SILEX INSIGHT

BLOCKCHAIN HARDWARE ACCELERATOR

INTRODUCTION

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. 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. Just like our Blockchain Hardware Accelerator which is a secure public key infrastructure engine.
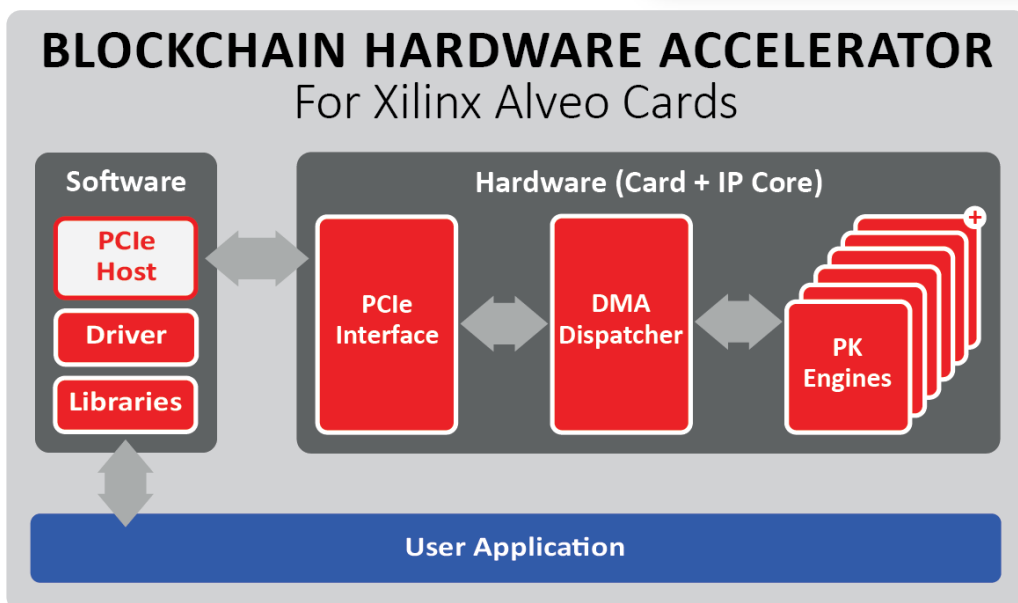
APPLICATIONS

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

Offload the compute intensive operations

- > Wide variety of ECC curves supported (Weierstrass, Edwards, Montgomery, Twisted-Edwards, …)
- > Easy Integration
- > Proven Solution

BLOCKCHAIN HARDWARE ACCELERATOR
For Xilinx Alveo Cards

Software
- PCIe Host
- Driver
- Libraries

Hardware (Card + IP Core)
- PCIe Interface
- DMA Dispatcher
- PK Engines
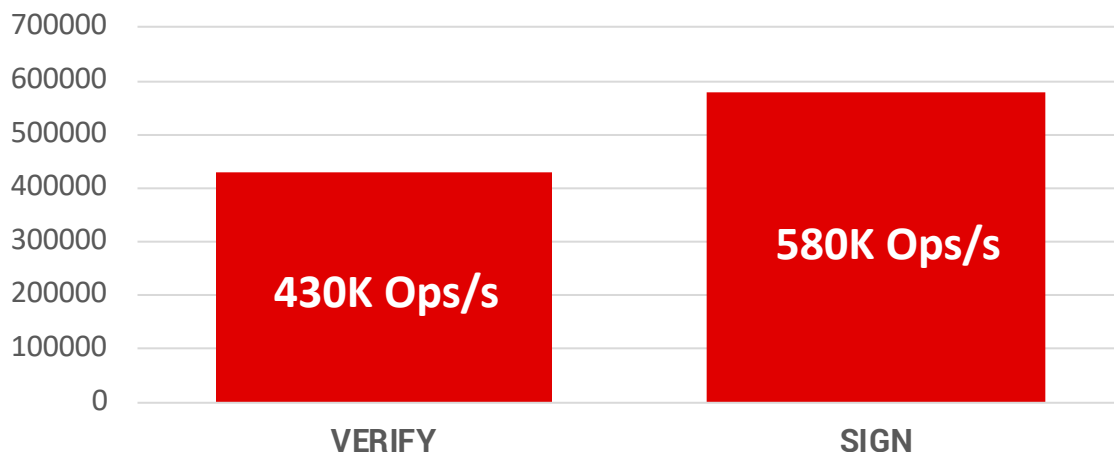
User Application

XILINX.

Adaptable. Intelligent.

SOLUTION OVERVIEW

The blockchain hardware accelerator uses a combination of a load dispatcher and a configurable number of instances of our Public Key Crypto Engine (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.

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. It supports a wide range of applications in blockchain scaling, cryptocurrency transactions, cloud computing and data centers. Our drivers provide an asynchronous API (or non-blocking API) which is integrated in OpenSSL Async.

RESULTS

secp256K1 Performance (Ops/s)

Bar chart showing VERIFY at 430K Ops/s and SIGN at 580K Ops/s.

TAKE THE NEXT STEP

Learn more about Silex Insight Blockchain Hardware Accelerator
Reach out to contact@silexinsight.com

Learn more about Xilinx Alveo accelerator cards