Licence 3 Informatique 2022-2023

TD6 Programmation Objet 2
Projet : une mini-plateforme d'enchères en ligne

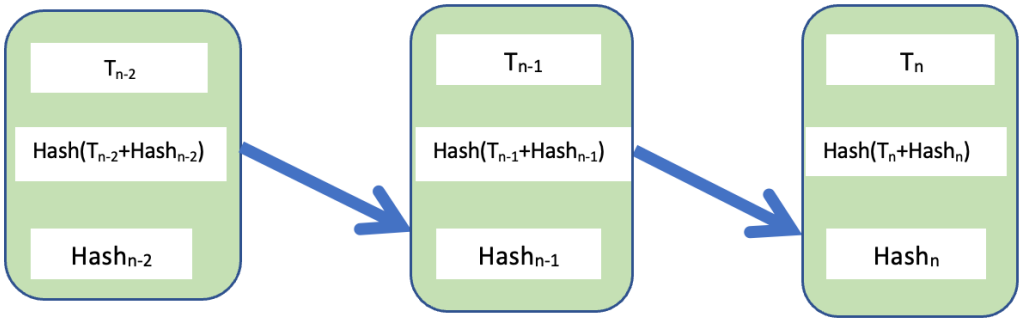
La technologie blockchain permet d'apporter des gages de confiance lors des transactions effectuées en ligne, par exemple lorsqu'il s'agit d'enchères. Le but de ce projet est de mettre en place une plateforme d'enchères décentralisée (c'est à dire sans serveur central) offrant aux participants aux enchères des garanties sur l'intégrité des transactions et sur l'évolution des prix.

Vous mettrez en place une enchère qui impliquera les participants suivants :

- Les vendeurs lancent l'enchère en mettant en vente des produits. Le vendeur définit sa durée dans le temps de l'enchère et le prix de départ.
- Les acheteurs qui vont faire des offres pour acheter.
- Les mineurs qui vérifieront la validité des transactions, par le biais de la technologie blockchain.

L'enchère se déroule dans plusieurs étapes :

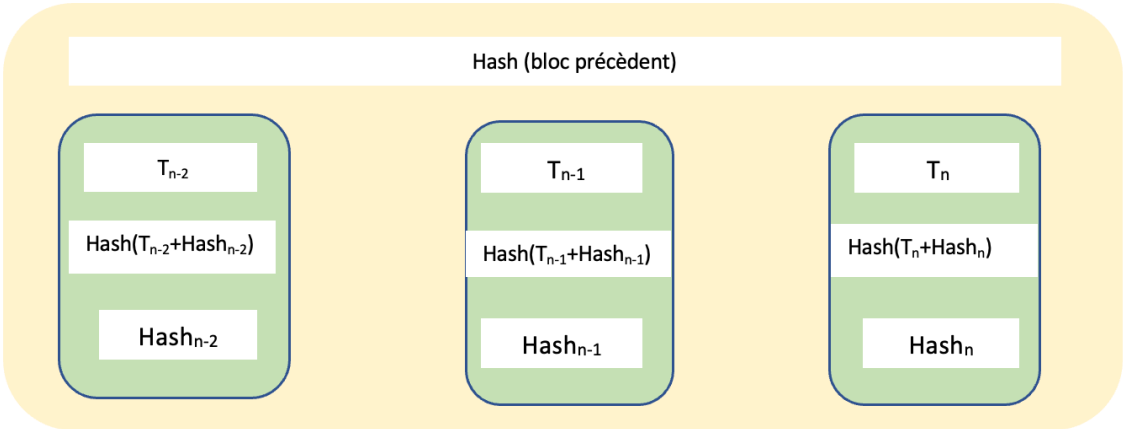
1) Le vendeur crée l'enchère. Il précise le produit en vente, le prix de départ, le temps de début de l'enchère et sa durée.
2) Un acheteur envoie une offre. Cette offre T_n doit être supérieure à l'offre précédente T_{n-1} sur le produit en vente, et l'acheteur doit faire preuve de disposer sur son compte des ressources pour payer. La transaction est confirmée et rajoutée à la chaîne de blocs, comme dans le schéma ci-dessous. Chaque bloc contient un hash du bloc précédent, ce qui rend la chaîne difficile à modifier.
3) Tous les acheteurs ayant fait des offres précédemment sont notifiés lorsque une nouvelle proposition est faite et la chaîne de transactions est mise à jour.



Sur la figure le + est une concatenation.

4) Les transactions sont "regroupées" dans une deuxième chaîne de blocs certifiés. Quand un bloc contiendra au moins *B* nouvelles transactions (*B* est un paramètre du système) les mineurs (pairs connectés) chercheront à déterminer un prefixe du bloc *X* tel que *Hash*(*P*+*X*) commence par 20 zéros.
Note: La recherche d'un tel hash s'appelle *preuve de travail* car elle est consommatrice de ressources. En effet, une preuve de travail prend 2^{20} essais (calculs de la fonction Hash) à partir de prefixes choisis aléatoirement .

5) Le pair qui trouve le premier un prefixe *P* correct (il en existe de multiples) est recompensé à terme par de l'argent numérique, mais seulement si la chaîne de transactions dans le bloc *X* est *valide*. Les pairs sont donc intéressés à vérifier que le bloc est valide. Un bloc valide est rajouté à la deuxième chaîne, comme sur la figure. Il s'agit donc d'une deuxième confirmation des transactions.
Attention: comme pour la première chaine, chaque bloc de la deuxième chaine. contiendra également le hash du bloc précedent.



6) L'enchère se clôture lorsque le temps s'est écoulé et le bloc contenant la dernière offre de prix a été validé par les mineurs.

Consignes

Ce projet est à réaliser en binôme !

Pour l'architecture de l'application vous êtes libres de choix de design pattern, parmi les designs patterns vus en cours. Vous devez néanmoins justifier ce choix.
Bien qu'elle ne soit pas obligatoire, vous pouvez rajouter une interface graphique permettant de participer aux enchères.

On vous demande de rendre sur Moodle pour le 6 janvier :

1) Une présentation courte (1-2 slides) présentant l'architecture de votre application et les design patterns choisis. Pour cela, soyez synthétiques et privilégiez les schémas.

2) Une archive contenant le code. Si nécessaire, rajoutez une README avec des explications pour déployer votre application.

Le jour de la soutenance vous montrerez la présentation ainsi qu'une démonstration du programme avec un vendeur, au moins deux acheteurs et au moins un mineur.