DLT5402:
Verification Techniques for Smart Contracts
Assignment

Deadline: 14 June 2021 at noon.

Necessary Preamble: *This document describes the assignment for study-unit DLT5402 Verification Techniques for Smart Contracts. This assignment is worth 100% of the total, final mark for this unit. The deadline for this assignment is* ***14 June 2021*** *at noon, and is to be submitted on the VLE portal. Late submissions will not be accepted. Questions regarding the assignment should only be posted in the Assignment VLE forum (and not via personal correspondence with the lecturers of this study-unit). This is an individual assignment. Under no circumstances are you allowed to share the design and/or code of your implementation. The University of Malta takes a very serious view on plagiarism.*

Note: Three smart contracts – an Auction, an Escrow and a PiggyBank implementation – are being provided with this assignment, and are required to answer the questions.

Question 0: Specification Languages
For each of the Escrow and PiggyBank smart contracts (provided with this assignment), write one property using each of: finite state automata, regular expressions (one positive and one negative), LTL and CTL (i.e. 5 properties per contract). Explain each property and argue why it should hold.

Question 1: Testing
For the Escrow and PiggyBank smart contracts (provided with this assignment), write tests, including ones based on specifications written as automata. Discuss (i) the test specifications written; (ii) argue about the completeness of the specifications (i.e. adherence to the properties should imply that the system works correctly); (iii) coverage achieved by the tests. You may use coverage and security tools to support your reasoning.

Question 2: Runtime Verification
For the Escrow and PiggyBank smart contracts (provided with this assignment), write specifications using Dynamic Event Automata. Implement them using Contract Larva, adding reparations as you may deem appropriate. Discuss (i) the specifications written; (ii) the reparations you implemented, and justify your choice; and (iii) overheads induced.

Question 3: Static Verification
For the Escrow and PiggyBank smart contracts (provided with this assignment), write functional specifications using the same notation and in a similar style as done for the Auction smart contract (also provided with this assignment).

A note of clarification. Your choice of properties should reflect the strength of the specification language and verification technique. This does not mean that some of the properties used for testing might not also be useful for runtime verification, for instance, but ensure that you use runtime verification on properties it is particularly useful for and similarly with testing.