SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127
STSM title: Communication analysis on blockchain based applications
STSM start and end date: 16/03/2019 to 24/03/2019
Grantee name: HÎRȚAN Liviu - Adrian

PURPOSE OF THE STSM:

The purpose of the STSM is to prepare and publish a paper to a conference or a journal regarding the analysis of the communications within peer-to-peer blockchain networks. One of the objectives was to identify the main vulnerabilities within the design of the blockchain-based IT networks. Secondly, we worked in more details on the systems that I have proposed, such as healthcare and car navigation systems based on blockchain technology. The analysis took into account all the involves entities, such as users, servers, databases, applications, and the network itself. In our study, we considered both malicious users and degraded/defective IT equipment over the network. Our goal was to provide a stable network design that ensures confidentiality, integrity and authenticity of the information against technology-related disasters and malicious human activities. In addition, out collaboration involved knowledge exchange, identification of the strengths and weaknesses of our projects, and the development of a common disaster-resistant communication system.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

During the STSM, the following activities have been carried out:

- Brief review regarding the activities of the Politehnica University of Bucharest and National College of Ireland, focusing on blockchain technologies
- Review the existing solutions proposed by Politehnica University of Bucharest and National College of Ireland regarding proper communication assurance within the blockchain technology and identify the positive and negative aspects of the aforementioned projects
- Review other published solutions that presents blockchain based applications or system designs, taking into account analysis of the peer-to-peer communications and the main actors involved
- Identify an optimal solution which will improve the accessibility, functionality and privacy of a blockchain based system that will cover all the needs of the users and will meet the requirements of a real world system

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The results obtained is the development of a system design for a public transport blockchain based application. The system .can track the location and the availability of public transport means and provide the best route to travel. The design integrates all the means of transport available within a city: personal car, bus, public bicycle, taxi, subway, tram, etc. and is able to collect information from users and provides information to other users, delivering high quality services such as time saving for end users. The system

architecture consists in two applications: the main application which is installed on a server and the client application which is installed on users' smart phones.
The main application's role is to:

- Receive data regarding traffic conditions, regarding the availability of means of public transport and regarding the availability of parking spaces;
- Queries other users from the same cluster / area regarding the traffic conditions
- Stores data regarding traffic conditions if it is approved by at least 51% of the users from the same cluster through the consensus algorithm. Data is stored in an immutable ledger (blockchain).
- Calculates the optimal route from the start location to the end location, taking into account the personal car, the availability of parking spaces, the availability of public transport (taxis, buses, trams, subways, trains, public bicycles, etc.) and user's preferences.

The client application's role is to:

- Request data regarding the optimal route from the start location to the end location
- Share two types of data, such as data regarding the availability of taxis, parking spaces, public bicycles, personal car sharing, etc. and data regarding traffic conditions – in this case, the information is validated by at least 51% of other users in the same cluster, through the consensus algorithm.
- Validates traffic conditions shared by other clients in the same cluser.

Regarding the communication analysis, the main application communicates with client applications using a unique shared key for each user.
Clients are grouped in clusters, depeding on their location (latitude and longitude) and have the option to share data with the system or not. More complex security policies (fine granularity) can be chosen by advanced users, like excluding location sharing in some areas, disable data sharing if the data traffic speed is greater than a certain threshold, disable data sharing in some areas, etc.

During our meetings, we also established the main modules of both applications and their role:

- Server application: blockchain module, processing module, network module, database module
- Client application: sensor module, processing module, database module, gateway module

In addition, we conceived the main algorithms of the application:

- Consensus algorithm regarding traffic conditions
- Optimal route algorithm

Within the STSM, we also identified some datasets on public transport in major cities. These were useful to us for some demonstrative simulations.

FUTURE COLLABORATIONS (if applicable)

Our future collaboration consists of the following:

- Perform simulations based on the system design previously described using large datasets
- Based on the results obtained in simulations, we have the possibility to improve the system design in order to provide a higher degree of functionality and privacy
- Our goal is to improve the performance of the design and to publish the obtained results within a joint publication

National College of Ireland
Cloud Competency Centre

Digitally signed by Dr Horacio González-Vélez
DN: cn=Dr Horacio González-Vélez, o=National College of Ireland, ou=Cloud Competency Centre, email=horacio@ncirl.ie, c=IE
Date: 2019.04.04 13:23:13 +01'00'

APPROVED

By Horacio Gonzalez-Velez at 1:24 pm, Apr 04, 2019