BLOCKCHAIN SECURITY MADE SIMPLE

THE KEY TO HSM INTEGRATION

accentureconsulting

UNLOCKING THE POTENTIAL OF BLOCKCHAIN

Blockchain has the potential to transform the way data is shared and value is transferred.

But for all the promise the technology holds, it also brings new challenges. If blockchain is to be broadly adopted in clearing and settling financial trades, payments, health care, trade finance, and for government and regulatory applications, its security must be airtight.

While the blockchain technology that underpins distributed ledgers has proven in itself to be very secure, there are many lingering questions about how to protect both the cryptographic keys that allow access to the ledger and blockchain applications. Both areas have proven to be points of vulnerability for blockchain systems.

For blockchain technology to reach its full potential, it must meet—or exceed—accepted security standards.

TODAY’S HIGH SECURITY INFRASTRUCTURE

Currently, many security-conscious institutions rely on hardware security modules (HSMs) to safeguard and manage their digital keys, protecting potential access points in virtually any application that requires secure, verified digital signatures. HSMs housed in bank data centers verify PIN numbers every time a customer withdraws cash from an ATM and validate transaction cryptograms when customers purchase goods at a merchant POS terminal. In both cases, only the HSMs under a bank’s control have access to the correct keys to perform the secure processing.

> “Leaving cryptographic keys in software sitting on a computer is the equivalent of leaving your house keys under the welcome mat.”

WHAT IS AN HSM?

An HSM is a crypto-processor that securely generates, protects, and stores keys.

HSMs have a certain level of regulatory assurance, such as the Federal Information Processing Standard (FIPS) certification, and Common Criteria, an international standard. These and other certifications ensure that each device meets strict industrial-grade security control requirements.

BENEFITS OF AN HSM:

SECURE STORAGE FOR KEYS:

The keys always live inside the secure, certified HSM boundary, rather than in software or on a hard drive, where they are vulnerable to attacks.

SOPHISTICATED CRYPTOGRAPHY:

HSMs use a certified, cryptographically secure random number generator to create keys that are of superior quality to those generated by a typical computer system.

TAMPER–RESISTANT HARDWARE:

FIPS 140-2 Level 2 and 3 certified HSMs are tested to stringent standards and are extremely difficult for unauthorized users to access.

BLOCKCHAIN'S UNIQUE SECURITY CHALLENGES

Blockchain's unique attributes will provide a new infrastructure on which the next generation of streamlined business applications will be built. But it also creates unique security challenges. Here's why:

FROM CENTRALIZED TO DECENTRALIZED

Blockchain shifts data storage and protection from a centralized to a decentralized model. In traditional centralized models, security methods can be consolidated with the technology products they serve. Blockchain, however, requires innovative security measures to protect the dynamic and highly distributed financial products the technology aims to support.

As with any crypto-based infrastructure, protecting keys is paramount to ensuring a blockchain system's security. A successful blockchain system needs highly reliable methods of interfacing with the strong key protection practices afforded by HSMs, and these HSMs must deliver the scaling and flexibility a decentralized blockchain model needs.

THE ASSET IS THE KEY

Blockchain and distributed ledger technology (DLT) applications combine the message and the asset in a single token. Once an asset is embedded into a blockchain or distributed ledger, possessing the associated cryptographic keys is the only way to retrieve or move the asset. In other words, the key becomes the asset. (By contrast, in a traditional IT model, a key protects the database, which in turn protects the data or the asset.)

INSTANT EXPLOITATION

When the key and the asset are one and the same, anyone who obtains the key can monetize and exploit the asset instantly. As we've seen in security breaches in public blockchain settings, such as Bitfinex, Mt. Gox and others, the malicious transfer of 'value' can be instantaneous, irreversible, and significant. Participants in these systems lost millions of dollars as a result of compromised security systems. It should be noted, however, that these attacks exploited vulnerabilities at the application layer—the wallets holding the keys to the assets—rather than the underlying blockchain protocol. So far, blockchain technology itself has proved tamper-resistant.

PROTECTING THE KEY IS CRITICAL

The ability to edit a distributed database broadens the technology's applicability. Accenture introduced a groundbreaking blockchain capability earlier this year that allows data within a block to be edited or removed under strict protocols in permissioned systems, leaving a scar as evidence of the edit. While the redaction capability broadens blockchain's applicability, it also makes the protection of the keys that must come together to "unlock" and relock the chain mission-critical.

BENEFITS OF CENTRALIZING CRYPTOGRAPHY ONTO HSMs

BOOST EFFICIENCY AND SCALE

HSMs can be clustered for greater performance and availability, allowing encryption functions to scale without sacrificing security.

By relieving servers from performing processor-intensive calculations, HSMs **increase operational efficiency**.

Moving the cryptographic functions from software to dedicated hardware devices **reduces the risk** of processor errors.

BOOST SECURITY

The keys stored in the Thales HSM architecture cannot be extracted and used except under a highly controlled protocol, making it possible to **keep track of who has access** to keys.

To mount a successful attack, attackers either need to have administrative privileges, access to data before it is encrypted, or **physical access to the HSM(s)**.

In HSM setups such as the Thales Security World architecture, attackers would need to possess a **quorum of cards** and their associated pass phrases in order to access the Control and Infrastructure keys.

BOOST COMPLIANCE

79% of auditors recommend an HSM over a software solution.

FIPS 140-2 Level 3 and Common Criteria EAL 4+ certifications means Thales Shield Edge, Solo, and Connect HSMs are positioned for use in **highly regulated environments**.

> “In order to create scalable, efficient, and highly secure blockchain solutions, Accenture, a leader in blockchain solutions, is collaborating with Thales, the HSM gold standard.”

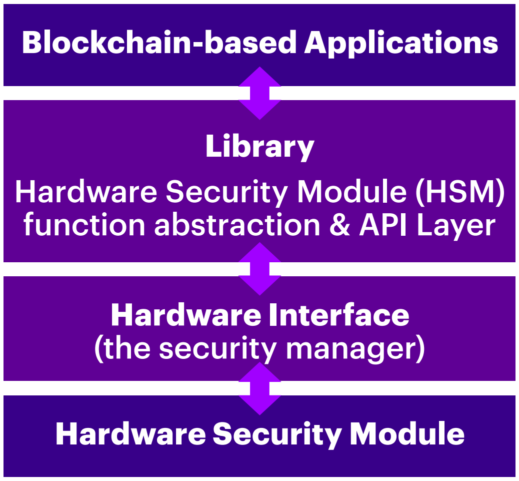
OUR SOLUTION

EASY INTEGRATION

The solution follows a patent-pending, general-purpose approach in creating a library that helps integrate hardware security devices with blockchain technology.

The library connects an HSM to a security manager, whose role is to manage the encryption and decryption of sensitive client data. The security manager is housed on premises to ensure that each participant in the blockchain protocol has end-to-end control over the cryptographic functionalities associated with relevant data transactions.

The creation of this library allows clients to use highly secure methods of cryptography, while also benefiting from emerging blockchain technology applications.


Blockchain-based Applications
Library
Hardware Security Module (HSM) function abstraction & API Layer
Hardware Interface
(the security manager)
Hardware Security Module

Accenture's solution creates a library that integrates blockchain applications with an HSM.

UNLOCK THE BENEFITS OF BLOCKCHAIN

The library allows users to write blockchain business applications at the top that are then implemented as blockchain applications in the middle layer. After that, they are integrated with hardware so that all keys are stored securely inside an HSM device. Once keys are created and stored in an HSM architecture, they are essentially impossible for unauthorized users to extract.

In this way, solutions move directly from the API to the HSM, rather than sitting in software on a server. No application could or should go into production until developers can secure keys in this way. It is impossible to protect millions of dollars of assets with keys that are simply stored on a server or in the software. Our solution provides the missing link that will give security-conscious institutions the reassurance they need to use blockchain.

EFFICIENT, EFFECTIVE DATA SECURITY, WITHOUT COMPROMISE

nShield HSMs integrate with Thales Security World architecture to abstract keys into fragments that live within the secure, FIPS-certified HSM boundaries. Administrators use smart cards with nShield HSMs, along with pass-phrases, to access and manage their keys within this unique architecture. This highly secure architecture also delivers the flexibility to readily add nShield HSMs to an organization's existing security world as performance needs grow, as well as the benefit of seamless failover, load-balancing, backup, and maintenance. With nShield HSMs, blockchain customers can obtain high-assurance security without compromising efficiency.

ACCENTURE IS COMMITTED TO MAKING BLOCKCHAIN A REALITY FOR CLIENTS

This turn-key solution provides the missing link that will give security-conscious institutions the assurance that no matter what blockchain solution they choose, it can have a highly-secure infrastructure that is virtually impenetrable.

Are you ready to make blockchain a reality for your institution?

CONTACT

To learn more about the benefits of blockchain for your business or discuss how any of the ideas in this paper could improve your organization's performance, please visit accenture.com/blockchain or contact:

ACCENTURE

David Treat
Managing Director – Financial Services
Blockchain Lead
david.b.treat@accenture.com

John Velissarios
Security Principal Director
john.velissarios@accenture.com

Sarah Francis
Delivery Lead – UKI Innovation
Programme
sarah.l.francis@accenture.com

Laurence Freeman
Analyst – Blockchain
laurence.freeman@accenture.com

Callum Hyland
Engineer – Blockchain
callum.hyland@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ABOUT THALES E-SECURITY

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.