nCipher

www.ncipher.com

High assurance security for blockchain

- Processing sensitive code within the HSM's secure boundaries reduces risk
- Support for growing list of elliptic curves increases the power of blockchain implementations
- nShield HSMs can be clustered to scale cryptographic functions without sacrificing security
- nCipher's Professional Services team offers decades of experience to help expedite implementations

Securing Blockchain

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 in some of its most relevant use cases—clearing and settlement, payments, health care, trade finance, government and regulations, and more—is the resolution of a critical issue: 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 using signing keys that are properly secured, and that the consensus logic is safeguarded against tampering, can we advance our use of this transformative technology and reap the rewards it promises.

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 nCipher Professional Services

Securing Blockchain

PROTECT THE KEYS, PROTECT THE SYSTEM

As with any crypto-based infrastructure, protecting 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 these HSMs must deliver the scaling and flexibility a decentralized blockchain model needs.

OUR APPROACH

nCipher 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'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. nCipher 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's unique CodeSafe capability provides a secure environment where the consensus logic code can execute. Because it is housed within the secure boundaries of the nShield HSM, CodeSafe delivers FIPS 140-2 Level 3 certified protection for your most sensitive code.

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

ABOUT NSHIELD HSMS

nShield HSMs

nShield HSMs offer tamper-resistant, FIPS- and Common Criteria-certified key generation and protection that meets the highest security and compliance standards. nShield HSMs also support a growing list of elliptic curves and are trusted by the most security-conscious organizations around the world to protect their mission-critical signing keys and cryptographic applications. Further, nShield HSMs can be clustered to scale with demand for increasing throughput.

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

Search: nCipherSecurity

nCIPHER