

THALES
CYBERSECURITY

Executive Guide to Securing Digital Assets:

Elevate Digital Asset Security with HSMs

cpl.thalesgroup.com

Digital Assets Landscape



What are Digital Assets?

Emergence of Web3 is accelerating Digital Assets Development

Web3 = Decentralized Internet

- represents the internet's shift to a **permissionless, decentralized model** where users own their data and interact with applications (dapps) running on **blockchain infrastructure**.

Digital Assets: (Blockchain-Based)

- These are digital representations of value that rely on distributed ledger technology (like blockchain) for secure ownership and transfer. Examples include:

Together, **they form a symbiotic relationship** whereby **Web3** expands the use cases and accessibility of **digital assets**, and digital assets enable the economic and operational functions of Web3.

Cryptocurrencies
Digital currencies like Bitcoin and Ethereum

NFTs (Non-Fungible Tokens)
Unique digital assets representing ownership of digital or physical items, like digital art or virtual real estate

Tokens:
Digital representations of assets (like a tokenized house deed) that are stored on a blockchain, such as Stablecoins

Central Bank Digital Currencies (CBDCs)
A digital form of a country's fiat currency, issued and regulated by its central bank

Same root problem: Who controls the private key?

Digital Asset Trust Model

Traditional Finance:

Trust the institution

Digital Assets:

Trust the cryptographic key

Compromised key = compromised ownership

Same root problem: Who controls the private key?
HSM = The Foundation of Digital Trust for both worlds.

Digital Asset Security Challenge



Digital Assets Become a Core Enterprise Strategy

Digital Assets Are Going Mainstream: Enterprise Adoption Accelerates

Gartner

- "Gartner forecasts that the business value generated by blockchain will grow rapidly, reaching $3.1 trillion by 2030." **Digital Disruption Profile: Blockchain's Radical Promise Spans Business and Society**
- "By 2026, **70% of large enterprises** will experiment with or deploy blockchain/distributed ledger technology (DLT) in production." Gartner Press Release, Oct 2024

Deloitte's CFO Signals™ survey

"Nearly **1 in 4 CFOs** expect their finance teams to **adopt digital currency** within two years."

"… more than one-third **(37%) of CFOs** say they have already engaged their boards in conversations about **cryptocurrency**, while **41%** report discussions with their chief information officers."

Coinbase Institutional Report

81% of Fortune 100 companies have **on-chain activity** (wallets, staking, tokenization pilots). Coinbase Institutional, Q1 2025

Digital Assets Ecosystems

Issuers	Stablecoins
	CBDCs
	Tokenized Assets
Custodians	Banks
	Exchanges
	Digital Asset Custodians
Infrastructure	Wallet Providers
	MPC Platforms
	Blockchain Networks

The Era of Digital Assets: Billions Lost, Trust at Risk



Digital assets have gone mainstream, with stablecoins now **processing more value** than Visa and Mastercard combined.

*Digital assets include **cryptocurrencies, stablecoins, tokenized assets** and represent the new foundation of global finance.*

*Over **$2.17B stolen** from cryptocurrency platforms in 2025 alone, already surpassing all of 2024.*

*Nearly half of all losses come from private-key compromise **(43.8 percent)**, making key security the single biggest point of failure.*



Securing Digital Assets: Key Challenges

Private Key Challenge

- **Irreversible Ownership:**
  - No password reset, chargeback, or transaction reversal.
  - A compromised key can mean permanent asset loss.
- **The Critical Trust Anchor:**
  - Private keys control digital asset ownership.
  - A single compromised key can expose treasury and customer assets.

Digital Asset Threat Landscape

- **External Threats**
  - Phishing and social engineering attacks.
  - Advanced malware targeting key usage.
  - Side-channel attacks against cryptographic operations.
- **Insider and Operational Risks**
  - Malicious or negligent insiders.
  - Accidental exposure through code, logs, or cloud storage.

Regulatory Compliance

- **Rising Regulatory Expectations:** Regulators increasingly require institutional-grade security controls.
- **Digital Asset Custody Requirements:** Traditional custody and security standards are being applied to digital assets.
- **Examples in APAC:**
  - **HK:** SFC VATP, Stablecoins Ordinance
  - **SG:** MAS TRM
  - **Taiwan:** Taiwan VASP Association (TVA) Self-Regulatory Code
  - **South Korea:** KoFIU and ISMS requirements

Operational Resilience

- **Cold Storage Security:**
  - Maximum protection through offline key storage.
  - Limited operational flexibility
- **Hot Wallet Operations**
  - Enables real-time transactions and trading.
  - Increases exposure to cyber threats.

The Balance

Securely manage assets across hot, warm, and cold environments.

Risks of Software-Based Key Management

- **System Vulnerabilities:** Keys exposed through OS, application, or malware attacks.
- **Weak Access Controls:** Limited governance and policy enforcement.
- **Co-Located Keys and Applications:** Compromised applications can expose keys.
- **Weak Key Generation:** Poor entropy can weaken cryptographic security.

Protecting Digital Assets:

Why HSMs Matter More Than Ever



HSMs: A Proven Enabler of Trust Across the Digital Asset Custody Market



Institutional & Service-Custody Providers

Rely on HSM-based key protection to meet compliance, insurance, and assurance requirements.



Traditional Financial Institutions

Adopt HSMs to extend their custody, settlement, and digital-asset offerings with regulatory level trust.



Infrastructure/ Tech Providers

Integrate HSM trust anchors into platforms for secure key management, signing, and policy enforcement.



Self-custody/ Wallets

Use HSM-backed security to protect keys, enable recovery, and ensure authentic ownership for users.

Luna HSM provides a secure foundation of trust behind today's leading digital asset custody solutions.

From Legacy to Digital:

How HSMs Secure the Future of Global Finance

Traditional



Legacy infrastructures rely on perimeter-based security and siloed infrastructures that were not built for tokenized or decentralized finance.

HSM



HSMs bridge legacy and digital finance by securing keys, enabling trusted signing, and extending assurance from on-premises to cloud and blockchain.

Digital



Modern finance need to implement a hardware root of trust to protect digital-asset custody, trading, and settlement with integrity and compliance.

As adoption accelerates across digital assets, Luna HSMs ensures trust in every transaction.

Why Luna HSMs for Securing Digital Assets



What Luna HSM Delivers for Digital Assets:
A Secure and Compliant Signing Solution

Full Private Key Ownership

Keys stay protected inside **FIPS 140-3 Level 3 and Common Criteria-certified** hardware, ensuring complete control and trust.

Policy-Based Signing Control

Set and enforce signing policies across **hot, warm, and cold environments** for flexible, secure operations.

Built-In Regulatory Compliance

Enables compliance with global standards including **MAS, HKSFC, PCI, FINMA, BaFin, and MiCA.**



How Luna HSM Reduces Risks in Digital Assets?

Keys secured in tamper-resistant hardware

Master private keys always protected by hardware

Crypto operations and authentication processed in a secure environment

Keys generated with strong hardware-based entropy

Crypto agility ensured with updates against evolving threats (e.g., quantum)

Certified to latest global standards: FIPS 140-3 L3, Common Criteria



Why the World's Largest Financial Institutions Rely on Luna HSM

1. **Proven Compliance:** First HSM validated to FIPS 140-3 Level 3, giving institutions confidence in meeting regulatory requirements.

2. **Trusted by Global Financial Leaders:** Some of the world's largest financial institutions and trusted brands rely on Luna HSMs to secure their valuable assets.

3. **Market Leadership:** We lead the global HSM market in shipments, market share, and integrations, backed by proven reliability and continuous innovation.

4. **Scale You Can Rely On:** Thales secure the most valuable corporate and government information, including more than $10 trillion of financial transactions every day.

5. **Future-ready security:** Luna HSMs help enable quantum-safe cryptographic workflows by incorporating NIST-standardized PQC algorithms, including ML-KEM (FIPS 203) and ML-DSA (FIPS 204), to protect keys and support post-quantum use cases.



Luna HSMs for Digital Assets

The Foundation of Digital Trust



Luna HSM for Digital Assets:
The Hardware Root of Trust

MPC

Splits key operations across multiple parties.

✓ Removes single point of failure

✗ Complex and computationally heavy

HSM

Trusted root of security

Anchors keys, policies, and operations.

✓ Elevates MPC and Multi-Sig with hardware assurance



Luna HSM acts as the trusted partner.

Enhancing MPC and Multi-Sig with compliance and resilience, through a proven root of trust.

Multi-Sig

Requires multiple private keys to approve transactions

✓ Simple, transparent governance

✗ On-chain overhead, less flexible

Luna HSM for Digital Assets:
The Hardware Root of Trust

Issuer / Treasury

Platform / Wallet



Luna HSM
Network, USB, PCIe and Cloud (DPoD)

Blockchain

Compliance / Regulators

Protect Keys in Hardware

Control Key Access

Sign Transactions Securely

Thales Accelerate:

Key Technology Partners in the Digital Assets Market

Fireblocks

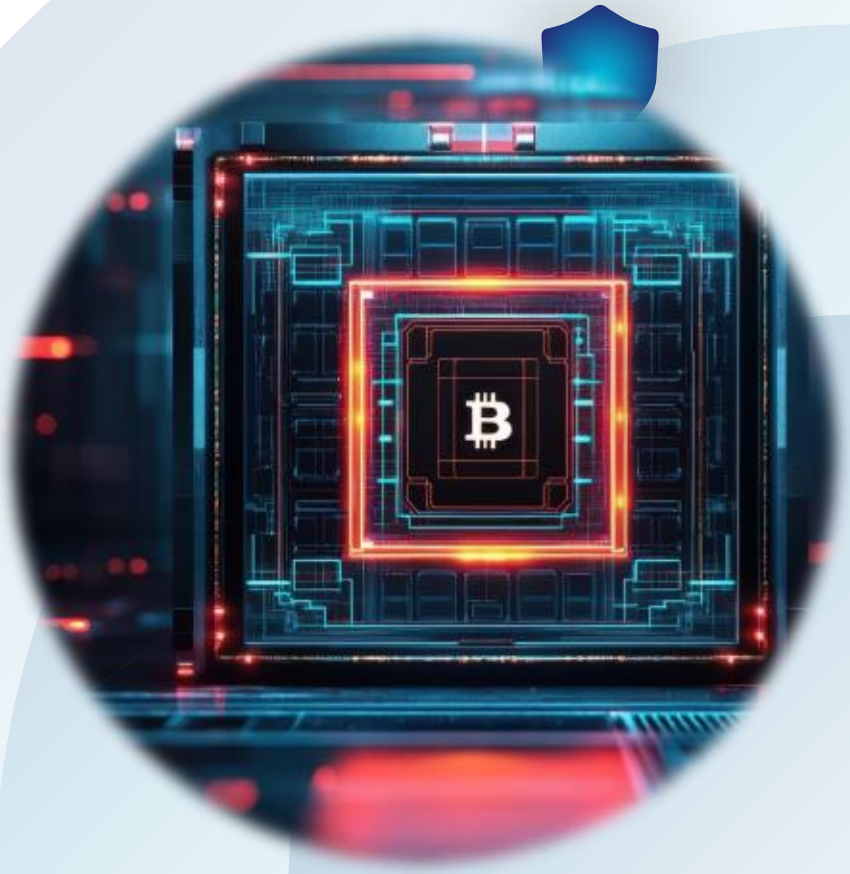
Dfns

kaleido

ripple

TAURUS

consensys



Advance Your Digital Asset Security Strategy



Assess your digital asset security architecture



Learn how HSMs **strengthen** custody and transaction signing



Explore deployment options for your environment



Speak with a Thales digital asset security specialist

Contact Us

For contact information, please visit
cpl.thalesgroup.com/contact-us

