Corrigé du laboratoire pratique : Le fonctionnement des crypto-monnaies

Exercice 1 : Configuration d'un portefeuille numérique

Questions :

1. **Quelle est la différence entre une clé publique et une clé privée ?**
    a. Une **clé publique** est l'adresse que l'on partage pour recevoir des fonds, comparable à un numéro de compte bancaire.
    b. Une **clé privée** est un code secret qui permet d'accéder et de gérer les fonds d'un portefeuille, similaire à un mot de passe. Elle ne doit jamais être partagée.
2. **Pourquoi est-il crucial de sécuriser sa clé privée ?**
    Si la clé privée est compromise, n'importe qui peut accéder aux fonds du portefeuille et les transférer, ce qui entraînerait une perte définitive des actifs.
3. **Quels avantages offrent les réseaux testnet pour les débutants en cryptomonnaies ?**
    Les testnets permettent d'expérimenter sans utiliser de fonds réels. Ils offrent un environnement sécurisé pour apprendre à configurer des portefeuilles, effectuer des transactions et explorer la blockchain.

Exemple de captures d'écran :

- Interface de Metamask affichant l'adresse publique.
- Configuration du réseau Sepolia avec les paramètres requis.

Exercice 2 : Envoi et réception de cryptomonnaie sur un testnet

Questions :

1. **Combien de temps la transaction a-t-elle pris pour être confirmée ?**
    En moyenne, une transaction sur le réseau Sepolia prend entre 15 et 30 secondes, mais cela peut varier en fonction de la congestion du réseau.
2. **Qu'est-ce qui se passe si vous essayez d'envoyer plus de fonds que ce que contient votre portefeuille ?**
    La transaction échoue avec un message d'erreur indiquant des fonds insuffisants.

3. **Pourquoi est-il important de vérifier le réseau avant d'effectuer une transaction ?**

   Envoyer des fonds sur un mauvais réseau peut entraîner leur perte, car les blockchains ne sont pas interopérables. Par exemple, une transaction sur Sepolia ne peut pas être reconnue sur le réseau Ethereum principal.

Exemple de captures d'écran :

- Confirmation de la réception des fonds depuis le faucet.
- Preuve de la transaction effectuée, incluant le hash.

Exercice 3 : Installation et utilisation d'une node Bitcoin

Questions :

1. **Pourquoi la synchronisation d'une node Bitcoin peut-elle prendre beaucoup de temps ?**

   La synchronisation télécharge et valide l'ensemble des blocs de la blockchain. Ce processus est long car la taille de la blockchain dépasse plusieurs centaines de Go, et chaque bloc doit être vérifié.
2. **Quelles différences observez-vous entre les outils Metamask et Bitcoin Core pour interagir avec leurs blockchains respectives ?**

   Metamask est une extension légère et conviviale pour interagir avec la blockchain Ethereum via des contrats intelligents. Bitcoin Core est une implémentation complète d'une node Bitcoin, nécessitant une synchronisation complète pour participer au réseau.
3. **Comment vérifier qu'une transaction testnet a été confirmée sur Bitcoin Core ?**

   Utilisez la commande `bitcoin-cli gettransaction [txid]` pour afficher les détails de la transaction. Une confirmation est indiquée par un champ "confirmations" avec une valeur supérieure à zéro.

Exemple de captures d'écran :

- Interface de Bitcoin Core montrant l'état synchronisé.
- Capture des commandes CLI (`getnewaddress`, `getbalance`, et `sendtoaddress`) et des résultats affichés.