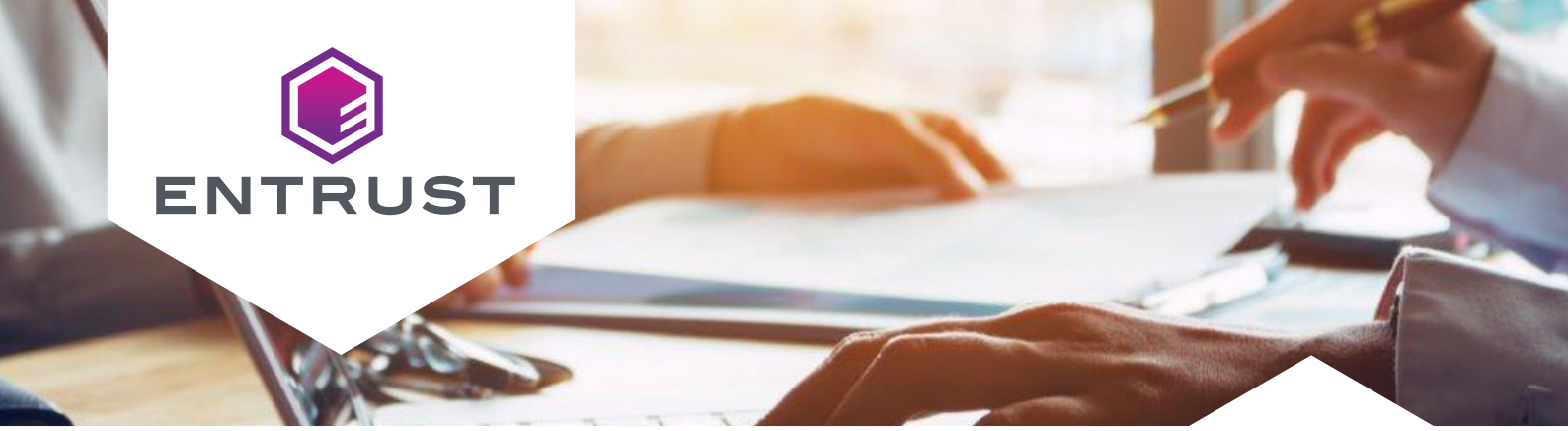

Sécuriser la blockchain

Une sécurité de haut niveau pour la blockchain

CARACTÉRISTIQUES

- Traiter le code sensible au sein d'un module matériel de sécurité (HSM) de confiance
- Prendre en charge un nombre croissant d'applications avec divers algorithmes de chiffrement à courbe elliptique
- Permettre une évolutivité des fonctions de chiffrement avec des déploiements de HSM regroupés
- Accélérer les mises en œuvre avec les services professionnels Entrust

Blockchain : possibilités et obstacles

Les technologies de blockchain et du registre distribué (DLT) représentent de nouvelles opportunités importantes, tant pour les organisations établies que pour les nouveaux arrivants sur le marché. La mise en œuvre de la blockchain peut potentiellement modifier les cas d'utilisation spécifiques des entreprises afin de simplifier les opérations, de réduire les coûts et de rationaliser les transactions.

L'un des principaux obstacles à l'adoption généralisée de la blockchain est la sécurité. Les cas d'utilisation tels que la compensation et le règlement, les paiements, les soins de santé, le commerce, la finance et la conformité aux réglementations gouvernementales exigent une sécurité de haut niveau.

Les organisations continuant à trouver de nouveaux cas d'utilisation novateurs pour la blockchain, la sécurité doit être intégrée dès le départ. Ce n'est qu'en veillant à ce que chaque transaction soumise à la blockchain soit signée numériquement que nous pourrons faire progresser notre utilisation de cette technologie de transformation et obtenir les résultats qu'elle promet. Il est donc impératif de sécuriser les clés de signature utilisées dans le processus de la blockchain et de protéger la logique du consensus contre toute modification.

Protection des clés de signature

Génération et protection des clés de signature au sein de HSM certifiés FIPS et Critères Communs

Protection des processus de signature

Contrôle du processus de signature à l'aide de l'environnement d'exécution CodeSafe nShield

Soutien pour les applications multi-signatures

Assistance au chiffrement

- Courbes elliptiques supportées :
  - secp256k1, ECDSA
  - Ed25519, EdDSA
- Hachage :
  - SHA-2
  - RIPEMD-160
- Dérivation des clés :
  - Hyperledger Client Dérivation des clés

Assistance à la mise en œuvre fournie par Les services professionnels Entrust

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Sécuriser la blockchain

Protéger les clés, protéger le système

Comme pour toute infrastructure basée sur le chiffrement, la protection des clés fondamentales est primordiale pour assurer la sécurité d'un système de blockchain. Le succès d'un système de blockchain dépend de la solidité des pratiques de protection des clés qu'offrent les HSM, et de leur capacité à s'adapter aux exigences du modèle du registre distribué.

Notre approche

Entrust aide à relever les défis de sécurité fondamentaux associés aux mises en œuvre de la blockchain : la protection des clés de signature et la logique de consensus. Grâce aux HSM nShield®, les entreprises peuvent :

- Signer des transactions en toute confiance en utilisant les algorithmes ECC comme secp256k1, Edwards Curve (Ed25519) et autres
- Protéger leurs clés de signature dans un périmètre matériel certifié FIPS et inviolable
- Protéger la logique commerciale derrière le processus de signature en utilisant la fonctionnalité CodeSafe unique du HSM nShield

Les transactions soumises à la blockchain sont signées numériquement à l'aide d'une clé privée afin de confirmer que l'entrée provient du prétendu utilisateur et d'empêcher toute altération. Les HSM nShield de Entrust protègent les clés racines sous-jacentes qui sont utilisées pour la délivrance et la révocation des clés privées.

Pour garantir que seules les transactions autorisées et conformes sont ajoutées à la blockchain, la fonctionnalité unique du HSM nShield, CodeSafe, fournit un environnement sécurisé dans lequel le code de la logique de consensus peut s'exécuter. Parce qu'il est logé dans les limites sécurisées du HSM nShield, CodeSafe offre une protection certifiée FIPS 140-2 niveau 3 pour vos codes les plus sensibles.

En outre, grâce à des dizaines d'années d'expérience, l'équipe des services professionnels Entrust peut aider à mettre en œuvre une application de blockchain sécurisée et efficace, s'appuyant sur une base de confiance des HSM nShield.

Les HSM de Entrust

Les HSM nShield d'Entrust représentent l'une des solutions HSM les plus performantes, les plus sécurisées et les plus faciles à intégrer, permettant de respecter les réglementations et de fournir les plus hauts niveaux de sécurité pour les données et les applications des entreprises, des organismes financiers et des administrations publiques. Notre architecture de gestion de clés Security World permet un contrôle granulaire et très robuste de l'accès aux clés et de leur usage.

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur **entrust.com/fr/HSM**
Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com