Mini-Blockchain en Python

Nom complet : ADDAOUI Bouchra

Groupe : 01

1. Introduction :

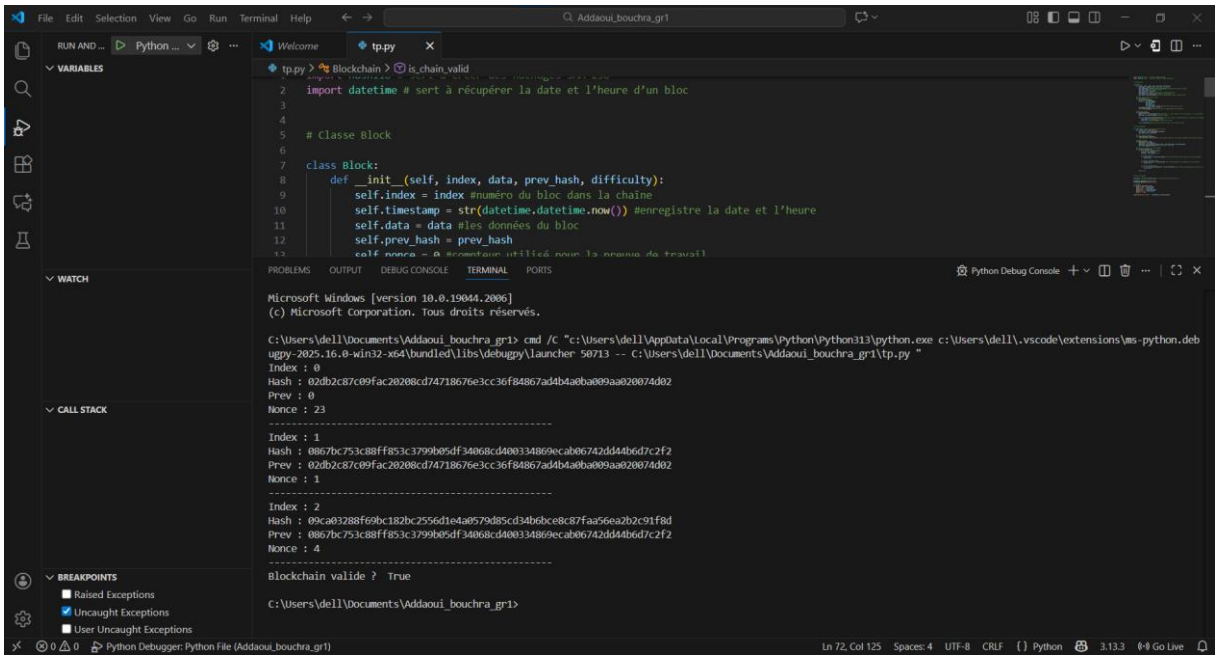
Une blockchain est une chaîne de blocs sécurisée grâce à la cryptographie. Le but de ce projet est de créer une mini-blockchain fonctionnelle en Python afin de comprendre les concepts de hachage, de minage et de validation.

2. Méthodologie :

- Création de la classe Block qui contient les informations essentielles d'un bloc : index, timestamp, données, hash du bloc précédent, nonce et le hash du bloc.
- Implémentation de la fonction de hachage avec l'algorithme SHA-256.
- Mise en place de la preuve de travail (minage) qui consiste à trouver un hash commençant par un certain nombre de zéros.
- Construction de la classe Blockchain qui contient la liste des blocs, crée le bloc de genèse et permet l'ajout de nouveaux blocs.
- Validation de la chaîne à l'aide d'une fonction vérifiant les haches et la cohérence de la preuve de travail.

3. Résultats :

Le programme permet d'ajouter plusieurs blocs à la chaîne, d'afficher leurs contenus détaillés, et de vérifier que la chaîne est valide.



- Le code source montre la classe Block, où chaque bloc est défini par ses attributs (index, timestamp, données, hash précédent, nonce, hash).
- Dans le terminal, on voit l'extraction et l'affichage de plusieurs blocs ajoutés à la blockchain :
  - ❖ Chaque bloc affiche son index, son hash, le hash du bloc précédent et la valeur du nonce.
- La dernière ligne « Blockchain valide ? True » indique que la chaîne est correcte et intègre, car tous les blocs respectent la preuve de travail et la structure attendue.

Discussion :

Le hachage garantit l’intégrité des données car toute modification d’un bloc change son hash, ce qui invalide la chaîne.

La preuve de travail sécurise la blockchain en rendant le minage coûteux en calcul.
La validation empêche toute falsification du contenu puisque le hash de chaque bloc doit correspondre et respecter la difficulté.

Conclusion :

Ce projet a permis de comprendre les concepts fondamentaux d’une blockchain simple.

Des améliorations sont possibles, comme augmenter la difficulté du minage ou implémenter un réseau décentralisé.