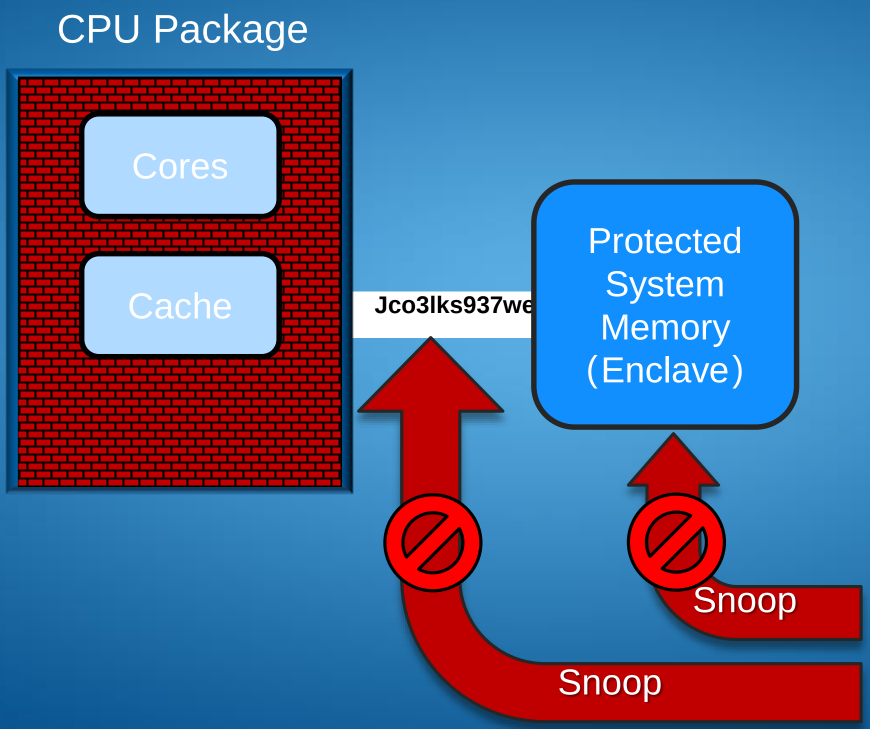
Intel® SGX and Blockchain

李志强

英特尔中国平台安全战略规划

Intel® SGX – Physical Attack Protection



- Security perimeter is the CPU package boundary
- Data and code unencrypted inside CPU package
- Data and code outside CPU package is encrypted and integrity checked
- External memory reads and bus snoops see only encrypted data
- SGX is an App Level TEE
- http://software.intel.com/sgx

Trusted Execution Environment for Blockchain

Intel security and performance technologies such as Intel® Software Guard Extensions (Intel® SGX), consist of built-in CPU instructions and platform enhancements that enable code to be executed in a Trust Execution Environment (TEE) with enhanced data protections without compromising performance for workloads.

For blockchain, a TEE can provide:

SECURE KEY MANAGEMENT
(private key storage)

TRUST
(off-chain interaction)

CONSENSUS
(high-performance and scalable consensus, PoET)

PRIVACY
(data protection from 3rd parties)

intel XEON inside

INTEL® SGX

Intel® Software Guard Extensions

基于芯片的可信执行环境

HYPERLEDGER SAWTOOTH

锯齿湖

ENTERPRISE ETHEREUM ALLIANCE

企业以太坊

HYPERLEDGER 超级账本联盟

INTEL'S TECHNOLOGY CONTRIBUTION TO BLOCKCHAIN

英特尔技术

助力

区块链

https://hyperledger.org/projects/sawtooth

Other names and brands may be claimed as the property of others.

Backup

SGX USE CASES – DATA CENTER, CLOUD & INTERNET OF THINGS

Privacy Preserving Analytics & Workloads

Enables multi-party joint computation on sensitive data in a privacy-preserving manner

Encrypted Databases

Encrypted database operations

Secure Containers

Running unmodified applications within enclave

NFV

Network Function Virtualization

Trust established for protecting & virtualizing network functions

HSM

Hardware Security Module

Customers and ISVs use Secure Enclave to protect encryption keys and/or HSM replacement

Key Protection

Protecting keys on local file system; hardening disk protection, building scalable cloud KMS

Blockchain

Secure transaction processing for Cryptocurrency, Secure Contracts, and Hyperledger protection

Internet of Things

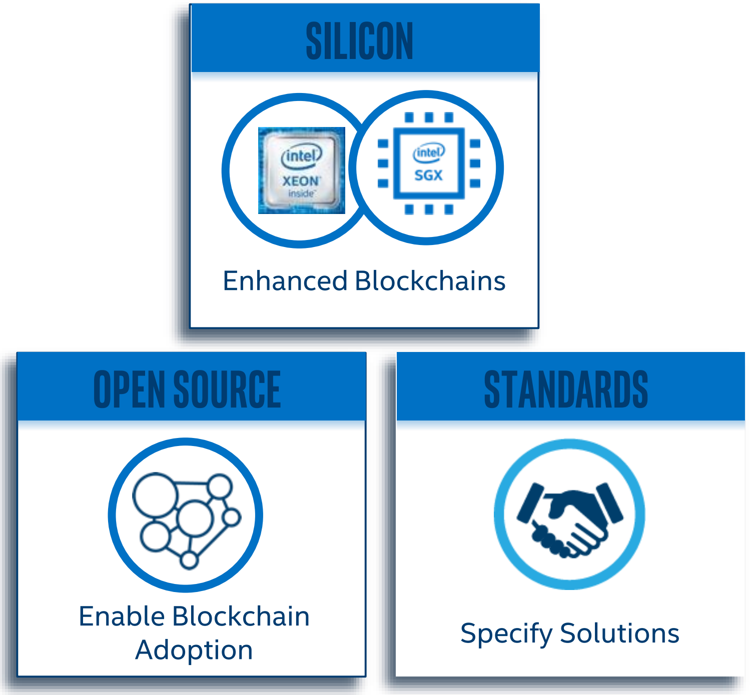
Secure IoT edge devices and cloud communications Boxcreek toolkit for secure enclave uses

INTEL'S BLOCKCHAIN STRATEGY英特尔与区块链

Silicon
Utilize silicon technologies like Intel SGX and Xeon SP to improve blockchain solutions and establish long-term value.

Solutions
Utilize Intel's open source blockchain software as building blocks for ecosystem scale - Sawtooth, Private Data Objects, and Intel SGX Components.

Standards
Ensure that specifications in industry consortiums yield the promise of trusted disintermediation - Hyperledger, Enterprise Ethereum Alliance, and R3.



SILICON

Enhanced Blockchains

OPEN SOURCE

Enable Blockchain Adoption

STANDARDS

Specify Solutions

DIFFERENTIATION WITH INTEL SGX

SECURITY

Private key storage mechanism for blockchain transactions.

Tencent 腾讯

Chain

Alibaba.com

PRIVACY

Enhance protections for data from 3rd parties on common infrastructure (incl. off-chain throughput).

AlphaPoint

iexec

r3.

SCALABILITY

Isolate blockchain consensus for transaction acceleration and larger networks.

Microsoft Azure

SAP

IBM

pokitdok

Developers are using isolation, attestation verification, and code integrity features of Intel SGX to address key issues that influence blockchain adoption

https://www.hyperledger.org/blog/2018/01/30/announcing-hyperledger-sawtooth-1-0
https://www.hyperledger.org/projects/sawtooth
https://hyperledger.org/members
https://entethalliance.org/members/
https://www.corda.net/wp-content/uploads/2017/05/R3FundingPressRelease.pdf

BLOCKCHAIN SOFTWARE AND ECOSYSTEM

HYPERLEDGER SAWTOOTH

An open source modular enterprise blockchain stack designed to run in distributed environments like hybrid cloud and cloud data centers.

PRIVATE DATA OBJECTS

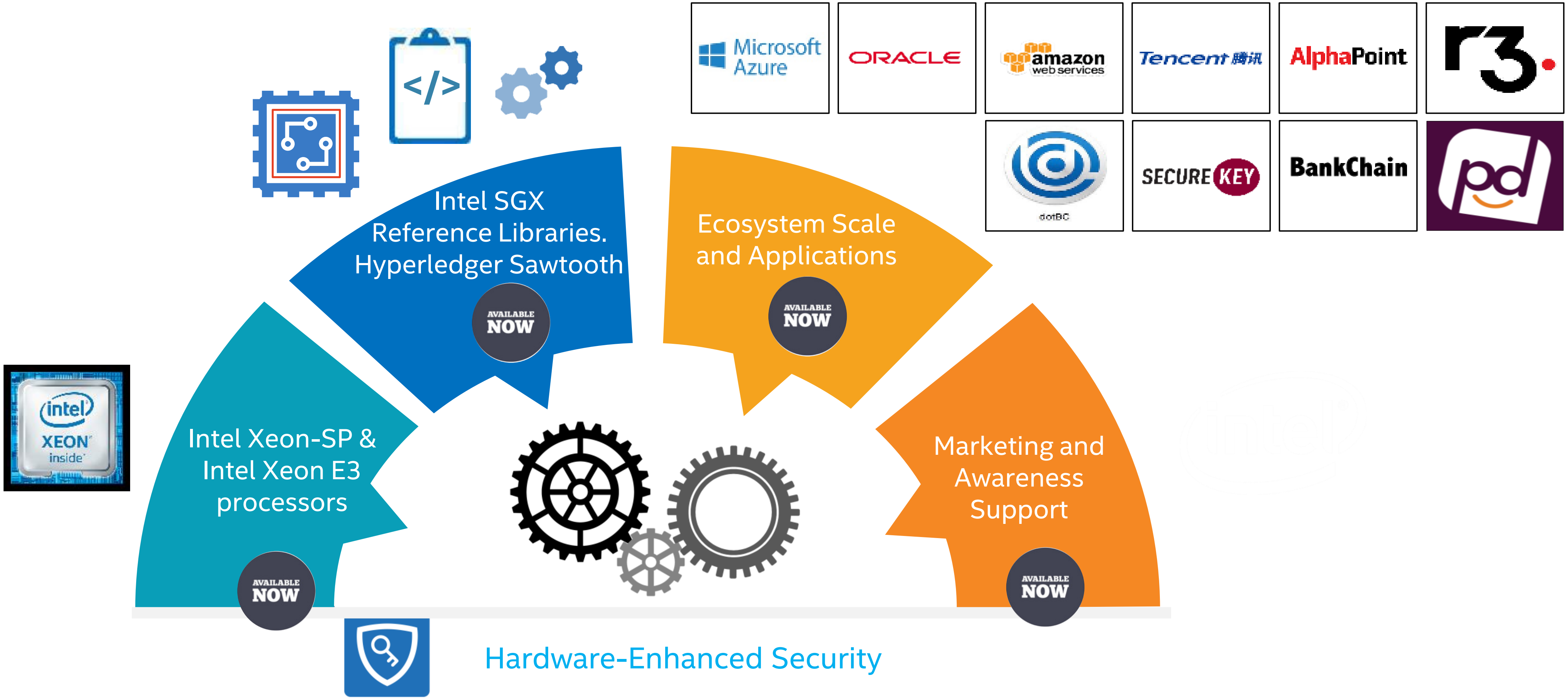
Open source software that utilizes Intel SGX to run blockchain code off-chain thereby improving data privacy and throughput

ENTERPRISE ETHEREUM ALLIANCE*

Motivate enterprise adoption of Ethereum on an IA-friendly specification

https://www.hyperledger.org/blog/2018/01/30/announcing-hyperledger-sawtooth-1-0
https://www.hyperledger.org/projects/sawtooth
https://hyperledger.org/members
https://entethalliance.org/members/
https://www.corda.net/wp-content/uploads/2017/05/R3FundingPressRelease.pdf

ASSETS AVAILABLE



Intel Xeon-SP & Intel Xeon E3 processors

AVAILABLE NOW

Intel SGX Reference Libraries. Hyperledger Sawtooth

AVAILABLE NOW

Ecosystem Scale and Applications

AVAILABLE NOW

Marketing and Awareness Support

AVAILABLE NOW

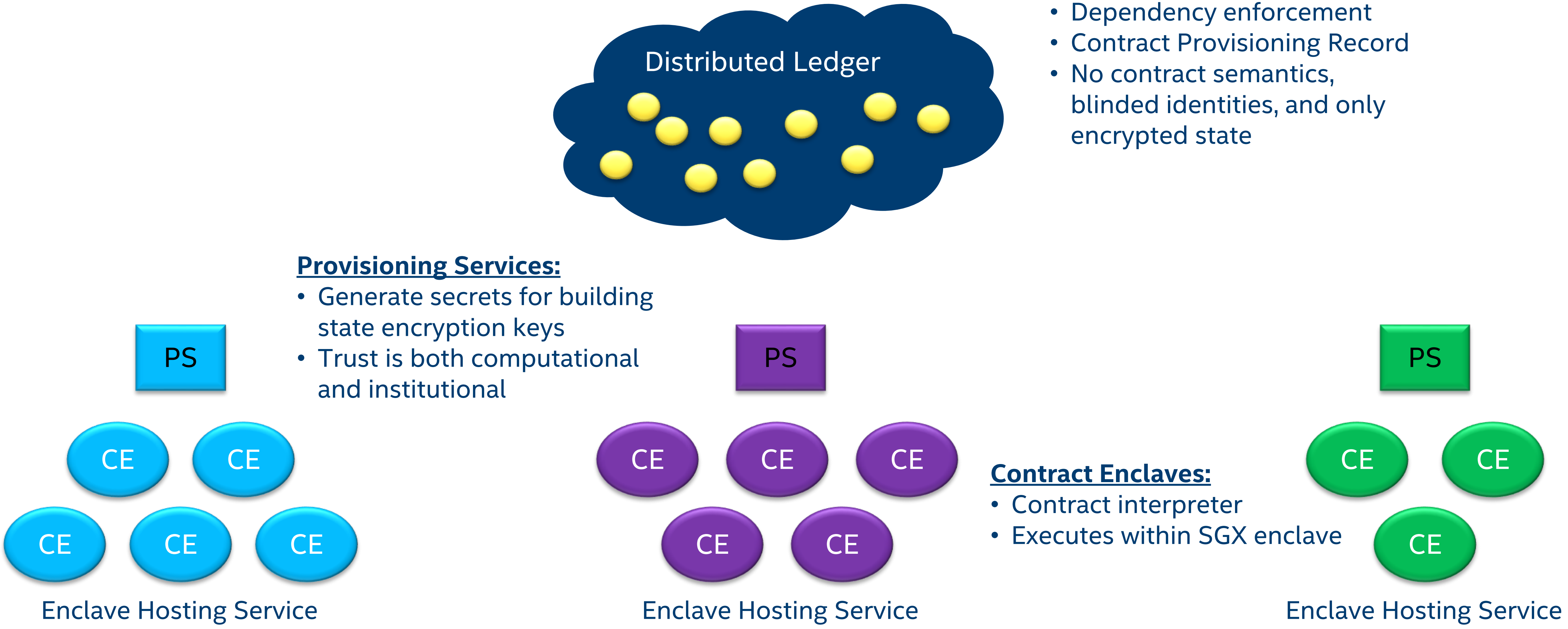
Hardware-Enhanced Security

More information : https://www.intel.com/content/www/us/en/security/blockchain-overview.html

Private Data Object
-Service Deployment Architecture

Distributed Ledger:

- Decentralized commit log
- Dependency enforcement
- Contract Provisioning Record
- No contract semantics, blinded identities, and only encrypted state



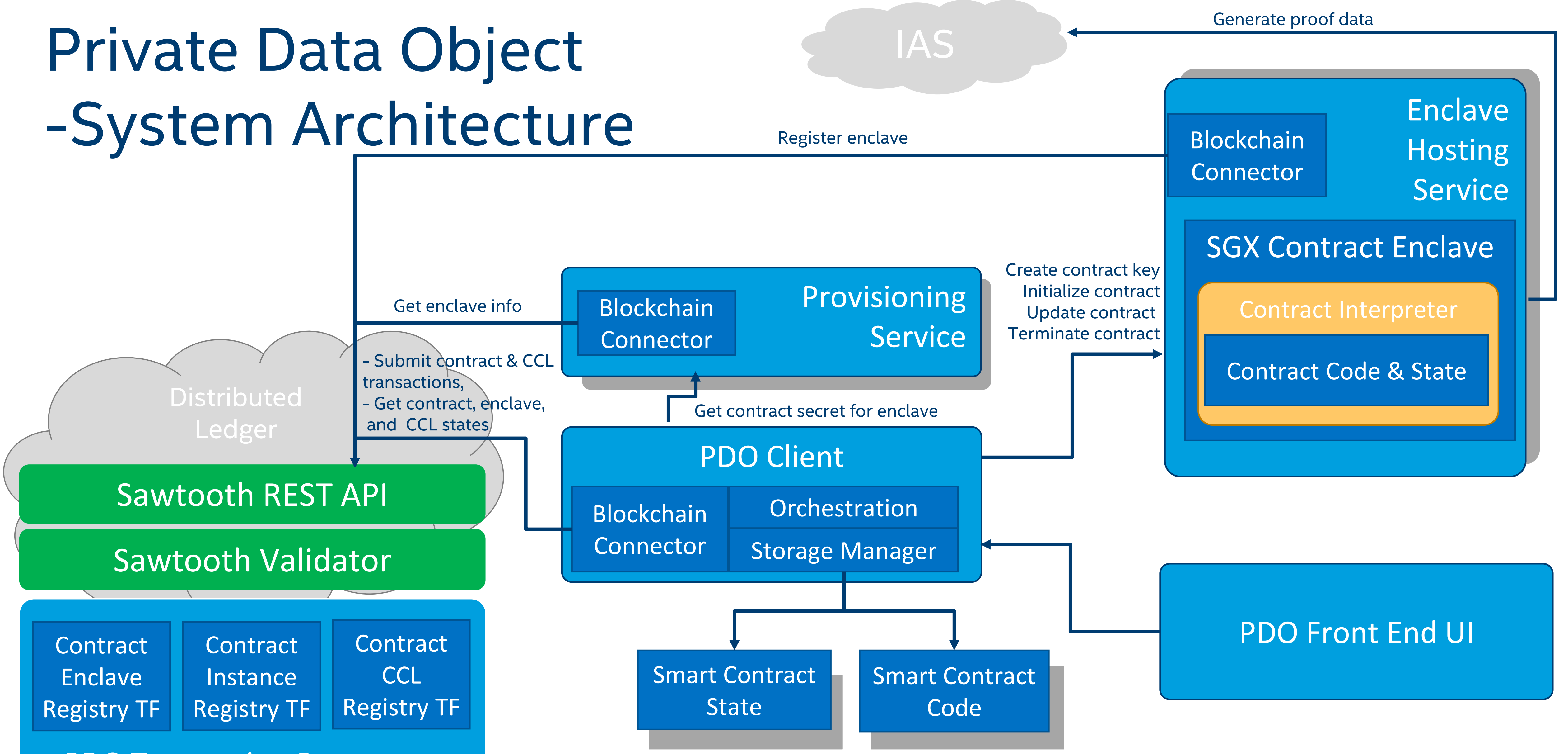
Provisioning Services:

- Generate secrets for building state encryption keys
- Trust is both computational and institutional

Contract Enclaves:

- Contract interpreter
- Executes within SGX enclave

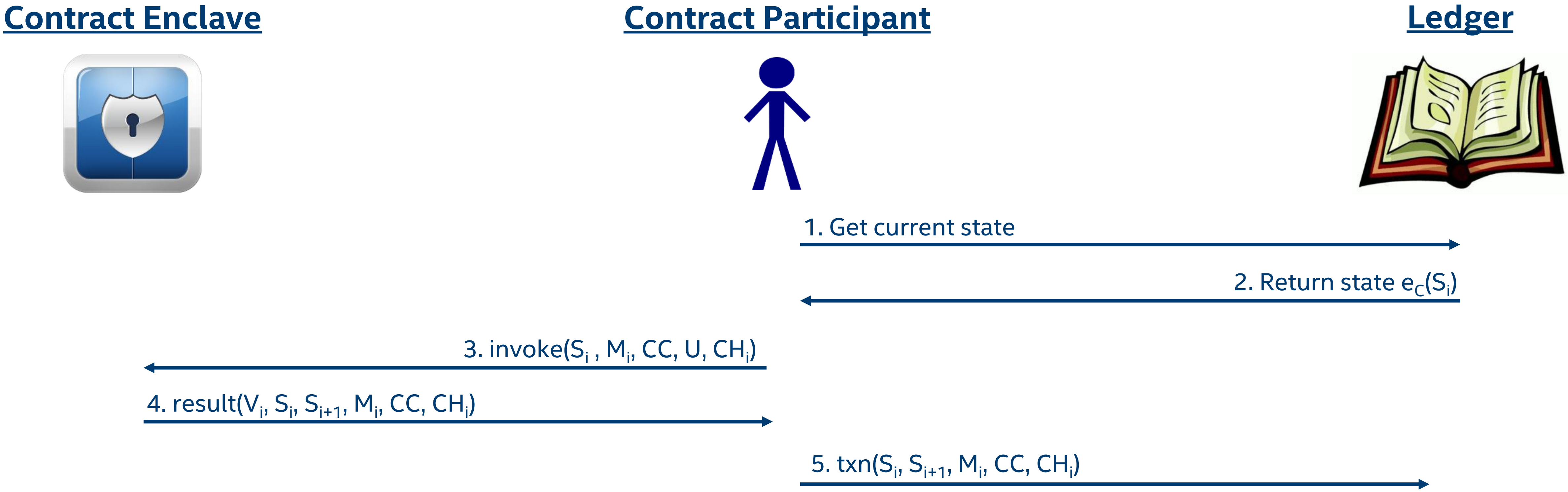
Private Data Object -System Architecture



CCL – Coordination and Commit Log
TF – Transaction Family

🟨🟩 Existing Sawtooth code & contract interpreter
🟦🟦 PDO POC code – new development

Private Data Object
-Method Invocation (Transaction)



Contract Enclave

Contract Participant

Ledger

1. Get current state

2. Return state $e_C(S_i)$

3. invoke(S_i , M_i, CC, U, CH_i)

4. result(V_i, S_i, S_{i+1}, M_i, CC, CH_i)

5. txn(S_i, S_{i+1}, M_i, CC, CH_i)

Ledger orders state transitions; a state change is not valid until it is committed in the ledger

Thanks