

Model Checking Correctness Properties of Electronic Contracts

Ellis Solaiman, Carlos Molina-Jimenez, and Santosh Shrivastava

School of Computing Science, University of Newcastle upon Tyne,
Newcastle upon Tyne, NE1 7RU, England
{Ellis.Solaiman,Carlos.Molina,Santosh.Shrivastava}@ncl.ac.uk

Abstract. Converting a conventional contract into an electronic equivalent is not trivial. The difficulties are caused by the ambiguities that the original human-oriented text is likely to contain. In order to detect and remove these ambiguities the contract needs to be described in a mathematically precise notation before the description can be subjected to rigorous analysis. This paper identifies and discusses a list of correctness requirements that a typical executable business contract should satisfy. Next the paper shows how relevant parts of standard conventional contracts can be described by means of Finite State Machines (FSMs). Such a description can then be subjected to model checking. The paper demonstrates this using Promela language and the Spin validator.

Keywords: Contract, electronic contract, finite state machine, contract representation, contract enforcement, model-checking, validation, correctness requirements, safety and liveness properties.