PoW

Concepts

La Preuve de Travail (Proof of Work) est un mécanisme de consensus où les participants doivent résoudre des problèmes mathématiques complexes pour ajouter des blocs à la chaîne, garantissant ainsi la sécurité et la validité des transactions.

#wallet

Taille du réseau

Concepts

La taille du réseau est le nombre de participants et de nœuds dans un réseau blockchain, ce qui rend les attaques plus difficiles en répartissant la puissance de calcul et en augmentant la résistance à la manipulation.

#wallet

Longueur de la chaîne

Concepts

La longueur de la chaîne est la mesure de la chaîne la plus longue dans un réseau blockchain, où la chaîne la plus longue est généralement considérée comme la version valide, assurant ainsi la sécurité contre les réorganisations malveillantes.

#wallet

Consensus

Concepts

Un consensus décentralisé est un système de prise de décision distribué où plusieurs participants sont impliqués dans la validation des transactions et la création de nouveaux blocs, évitant ainsi le contrôle centralisé et les attaques par une seule entité.

#wallet

Incentives

Concepts

Les incentives économiques sont des récompenses économiques, telles que des jetons ou des frais de transaction, offertes aux participants du réseau pour les inciter à agir dans l'intérêt du système et à sécuriser la blockchain.

#wallet

Gouvernance

Concepts

Les mécanismes de gouvernance sont des processus et les protocoles qui permettent aux participants de prendre des décisions collectives concernant les mises à jour du protocole, les règles du réseau et d'autres aspects importants pour assurer la sécurité et l'évolution de la blockchain.

#wallet

Audits de sécurité

Concepts

Les audits de sécurité sont des examens approfondis du protocole, du code source et des contrats intelligents pour identifier les vulnérabilités potentielles et renforcer la sécurité du réseau blockchain.

#wallet

PoS

Concepts

La Preuve d'Enjeu (Proof of Stake) esr un mécanisme de consensus où les participants prouvent leur engagement en verrouillant une quantité de cryptomonnaie dans le réseau, ce qui leur donne le droit de valider les blocs, réduisant ainsi la consommation d'énergie associée à la preuve de travail.

#wallet

Délégation de confiance

Concepts

La délégation de confiance est le processus permettant aux participants de confier la validation des transactions et la création de blocs à d'autres participants de confiance, garantissant la sécurité et l'efficacité du réseau blockchain.

#wallet

Preuve d'identité

Concepts

La Preuve d'identité vérifiable (Verifiable Identity Proof) est un mécanisme qui permet de vérifier l'authenticité et l'intégrité des identités numériques des utilisateurs sur la blockchain, renforçant ainsi la confiance et la sécurité des interactions.

#wallet

Réputation

Concepts

Les mécanismes de réputation et de crédibilité sont des systèmes permettant d'évaluer la fiabilité des participants et de récompenser ceux qui ont une bonne réputation, favorisant ainsi des interactions plus sûres et plus fiables sur la blockchain.

#wallet

Confirmation multiple

Concepts

Les confirmations multiples des transactions sont des transactions sont confirmées par plusieurs participants de la blockchain, ce qui réduit le risque de double-dépense et renforce la sécurité du réseau.

#wallet

Temps de blocage

Concepts

Une fois qu'un bloc est ajouté à la blockchain, le temps de blocage (Block Finality) est considéré comme définitif et ne peut plus être modifié, garantissant ainsi l'intégrité et l'immutabilité des transactions enregistrées.

#wallet

Chiffrement

Concepts

Les données sur la blockchain sont cryptées pour assurer la confidentialité et la sécurité des informations sensibles, empêchant ainsi l'accès non autorisé.

#wallet

Immuabilité

Concepts

La blockchain est une structure de données immuable, ce qui signifie que les blocs précédents ne peuvent pas être modifiés, garantissant ainsi l'intégrité et l'auditabilité des enregistrements.

#wallet

Signature numérique

Concepts

Les transactions sur la blockchain sont signées numériquement, ce qui garantit l'authenticité des transactions et empêche leur falsification.

#wallet

Gestion des clés

Concepts

Les clés privées utilisées pour accéder aux comptes et aux actifs sur la blockchain doivent être gérées de manière sécurisée pour éviter tout accès non autorisé.

#wallet

Décentralisation

Concepts

Les blockchains décentralisées répartissent les données et les opérations sur un réseau de nœuds, ce qui renforce la résilience du système et limite les risques d'attaques centralisées.

#wallet

Nonce

Concepts

Un nonce est un nombre utilisé dans le processus de preuve de travail pour trouver un hash valide et ajouter un nouveau bloc à la chaîne.

#wallet

Timestamps

Concepts

Les horodatages (timestamps) sont utilisés pour enregistrer le moment précis où les transactions sont ajoutées à la blockchain, permettant une traçabilité et une vérification chronologique.

#wallet

Confirmation des blocs

Concepts

Les blocs nouvellement créés doivent être confirmés par un certain nombre de blocs suivants pour assurer la sécurité et la finalité des transactions enregistrées.

#wallet

Id de chaînes

Concepts

Les identifiants de chaînes sont des valeurs uniques qui identifient de manière univoque chaque bloc et chaque transaction sur la blockchain.

#wallet

Hard forks

Concepts

Les hard forks sont des mises à jour majeures du protocole de la blockchain qui entraînent une séparation de la chaîne existante et peuvent résoudre des problèmes de sécurité ou introduire de nouvelles fonctionnalités.

#wallet

Limite de taille

Concepts

Les blockchains peuvent imposer des limites à la taille des blocs pour prévenir les attaques de saturation du réseau et garantir une performance optimale.

#wallet

Ajustement de la difficulté

Concepts

Les blockchains peuvent ajuster la difficulté de la preuve de travail en fonction de la puissance de calcul du réseau pour maintenir un rythme de création de blocs constant et sécurisé.

#wallet

Analyse des contrats

Concepts

Les contrats intelligents peuvent être analysés statiquement et dynamiquement pour détecter les vulnérabilités et les erreurs de programmation, renforçant ainsi la sécurité des applications décentralisées.

#wallet

Normes de codage

Concepts

Les normes de développement sécurisé fournissent des directives et des bonnes pratiques pour réduire les risques de vulnérabilités et de failles de sécurité dans les applications blockchain.

#wallet

Vérification formelle

Concepts

La vérification formelle consiste à utiliser des méthodes mathématiques pour prouver que les contrats intelligents se comportent conformément aux spécifications, améliorant ainsi la confiance dans leur fonctionnement.

#wallet

Virtualisation

Concepts

Les mécanismes de sandboxing et de virtualisation permettent d'exécuter les contrats intelligents dans des environnements isolés, minimisant les risques d'interférences ou de manipulations malveillantes.

#wallet

Trans. non sollicitées

Concepts

Les blockchains peuvent mettre en place des mécanismes pour prévenir ou atténuer les transactions non sollicitées ou indésirables, garantissant ainsi l'intégrité du réseau.

#wallet

Surveillance

Concepts

Les systèmes de surveillance peuvent analyser les modèles de comportement sur la blockchain pour détecter les activités suspectes ou malveillantes, aidant à prévenir les attaques et les fraudes.

#wallet