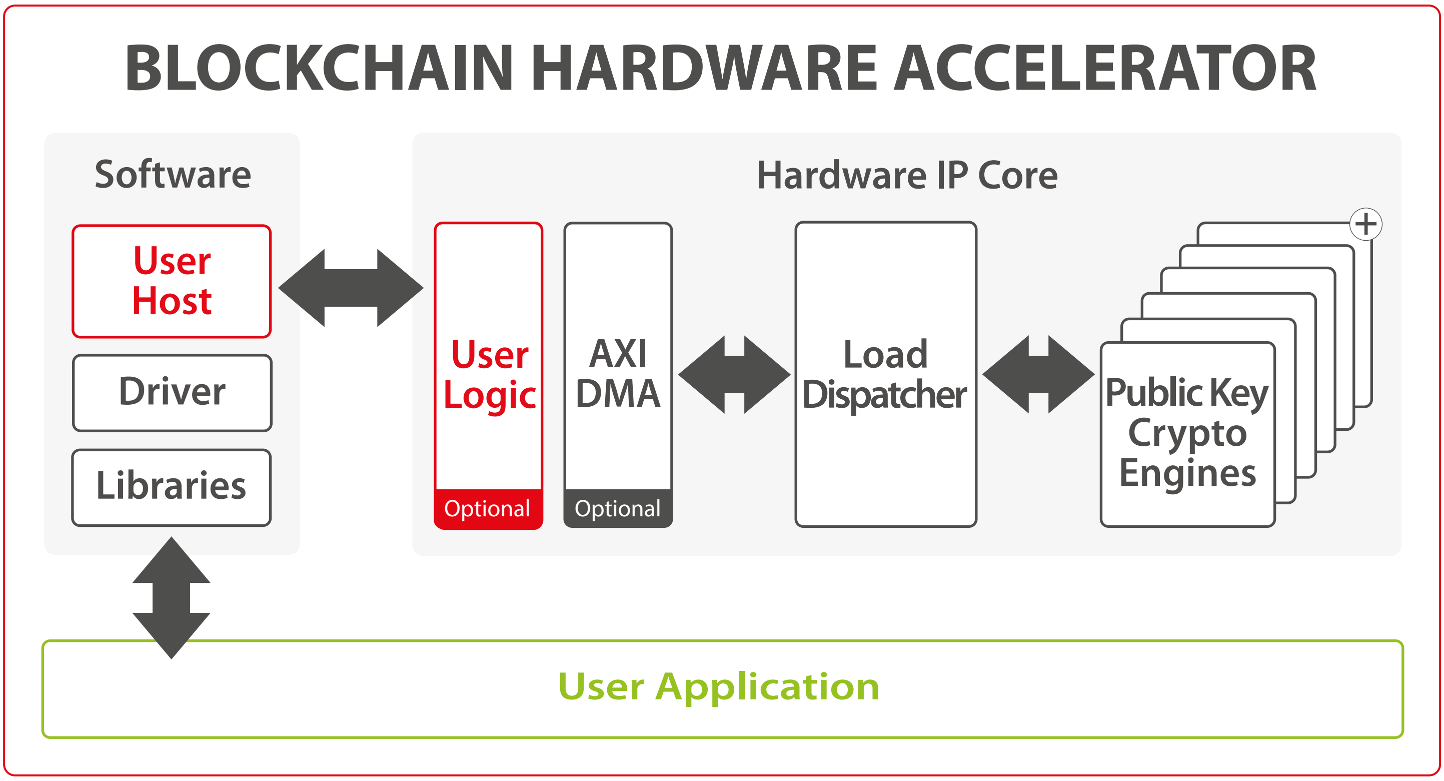
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Secure Protocol Engines > SCZ_SP_BA452

BLOCKCHAIN HARDWARE ACCELERATOR

Blockchain has a wide range of applications on the internet. As it is decentralized by design, it is an alternative to the many traditional transactional systems. In order for a blockchain system to be viable (scalability, interoperability and sustainability), the complex and time/power consuming cryptographic operations associated with the blockchain should be offloaded to an accelerating system. Our solution is a secure public key infrastructure engine that can be used to offload compute-intensive public key operations such as signature generations and verifications.

The blockchain hardware accelerator uses a combination of a load dispatcher and a configurable number of instances of our Public Key Crypto Engine (SCZ_IP_BA414EP). This saves time and space as the transaction load is distributed among several components, thereby increasing the overall transaction speed and output. The architecture allows for high performance offloading and supports all the cryptography algorithms such as ECC. ECDSA operations that are used by popular blockchain applications like Ethereum, Ripple and Bitcoin and Hyperledger are supported next to EdDSA using the Edwards25519 curve as used in the Libra blockchain.



Features

- Wide variety of ECC curves supported (Weierstrass, Edwards, Montgomery, Twisted-Edwards, ...)
- Ideal for FPGA/ASIC integration

Blockchain based applications

- Digital (crypto) currency
- Transaction verification
- Governance
- Healthcare
- Online voting
- Data storage
- IoT
- Insurance

Implementation aspects

The unique architecture of our solution enables high scalability that in turn provides a trade-off between throughput, area and latency. This flexibility allows for an optimal performance for any application regardless of the platform on which the solution is implemented. It can easily be ported to ASIC and FPGA, and supports a wide range of applications in blockchain scaling, cryptocurrency transactions, cloud computing and data centers. In addition our drivers have an asynchronous API (or non-blocking API) which are integrated in OpenSSL Async.

Deliverables

- ✓ Netlist or RTL
- ✓ SW drivers (Linux)
- ✓ Scripts for synthesis & STA
- ✓ Self-checking RTL test-bench based on referenced vectors
- ✓ Documentation

V1.2

SECURE-iC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com