Product brief

SECORA™ Blockchain

Infineon's Java Card™ solution for block chain applications

SECORA™ Blockchain is a fast, easy-to-use Java Card™ solution supporting best-in-class security for block chain system implementation. It relies on Infineon's field-proven security chip featuring Integrity Guard security technology.

The **SECORA™ Blockchain** offers to the user a hardware supported key handling/backup tool for generating key pair, secure storage and backup of private key. It makes the application more secure and easier to design for customer's block chain system. By providing a safe "vault" for user credentials, SECORA™ Blockchain also reduces the final user's commercial risk and helps to increase trust in the block chain system.

Generally speaking, a block chain is a decentralized digital ledger that manages a continuously growing list of data points (chain of blocks). Every block in the block chain is cryptographically linked to the previous block. The ledger records all transactions used to send assets (e.g. cryptocurrency) or confidential information from one account to another. Each transaction is protected by a digital signature. To create this digital signature, a secret private key that corresponds to the public key of every single account is needed.

In the block chain system, the public key is used to derive addresses and verify signatures; whereas the private key is used to generate signatures and sign transactions. As there is no centralized trust scheme in the block chain system, security is particularly important for every user to protect their private key. If the user loses their private key, they also lose all their assets/information. Moreover, if the private key is stolen or hacked, the attacker has full access to all of the account holder's assets/information. This allows the attacker to create seemingly valid transactions. Hardware-based security tokens are the best possible way to protect private keys against attacks and unauthorized access.

Key features

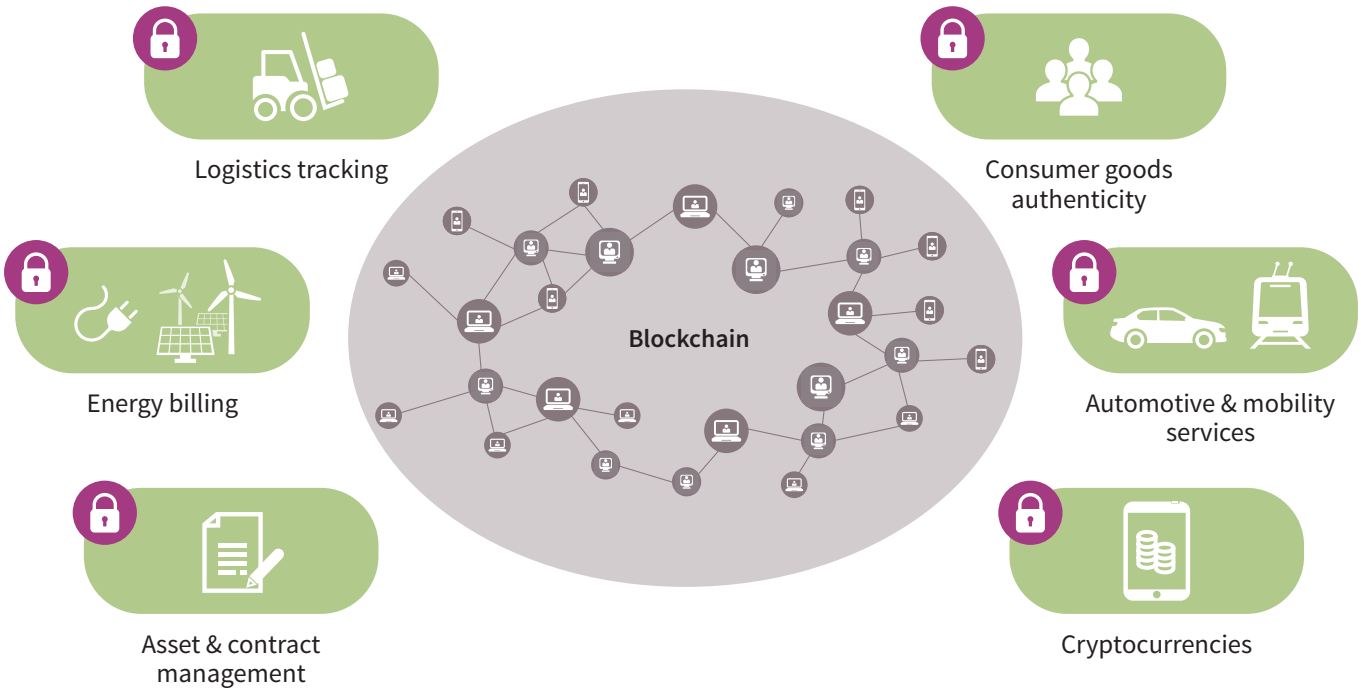
- Supports contact based and contactless communication protocol
- SCP03 for secure authentication and encrypted communication
- Creation and storage of up to 100 key pairs
- Supports key labeling
- Supports enhanced secure reset of PIN/PUK
- Supports customer-specific master key
- Secure backup of user key
- Signature generation for signing block chain transaction
- User authentication with PIN
- Supports various signature schemes, e.g. Ethereum, Bitcoin and ETR ERC-20
- Module delivery forms
  - For card form factors
    - Contactless
    - Dual interface
    - Coil on Module
  - For non-card form factors
    - SPA (Smart Payment Accessory) for contactless interface

Blockchain Security 2Go starter kit

SECORA™ Blockchain evaluation tool

To accelerate time-to-solution, Infineon's **Blockchain Security 2Go starter kit** gives designers a smart and efficient evaluation tool enabling fast design-in coupled with rapid, smooth transition from starter kit to high-volume ramp-up.

Blockchain technology use cases



Published by
Infineon Technologies AG
81726 Munich, Germany

Document number: B181-I1013-V1-7600-EU-EC
Date: 05 / 2020

Please note!

This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.