thalescpl.com

THALES

Securing Blockchain with Ledger and SafeNet ProtectServer HSMs

Hardware Security Architecture for Multi-Currency & Multi-Signature Wallets

Secure cold storage of cryptocurrencies such as Bitcoin or Ethereum, is a difficult and complex challenge. Traditional paper wallet-based solutions may be effective for the most basic use cases, but they present a substantial challenge for more complex environments as they do not scale, or address compliance requirements for strong key management.

Thales and Ledger have partnered to create an enterprise-grade solution for secure cold storage based on SafeNet ProtectServer Hardware Security Modules (HSM) and Personal Security Devices (PSD). This solution enables multi-currency and multi-signature authorization wallet management, without any limitation of the number of accounts or addresses, and with a full customization of signature policies for each account.

Solution Features

- HSM-based management of cryptographic secrets (full isolation in encrypted chips)
- Protect the entire key lifecycle within the FIPS 140-2 validated confines of the SafeNet HSM appliance
- BIP32/BIP44 derivation of private keys for all coins, from a BIP39 unique master seed
- Provisioning key ceremony of master seed with MofN backup
- MofN signature authorization scheme based on Personal Security Devices (Ledger Blue)
- Time lock and rate limiting options
- Full signature rulesets customization for each wallet / account
- Multi-currency blockchain wallet support

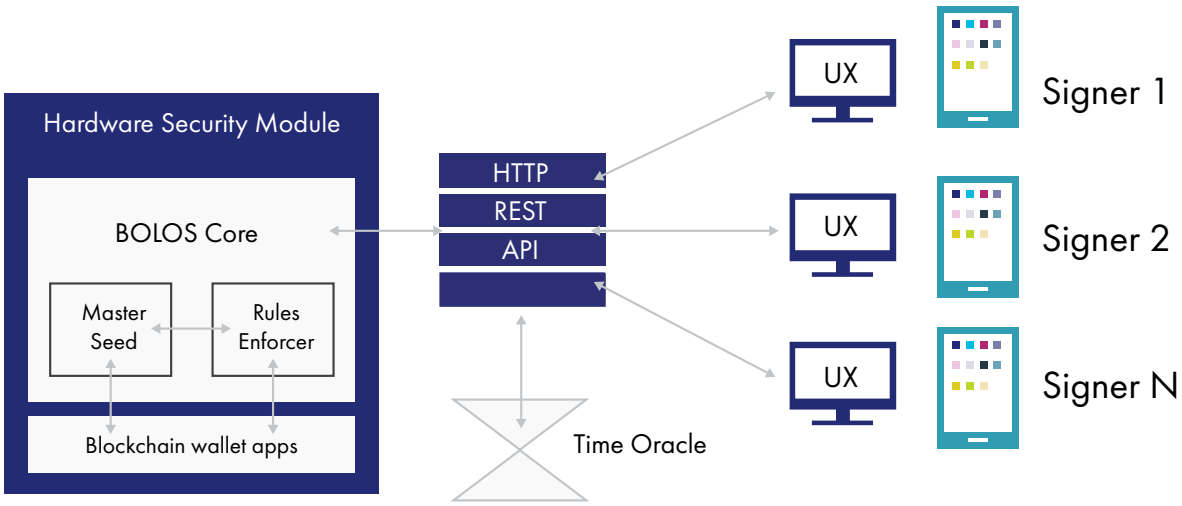
Combined Solution Benefits

- HSM hardware root of trust for private keys – your anchor of trust
- High assurance security with FIPS 140-2 Level 3 certified product
- Proven HSM market leadership
- Support for multiple blockchain wallet applications (Bitcoin, Altcoins, Ethereum, Monero, and more)
- Rules engine to manage provisioning of external signers, MofN signature authorization, internal rate limiting, and time oracle for delayed actions

Ledger Blockchain Solutions

Ledger builds solutions to bridge the physical world and the blockchain with three families of products: Personal Security Devices for end-users; Hardware Security Modules for servers; and Hardware Oracles for connected objects, machines, and the Internet of Things (IoT).

The core technology platform is a low footprint embedded Operating System (OS) built for secure elements and CPU enclaves. With an asynchronous architecture, the Ledger OS enables full orchestration of code and systems directly from the secure world.



SafeNet ProtectServer HSM from Thales

SafeNet ProtectServer HSMs are designed to protect cryptographic keys against compromise while providing encryption, signing, and authentication services.

The SafeNet ProtectServer HSM offers a unique level of flexibility for application developers to create their own firmware in the form of a Functionality Module (FM) and execute it within the secure confines of the HSM. These FMs provide a comprehensive facility to develop and deploy custom firmware.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

What is a blockchain?

- A blockchain is a distributed ledger technology that maintains a continuously growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block.
- Blockchain as a technology is not limited to cryptocurrency applications. It has the potential for enabling transaction processing efficiencies and smart contracts across many verticals including: healthcare; insurance; government; financial; and IoT.

Features:

- Inherently resistant to modification of the data
- Once recorded, the data in a block cannot be altered retroactively
- Open, distributed ledgers record transactions between two parties efficiently and in a verifiable and permanent way
- Ledger itself can also be programmed to trigger transactions automatically

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com