# How to set up a decentralized digital token payment system?

## 1 Introduction

A decentralized digital token payment system can be easily achieved by implementing a Hash function for multiple times. It facilitates public transaction without a central agent, ensures users' privacy, is robust to Byzantine attack and has low risk of double spending.

## 2 Problem Statement

In this lab, the students are required to simulate a prototyping decentralized digital token payment system by implementing a Hash function (which is programmed by themselves) for multiple times, and are required to demonstrate a Byzantine attack, an identity attack and a double spending test.

Demonstrate your system via computer simulation. You are only allowed to use one of the following languages: Java, C++ or Matlab. Proper commenting of the code is important, as well as applying good software engineering practices.

## 3 Deliverables

The lab must be carried out in groups of not more than 2 students. Each group member must hand in an individual report. The technical report style must be used, conforming to the school standard (Blue Book). You will be assessed on the following deliverables:

A complete technical report that contains the following:

- A detailed description of your implementation (diagrams, descriptions, etc.), why a particular approach was taken, the limitations as well as advantages and disadvantages of the chosen approach.
- Discussion on how your code was tested, with fully documented test results.
- Discuss how to defend your cryptosystem from the Byzantine attack.
- Discuss how to defend your cryptosystem from the double spending.
- Discuss how to ensure users' privacy.
- Problems in the design and implementation.
- An appendix detailing the division of work between team members, the milestones used to manage the project and a signed-off section, by both team members, of the work division.

Your code must be submitted.

# 4 Plagiarism

The report is an individual effort, equivalent to an exam; so if there is the slightest indication of copied or plagiarised work all parties, i.e. the offender and supplier of information, will be given zero and reported to the University Disciplinary Committee.