Université Abdelmalek Essaâdi
École Nationale des Sciences Appliquées - Tétouan
Département : Intelligence Artificielle et Digitalisation
Filière : Sciences des Données, Big Data & Intelligence Artificielle
Module : Fondamentaux de la Blockchain (M356)
Prof. Imad Sassi

TP N°1 Implémentation d'une blockchain

Objectifs du TP

Cet exercice constitue une première étape vers la technologie blockchain. Dans ce TP, nous allons apprendre à créer notre propre blockchain à l'aide de Python.

Exercice

Partie I

L'objectif de ce projet est de créer une blockchain à l'aide de Python, d'extraire de nouveaux blocs, puis d'afficher l'intégralité de la blockchain. Pour ce faire :

- Chaque bloc contient un ensemble d'informations. Après quelques minutes, plusieurs blocs sont ajoutés et, pour les différencier les uns des autres, chaque bloc possède une signature numérique.
- Pour simplifier, nous n'allons pas nous soucier de représenter les transactions dans un arbre Merkle, ni séparer un bloc en en-tête et contenu.
- L'empreinte est créée à l'aide d'un hachage basé sur l'algorithme SHA256.
- Le nouveau bloc est extrait en trouvant la réponse à la preuve de travail. Pour rendre le minage difficile, la preuve de travail doit être suffisamment difficile à exploiter (e.g. Fixer la cible de difficulté à un résultat de hachage commençant par quatre zéros « 0000 »).
- Lorsqu'un mineur réussit à miner un bloc, il doit recevoir une récompense pour avoir trouvé la preuve. Nous ajouterons une transaction pour envoyer une unité de récompense au mineur afin de symboliser la récompense pour avoir réussi à miner le bloc.
- Après avoir miné plusieurs blocs, la validité de la chaîne doit être vérifiée afin d'éviter toute altération de la blockchain.
- Enfin, pour cette blockchain, l'exécuter en tant qu'API REST, afin de pouvoir interagir avec elle via des appels REST.

Partie II

- Le principe de décentralisation de la blockchain stipule qu'elle doit être maintenue par plusieurs nœuds qui stockent des copies de la même blockchain, plutôt que par un seul nœud.
- Modifier le programme, en ajoutant les méthodes, voire les classes convenables, pour permettre d'ajouter des nœuds et afin que chaque nœud puisse être informé des nœuds voisins sur le réseau, garantissant ainsi la synchronisation de la blockchain.