Fortanix®

Solution Brief

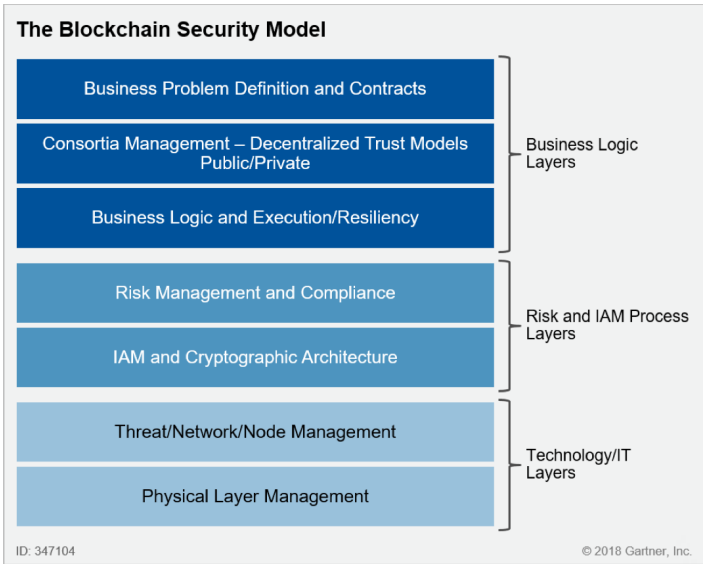
Secure Key Management for Blockchain applications

Blockchain Security Risks

Blockchain, given its ability to generate an immutable cryptographic record, can be useful for business transactions and has the potential to carry significant economic value. This inevitably increases the risk of theft and misuse. Additionally, some platforms like Ethereum support running "Smart contract" code that opens up new exposure risks. Security issues unique to Blockchain can be summarized as:

1. Security of Private Key: Private keys, regarded as the identity and security credential, are associated with financial value, which is what attackers are after.
2. Smart Contract Security: Complex smart contract code can leave open vulnerabilities. Lack of robust privacy protection measures can lead to risk of confidential data leak.
3. Consensus Security: Breach of consensus mechanism can be considered as a highest-level breach but is currently a theoretical risk.

Gartner has defined the following model for tracking security risks of Blockchain projects:



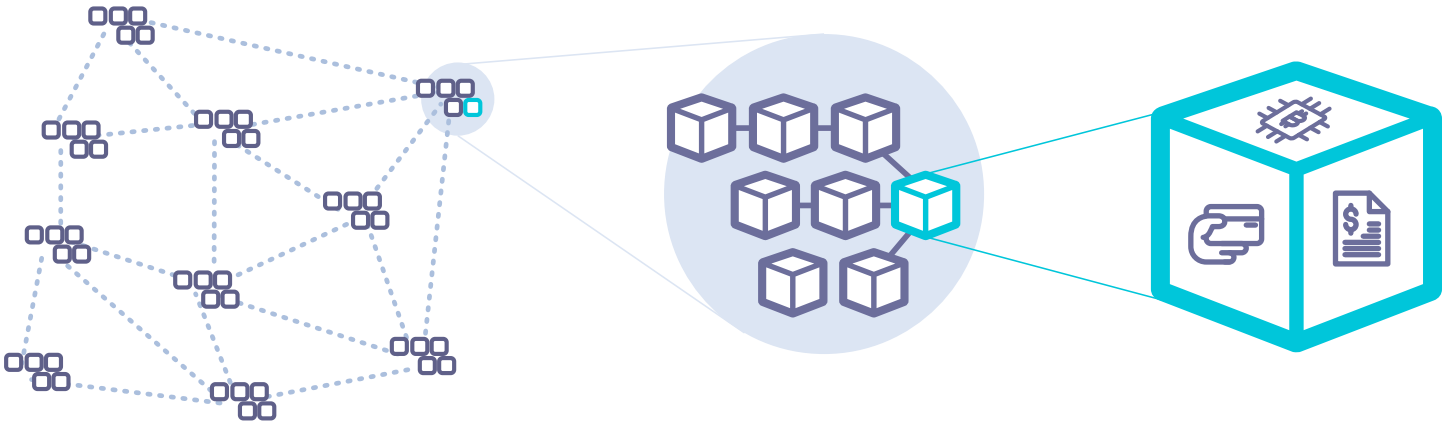
Source: Gartner, Inc., [Evaluating the Security Risks to Blockchain Ecosystems], Figure 1, [March 2018].

This paper focuses on the identity and encryption key management challenges that are barriers to successful enterprise blockchain deployments and proposes a solution based on Fortanix Data Security Manager™. Fortanix also delivers Runtime Encryption™, leveraging Intel® SGX, for enhanced confidentiality and privacy for data in use of Blockchain applications and this is a focus of a subsequent solution brief.

Background (Skip if familiar with Blockchain)

Blockchain is a distributed ledger, a type of database that is shared and synchronized across a decentralized network. Transactions in the database are sequentially chained into blocks thus giving it the name Blockchain. Blockchain acts as a single source of truth with each block being immutably recorded using cryptography across a distributed network.

Just like cloud computing, blockchains can be public, private or hybrid. While Blockchain has its origins as a public way to track transactions for cryptocurrencies such as Bitcoin, the business benefits now overshadow that. Blockchain continues to show promise in transforming business processes, delivering new levels of efficiencies, and enabling new marketplaces across industries ranging from supply chain, asset management, financial services, health care, and real estate. Private or enterprise blockchains can deliver the benefits while giving organizations complete control over who is allowed on the network.



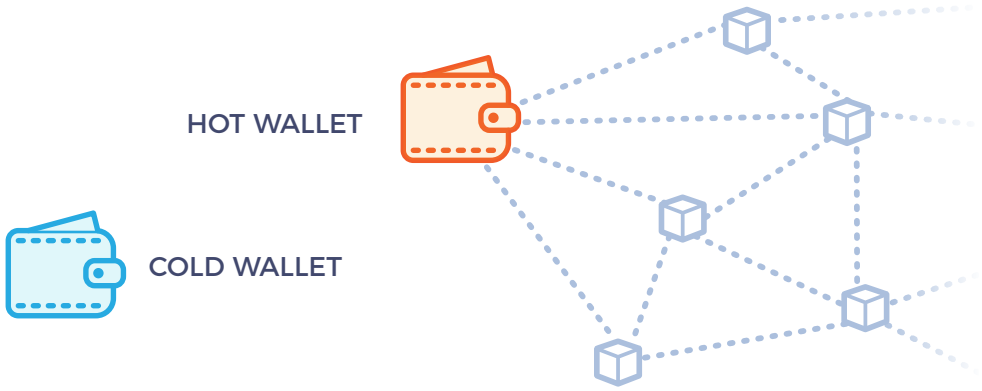
Fortanix

Encryption and Key Management Requirements

Blockchain relies on cryptography for trust and assurance. Every block is fingerprinted with a cryptographic hash that subsequent blocks will reference for chaining. Blockchain also relies heavily on public key infrastructure (PKI) to ensure authentication and integrity of messages. Private keys are used to digitally sign transactions.

Organizations looking to implement a private enterprise blockchain or a hybrid blockchain face some familiar and some unique key management challenges:

- Each participant in a blockchain possesses a private key used to digitally sign transactions. Private keys are tokenized into assets representing economic value increasing the risk of theft and misuse. Security of the private keys is paramount, yet keys are often generated using software-based key managers that are vulnerable to compromise. Traditional Hardware Security Modules (HSMs) are complex, expensive, and do not scale well to the requirements of Blockchain. Some of the recent hacks that highlight this gap and the need for stronger protection of private keys include Coincheck, Bitfinex, or Mt. Gox.
- Handing over partial control to 3rd party such as exchanges requires support for multi-signature (multisig) – splitting access to keys across multiple parties (example: 2 out of 3 signatures for approval)
- Rate limiting usage of private keys mitigates the risk of misuse. A tiered model that separates hot wallets for frequent usage from cold wallets where majority of tokens are kept in a secure tamper-proof storage, offers additional safeguards.

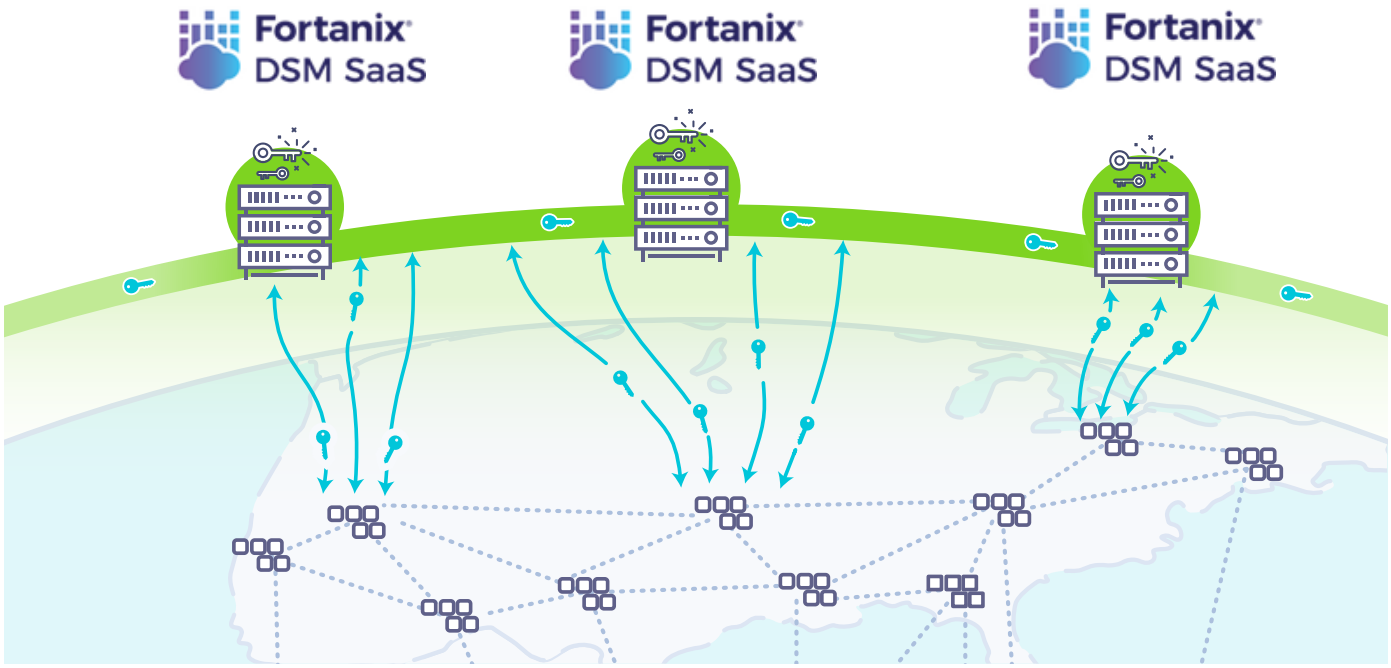


- Loss of availability and loss of keys due to a disaster are equally a major concern.
- Blockchain applications such as Bitcoin uses new cryptographic algorithms such as ECDSA secp256k1 and private key seeding. Considerable innovation is focused on blockchain and as result newer cryptographic schemes and algorithms are emerging
- Auditing of key usage is critical given the distributed nature of trust in a blockchain
- Blockchain requires a large number of keys across a distributed environment along with a high-degree of scalability for transactions.
- Blockchain can have encryption requirements for server-side components and wallets that are typically mobile, or endpoint device based.

Fortanix

Fortanix Data Security Manager™: Security and Ease of Integration for Blockchain Applications

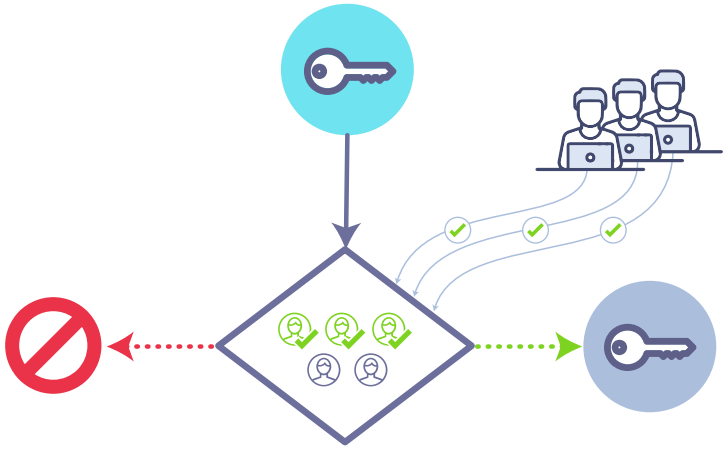
Fortanix Data Security Manager is an ideal key management solution for an enterprise blockchain. It is secure, scalable, and programmable.



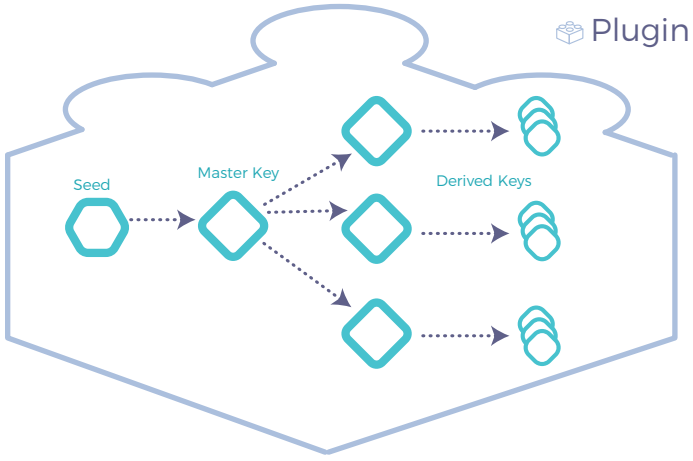
1. **Flexible Deployment:** Organization can deploy Fortanix Runtime Encryption appliance nodes centrally or in a distributed manner. In each case the Fortanix DSM cluster delivers centralized key management capabilities to any blockchain application or any device. For organizations that prefer a SaaS consumption model, Fortanix Data Security Manager™ delivers HSM and Key Management as a global cloud service. Regardless of the deployment model, organizations have centralized visibility and control over the entire solution. Multiple clusters can also be deployed to separate hot and cold wallets.

2. **HSM-grade Security:** Fortanix DSM, leveraging Runtime Encryption and Intel® SGX, delivers unmatched privacy for the protection of the private keys. Only authorized users can access their keys.

3. **Multi-Signatures (multisig) support:** Fortanix natively supports quorum approval (M of N) policy for enhanced protection of sensitive key operations. Organizations can define flexible quorum approval policies such as approval required by 3 out of 5 users, approval required by specific users or multi-level approvals. Easy to use intuitive workflows enable secure remote collaboration. This can be useful for hot wallets where fiduciary control is given partially to 3rd parties, and also for cold wallets where coordination among various parties may be difficult.

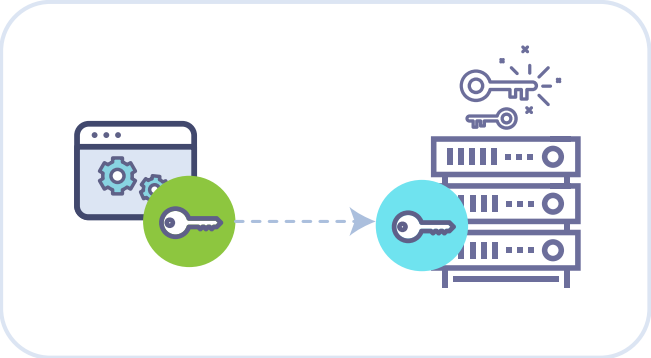


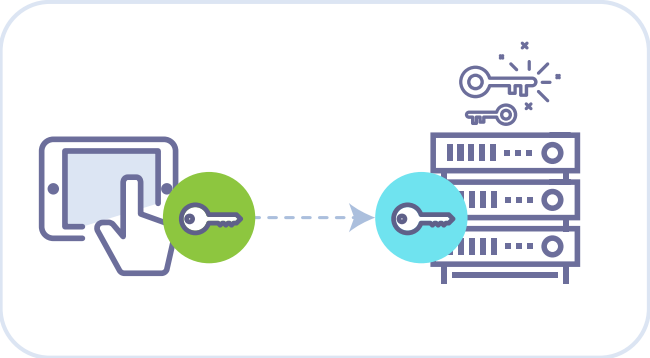
4. **Runtime Encryption Plug-ins:** Fortanix Runtime Encryption plug-in capability allows organizations to customize cryptographic logic and run it securely inside the trusted execution environment of Intel® SGX. This allows unique policies for key usage such as applying thresholds as well as access control to be enforced as per an organizations' requirements. Plug-ins can also support secure key derivation for HD wallets such as defined by BIP 32.
https://support.fortanix.com/hc/en-us/articles/360015941372-Plugins-Getting-Started



5. **Access Control and Auditing:** Fortanix DSM supports strong multi-factor authentication as well as the flexibility to integrate with authentication providers. A concept of groups enables fine-grained access control for users, applications and keys. Fortanix DSM performs comprehensive auditing of all security events including key usage that can be integrated with SEIM tools.

6. **REST APIs:** Fortanix DSM supports RESTful APIs in addition to a wide variety of cryptographic interfaces. As a result, web applications or mobile applications can securely connect to Fortanix DSM for their key management needs.





7. **Scale-out:** Fortanix DSM can manage millions of keys from an initial deployment and can scale-out easily as the demand for keys and transactions grows. The solution minimizes availability risk while maximizing operational simplicity, by leveraging a distributed systems architecture that provides automated high availability and disaster recovery.

8. **Algorithms:** Fortanix DSM supports comprehensive NSA Suite B algorithms. Additionally, given the software-defined approach to HSM and Key Management, Fortanix is able to continuously deliver support for new algorithms. For example, Fortanix DSM supports ECDSA secp256k1 used by Bitcoin applications. https://support.fortanix.com/hc/en-us/articles/360016160411-Algorithm-Support

Security and Flexibility

Blockchain has the potential for transformative benefits to businesses or organizations that track transactions, assets, or maintain records. By adopting a blockchain style ledger system, organizations can significantly increase efficiency and enhance collaboration internally as well as across business eco-systems.

Fortanix DSM eliminates one of the largest obstacles to blockchain adoption – secure and compliant key management. Fortanix DSM delivers unmatched security for the generation and use of keys. The private keys are kept secured at rest, in motion and even when in use. Complete key management and policies for key usage are enforced inside Intel® SGX enclaves ensuring confidentiality and integrity of the policies. Fortanix DSM runs on hardened FIPS 140-2 Level 3 compliant Fortanix Runtime Encryption Appliances that deliver enhanced physical security.

Fortanix DSM delivers HSM-grade security designed for easy integration into a blockchain environ-ment with complete flexibility in terms of deployment model, application integration with REST API support, and support for enhanced cryptographic algorithms as well as policies for multisig, key signing and access control.