

TP n°2 - Modélisation d'un Système de Confiance dans un Réseau Blockchain

Module: Blockchain

Objectif

L'objectif de ce TP est de modéliser un **système de confiance** dans un réseau Blockchain en utilisant un langage de programmation orientée objet, comme Java ou Python. Vous allez implémenter des nœuds (participants) et calculer la confiance entre eux en se basant sur l'historique des transactions.

Contexte

Chaque nœud dans la blockchain représente un participant du réseau. Ce participant dispose d'un historique d'interactions (transactions) avec d'autres participants. La **confiance** entre deux participants est calculée comme la proportion d'interactions réussies entre eux. Votre tâche est de modéliser cette relation de confiance et de coder un programme qui simule ces interactions et calcule la confiance.

Énoncé

1. Classe Participant :

- Chaque participant doit avoir un identifiant unique.
- Chaque participant a une liste d'interactions (transactions) avec d'autres participants.
- Implémentez une méthode pour ajouter des transactions et une autre pour calculer la confiance basée sur l'historique.

2. Classe Transaction :

- Chaque transaction doit avoir un **expéditeur (sender)** et un **destinataire (receiver)**.
- Chaque transaction doit être marquée comme **réussie** ou **échouée**.

3. Classe Blockchain :

- La blockchain contient une liste de participants.
- Elle contient également toutes les transactions du réseau.
- Implémentez une méthode pour simuler une transaction et mettre à jour l'historique des participants.

4. Calcul de la Confiance :

- La confiance entre deux participants i et j est définie par le nombre de transactions réussies entre eux divisé par le nombre total de transactions entre eux.

Consignes

- Implémentez les classes et méthodes nécessaires pour simuler des transactions entre les participants.
- Calculez la confiance entre deux participants et affichez-la à l'écran.
- Utilisez le langage de programmation de votre choix : **Java** ou **Python**.

Instructions supplémentaires

- Pensez à inclure des transactions réussies et échouées dans vos simulations.
- Testez différentes configurations d'interactions entre les participants pour analyser l'évolution de la confiance.
- Veillez à commenter votre code et à respecter les bonnes pratiques de programmation.

Exemple de Cas d'Utilisation

Vous pouvez envisager les interactions suivantes pour démarrer votre simulation :

- Ajoutez deux participants, **Alice** et **Bob**.
- Simulez plusieurs transactions entre eux : certaines réussies et d'autres échouées.
- Calculez et affichez la confiance d'**Alice** envers **Bob** à la fin de la simulation.

Annexe : Formalisation Mathématique de la Confiance dans les Systèmes Blockchain

La formalisation mathématique de la confiance dans les systèmes blockchain peut être abordée sous plusieurs perspectives, telles que la théorie des jeux, la cryptographie et la théorie des probabilités. La confiance dans une blockchain est souvent liée à la manière dont les participants interagissent, vérifient et contribuent au réseau de manière décentralisée. Voici une approche pour formaliser la confiance mathématiquement :

1. Modélisation de la Confiance par Probabilités :

- Soit $P(i \rightarrow j)$ la probabilité que le participant i fasse confiance au participant j .
- Cette probabilité peut être calculée comme le rapport entre le nombre de transactions réussies $T_{succ}(i, j)$ et le nombre total de transactions $T_{total}(i, j)$ entre i et j :

$$P(i \rightarrow j) = \frac{T_{succ}(i, j)}{T_{total}(i, j)}$$

2. Modèle de Confiance Basé sur les Récompenses et Punitons :

- Dans un réseau blockchain, la confiance peut être affectée par des récompenses (transactions réussies) et des punitons (transactions échouées).
- On peut définir un score de confiance $C(i \rightarrow j)$ pour chaque participant basé sur un modèle de récompenses $R(i, j)$ et de punitons $P(i, j)$:

$$C(i \rightarrow j) = \frac{R(i, j) - P(i, j)}{R(i, j) + P(i, j)}$$

- Un score positif indique une bonne confiance, tandis qu'un score négatif suggère un manque de confiance.

3. Théorie des Jeux et Stratégies de Confiance :

- La théorie des jeux permet de modéliser les interactions stratégiques entre participants. Chaque participant peut choisir une stratégie basée sur la confiance.
- Par exemple, dans un jeu de la confiance, les participants i et j choisissent d'effectuer ou non une transaction en fonction du gain perçu $G(i, j)$ et de la confiance actuelle.

4. Propagation de la Confiance :

- La confiance dans un réseau décentralisé peut également être propagée d'un nœud à un autre. Si i fait confiance à j , et que j fait confiance à k , alors i peut indirectement faire confiance à k .
- Cette confiance propagée peut être exprimée par la relation transitive :

$$P(i \rightarrow k) = P(i \rightarrow j) \times P(j \rightarrow k)$$

Ces modèles fournissent une base mathématique pour formaliser la confiance dans un réseau blockchain, tout en tenant compte des interactions et des transactions entre les participants.