part of the ACE-SUPPRA project (Security, Usability, Performance, and Privacy Research in Algorand) we are investigating ways to accelerate the forwarding and broadcasting of Algorand messages throughout the blockchain network with the help of SmartNIC-based HW accelerators to increase the achievable transmission throughput and decrease latencies as well as power consumption.

To this end, the goal of this master thesis is to develop an extension of an existing packet reception, forwarding and delivery SmartNIC design to detect and relay Algorand transaction, block proposal, voting and consensus messages to a given set of network peers. The implementation will require an Algorand message detection entity consisting of a modified packet header parser and a Match-Action-Table. Furthermore, a PCIe-based configuration module for communicating with an attached host PC will be necessary to receive updates on new TCP connections and the IP addresses of the current peer list. The design will also encompass a high priority and bulk broadcast queue for Algorand messages alongside a suitable egress scheduler as well as a message memory and broadcast module for the transmission to four connected peers. Finally, a Packetizer unit will have to be designed, assembling TCP/IP packets and Algorand messages out of multiple Ethernet frames after reception, and vice versa also splitting messages into individual Layer 2 frames prior to their transmission.

Towards this goal you will complete the following tasks:

- Research existing methods for relaying and broadcasting blockchain messages
- Implement the design on the NetFPGA-SUME or AMD Alveo U55C prototyping platform
- Compare and evaluate the implementation with the SW-based Golang implementation of Algorand
- Document your work in a written thesis report and present your work in a presentation

Prerequisites

To successfully complete this project, you should already have the following skills and experiences.

- Project Laboratory IC-Design or equivalent course
- Good knowledge about Verilog or VHDL
- Xilinx Vivado Design Suite and Synopsys VCS / Mentor Graphics ModelSim (tools will be provided)
- Self-motivated and structured work style

Contact

Interested? Questions? Do not hesitate to contact me!

Franz Biersack
Chair of Integrated Systems
Arcisstraße 21, 80333 Munich
Tel. +49 89 289 23869
franz.biersack@tum.de
www.ce.cit.tum.de/lis

Advisors

Franz Biersack