Sujet de Thèse:

Contribuer au développement des identités décentralisées (DIDs)

Objectif :

Identifier les points clefs de la conception d'une DID selon la complexité des usages, de l'implémentation et de la maintenance pour les secteurs de la Finance et de l'EdTech

Encadrants universitaires :

Pr Parisa Ghodous,
Dr Pierre Valiorgue
Dr Jean-Patrick Gelas,

Contexte :

- **le sujet proposé en préparation d'une thèse dont le financement est acquis suite à la réussite de l'appel à projet DémoES proposant de délivrer des certificats sur les compétences acquises tout au long des études pour apporter de la reconnaissance et épauler les étudiants dans leurs recherches de stages/alternances/jobs**

Pour répondre au besoin de gestion de l'identité numérique, des solutions de gestion d'identité sur la blockchain ont été proposées au cours des dernières années. Une technologie réellement décentralisée accroîtrait la liberté de choix ainsi que l'indépendance vis-à-vis des grandes entreprises/organisations en devenant une alternative solide face aux systèmes d'identification/authentification existants et largement utilisés (par exemple, via Google ou Facebook). De plus, les solutions d'identité souveraine (Self-Sovereign Identity) donnent, en théorie, un contrôle total à l'utilisateur sur ses données, diminuant ainsi le risque d'usurpation d'identité.

Ce risque d'usurpation d'identité peut devenir critique pour de nombreux secteurs comme celui de la Finance (Timechain) ainsi que celui des Edtech (BCdiploma) notamment pour l'émission de diplômes universitaires et certificats de compétences. Cependant, la technologie est encore émergente et des recherches doivent être menées pour consolider les systèmes d'identité existants sur la blockchain.

Motivés par cela, nous proposons d'étudier des solutions de gestion d'identité sur blockchain pour les secteurs sus-cités de la Finance et de l'Edtech dans l'intention de contribuer à faire émerger des solutions spécifiques à chaque secteur mettant l'accent sur les aspects de confidentialité et de sécurité pour permettre à l'utilisateur de prendre le contrôle de sa propre identité.

Le travail proposé dans cette étude consistera dans un premier temps à évaluer les risques liés à la gestion des identités basée sur la blockchain selon le cahier des charges des deux domaines d'intérêt des sponsors. Parmi les risques de gestion des identités, il sera proposé

de réfléchir à des questions qui restent ouvertes concernant la vérification de l'identité réelle, le contrôle des administrateurs malveillants ou encore la mitigation du risque de fausses identités (créées par des combinaisons de différents attributs d'entités réelles). Nous pourrons alors concevoir des solutions pour améliorer la confiance entre les demandeurs et les vérificateurs ainsi que la confiance dans la majorité des participants. Parmi les risques hérités de la technologie blockchain, il sera proposé d'évaluer les risques provenant d'une insuffisance du caractère décentralisé de la blockchain et ceux liés aux questions de récupération de clé. La récupération ne peut se faire via des administrateurs (qui peuvent être exposés à des vulnérabilités) et il est fortement déconseillé de le faire via la récupération de clé privée à partir de mots de passe. Nous pourrons alors réfléchir à des mécanismes qui devront être disponibles en cas de perte de clés privées, afin d'éviter la perte d'identité. Trouver des solutions de récupération de clés appropriées est un sujet très pertinent pour la sécurité du système.

Dans un deuxième temps, nous nous intéresserons aux aspects cryptographiques qui ont un impact direct sur la confidentialité et la sécurité de la gestion des identités sur la blockchain. Nous focaliserons particulièrement sur le cryptage des données et des métadonnées stockées, technologie qui est la spécialité de BCdiploma et qui est essentielle pour respecter le RGPD. Nous pourrons nous interroger sur la vulnérabilité des solutions vis-à-vis de l'analyse des modèles des données en chaîne et des messages échangés. Par ailleurs, considérant que la plupart des solutions à clé publique existantes sont connues pour être vulnérables aux attaques quantiques, nous pourrons nous intéresser aux solutions où des primitives résistantes aux attaques quantiques sont implémentées dans le système de gestion d'identité sur la blockchain. Comment cela peut-il être fait et dans quelle mesure cela influencera-t-il l'efficacité et la fonctionnalité est une direction de recherche. Enfin, la gestion efficace des clés reste également un défi en termes cryptographiques. Un cahier des charges technologique sera établi pour correspondre au cahier des charges fonctionnels des domaines concernés.

Enfin nous pourrons nous intéresser aux aspects d'usage qui sont primordiaux pour un système de gestion des identités. Cependant, les recherches sur la convivialité et l'expérience utilisateur semblent être à un stade naissant. Nous pourrions essayer de répondre à des questions sur l'acceptabilité par les utilisateurs finaux et les développeurs à utiliser de telles solutions sur le long terme. Nous pourrions également tenter d'évaluer la capacité des utilisateurs finaux à gérer en toute sécurité leurs identifiants et leurs informations d'identification par eux-mêmes. Ils pourraient (partiellement) déléguer le contrôle pour certaines périodes ou s'appuyer sur des services tels que les mécanismes de récupération en cas de perte. Les aspects démographiques font que les utilisateurs se comportent différemment et une bonne compréhension de ces aspects est nécessaire.