

# Sujet de Stage

**Titre : Un Système d'Effets pour un Langage de Programmation de Smart Contracts de Confiance**

## Sujet de Stage :

Les « smart contracts » (programmes exécutés par une machine virtuelle dédiée sur une blockchain) sont devenus le paradigme privilégié pour le développement d'applications décentralisées dans une multitude de domaines ayant un fort impact socio-économique. Dans ce cadre, la vérification formelle des smart contracts est obligatoire, compte tenu de l'impact très élevé qu'ils mettent en jeu (tel que les crypto-monnaies). Les techniques existantes de vérification formelle des smart contracts posent souvent des problèmes de réutilisation du code et de vérification séparée. Pour répondre à ces défis, nous avons proposé au CEA List un langage de programmation de smart contracts basé sur les effets algébriques et le typage statique. Les effets algébriques permettent au programmeur de formaliser le comportement computationnel attendu du programme, qui est encodé dans le type du programme et automatiquement vérifié en temps de compilation par le type checker. Notre proposition se base sur une discipline de types nouvelle, nommée « Pure Subtype Systems » (PSS), qui combine la dépendance de type (pour une plus grande expressivité) et le sous-typage d'ordre supérieur (pour faciliter la réutilisation).

## Description de l'offre :

L'objectif de ce stage est de implémenter un système d'effets sur un langage noyau de smart contracts basé sur les PSS que nous avons mis en place au CEA List. Le système d'effets que nous envisageons possède des propriétés avancées telles que la composabilité, les effets d'ordre supérieur et la dépendance de type. Les effets computationnels à prendre en compte comprennent la termination, les exceptions, la consommation de gaz bornée, les changements de l'état des smart contracts, les changements des balances des comptes, etc.

Une spécification de haut niveau du système d'effets sera disponible et remise au stagiaire. Le candidat interagira avec des chercheurs et des ingénieurs spécialisés dans la technologie blockchain et la théorie des langages de programmation.

Le candidat retenu rejoindra le Laboratoire des systèmes d'information fiables, intelligents et auto-organisés (LICIA) du CEA List.

## Méthodologie :

Le stagiaire aura les responsabilités suivantes :

- 1) Se familiariser avec l'état de l'art en matière de typage statique et des systèmes d'effets algébriques.
- 2) Se familiariser avec le langage noyau de smart contracts basé sur les PSS mis en place au CEA List, et avec la spécification du système d'effets qui sera remise au stagiaire.
- 3) Étendre le langage de smart contracts développé au CEA List en mettant en place un système d'effets d'après la spécification remise au stagiaire, et produire une implémentation réaliste du dit langage (telle qu'un interpréteur efficace ou une machine virtuelle).
- 4) Vérifier l'exactitude de l'implémentation réaliste en effectuant des tests et des benchmarks.
- 5) Documenter le développement du système d'effets en rédigeant un rapport technique et/ou en collaborant à un article scientifique.

## Compétences :

Le/La candidat(e) doit avoir les compétences suivantes :

- Étudiant(e) master 2 en informatique/ingénierie.
- Connaissance en théorie des langages de programmation et systèmes de type (expérience préalable d'implémentation des langages de programmation d'ordre supérieur est un atout).
- Connaissance en blockchain, smart contracts (expérience préalable de développement dans un langage de smart contracts est un atout).

**Domaine de spécialité requis :** Informatique

**Autres domaines de spécialités, mots clés :** conception du logiciel, théorie des langages de programmation, systèmes de types, blockchain, smart contracts

**Moyens mis en œuvre (expériences, méthodes d'analyses, autres...) :** recherche, programmation

**Niveau souhaité :** Bac + 5 - Master 2

**Durée :** 6 mois

**Niveau d'habilitation défense (AS au minimum):**AS

**Formation souhaitée :** Ingénieur/Master

**Possibilité de poursuit en thèse :**Oui

**Lieu du stage :** CEA, Centre de Saclay Nano-Innov, 91191 Gif sur Yvette

**Contacts :**

GARCIA PEREZ Alvaro : [alvaro.garciaperez@cea.fr](mailto:alvaro.garciaperez@cea.fr)

MAHE Erwan : [erwan.mahe@cea.fr](mailto:erwan.mahe@cea.fr)