Blockchain CheatSheet - Vue d’Ensemble

🕓 **Temps de lecture : 5 min**

Table des matières

§ Fondamentaux

Blockchain : Une Base de Données Distribuée Peer-to-Peer

- **Définition** : La blockchain est une technologie de base de données distribuée peer-to-peer où chaque machine (pair) agit comme un nœud-bloc.
- **Mécanisme** : Chaque bloc est lié au suivant par un hash cryptographique ; la fin d'un bloc contient la clé pour le début du bloc suivant.
- **Objectif** : Chaque technologie blockchain doit être adaptée à l'application spécifique pour laquelle elle est conçue. Les cryptomonnaies ne sont qu'une application qui peut utiliser les protocoles blockchain.

Confiance et Immuabilité

- **Pas de Confiance Nécessaire** : Les caractéristiques des blocs et la propriété sont enregistrées dans l'historique immuable de la chaîne (les livres).
- **Contrôle par Consensus** : Le consensus est toujours contrôlé par chaque bloc de la chaîne par le biais de la Preuve de Travail ou de la Preuve d'Enjeu.

Sécurité et Efficacité Inégalées

- **Vérification de Propriété** : Cela résout la vérification et l'échange de propriété de manière sécurisée sans intermédiaire.
- **Vitesse** : Les temps de transfert des données sont considérablement plus rapides, presque instantanés, ce qui est utile pour les échanges de marché et les transferts de propriété.
- **Caractéristiques Clés** : La sécurité, la vitesse et la vérification de propriété sont les principales caractéristiques qui rendent la blockchain cruciale pour les services économiques.

Anti-Falsification

- **Vérification des Livres** : La blockchain résout le problème de la falsification en vérifiant les livres des blockchains.

Potentiel Disruptif

- **Applications** : Les applications pratiques de la blockchain sont nombreuses : vote par des tokens uniques, sécurité IoT, améliorations des écosystèmes médicaux, états financiers, validations de processus sécurisées, transparence des transactions pour la gouvernance, passeports, coûts des transactions, et plus encore.

---

§ Vue d'Ensemble de la Technologie Blockchain

Fonction de Hash

- Une fonction de hash crée un « empreinte digitale » des éléments du bloc de manière dynamique, utilisée comme clé pour connecter les blocs.

Informations Approfondies

Blockchain Cheat Sheet - Hashing

Système Clé Privée/Public

- **Relation** : La clé privée et la clé publique sont mathématiquement liées.
- **Facile à Rechercher** : Clé Privée => Clé Publique
- **Difficile à Rechercher** : Clé Publique => Clé Privée

Informations Approfondies

Blockchain Cheat Sheet - Cryptographie & Signatures

Adresse Publique

- **Relation avec la Clé Publique** : L'adresse publique est liée à la clé publique.
- **Dérivation** : Elle peut être la clé publique elle-même ou une valeur dérivée de la clé publique par une fonction.

Algorithmes de Signature Numérique (DSA)

- **Preuve de Propriété** : DSA prouve qui est le propriétaire de la clé privée.
- **Vérification sans Révélation** : Ils permettent de vérifier la signature sans révéler la clé privée.

Informations Approfondies

Blockchain Cheat Sheet - Cryptographie & Signatures

Mécanique des Transactions

Concept UTXO : Le système fonctionne avec le concept de UTXO (outputs de transactions non dépensés), représentant la valeur que possède le bloc et établissant les unités non dépensées et dépensables.

1. **Début** : Début du processus de transaction.
2. **Vérifier les UTXO non dépensés** : Vérifier les UTXOs disponibles.
3. **Générer des Clés (Expéditeur)** : L'expéditeur génère une nouvelle paire de clés privées et publiques.
4. **Générer des Clés (Destinataire)** : Le destinataire (Jenna) génère une nouvelle paire de clés privées et publiques.
5. **Créer la Transaction** : Créer une transaction pour envoyer 7 unités à Jenna et 3 unités comme monnaie de retour à l'expéditeur.
6. **Signer la Transaction** : L'expéditeur signe la transaction avec sa clé privée.
7. **Diffuser la Transaction au Réseau** : La transaction signée est diffusée au réseau blockchain.
8. **Valider la Transaction** : Les nœuds du réseau vérifient et valident la transaction.
9. **Mettre à Jour la Blockchain** : La blockchain est mise à jour avec la nouvelle transaction.
10. **Nouveau UTXO** : L'expéditeur a un nouveau UTXO de 3 unités, tandis que l'ancien UTXO est désormais sans valeur.
11. **Fin** : Fin du processus de transaction.

Cryptographie

- **Partie Intégrante de l'Écosystème** : La cryptographie circule dans la structure de l'écosystème.
- **Utilisation** : Elle est utilisée pour générer des clés privées et stocker des données cryptées dans le bloc.

Informations Approfondies

Blockchain Cheat Sheet - Cryptographie & Signatures

Mécanisme de Consensus

- **Différentes Méthodes** : Il existe différentes façons d'atteindre le consensus, telles que :
  - **Preuve de Travail (PoW)** : Les mineurs résolvent des problèmes complexes pour valider les transactions.
  - **Preuve d'Enjeu (PoS)** : Les principaux détenteurs de tokens créent le consensus, car ils ont le plus grand intérêt à valider des transactions correctes.

Informations Approfondies

Blockchain Cheat Sheet - Consensus

Incentives

- **Objectif** : Les incentives sont conçus pour encourager la participation au système.
- **Systèmes Proof-of-Work** : Dans les systèmes PoW, des récompenses sont attribuées à ceux qui contribuent au bien-être du système, par exemple en validant des transactions.
- **Récompenses** : Ces récompenses ont généralement une certaine valeur et motivent les participants à maintenir le réseau.

---

§ Questions Clés et Résolutions 08/2024

Questions Clés Résolues :

1. **Comment la technologie blockchain peut-elle dépasser les vitesses de transaction traditionnelles ?**
   - La blockchain peut traiter les transactions plus rapidement que les méthodes traditionnelles en raison de sa nature décentralisée et de ses algorithmes de consensus avancés.
2. **Pourquoi utiliser de grandes bases de données dans une blockchain ?**
   - Les grandes bases de données garantissent la redondance, la sécurité et la disponibilité des données à travers le réseau.
3. **Comment atteindre l'interopérabilité entre les différentes chaînes ?**
   - L'interopérabilité entre les chaînes peut être atteinte grâce à des protocoles et des technologies permettant à différentes blockchains de communiquer et de réaliser des transactions entre elles.

Questions Non Résolues Complètement :

1. **Vie Privée :**

- La vie privée reste un problème non résolu, car améliorer la transparence nécessite souvent de sacrifier un certain niveau de confidentialité.

2. **Vérification du Monde Réel :**
   - Comment vérifier des éléments du monde réel avec la blockchain, par exemple en utilisant des étiquettes RFID ? Cette question est encore ouverte.
3. **Immuabilité et Forks :**
   - Améliorer l'immuabilité d'une chaîne peut créer des forks, conduisant à de nouvelles technologies blockchain et rendant l'écosystème plus fragmenté.
4. **Gouvernance :**
   - Si ces technologies deviennent omniprésentes, les algorithmes devront être mis à jour pour suivre les changements sociétaux. Atteindre un consensus pour ces changements substantiels sera très difficile.
5. **Régulations :**
   - Il manque des réglementations en raison de la nature disruptive de ces technologies. De nouvelles lois sont nécessaires pour réguler ce domaine efficacement.

La technologie blockchain permet aux personnes des marchés émergents de monétiser des produits de manière sans précédent, entraînant une croissance significative en accédant aux finances modernes et en surmontant les contraintes antérieures. Cette montée du capital humain bénéficie à la fois aux marchés émergents et développés, conduisant à des avancées inattendues et significatives.

Suivi Suggéré

Blockchain CheatSheet - La Vision

Auteur : Kenneth Boldrini