Avis de Soutenance

Monsieur Mouhamed Amine BOUCHIHA

Informatique et Applications

Soutiendra ses travaux de thèse intitulés

« Vers des systèmes de réputation basés Blockchain améliorés: Efficacité, protection de la vie privée et évolutivité »

dirigés par Monsieur Ronan CHAMPAGNAT

le jeudi 18 juillet 2024 à 10h00

Lieu : La Rochelle Université
Pôle Communication Multimédia Reseaux,
Amphithéâtre Michel Crépeau
44 Av. Albert Einstein
17000 La Rochelle

Composition du jury proposé

M. Ronan CHAMPAGNAT	La Rochelle Université
M. Pascal ESTRAILLIER	La Rochelle Université
M. Yacine GHAMRI-DOUDANE *(Invité)*	La Rochelle Université
M. Abdelhakim HAFID	Université de Montréal
M. Raja JURDAK	Queensland University of Technology
Mme Leïla MERGHEM-BOULAHIA	Université de technologie de Troyes
Mme Maria Cristina ONETE	Université de Limoges,
Mme Maria POTOP-BUTUCARU	Sorbonne Université
M. Mourad RABAH	La Rochelle Université

Résumé :

La gestion décentralisée de la réputation a connu une croissance importante ces dernières années, ce qui a conduit à de nouvelles solutions connues sous le nom de systèmes de réputation basés sur la blockchain (BRSs). Un BRS est un système de réputation qui fonctionne sur un réseau blockchain. Son introduction répond au besoin d'une gestion transparente, immuable et décentralisée de la réputation qui contribue à promouvoir la confiance, la crédibilité et la responsabilité. Cependant, les performances et la sécurité des BRSs actuels sont limitées et empêchent leur adoption à grande échelle. En particulier, les BRSs existants sont peu performants en cas de charge accrue et peuvent perdre des transactions. Ils sont également très limités dans leur capacité à gérer la confidentialité des utilisateurs sans compromettre l'évolutivité de la blockchain sous-jacente. Dans cette thèse, nous présentons plusieurs contributions visant à améliorer les performances et la sécurité des BRSs afin d'élargir leur adoption. Pour améliorer les performances des BRS, nous présentons tout d'abord GuRuMarket. GuRuMarket est un BRS qui introduit la gestion de la réputation à la fois au niveau de l'application et du consensus. Il favorise la confiance et la responsabilité entre les commerçants grâce à une gestion transparente de la réputation et des garanties sur la chaîne. Il améliore l'évolutivité et l'équité de la blockchain sous-jacente grâce à un protocol de consensus léger appelé preuve de garantie et de réputation (PoGR). Pour répondre aux problèmes de la protection de la vie privée dans les BRSs actuels, nous présentons DARS, un système de réputation anonyme décentralisé. Ce système permet aux utilisateurs et aux entités d'utiliser plusieurs pseudonymes dans leurs interactions, protégeant ainsi leur véritable identité tout en maintenant leur réputation exacte et à jour. Pour ce faire, DARS utilise des preuves zkSNARK sur deux grands livres différents, séparant ainsi la gestion de l'identité des opérations commerciales. PoGR, proposé dans GuRuMarket comme technique de mise à l'échelle de la couche 1, n'est pas suffisant pour servir à la fois la réputation et les charges de travail commerciales. C'est pourquoi nous présentons RollupTheCrowd, une extension des BRSs proposés dans GuRuMarket et de DARS qui exploite zkRollups en tant que technique de mise à l'échelle de la couche 2 pour améliorer les performances et réduire les coûts. RollupTheCrowd présente un cadre pour une application commune des BRS, qui est le crowdsourcing. Il introduit un modèle de réputation efficace et respectant la vie privée qui mesure la crédibilité des participants en évaluant leurs interactions dans le cadre du crowdsourcing. Poursuivant nos efforts pour élargir l'adoption du BRS, nous explorons son utilisation dans un domaine émergent, l'évaluation des grands modèles linguistiques (LLMs). Par conséquent, pour une évaluation transparente et sécurisée des LLMs, nous présentons LLMChain. LLMChain présente un nouveau cadre qui permet aux fournisseurs de LLM de partager l'accès à leurs modèles. Les utilisateurs ayant une expertise différente peuvent alors interagir avec les LLMs et fournir un retour d'information. Comme l'évaluation humaine dépend de la volonté des utilisateurs de fournir un retour d'information, nous utilisons une évaluation automatique supplémentaire qui montre une bonne corrélation avec l'évaluation humaine.