TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

Ecole Supérieure Privée Technologies & Ingénierie

Type d'épreuve	: ■ Devoir	☐ Examen
Enseignant	: Rim Farhat	
Matière	: **Commerce électronique et Blockchain**	
Année Universitaire	: 2023-2024	**Semestre:** 1
Classe	: **cii3-DMWM-A**	
Documents	: ☐ Autorisés	■ Non autorisés
Date	: 13/10/2023	**Durée :** 1h30
Nombre de pages	: **5**	
Barème	: 7/13	

Nom :…… Prénom : ……

QCM : (7pts)

Mettre une croix devant la (ou les) bonne(s) réponse(s):

1- Qu'est-ce qu'une transaction coinbase dans le contexte de Bitcoin ?

a) Une transaction effectuée avec une pièce de monnaie virtuelle.

b) La première transaction dans chaque bloc miné, récompensant le mineur avec des Bitcoins nouvellement créés et des frais de transaction.

c) Une transaction qui nécessite une autorisation spéciale pour être ajoutée à la blockchain.

2- Qu'est-ce qu'une adresse Bitcoin ?

a) L'adresse e-mail associée à un portefeuille Bitcoin.

b) Une chaîne de caractères alphanumériques permettant de recevoir des Bitcoins.

c) Le nom d'utilisateur d'un portefeuille Bitcoin.

3- Quels sont les avantages et les inconvénients du mécanisme de consensus Proof of Work (PoW) par rapport au Proof of Stake (PoS) dans le contexte de Bitcoin ?

a) PoW est économe en énergie, tandis que PoS consomme moins d'énergie.

b) PoW nécessite des équipements matériels spécialisés coûteux.

c) PoS favorise les détenteurs de grandes quantités de cryptomonnaie, ce qui peut entraîner une centralisation du pouvoir.

d) PoW rend le réseau plus résistant aux attaques des 51%.

4- Quel est l'objectif principal d'une blockchain privée par rapport à une blockchain publique ?

a. Permettre une participation ouverte à tous.

b. Restreindre l'accès aux seules personnes autorisées.

c. Assurer une meilleure transparence.

5- Qu'est-ce que le halving (réduction de moitié) dans le contexte de Bitcoin ?

a. Une réduction de moitié de la taille des blocs

b. La réduction de moitié de la récompense de minage

c. La réduction de moitié de la vitesse de création de blocs

6- Quelle est la fonction du nonce dans le processus de minage de Bitcoin ?

a. Il s'agit du nom de l'ordinateur du mineur.

b. Il est utilisé pour chiffrer les transactions.

c. Il est un élément aléatoire utilisé pour modifier le hachage du bloc jusqu'à ce qu'il atteigne les exigences de PoW.

7- Comment est déterminée la taille des frais de transaction dans le réseau Bitcoin ?

a. Les frais de transaction sont fixés par le protocole Bitcoin.

b. Les mineurs choisissent arbitrairement les frais de transaction.

c. Les utilisateurs proposent des frais de transaction, et les mineurs sélectionnent les transactions avec les frais les plus élevés.

8- Quelle est la fonction du merkle tree dans un bloc Bitcoin ?

a. Stocker les clés privées des utilisateurs.

b. Regrouper les transactions pour réduire la taille du bloc.

c. Générer de nouveaux bitcoins.

9- Quelle est la taille actuelle de la récompense de minage (block reward) pour l'extraction d'un nouveau bloc Bitcoin ?

a. 6,25 bitcoins

b. 25 bitcoins

c. 50 bitcoins

10- Qu'est-ce qu'un « genesis block » ?

a. Un bloc célèbre qui a codé en dur un hash du livre de la genèse sur la blockchain

b. Le premier bloc après chaque bloc de moitié

c. Le premier bloc d'une blockchain

11- Qu'est-ce qu'une Blockchain ?

a. Un grand livre distribué sur un réseau peer to peer

b. Un type de crypto-monnaie

c. Un livre centralisé

12- Comment la blockchain peut-elle améliorer la traçabilité et la transparence dans la chaîne d'approvisionnement ?

a. En stockant les données de la chaîne d'approvisionnement dans un format propriétaire.

b. En permettant l'enregistrement immuable de chaque étape de la chaîne d'approvisionnement, accessible à tous les participants autorisés.

c. En supprimant complètement les informations de la chaîne d'approvisionnement pour des raisons de sécurité.

13- Quel est l'objectif de la fonction de hachage dans la technologie blockchain ?

a. Chiffrer les données pour les rendre secrètes.

b. Créer un identifiant unique pour chaque bloc de données.

c. Diviser les données en petits morceaux.

14- Quelle est la principale caractéristique de la technologie blockchain qui assure l'immuabilité des données?

a. Registre distribué.

b. Contrats intelligents.

c. Vérification centralisée.

Exercice (13 pts)

1. Donner quatre avantages clés de la Blockchain. (2 pts)

Sécurité et Intégrité des Données
Décentralisation
Transparence et Traçabilité
Automatisation à l'aide des Contrats Intelligents

- 2. a. Discutez des menaces de sécurité auxquelles sont confrontées les utilisateurs de Bitcoin, telles que les attaques à 51% et les attaques par double dépense. (2 pts)

Attaque à 51% :

Description : Une attaque à 51% se produit lorsqu'une entité acquiert plus de 50% de la puissance de calcul totale du réseau Bitcoin. Cela lui donne un contrôle majoritaire sur le processus de validation des transactions.
Menace : Avec un tel contrôle, l'entité malveillante pourrait potentiellement empêcher la confirmation de transactions légitimes, exclure d'autres mineurs de l'ajout de blocs à la blockchain, et même réaliser des attaques de double dépense.
Conséquences : Cela pourrait compromettre la décentralisation et la sécurité du réseau, remettant en question la confiance dans la validité des transactions et la résistance aux censures.
Attaque par Double Dépense :

Description : Une attaque par double dépense se produit lorsqu'un utilisateur dépense les mêmes bitcoins deux fois en envoyant deux transactions différentes, en utilisant la même sortie de transaction.
Menace : Dans une attaque réussie par double dépense, l'utilisateur pourrait obtenir des biens ou des services en échange de la première transaction, puis réorganiser la blockchain pour invalider cette transaction tout en conservant les bitcoins dépensés.
Conséquences : Cela compromettrait la confiance des commerçants et des utilisateurs dans la finalité des transactions, ce qui pourrait avoir des implications sérieuses pour l'adoption et l'utilisation généralisée de Bitcoin.

b. Expliquez comment Bitcoin protège contre ces menaces. (3 pts)

Preuve de Travail (Proof of Work) :

Protection contre les attaques à 51% : Bitcoin utilise le mécanisme de Proof of Work, qui nécessite que les mineurs résolvent des problèmes mathématiques complexes pour ajouter un nouveau bloc à la blockchain. Acquérir plus de 50% de la puissance de calcul totale du réseau pour une attaque à 51% serait extrêmement coûteux et peu pratique. De plus, la détection d'une telle attaque serait rapide, car elle perturberait le consensus et la confiance dans la validité des transactions.
Confirmations de Transaction :

Protection contre les attaques par double dépense : Les utilisateurs de Bitcoin sont encouragés à attendre plusieurs confirmations avant de considérer une transaction comme finalisée. Chaque bloc ajouté à la blockchain constitue une confirmation supplémentaire. Plus le nombre de confirmations est élevé, plus la probabilité d'une attaque par double dépense devient faible, car elle nécessiterait de réorganiser un nombre croissant de blocs.
Décentralisation :

Protection générale : La décentralisation du réseau Bitcoin, avec de nombreux mineurs indépendants et concurrents, rend difficile la coordination d'une attaque à grande échelle. Même si un mineur malveillant parvient à contrôler temporairement plus de 50% de la puissance de calcul, la nature décentralisée du réseau limite l'impact de cette domination.

……

……

……

3. Explorez le fonctionnement du consensus Proof of Work (PoW) dans le réseau Bitcoin. Comment les mineurs sont-ils incités à valider les transactions ? (3 pts)

……

……

Chapitre 2 page 18

……

……

4. Donnez un exemple de transaction Bitcoin et détaillez ses composants, y compris les entrées, les sorties et les frais de transaction. Comment les frais de transaction sont-ils calculés pour cette transaction ? (2 pts)

……

……

mayjiiiich

……

……

……

5. Imaginez que vous souhaitez envoyer une transaction Bitcoin avec une confirmation rapide. Quels ajustements pourriez-vous faire dans les frais de transaction pour atteindre cet objectif ? (1 pts)

……

……

……

Pour obtenir une confirmation rapide dans le réseau Bitcoin, vous pouvez ajuster les frais de transaction en les fixant à un niveau plus élevé. Les mineurs sont incités à inclure les transactions avec les frais les plus élevés dans les blocs qu'ils minent. Ainsi, en offrant des frais plus élevés, votre transaction a plus de chances d'être traitée rapidement.