Maitriser la cryptographie pour la sécurité de la blockchain

Date et durée

Code formation : SSR004FR
Durée : 3 jours
Nombre d'heures : 21 heures

Description

La **cryptographie** est la science et l'art de sécuriser les communications et les données, en les rendant incompréhensibles à des tiers. La **blockchain**, quant à elle, est une technologie de stockage et de transmission d'informations, fonctionnant sans organe central de contrôle. Elle s'appuie sur la cryptographie pour garantir l'intégrité, l'authenticité et la traçabilité des données, créant ainsi un registre numérique immuable et distribué. Cette formation intensive de 3 jours aborde les principes et les **techniques de la cryptographie moderne** avant de se concentrer sur leur application concrète aux systèmes blockchain. Le programme vous guidera de l'analyse des algorithmes cryptographiques et de la gestion des clés à l'architecture des blockchains et à la sécurisation des **smart contracts**.
À l'issue de ce parcours, vous développerez une expertise pour **comprendre les algorithmes cryptographiques** et les mécanismes de consensus. Grâce à des **ateliers pratiques**, vous apprendrez à manipuler des outils de chiffrement et à simuler des transactions sécurisées, vous préparant à évaluer les enjeux de sécurité liés aux blockchains.

Objectifs

À l'issue de cette formation avancée en cryptographie et blockchain, vous atteindrez les objectifs de compétences suivants :

- saisir les principes fondamentaux de la cryptographie symétrique et asymétrique ;
- identifier les algorithmes cryptographiques exploités dans les réseaux de blockchain ;
- démontrer l'importance de la cryptographie pour la sécurisation des transactions sur la blockchain ;
- utiliser les outils de chiffrement et de signature numérique en pratique ;
- analyser les risques et les limites des systèmes cryptographiques dans le contexte de la blockchain.

Points forts

- **Approche pédagogique intensive :** bénéficiez d'une formation qui explore les fondements de la cryptographie moderne et leur application dans les systèmes blockchain.
- **Mise en pratique interactive :** maîtrisez les concepts grâce à des ateliers pratiques qui vous permettront de manipuler des outils cryptographiques et de simuler des transactions blockchain sécurisées.
- **Acquisition de compétences clés :** le contenu de la formation est conçu pour vous permettre de comprendre les algorithmes cryptographiques et les mécanismes de consensus , et d'évaluer les risques et les limites des systèmes cryptographiques dans la blockchain.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Connaissances en programmation :** une familiarité avec au moins un langage de programmation (comme Python ou JavaScript) est un atout pour les ateliers pratiques.
- **Concepts mathématiques de base :** avoir des notions en algèbre et en arithmétique modulaire pour comprendre les fondements de la cryptographie.
- **Bases en informatique et réseaux :** une compréhension des architectures client-serveur et des protocoles de communication est recommandée.

Public

Cette formation s'adresse aux publics suivants :

- Les **développeurs blockchain** qui désirent approfondir leur expertise sur les fondements cryptographiques et les mécanismes de sécurité de la blockchain.
- Les **ingénieurs sécurité** et **architectes IT** qui désirent approfondir leur expertise sur la sécurité des systèmes blockchain.
- Les **étudiants en cybersécurité ou cryptographie** qui cherchent à lier la théorie à l'application pratique dans un contexte de blockchain.
- Les **recruteurs IT** qui veulent comprendre les compétences clés requises pour exercer dans les métiers de la cryptographie et de la blockchain.

Programme

Module 1 : comprendre les fondamentaux de la cryptographie

- Les concepts clés de la cryptographie : confidentialité, intégrité, authenticité et non-répudiation.
- Les modèles de sécurité : canal sécurisé, adversaire passif ou actif.

Module 2 : analyser les algorithmes cryptographiques

- La cryptographie symétrique : AES, ainsi que ses modes de chiffrement (CBC, GCM).
- La cryptographie asymétrique : RSA, Diffie-Hellman et ECC.
- Les fonctions de hachage : SHA-2, SHA-3 et BLAKE2.

Travaux pratiques

- Chiffrer et déchiffrer des données avec OpenSSL et Python.
- Générer des clés RSA/ECC et signer des messages.

Module 3 : gérer les signatures, l'intégrité et les clés

- Le fonctionnement des signatures numériques (RSA, ECDSA).
- L'infrastructure à clés publiques (PKI) et les certificats X.509.
- La gestion des clés et des secrets (HSM, Vault, KMS).

Module 4 : s'initier à la cryptanalyse et aux attaques

- Les attaques par canal auxiliaire et les collisions de hachage.
- Les vulnérabilités courantes dans les implémentations (Heartbleed, ROCA).

Travaux pratiques

- Créer et vérifier des certificats.
- Simuler une attaque par collision de hachage.

Module 5 : appliquer la cryptographie à la blockchain

- L'architecture des blockchains : structure des blocs, Merkle Trees et horodatage.
- Les protocoles de consensus : PoW, POS, DPoS et BFT.
- L'application de la cryptographie aux blockchains majeures, comme le Bitcoin, l'Ethereum et le Zcash.

Module 6 : sécuriser les smart contracts

- Les langages de programmation (Solidity, Vyper) et l'EVM (Ethereum Virtual Machine).
- Les vulnérabilités courantes : reentrancy, overflow et front-running.
- L'utilisation d'outils d'audit, comme MythX, Slither et Remix.

Travaux pratiques

- Déployer un smart contract sur un testnet Ethereum.
- Analyser les vulnérabilités dans un contrat réel.