51%

Solutions

CONCEPTS : 1. Preuve de travail (Proof of Work) 2. Taille du réseau 3. Longueur de la chaîne 4. Consensus décentralisé 5. Incentives économiques 6. Mécanismes de gouvernance 7. Audits de sécurité.
EXEMPLE : L'attaque contre la blockchain Ethereum Classic en janvier 2019, où un attaquant a réussi à contrôler plus de 50% de la puissance de calcul et à réaliser des double-dépenses.

#attaque

Double-dépense

Solutions

CONCEPTS : 1. Consensus 2. Confirmation multiple des transactions 3. Temps de blocage (Block Finality) 4. Chiffrement 5. Signature numérique 6. Chaîne de blocs immuable 7. Auditabilité transparente.
EXEMPLE : L'attaque contre la plateforme d'échange de cryptomonnaies Bitfinex en 2016, où des bitcoins ont été volés par une exploitation de failles dans le protocole pour effectuer des double-dépenses.

#attaque

L'homme du milieu

Solutions

CONCEPTS : 1. Chiffrement 2. Signature numérique 3. Mécanismes de validation des transactions 4. Gestion sécurisée des clés 5. Utilisation de réseaux décentralisés.
EXEMPLE : L'attaque contre le projet MyEtherWallet en 2018, où des pirates ont utilisé une attaque MITM pour détourner les fonds des utilisateurs.

#attaque

Rejeu

Solutions

CONCEPTS : 1. Nonce 2. Timestamps 3. Confirmation des blocs 4. Identifiants de chaînes 5. Hard Forks.
EXEMPLE : L'attaque contre la blockchain Ethereum Classic en janvier 2019, où des transactions précédemment validées ont été rejouées sur une blockchain alternative pour effectuer des double-dépenses.

#attaque

DDoS

Solutions

CONCEPTS : 1. Preuve de travail (Proof of Work) 2. Limite de taille de bloc 3. Mécanismes d'ajustement de la difficulté 4. Protection contre les transactions non sollicitées 5. Systèmes de surveillance et de détection des comportements anormaux.
EXEMPLE : L'attaque contre le réseau Bitcoin en 2015, où des attaquants ont inondé le réseau avec une quantité massive de transactions, entraînant une congestion du réseau.

#attaque

Contracts malveillants

Solutions

CONCEPTS : 1. Analyse statique et dynamique des contrats intelligents 2. Audits de sécurité 3. Normes de développement sécurisé 4. Mécanismes de gouvernance et de mise à jour 5. Vérification formelle 6. Mécanismes de sandboxing et de virtualisation.
EXEMPLE : L'attaque contre le projet de contrat intelligent The DAO en 2016, où des attaquants ont exploité une vulnérabilité du smart contract pour dérober environ un tiers des fonds investis.

#attaque

Sybil

Solutions

CONCEPTS : 1. Preuve de travail (Proof of Work) 2. Preuve d'enjeu (Proof of Stake) 3. Délégation de confiance 4. Preuve d'identité vérifiable (Verifiable Identity Proof) 5. Mécanismes de gouvernance 6. Mécanismes de réputation et de crédibilité.
EXEMPLE : L'attaque contre la blockchain Peercoin en 2012, où un attaquant a réussi à contrôler une grande partie des nœuds du réseau en créant de multiples identités, remettant en question la sécurité du consensus.

#attaque