

FORMULAIRE DE STAGE 2021

Intitulé du stage : Réalisation et déploiement d'un consensus particulier pour une BlockChain particulière

Nom de la personne proposant le stage : Abderrahim Benslimane
(abderrahim.benslimane@univ-avignon.fr)

Lieu du stage : LIA Université d'Avignon

Descriptif du stage :

La BlockChain s'appuie sur une méthode de consensus pour valider toute nouvelle donnée. Le Proof Of Work, entre autres, est utilisé dans le minning de Blockchain pour valider les blocs et trouver le bon hachage et pour préserver l'intégrité du réseau, dépense beaucoup de temps, d'énergie et de ressources. En consacrant ces ressources à la maintenance du réseau et à l'ajout de blocs à la Blockchain (et en permettant à tout le monde de faire face à différents défis), les mineurs sont récompensés par l'actif cryptographique pour lequel ils calculaient les hachages. Plusieurs nœuds exécutent le protocole de consensus et donc sont participants du réseau BlockChain. Les nœuds rationnels effectuent des actions ou stratégies qui permettent de maximiser leurs utilités. De plus les nœuds malicieux peuvent lancer des attaques qui endommagent le réseau. Plusieurs approches d'optimisation ont été proposées dans la littérature, telle que Markov Decision Process (MDP) utilisée pour analyser et optimiser les stratégies de nœuds BlockChain pour prévenir leurs mauvais comportements. Cependant, ces approches d'optimisation ne prennent pas en compte les interactions entre les nœuds.

La théorie des jeux a été aussi appliquée comme solution pour les réseaux de BlockChain. Une étude récente énumère tous les travaux utilisant la théorie des jeux pour le mining. Mais, elle montre aussi qu'aucun des travaux ne s'est intéressé à la complexité que nous cherchons à réduire et au contrôle particulier que nous cherchons à faire pour des besoins d'applications critiques.

Dans ce travail, nous envisageons de proposer un nouveau protocole de consensus, basé Fog computing, avec une authentification intelligente permettant une sorte d'anonymat... avec une étude aussi détaillée des performances de la sécurité rendue (hachage, gestion des clés, contrôle d'accès et identification). Le tout doit répondre à une application particulière.

Thématique(s) associée(s) au stage :

Réseaux Informatiques