ENTRUST

Securing Blockchain

High assurance security for blockchain

HIGHLIGHTS

- Process sensitive code within a hardware security module (HSM) root of trust
- Support increasing applications with diverse elliptic curve cryptography (ECC) algorithms
- Scale cryptographic functions with clustered HSM deployments
- Expedite implementations with Entrust's Professional Services

Blockchain: opportunities and obstacles

Blockchain and distributed ledger technologies represent significant new opportunities for both established organizations and new market entrants. Blockchain implementations have the potential to fundamentally change specific business use cases to simplify operations, reduce costs and streamline transactions.

One of the primary roadblocks to the broader adoption of blockchain is security. Use cases such as clearing and settlement, payments, healthcare, trade, finance, and compliance to government regulations require high assurance security.

As organizations continue to find new and innovative use cases for blockchain, security must be incorporated from the outset. Only by ensuring that each transaction submitted to the blockchain is digitally signed can we advance our use of this transformative technology and reap the rewards it promises. Securing the signing keys used in the blockchain process, and safeguarding the consensus logic from tampering, is therefore imperative.

Protect signing keys

Generation and protection of signing keys within FIPS and Common Criteria-certified HSM

Protect signing process

Control over the signing process using the nShield CodeSafe execution environment

Support for multi-signature applications

Crypto support

- Elliptic curves supported:
  - secp256k1, ECDSA
  - Ed25519, EdDSA
- Hash:
  - SHA-2
  - RIPEMD-160
- Key derivation:
  - Hyperledger Client Key Derivation

Implementation support provided by Entrust professional services

LEARN MORE AT ENTRUST.COM/HSM

Securing Blockchain

Protect the keys, protect the system

As with any crypto-based infrastructure, protecting underpinning keys is paramount to ensuring a blockchain system's security. A successful blockchain system depends on the strong key protection practices afforded by HSMs, and their ability to scale to support the demands of the distributed ledger model.

Our approach

Entrust helps address fundamental security challenges associated with blockchain implementations: protecting the signing keys and consensus logic. With nShield® HSMs, enterprises can:

- Sign transactions with confidence using ECC algorithms like secp256k1, Edwards Curve (Ed25519) and others
- Protect their signing keys within a FIPS-certified, tamper-resistant hardware boundary
- Protect the business logic behind the signing process using nShield HSM's unique CodeSafe capability

Transactions submitted to the blockchain are digitally signed using a private key to confirm that the entry comes from the purported user and to prevent any alterations. Entrust nShield HSMs protect the underlying root keys that are used for the issuance and revocation of private keys.

To help ensure that only authorized and compliant transactions are added to the blockchain, nShield HSM's unique CodeSafe capability provides a secure environment where the consensus logic code can execute. Because it is housed within the secure boundary of the nShield HSM, CodeSafe delivers FIPS 140-2 Level 3 certified protection for your most sensitive code.

Additionally, drawing on decades of experience, Entrust's Professional Services team can help implement a secure and effective blockchain application built on a secure foundation of nShield HSMs.

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at

entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com