Protección del Blockchain

Seguridad de alta garantía para blockchain

CARACTERÍSTICAS PRINCIPALES

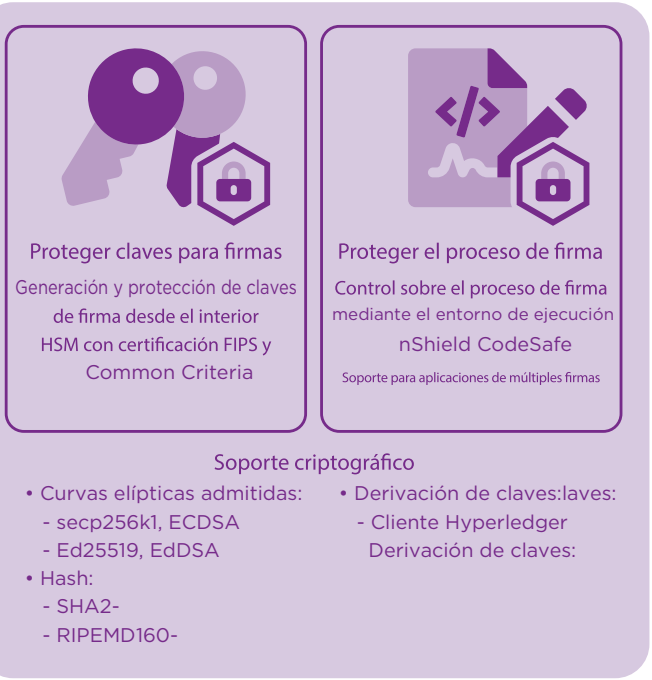
- Procese códigos confidenciales dentro de una raíz de confianza del módulo de seguridad de hardware (HSM)
- Admita aplicaciones cada vez mayores con diversos algoritmos de criptografía de curva elíptica (ECC)
- Escale las funciones criptográficas con implementaciones de HSM en clúster
- Acelere las implementaciones con los servicios profesionales de Entrust

Blockchain: oportunidades y obstáculos

Las tecnologías blockchain y de de libro mayor distribuido representan nuevas oportunidades importantes tanto para las organizaciones establecidas como para los nuevos participantes del mercado. Las implementaciones de blockchain cuentan con el potencial de cambiar fundamentalmente casos de uso de negocios específicos para simplificar las operaciones, reducir los costos y optimizar las transacciones.

Uno de los principales obstáculos para la adopción más amplia de blockchain es la seguridad. Casos de uso tales como compensación y liquidación, pagos, atención médica, comercio, finanzas y cumplimiento de las regulaciones gubernamentales, requieren de una seguridad de alta confiabilidad.

A medida que las organizaciones continúan encontrando casos de uso nuevos e innovadores para blockchain, la seguridad debe incorporarse desde el principio. Solo asegurándonos de que cada transacción enviada al blockchain esté firmada digitalmente podemos avanzar en el uso de esta tecnología transformadora y cosechar las recompensas que promete. Se vuelve por tanto un imperativo asegurar las claves de firma utilizadas en el proceso de blockchain y salvaguardar la lógica de consenso contra la manipulación.



Soporte de implementación proporcionado por Servicios profesionales de Entrust

APRENDA MÁS EN ENTRUST.COM/HSM

Protección del Blockchain

Proteger las claves, proteger el sistema

Al igual que con cualquier infraestructura basada en criptografía, la protección de las claves subyacentes es fundamental para garantizar la seguridad de un sistema blockchain. Un sistema de blockchain exitoso depende de las sólidas prácticas de protección de claves que ofrecen los HSMs, así como de su capacidad de escalar para atender las demandas del modelo de libro mayor distribuido.

Nuestro enfoque

Entrust ayuda a abordar los desafíos de seguridad fundamentales asociados con las implementaciones de blockchain: proteger las claves de firma y la lógica de consenso. Con los HSMs nShield®, las empresas pueden:

- Firmar transacciones con confianza utilizando algoritmos ECC como secp256k1, Edwards Curve (Ed25519) y otros
- Proteger sus claves de firma dentro de un límite de hardware a prueba de manipulaciones indebidas y certificado por FIPS
- Proteger la lógica empresarial detrás del proceso de firma utilizando la capacidad única CodeSafe del HSM nShield

Las transacciones enviadas al blockchain se firman digitalmente con una clave privada para confirmar que la entrada proviene del presunto usuario y evitar cualquier alteración. Los HSMs nShield de Entrust protegen las claves de raíz subyacentes que se utilizan para la emisión y revocación de claves privadas.

Para ayudar a garantizar que solo se agreguen transacciones autorizadas y compatibles con el blockchain, la capacidad única de CodeSafe del HSM nShield proporciona un entorno seguro donde se puede ejecutar el código lógico de consenso. Debido a que se encuentra alojado dentro de los límites seguros del HSM nShield, CodeSafe ofrece protección certificada FIPS 140-2 Nivel 3 para su código más confidencial.

Además, basándose en décadas de experiencia, el equipo de Servicios Profesionales de Entrust puede ayudar a implementar una aplicación de blockchain segura y efectiva construida sobre una base segura de HSMs nShield.

HSMs de Entrust

Los HSMs de Entrust nShield se encuentran entre las soluciones de HSMs de mayor rendimiento, más seguras y fáciles de integrar que se encuentran disponibles, lo cual facilita el cumplimiento normativo y ofrece los niveles más altos de seguridad de datos y aplicaciones para organizaciones empresariales, financieras y gubernamentales. Nuestra exclusiva arquitectura de administración de claves Security World proporciona controles sólidos y granulares sobre el acceso y uso de claves.

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para conocer más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Aprenda más en
entrust.com/HSM

ENTRUST

Contáctenos:
HSMinfo@entrust.com