Blockchain and multi-party computation for trust-free, transparent and verifiable voting protocols

INSA Lyon

NICOLAS BAUDIN
INTERNSHIPS IN FRANCE INITIATIVE

Name of the hosting institution in France	INSA Lyon
Name of the host laboratory / research team	LIRIS, DRIM
Address	INSA Lyon Bâtiment Blaise Pascal Campus de la Doua 69621 Villeurbanne Cedex
Web site	https://liris.cnrs.fr/
Name of the supervisor	Omar Hasan
Function	Maître de conférences
Email	omar.hasan@insa-lyon.fr

Internship offer

Topic of the internship (title)	Blockchain and multi-party computation for trust-free, transparent and verifiable voting protocols			
Proposed dates of the internship*	Start	2020-09-01	End	2020-12-31

* The supervisors have indicated the dates proposed are flexible and are able to be postponed subject to COVID-19 border closures.

Scientific and academic objectives of the internship (detailed description of the internship content, work expected from the intern and expected outcomes):

In this internship, the student will work with the research team on the solution of a voting protocol that ensures transparency, confidentiality and integrity in trust-less networks. The building blocks explored for designing such a protocol are Multi-Party Computation (MPC) and Distributed Ledger or Blockchain technology.
In the proposed solution, the persistence and immutability of the protocol communication should allow verifiability of the referendum outcome on the client side. Voters should also not need to trust in third parties.

Expected profile of applicant

Level of study	Bachelor's, Honours, or Masters
Discipline	Computer Science
Required qualities, knowledge and skills	Strong background in computer science

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
AMBASSADE DE FRANCE EN AUSTRALIE

Nicolas Baudin Program: “Internships in France” initiative

Call for applications for a research internship in the laboratory LIRIS at INSA Lyon, France

TOPIC: Blockchain and multi-party computation for trust-free, transparent and verifiable voting protocols

Abstract
High voter turnout in elections and referendums is very desirable in order to ensure a robust democracy. Electronic voting is a vision for the future of elections and referendums. Such a system can counteract factors that hinder strong voter turnout such as the requirement of physical presence during limited hours at polling stations.

However, this vision brings transparency and confidentiality requirements that render the design of such solutions challenging. Specifically, the counting must be implemented in a reproducible way and the ballots of individual voters must remain concealed.

Content
In this internship, the student will work with the research team on the solution of a voting protocol that ensures transparency, confidentiality and integrity in trust-less networks. The building blocks explored for designing such a protocol are Multi-Party Computation (MPC) and Distributed Ledger or Blockchain technology. In the proposed solution, the persistence and immutability of the protocol communication should allow verifiability of the referendum outcome on the client side. Voters should also not need to trust in third parties.

The student will also be a member of the **IRIXYS international research center** (https://irixys.uni-passau.de/) at INSA Lyon. As part of this center, the student will have the opportunity to collaborate with the computer science laboratories at the University of Passau (Prof. Harald Kosch) in Germany and at the University of Milan (Prof. Ernesto Damiani) in Italy.

Keywords: Blockchain, E-Voting

MS Student profile
A strong background in computer science is required for this internship.

Supervision
This topic will be supervised by Dr. Omar Hasan, Associate Professor at the LIRIS laboratory, INSA Lyon. He is active in the areas of distributed systems, blockchain and distributed ledger technology, data privacy, and reputation systems. He has published in top international journals such as Elsevier Computer Networks and Elsevier Ad Hoc Networks.
Supervisor's email: omar.hasan@insa-lyon.fr

Time and duration of the internship: September 2020. Duration: Three to six months.

About LIRIS:
The LIRIS is a joint research unit to CNRS (UMR 5205), INSA Lyon, Université Claude Bernard Lyon 1, Université Lumière Lyon 2 and Ecole Centrale de Lyon. Its main scientific research area is Computer Science and, more generally, Information Technologies.
The spectrum of its research activities is wide and its workforce allows the laboratory to be a major actor of research - theoretical and applied - in its fields of competences. The laboratory develops know-how and expertise capable of responding to major societal challenges in close collaboration with the disciplines of Engineering, Human and Social Sciences, Environmental Sciences and Life Sciences.

IRIXYS is:
- An International Research and Innovation Centre in Intelligent Digital Systems) created in March 2016 out of a partnership initiated by the departments of Computer Science of the University of Passau, Germany, the engineering school INSA Lyon, France and the Università degli Studi di Milano, Italy.
- A fully-integrated centre of excellence “without walls” preserving the contribution of each research team to their local research and academic ecosystems.
- A single identity and entity encompassing research activities carried out within the doctoral college MDPS in the fields of multimedia, data security as well as distributed and pervasive systems.
- An instrument for simplification of common and management procedures.

About INSA Lyon:
INSA Lyon boasts 23 research laboratories, more than 600 researchers and teacher-researchers, 650 PhD students, and over 1,000 industrial contracts with the socio-economic world.
In addition to fundamental studies, a large part of the INSA research is done in close collaboration with companies and authorities. According to these strong involvements, highly relevant researches are performed for solving societal issues and generate non-conventional scientific questions. From this model based on excellence, innovation perspective, and community involvement, INSA Lyon expends its research activities within five main fields:
• Digital Society and Information
• Energy for a Sustainable Development
• Environment: Natural, Industrial, and Urban Environments
• Global Health and Bioengineering
• Transport: Structures, Infrastructures, and Mobilities

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
AMBASSADE DE FRANCE EN AUSTRALIE