Blockchain sichern

Höchste Sicherheit für die Blockchain

ECKPUNKTE

- Verarbeiten Sie sensiblen Code mit einem Hardware-Sicherheitsmodul (HSM) als Vertrauensanker
- Unterstützen Sie mehr und mehr Anwendungen mit unterschiedlichen ECC-Algorithmen (Elliptic Curve Cryptography)
- Skalieren Sie kryptographische Funktionen mithilfe von HSM-Clustern
- Beschleunigen Sie die Umsetzung mit Unterstützung des Professional Services Teams von Entrust

Blockchain: Chancen und Hindernisse

Blockchain- und Distributed-Ledger-Technologie bieten etablierten Unternehmen und neuen Marktteilnehmern erhebliche Chancen. Die Blockchain vereinfacht die Abläufe, senkt die Kosten und optimiert Transaktionen. Damit hat sie das Potenzial, bestimmte Geschäftsanwendungsfälle grundlegend zu verändern.

Einer großflächigen Einführung der Blockchain stehen jedoch Sicherheitsbedenken gegenüber. Geschäftsanwendungen wie Clearing und Abwicklung sowie Zahlungen, Bereiche wie das Gesundheitswesen, Finanzen und Handel sowie die Einhaltung staatlicher Verordnungen erfordern ein hohes Maß an Sicherheit.

Unternehmen entdecken immer mehr neue und innovative Anwendungsmöglichkeiten für die Blockchain. Bei deren Umsetzung ist Sicherheit von Anfang an ein Muss. Wir können diese transformative, vielversprechende Technologie nur dann in größerem Maße nutzen und von ihr profitieren, wenn wir gewährleisten, dass alle an die Blockchain gesendeten Transaktionen digital signiert sind. Daher ist es unumgänglich, dass die beim Blockchain-Verfahren eingesetzten Schlüssel gesichert und die Konsensus-Algorithmen vor Manipulation geschützt werden.

Schützt Signaturschlüssel

Erstellen sowie Schutz von Signaturschlüsseln innerhalb nach FIPS und Common Criteria zertifiziertes HSM

Schützt Signaturverfahren

Kontrolle über das Signaturverfahren mithilfe der Ausführungsumgebung nShield CodeSafe

Unterstützung von Multi-Signatur-Anwendungen Signaturen

Krypto-Support

- Unterstützte elliptische Kurven:
  - secp256k1, ECDSA
  - Ed25519, EdDSA
- Hash:
  - SHA-2
  - RIPEMD-160
- Schlüsselableitung:
  - Hyperledger Client Schlüsselableitung

Die Bereitstellung kann durch Professional Services von Entrust unterstützt werden.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Blockchain sichern

Wer die Schlüssel schützt, schützt das gesamte System

Wie bei allen auf Kryptographie basierenden Infrastrukturen ist der Schutz der zugrunde liegenden Schlüssel auch im Fall der Blockchain entscheidend für die Sicherheit des Systems. Ein gut funktionierendes Blockchain-System erfordert, dass Schlüssel mithilfe strikter Verfahren durch HSM geschützt werden. Diese müssen zudem in der Lage sein, die Anforderungen des Distributed-Ledger-Modells zu erfüllen.

Unser Ansatz

Entrust unterstützt Unternehmen dabei, die grundlegenden Sicherheitsprobleme von Blockchain-Bereitstellungen zu lösen: die Signaturschlüssel und Konsensus-Algorithmen schützen. Mit den nShield® HSM können Unternehmen:

- mit ECC-Algorithmen wie unter anderem secp256k1 und Edwards Curve (Ed25519) Transaktionen sicher signieren
- ihre Signaturschlüssel mit FIPS-zertifizierter, manipulationssicherer Hardware schützen
- mit der einzigartigen CodeSafe-Funktion der nShield HSM die Geschäftslogik schützen, die hinter dem Signaturprozess steht

An die Blockchain übermittelte Transaktionen werden mit einem privaten Schlüssel digital signiert. Dadurch wird bestätigt, dass diese vom mutmaßlichen Benutzer stammen. Änderungen werden so verhindert. Die nShield HSM von Entrust schützen die zugrunde liegenden Root-Schlüssel, mit denen die privaten Schlüssel ausgestellt und widerrufen werden.

Sie bieten eine sichere Umgebung für die Ausführung der Konsensus-Algorithmen, damit tatsächlich nur autorisierte und den Vorgaben entsprechende Transaktionen der Blockchain hinzugefügt werden können. CodeSafe wird in den sicheren Grenzen der nShield HSM bereitgestellt und schützt so Ihren sensiblen Code gemäß FIPS 140-2 Level 3.

Darüber hinaus unterstützt das Professional Services Team von Entrust auf Grundlage seiner jahrzehntelangen Erfahrung Unternehmen bei der Bereitstellung einer sicheren und effektiven Blockchain-Anwendung auf der Basis von nShield HSM.

HSM von Entrust

nShield HSM von Entrust gehören zu den leistungsstärksten, sichersten und am einfachsten integrierbaren HSM-Lösungen am Markt. So erleichtern sie die Einhaltung regulatorischer Vorschriften und bieten höchste Daten- und Anwendungssicherheit für Unternehmen sowie Finanz- und Regierungsbehörden. Unsere einzigartige Security World-Architektur für die Schlüsselverwaltung bietet starke, granulare Schlüsselkontrollen hinsichtlich Zugriff und Nutzung.

Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

Weitere Informationen auf

entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com