Sécurisation des crypto-actifs : clé privée & clé publique

1 j (7 heures) Ref : IABG005

Public

Professionnels de la finance, du droit, ainsi que de la gestion d'entreprise souhaitant comprendre les fondamentaux de la sécurisation des crypto-actifs

Pré-requis

Aucun pré-requis technique spécifique n'est nécessaire
Intérêt pour les crypto-actifs et leur sécurisation recommandée

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Nombreux exercices pratiques et mises en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif. Vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

La formation "Sécurisation des Crypto-Actifs : Clé Privée & Clé Publique" est une session d'une journée destinée aux professionnels de divers secteurs, notamment la finance, le droit, et la gestion d'entreprise, qui souhaitent comprendre les fondamentaux de la sécurisation des crypto-actifs. Cette formation aborde les concepts de base et avancés des clés privées et publiques, leur rôle crucial dans la sécurisation des transactions et des actifs numériques, ainsi que les meilleures pratiques pour gérer et protéger ces clés. Les participants apprendront à sécuriser leurs actifs numériques de manière efficace, en comprenant les risques associés et les techniques de mitigation.

Cette formation d'une journée offre une introduction complète et pratique aux techniques de sécurisation des clés privées et publiques, permettant aux participants de protéger efficacement leurs crypto-actifs contre les menaces potentielles.

Objectifs

Comprendre le rôle des clés privées et publiques dans la sécurité des crypto-actifs
Apprendre à générer, stocker et gérer des clés privées et publiques de manière sécurisée
Identifier les risques associés à la gestion des clés et les techniques pour les atténuer
Mettre en œuvre les meilleures pratiques pour la sécurisation des portefeuilles de crypto-actifs
Appliquer des méthodes de récupération de clés et de gestion des pertes

Programme détaillé

INTRODUCTION AUX CLES PRIVEES ET PUBLIQUES

FONDAMENTAUX DE LA CRYPTOGRAPHIE ASYMETRIQUE

Nous débutons par une exploration des concepts de base de la cryptographie asymétrique, mettant en lumière l'importance des clés privées et publiques dans la sécurisation des transactions blockchain. Les participants acquièrent une compréhension approfondie du chiffrement asymétrique et de son rôle crucial dans la confidentialité et l'authenticité des données échangées.

GENERATION ET GESTION DES CLES

PROCESSUS DE GENERATION DES CLES

Nous examinons les techniques modernes de génération sécurisée des clés privées et publiques, en soulignant les bonnes pratiques pour minimiser les risques de compromission. Les outils et logiciels utilisés pour générer ces clés sont présentés, avec un accent particulier sur la sécurité et la robustesse des processus.

STOCKAGE SECURISE DES CLES

Cette section explore les différentes méthodes de stockage des clés, telles que les hardware wallets, software wallets et paper wallets. Nous comparons ces méthodes en termes de sécurité et de praticité, offrant des recommandations pour choisir la meilleure solution en fonction des besoins spécifiques.

SECURISATION DES CLES PRIVEES ET PUBLIQUES

RISQUES ET VULNERABILITES

Une analyse approfondie des principales menaces pesant sur les clés privées et publiques est présentée, incluant le phishing, les malwares et les attaques par force brute. Des études de cas de compromissions de clés privées illustrent les conséquences potentielles d'une sécurité inadéquate.

TECHNIQUES DE PROTECTION

Les meilleures pratiques pour sécuriser les clés sont examinées, notamment l'utilisation de la multi-signature, le cold storage et l'emploi de HSM (Hardware Security Modules). Nous discutons également des politiques et procédures recommandées pour la gestion des clés au sein des entreprises afin de renforcer la sécurité des actifs numériques.

METHODES DE RECUPERATION ET GESTION DES PERTES

PLANS DE REPRISE ET CONTINUITE

Les stratégies de récupération en cas de perte ou de compromission des clés sont détaillées, avec une exploration des outils et services disponibles pour faciliter la récupération des clés perdues. Cette section vise à garantir la continuité des opérations même en cas de perturbation majeure.

ATELIER PRATIQUE

Les participants sont engagés dans des exercices pratiques de génération et de stockage de clés privées et publiques. Des simulations de sécurisation de portefeuilles de crypto-actifs sont effectuées, permettant une mise en pratique des techniques apprises dans un environnement contrôlé.

SESSION DE CLOTURE : SYNTHESE ET Q&R

Récapitulatif des Concepts et Techniques Appris

La session finale offre un récapitulatif approfondi des concepts et des techniques enseignées tout au long du programme. Nous discutons de l'importance critique de la sécurisation des clés dans le contexte des crypto-actifs et explorons les applications futures de ces connaissances. Les participants ont l'occasion de poser des questions et de bénéficier de réponses détaillées pour clarifier les concepts abordés et envisager des stratégies de sécurité adaptées à leurs besoins spécifiques.