****

PhD offer (CIFRE Program):

Correct-by-construction smart contracts for secure Web3 architectures

Keywords:

Smart Contracts, Web3 architectures, Security, Reliability, Formal Methods, Domain-Specific Languages.

Context:

Considered as large, decentralized data ledgers that are always available, immutable and replicated, Blockchain technologies allow untrusted users to reach agreements on verifiable data as well as exchange digital assets without third-party intermediaries. In other words, these technologies represent a legitimate disruptor to many business areas such as payments, cybersecurity, health, and logistics, etc.

In the context of the so-called programmable blockchains, *smart contracts* are designed to directly and automatically control the interactions and the behavior of digital assets. For that purpose, the business logic and the underlying conditions must be first defined and implemented, before deploying them to the blockchain. Harnessing blockchains to exchange financial and digital assets also induces safety and security needs. Many technical and financial risks are indeed inherent to the use of *smart contracts*. As computer algorithms, with all that this may entail, *smart contracts* may contain functional and security vulnerabilities.

The adoption of *smart contracts* in the context of Web3 - the next generation of internet - requires a very high level of trust. Therefore, ensuring a proper and secure functioning of *smart contracts* implies the use of reliable security techniques based on solid mathematical foundations. This thesis proposes to tackle these by defining a formal approach supported by automatic reasoning tools (i.e., provers, model-checkers, and constraint solvers). The goal is to neutralize all risks of error throughout the *smart contracts* implementation process.

As part of its mission to democratize the use of *smart contracts* and Web3 architectures, FeverTokens places the use of formal methods at the heart of its security policy. However, so far, there are too few works exploring formal methods in the context of *smart contracts*, especially ones with successful industrial applications. At this time, research works have been limited to feasibility studies and theoretical concepts without really addressing the scale-up and production constraints.

In this regard, the objectives of this thesis include the definition of a tool-supported approach that enables building safe-by-construction *smart contracts.* We will particularly focus on the design of a *Domain Specific Language* (DSL) that would permit to represent and consider both *smart contracts* and their functional/safety properties. Therefore, tested and/or proved transformation mechanisms will be proposed.

****

Finally, this thesis aims at exploring and extending the Meeduse toolset developed by the VASCO, LIG team. Meeduse is an IDE for the formal design of DSL, it allows proving the correctness of a DSL using the B formal method. It has been successfully applied to several case studies and was recently awarded two prizes at the TTC'19 challenge (Transformation Tool Contest): Best Verification Award and Audience Award.

Environment:

- Funding: the thesis will be funded under the CIFRE arrangement
- Principal Hosting laboratory: **SAMOVAR (Télécom SudParis)**
- Hosting company: **FeverTokens**
- Partner laboratories/institutions: **LIG (Grenoble INP), Faculté des Sciences de Rabat (Université Mohammed V)**
- Location: the thesis will take place mainly at FeverTokens office in Paris, as well as at the SAMOVAR laboratory, Télécom SudParis, Evry. Some travels to the LIG laboratory, Grenoble, are also expected
- Duration: 3 years, starting as soon as possible

Profile and skills:

- A master's degree, engineering diploma or equivalent, ideally in computer science/ automation
- Good level in mathematics (i.e., logic, set theory, formal methods etc.)
- Proven ability in algorithms and programming
- Knowledge about blockchain and smart contracts is appreciated
- Fluent in English
- Sense of initiative, autonomy and ability to work in a team

Application:

Applications are to be sent by email to:

- Pr. Amel Mammar <amel.mammar@telecom-sudparis.eu>
- Dr. Akram Idani <akram.idani@univ-grenoble-alpes.fr>
- Dr. Zakaryae Boudi<boudi@fevertokens.io>
- Dr. Abderrahim Ait Wakrime <a.aitwakrime@um5r.ac.ma>

They should include:

- A detailed CV
- A copy of all diplomas
- A copy of all post-bac transcripts
- A motivation letter
- Recommendation letter(s)