Guide TP Blockchain

ADAM Emilien, BOUQUET Nathan, BUYAT Dorian, NDIAYE Alhousseyni
19/05/2022

But du TP

Le TP à pour but de faire comprendre aux étudiants le fonctionnement d'une blockchain. Pour cela, une application web a été mise en place pour leur laisser manipuler et observer les composants et les aspects techniques d'une réelle blockchain.

Déroulé du TP

Le TP est divisé en 10 questions, de recherche ou de manipulation de l'application, voici les réponses et actions attendues :

Question 1 – Créer un compte. Qu'est-ce qu'un exchange de cryptomonnaies ?

Pour la création de compte, les élèves doivent simplement créer un compte sur le site afin de pouvoir réaliser le TP.

La réponse attendue a la question est qu'un exchange est une application permettant d'échanger ses cryptomonnaies contre d'autre ou contre des monnaies dites FIAT. On peut associer les exchanges centralisés aux banques.

Question 2 – Démarrer le TP. Qu'est-ce qu'un block « Genesis » d'une blockchain. Que contient le block Genesis de la blockchain BTC ?

Pour démarrer le TP, il suffit de cliquer sur le bouton au milieu de l'écran une fois connecté.

La réponse à la première partie de la question est qu'un block « Genesis » est le block initial d'une blockchain, c'est sur ce block que va se baser l'entièreté de la chaine.

Pour le block Genesis de la blockchain BTC, son contenu est : "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

Question 3 – Réaliser des transactions. Que se passe-t-il ?

Les étudiants utilisent l'interface pour réaliser des transactions en choisissant une adresse dans la liste donnée.

Ils devraient remarquer que leurs transactions sont mises en attentes, jusqu'à ce qu'il y ait assez des transactions. Alors, leurs transactions sont ajoutées dans un block est visible dedans.

Question 4 – Expliquer le Proof of Work ? A quoi correspond la preuve de travail ?

Pour la première partie de la question, on attend une explication de ce qu'est le proof of work. La raison pour laquelle il représente la sécurité de la chaine, le principe de mineur et une simplification de son fonctionnement.

Question 5 – Miner un block. Quel est l'algorithme de hachage utilisé par la blockchain BTC ?

Pour miner un block, les étudiants doivent utiliser l'application mise à disposition.

L'algorithme utilisé par la blockchain BTC est SHA-256.

Question 6 – Regardez votre solde, comment sont payés les mineurs sur le réseau BTC ?

Après avoir miné un block, le solde de l'étudiant a augmenté. Sur le réseau BTC, les mineurs sont payés par la création de nouveaux bitcoins. Une fois que les 21 millions de bitcoins auront été créés, les mineurs seront payés par les frais de transaction des utilisateurs.

Question 7 – Générer (ou attendre) de nouveaux blocks. Que remarque-t-on avec les hash ? Expliquez le prince de difficulté d'une blockchain.

Pour générer de nouveaux blocks, les étudiants peuvent réaliser des transactions, miner des blocks ou attendre qu'ils soient ajoutés avec les transactions automatiques.

Les étudiants peuvent alors remarquer que :

- Les hash des blocks sont bien présents dans le block suivant
- Les hash commencent par un « 0 »

Ce 0 représente la difficulté de la blockchain. Pour gérer la sécurité du système de PoW, on force le hash du block à répondre a des critères plus ou moins difficiles. Par exemple : le hash doit commencer par 3 0 puis une lettre. Plus il existe de blocks sur la blockchain BTC, plus le paterne de difficulté est augmenté.

Question 8 – Trouver combien de tokens a envoyé « ff69e58d0686f5e708df2a04893f55deef8015e54667c592644103f799a0a864 » ?

Les étudiants doivent chercher dans les blocks générés combien de tokens l'adresse données à envoyé de tokens. La bonne réponse est 250.

Question 9 – Sur la blockchain BTC trouver combien de BTC sont sur l'adresse « 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo ».

Pour cela, les étudiants doivent utiliser un site d'exploration de blockchain qui leur permettra de trouver combien de BTC sont sur une adresse. (réponse : https://www.blockchain.com/btc/address/34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo)

Question 10 – Quel-est le trilemme d'une blockchain ?

Les blockchains et cryptomonnaies doivent répondre à 3 critères primordiaux.

La scalabilité : la blockchain doit pouvoir répondre à une très forte évolution et utilisation de son réseaux. La vitesse d'exécution des transactions doivent être les mêmes qu'il y ait 100 ou 1 millions d'utilisateurs.

La sécurité : La sécurité du réseau doit être constante et garantir que les transactions ne soient pas modifiables et doit pouvoir vérifier leur authenticité.

La décentralisation : Le principe même d'une blockchain est qu'elle ne doit pas être contrôlé par un organe qui a tout pouvoir dessus. La blockchain doit garantir que tout appareil se connectant dispose des mêmes droits.