Blockchain Solutions

Transaction signing and cryptographic key lifecycle management

Introduction to transaction signing and key lifecycle management using blockchain

Blockchain is a records management technology using a series of cryptographically authenticated “blocks” on a “chain”. These blocks consist of transactions entered by different users, often financial transactions, but also other data types such as supply chain provenance. They are “chained” together by hashes which have their own often cryptographic identifiers. These identifiers are generated from data inside the block, and when signed using a FIPS 140-2 Level 3 validated HSM, provide a high-assurance method of verifying blockchain integrity.

Benefits of using blockchain

- Greater transparency
- Increased traceability
- Robust security features
- Increased efficiency and speed
- Reduced cost
- Widely accepted and trusted
- Distributed ledger

Using blockchain with Futurex HSMs

Futurex HSMs add an essential layer of security to blockchain implementations by providing FIPS 140-2 Level 3 validated cryptography. Futurex HSMs provide two key steps for securing the blockchain:

- Digitally sign transactions or blocks added to the blockchain using strong cryptography.
- Manage the full lifecycle for the keys used in securing the blockchain, from generation to rotation to retirement.

How blockchain is secured by Futurex HSMs

1

A user requests access to the blockchain to make a transaction.

2

The user is validated and the transaction is digitally signed through FIPS 140-2 Level 3 validated HSMs.

3

The transaction is broadcast to the network, stored into a block and a hash value is generated.

4

These secured, validated transactions become part of the blockchain and can be cryptographically authenticated.

5

Transaction signing keys are rotated periodically, depending on preference and regulatory requirements.

6

Once validated, the blockchain cannot be altered, making auditing and dispute resolution simpler and faster.

Learn more about how blockchain is used

For more information about Futurex products and services, please visit https:www.futurex.com

FUTUREX

Engineering Campus - 864 Old Boerne Road, Bulverde, Texas 78163 - USA
TF/ (800) 251-5112 P/ +1 (830) 980-9782 info@futurex.com

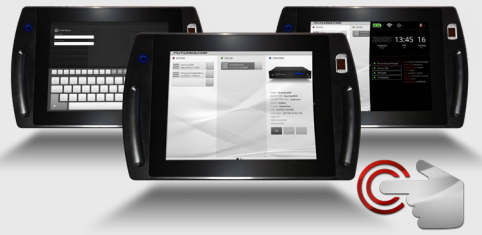
Futurex and blockchain

The Vectera Plus digitally signs blockchain transactions using standards-based interfaces such as PKCS #11.

The Key Management Enterprise Server (KMES) Series 3 provides full key lifecycle management, from generation to rotation, use, and revocation. It supports common interfaces such as KMIP and PKCS #11.

Integrate the Excrypt Touch

Combine the KMES Series 3 and Vectera Plus with the Excrypt Touch for remote access and management.



Blockchain use cases

- Syndicated loan market - verify, communicate, and enter data on one, shared “Golden Book” ledger
- Interbank reconciliation - control, manage, and cut down on disputes between different banks, reducing time and labor significantly
- Supply chain - prove the authenticity of your product to end customers, guarding against counterfeiting and fulfilling regulatory requirements