SUPINFO Academic Dept.

SUPINFO International University

INSTITUTE OF INFORMATION TECHNOLOGY

# Group Projects
# M.Sc.1 - Project

**Contents**

2018-2019

Version 1.0
Last update: 22/10/2018
Use: Students/Staff
Author: CHERVY Brian / SAD

# TABLE OF CONTENTS

# 1. Project Overview

SupBank is an online European banking company focused on deposit accounts, overdraft, credit and investment products. As with all existing banks, SupBank faces the limitations of the international SWIFT and SEPA payment systems for international and European transfers.

In order to address the needs of its clients, SupBank has decided to create its own system for storing and transmitting banking transaction information. This new system will have the following features:

- Instant (nearly) wires
- Fee-less foreign exchange
- Decentralized
- Tamper-proof and secure
- Seamless transition for users
- Full transaction history

During the launch process, the first available operation will be transfers between customers of the bank. A set of subcontractors have been chosen, including you, to develop the best blockchain Proof Of Concept.

# 2. Functional Expression

The main goal of this first PoC is to allow transactions between users. User will be able to send funds via their wallet application. Once the transaction has been validated by the user, the transaction will be converted into tokens and then submitted for validation on the decentralized network of the blockchain.

A transaction is made of: A sender public address, a receiver public

- A sender public address
- Receiver public address (one or more)
- Transaction amount

Each node of the blockchain network will have to validate (or not) the transaction through a cryptographic algorithm. Each transaction is timestamped and added to the blockchain upon validation.

Each node must have a copy of the blockchain. You are free to use any suitable storage engine (database, files, ...) as long as the blockchain is always available and decentralized.

## 2.1. Software development

The software is divided in 3 main parts:

- The blockchain engine which validates and stores each and every transaction
- The wallet app that allows users to send/receive transaction and store money.
- The web application that let users explore the blockchain

### 2.1.1. Blockchain

You are free to use any language and libraries and existing solutions. The solution you implement/select has to meet the following criteria:

#### 2.1.1.1. Tokens

To avoid direct conversion between currencies, you need a token/money that will be used in all transaction. You are free to choose the price/value of the token.

#### 2.1.1.2. Peer-to-peer network

The peer-to-peer blockchain network prevents any participant or group of participants from controlling the underlying infrastructure or undermining the entire system. Participants in the network are all equal, and adhere to the same protocols.

A participant or group of participants is a node. Whenever a new transaction occurs, all nodes in the network that want to maintain the latest version of the blockchain must update their copy of the blockchain by adding the new transaction.

#### 2.1.1.3. Blockchain security

The solution must prevent fraud and falsification. The blockchain must be immutable (no deletion/ modification after a transaction has been validated).

#### 2.1.1.4. Consensus mechanism

The consensus mechanism is the most important and vital aspect of the blockchain design. It is the foundation of trust between users that data stored on the blockchain cannot be tampered with. As such, it must have the following features:

- High performance (low latency, large number of transactions per second)
- Low power consumption
- Irrevocability of transactions

#### 2.1.1.5. Privacy

The blockchain must be "private by design" to respect users privacy. You have to implement a "pseudonymization" solution to ensure that all data is kept in a form that does not allow direct identification of a user.

#### 2.1.1.6. Useful resources

Here is a non-limitative list of resources you can use to design/select your system:

- https://www.youtube.com/watch?v=SccvFbyDaUI
- https://www.youtube.com/watch?v=SSo_EIwHSd4
- https://www.youtube.com/watch?v=l9jOJk30eQs
- https://www.youtube.com/watch?v=Lx9zgZCMqXE
- https://bitcoin.org/en/developer-guide

### 2.1.2. Wallet

The wallet application enable users to interact with the blockchain engine. It will let users:

- Create accounts
- Send/receive transactions
- See how many tokens they currently have

You are free to use any language/libraries/platform you want for the app. For the POC, it can be a command line tool or a full-fledged desktop/mobile application.

### 2.1.3. Web application

The web application allows users to graphically explore the content of the blockchain.

A typical use case for a blockchain explorer is to check the balance of a given address/pubkey or to verify that a given transaction is included in the blockchain.

#### 2.1.3.1. User accounts

Users will need an account to use the web application features. If they already have a Facebook or Google account, they can automatically link it to their SupBank account. If they do not, they can create an account with their email address.

#### 2.1.3.2. Web interface

The home page show the last blocks of transactions and the last transactions that have been validated by the different nodes.

Users can click on transactions to get details (sender/recipient/amount).

Users can also use a search bar to filter transactions by:

- Wallet address (public key)
- Nodes
- Block identifier

A status page show a live map of the network, including all known nodes.

## 2.2. Supporting architecure

Your POC must include a demo network with several nodes. The network must be able to perform all required tasks to ensure proper blockchain operation.

# 3. Deliverables

Students should include the following elements in their final delivery:

- A zip archive with the project source code. The source code must also come with the build system used (Project file, autotools, libraries, ...), if any.
- Project documentation.
    - Technical documentation explaining your choices and/or implementation choices/details on the following items (at least):
        - Selected blockchain solution
        - Network map
    - User manual

**The first document is an academic document. Address the reader as a teacher, not a client. This document can be in French or in English, at your option. On the other hand, user manual must be understandable by the client.**

# 4. Graded Items

The project will be graded as follows, on a 120/145 scale:

- Documentation: 10 points
  - User documentation (5 points)
  - Technical documentation (5 points)
- Blockchain: 60 points
  - Decentralized network: A new node can join in at any time (5 points)
  - Nodes within the network keep in sync (10 points)
  - Data can be stored in the blockchain (30 points)
  - Nodes receive compensation for their work (5 points)
  - The blockchain can't be modified (only additions) (5 points)
  - Consensus algorithm is time-efficient (2.5 points)
  - Consensus algorithm is power-efficient (2.5 points)
- Wallet: 30 points
  - Users can create "accounts" (5 points)
  - Users can send transactions (13 points)
  - Users can receive transactions (12 points)
- Web application: 35 points
  - Users can create accounts (5 points)
  - Users can link their facebook/google accounts (5 points)
  - Users can explore the blockchain (10 points)
  - Users can get details on a transaction (5 points)
  - There is a live network map (10 points)
- Supporting architecture: 10 points
  - The network can perform all needed tasks (10 points)

- Bonus : 20 points
    - Extra features done by the students (20 points)