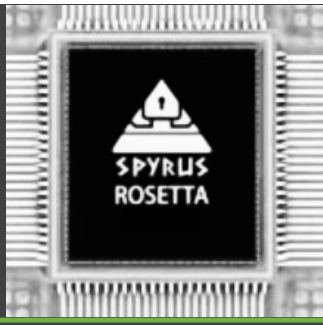
SPYRUS®

SPYRUS Blockchain Security

Ensuring Data Provenance in Trustworthy Systems with K of N Multiparty Access and Hardware Roots of Trust



Hardware Approach to Blockchain Security Offsets Vulnerabilities in a Wide-Open Environment

The efficiency and process streamlining that blockchain offers to business and investment has been established in recent years. The potential for providing rapid transit for funds, goods and services and a host of digital assets packaged as tokens appears to be unlimited. Technology embodied in smart contracts and decentralized applications (DApps) have extended far past the initial financial services applications to defense, critical infrastructure, manufacturing, marketing, distribution and supply chain management. The recent explosion in IoT technology and its obvious synergy with blockchain promises untapped power and reach of blockchain-enabled technology. Achieving its potential will require early addressing of vulnerabilities and ensuring security in the design and implementations of both.

Hardware Security Modules (HSM) provide simple and proven functionality to address the protection of blockchain end-point peer transaction devices. HSMs fill the gaps in secure digital storage, governance of security, and overall provenance of stakeholder data and operations necessary for a trusted global infrastructure based on the wide-open Internet. The vulnerability landscape that software solutions alone cannot address are vital to securing the vital privacy of cryptographic keys and critical parameters which are essential to the protection of point-to-point or shared content. Safeguarding all stakeholder's investment in blockchain applications with HSM technology makes absolute sense as a highly cost effective, powerful defense to bridge the gaps of software security solutions that are acknowledged to be much vulnerable to penetration by persistent and capable attackers.

With ever increasing stakes in a globally distributed enterprise, end-point transaction devices, e.g., a wallet, sensor aggregation node, or a medical monitoring apparatus, we must keep pace with developing threats to provide the best security available. Only hardware protected cryptography can ensure the quality of the protection and the absence of any backdoor attacks. Hardware with quality and effectiveness certified by independent laboratories against rigid internationally-recognized government and industry standards such as U.S. government FIPS-140-2 fulfils this criterion.

SPYRUS HSM products, available in different form factors, fulfil this security, protection and trust gap. Whether furnished as a P-3X USB 3.0 encrypted storage drive, a bootable Windows To Go or Linux2Go Live Drive, a Rosetta USB digital signature/ OTP/ authentication device, or a microSD TrustedFlash® memory/ bootable card, all SPYRUS HSMs include an integrated Rosetta® Micro with our embedded SPYCOS® operating system, the foundation for protecting the critical cryptographic parameters that are independently verified at FIPS 140-2 level 3.

A Well-Publicized Example of Compromise – The Cryptocurrency Threat-scape

Vulnerabilities in blockchain end-to-end transaction applications, such as those used for cryptocurrency and trade, finance and commerce can impact business and investment profoundly. Threats abound, particularly among the glamour of the cryptocurrency world and have wreaked havoc with investor's hard-earned assets. Well-known attacks such as the Mt. Gox (half a billion dollars-worth of BTC lost), Good Samaritan White Hat (800 BTC stolen from users' wallets) have set the stage for more and greater threats. A flaw in the Parity multi-signature wallet on the Ethereum network (2017) enabled hackers to steal over $31M worth of Ether in minutes. In the case of the Parity attack, it was only the actions of white-hat hackers that limited the damages to the above figures. They saved Parity wallet-owners over $150M by hacking the remaining wallets and saving those funds in a protected account that the thief could not access.

If it sounds like the Wild West, sadly it is. In many cases the stunning Parity defence fails to materialize in the seconds it takes to complete a transaction.

In most cases, there can be no sheriff and no posse at the instant when the outlaws strike. Even with well-designed software security protection, there are inherent weaknesses in software wallets and end-point programs and similar fund-control applications that have often failed spectacularly to enforce privacy and access control on accounts, particularly those containing sizeable cryptocurrency assets.

SPYRUS®

The Broader View

The blame cannot be placed solely on the blockchain operational infrastructure, its languages and technology. Individual integration and deployment errors remain a common culprit. This leads to some fundamental keystones in blockchain security:

- the threat base exists and is both capable and motivated;
- the attack surface is broad and in hard-to-see places, soft; and,
- there obviously needs to be more and better protection engineered by integration and deployment developers into each smart contract and DApp for use by individuals and corporations.

Blockchain solutions are not uniform and like all IT solutions, "one size does not fit all" concerning the problems of security. There are common denominators of security implementations that must be planned and integrated early in the design processes of blockchain in the case of permission-less systems (such as in cryptocurrency) and permissioned systems for business transactions.

The value of the assets/objects of blockchain applications far outweigh the costs of integrating HSMs. Against any measure of risk, the value of strong cryptographic protection, integrity and trust provided by HSMs to protect the goods or services being transacted and the brand of the blockchain is material to every stakeholder.

Although blockchain technology provides an immutable auditable transaction ledger to prevent fraudulent activities after creation, it does nothing to ensure the accurate identification of the parties involved in transactions, or the integrity of the vital processes themselves such as consensus approval voting. Proof that essential elements in the peer-to-peer chain of end points can be trusted and were not compromised or corrupted in a blockchain are essential to trust of recorded transaction.

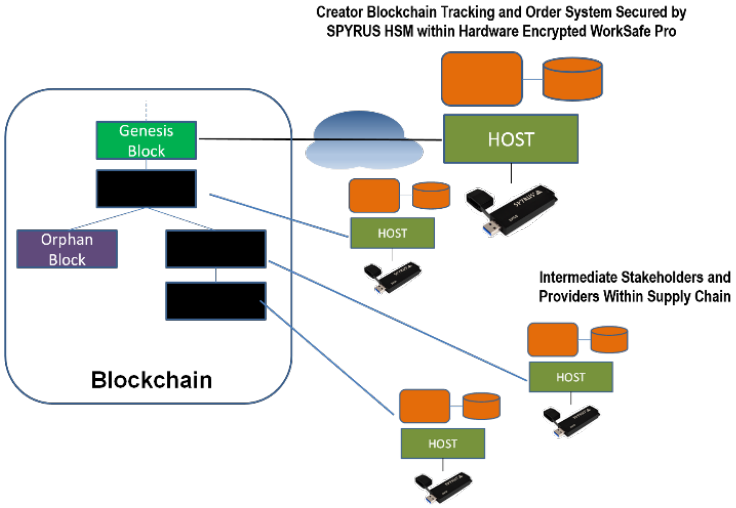
Whether there is a transaction involving real estate, international trade of goods, supply chain, or cryptocurrency payments, the resulting transaction establishment of trustworthiness and acceptance is impossible if all of the essential active elements are not adequately protected. Validated authentication and authorization of the participating parties, protection of private keys used for transaction signatures (even anonymous parties), and protection against fraud by unauthorized voters in a consensus voting process used to create or approve a transaction are all essential.

SPYRUS HSMs security tools, firmware and software are currently use for sensitive government certified cryptographic boundaries protecting blockchain critical functions such as K of N Secret Sharing and proof of identification. SPYRUS HSMs divide credentials into parts, where each participant/operation has a unique share. Policies can be applied to require some or all of the shares in order to initiate a transaction.

The SPYRUS patent-pending technology to apply cryptographic authentication provides binding of parties to the specific transaction objects as well as a novel secure and automated approach to stakeholder consensus voting for transaction approval. These provide quick and easy construction of the distributed applications and smart contracts that securely drive the execution of the transactions processes through the chain of review and approvals prior to adding to the blockchain.

Some Real Life Examples

The figure below is a high-level architecture of a blockchain ledger-enabled "Order and Tracking System secured by SPYRUS HSMs, which is applicable to supply chain management, medical records, IoT sensor integration, and even disparate applications such as preserving the chain of custody for electronic surveillance information. Unique to SPYRUS are "read only" HSM modules which can be distributed to auditors, analysts, and end users of product to validate entries without supporting the ability to make new entries or otherwise corrupt data. Intermediate stakeholders will have similar subsystems to create blocks. SPYRUS HSMs contain Hardware Roots of Trust to ensure that that local system is not affected by compromise. It consists of three specialized subsystems:



Application order and tracking data

(Figure lower left) has the functionality to track activity, assign assets, review and audit history, print reports and management interfaces that accurately reflect the state of the system. Encryption of sensitive data is implemented with SPYRUS HSM devices. This may be an encrypted bootable HSM drive in a laptop or tablet, a microSDHC HSM, or an embedded Rosetta Micro (QFN) in a sensor node. A SPYRUS HSM would be integrated with server architecture to create the "Genesis Block" to begin the hardware chain of trust.

SPYRUS®

Blockchain ledger of order and tracking transactions

Since only metadata is present in blocks and transaction records, no encryption of the blockchain information content is required. A blockchain ledger can be sharable across a network or privatized to a small group of peers. By its design, the blockchain subsystem will be instrumental in preserving the integrity of the ledger and prevent fraud, censorship or third-party interference. It can also serve as an index into all transactions of the order and tracking system and support audit of the authorized events of the system.

Cryptographic services to support enhanced authentication

The validated FIPS 140-2 Level 3 hardware level of protection offered by SPYRUS HSMs secure sensitive crypto-variables, as well as temporary data such as orders, events and delivery origin, current location, routing and destination information. SPYRUS HSMs unique "Read Only" capabilities preserve consumers' and auditor's functions.

Strong authentication prevents the insertion of "Orphan Blocks" such as those which may be caused by an attacker attempting to modify transactions or otherwise compromise the supply chain. Operations such as reading, initiating or modifying an order, or accessing tracking information for an existing order would require the interface with the secure order and tracking application, as well as the blockchain client service, where the transaction recording the event is entered.

In Summary: Fortifying Blockchain -- A New Use for Proven Technology

SPYRUS FIPS 140-2 Level 3 certified Hardware Security Modules draw on over two decades of proven performance to provide the strongest possible security for such critical applications such as PKI- based identity management, data security, data integrity, and non-repudiation.

The security solutions outlined in this paper have been proven in military and commercial IT use cases. Certified high-assurance hardware repositories based on secure authentication and encrypted storage ensure data provenance and ensure trustworthy computing environments.

One of the key features of current blockchain business practice is the use of multi-signed consensus in smart contracts and DApps. Fortified by a unique SPYRUS HSM embodiment the SSS-based K of N ensures repeatable and trusted auditability of a blockchain.

The necessary protection and secure backup of keys and other critical security parameters demand Hardware Roots of Trust.

SPYRUS HSMs, supporting SDKs and development tools provide a high assurance migration path that uses proven hardware-based components beginning with devices that can be added to standard USB or MicroSD ports to embedded QFN HSMs.

SPYRUS is dedicated to support global security standards, particularly, NIST certified cryptography, that assures secure physical protection for key generation and lifecycle management. Our leadership in Hardware Roots of Trust also affords us the agility to support nonstandard cryptography to manage unique requirements to protect blockchain transactions both now and for the future.

SPYRUS HSMs, supporting SDKs and development tools provide a high assurance migration path that uses proven hardware-based components beginning with devices that can be added to standard USB or MicroSD ports to embedded QFN HSMs.

Contact SPYRUS at info@spyrus.com to obtain information on availability and pricing on the Rosetta HSM Secure Key Backup System and CA in a Box.

Developers may access the SPYRUS Developers Portal at developer.spyrus.com and request a login to access detailed descriptions of typical applications and purchase prototyping quantities of SPYRUS HSMs

Corporate Headquarters
103 Bonaventura Drive
San Jose, CA 95134
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document number 402-000003-01