CLOUD NATIVE

Wasm DAY

Build Trusted Cloud Apps with Wasm: WebAssembly Micro Runtime is Ready

Xin Wang (Intel)

Acknowledges: Mic Bowman (Intel), Jia Zhang (Alibaba)

Build trusted cloud apps: the challenges

The owners of cloud applications:

- How to protect my cloud code and data from being accessed by either the CSP, hackers or other malicious cloud applications?

The cloud service providers:

- How to solve the customers' security concerns of moving critical application and data to the cloud?
- How to prevent the client applications from attacking the host systems?

The data suppliers (optionally):

- How to ensure the certificated apps for consuming my data are running in a secure environment with full integrity?

WebAssembly on SGX as a solution

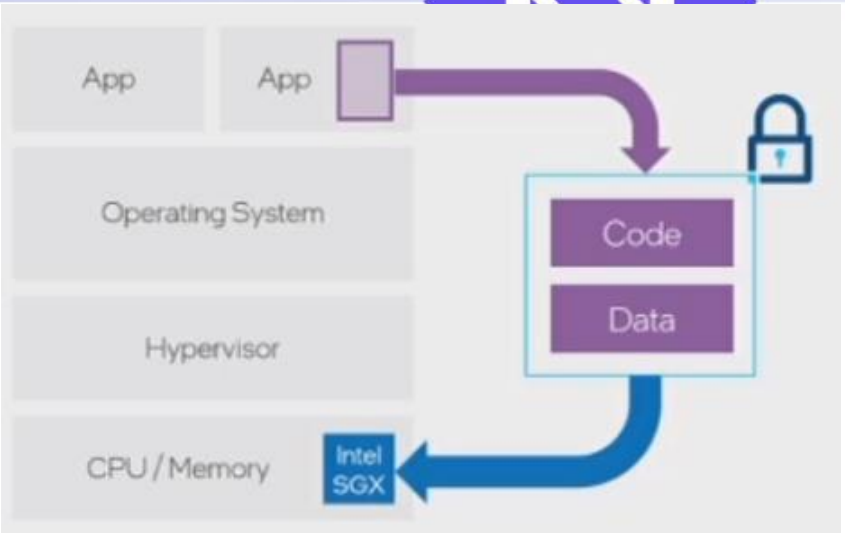
Trust Execution Environment (TEE) provides hardware isolation for code execution and data

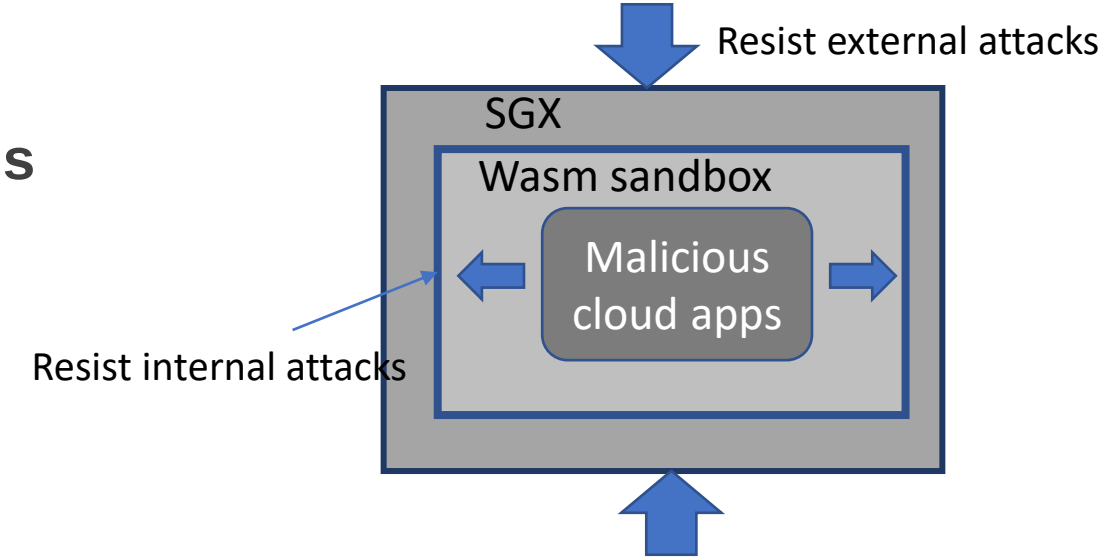
Intel Software Guard Extension (SGX) for data center

- Available cross the entire line of Ice Lake Scalable processors

WebAssembly provides a lightweight sandbox that supports scalable concurrent executions

WebAssembly on SGX provides bi-directions protections for both CSP and cloud applications





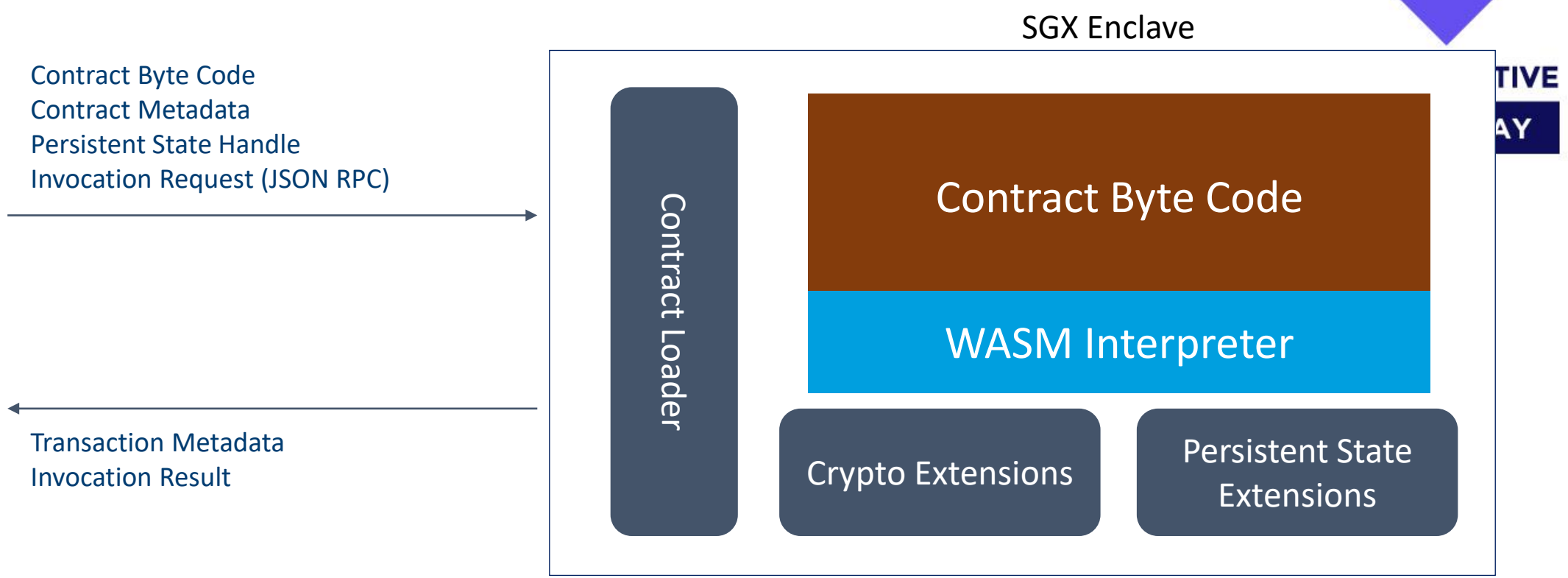
WebAssembly Micro Runtime for SGX

WebAssembly Micro Runtime (WAMR) is a Bytecode Alliance open-source project with supporting SGX as the first-class citizen

- Extremely small TCB (<100KB binary size)
- Supporting both interpreter and Ahead of time compilation for SGX
- Supporting WASI (libc) based on the Intel SGX SDK
- Supporting Wasm SIMD for SGX
- Supporting multiple AI frameworks (TF, XNNPACK) on WASM inside SGX enclave
- Adoptions by SGX/TEE based commercial solutions and open-source projects
    - PDO, Inclavare, TFaaS

Private data objects: Smart Contracts for SGX

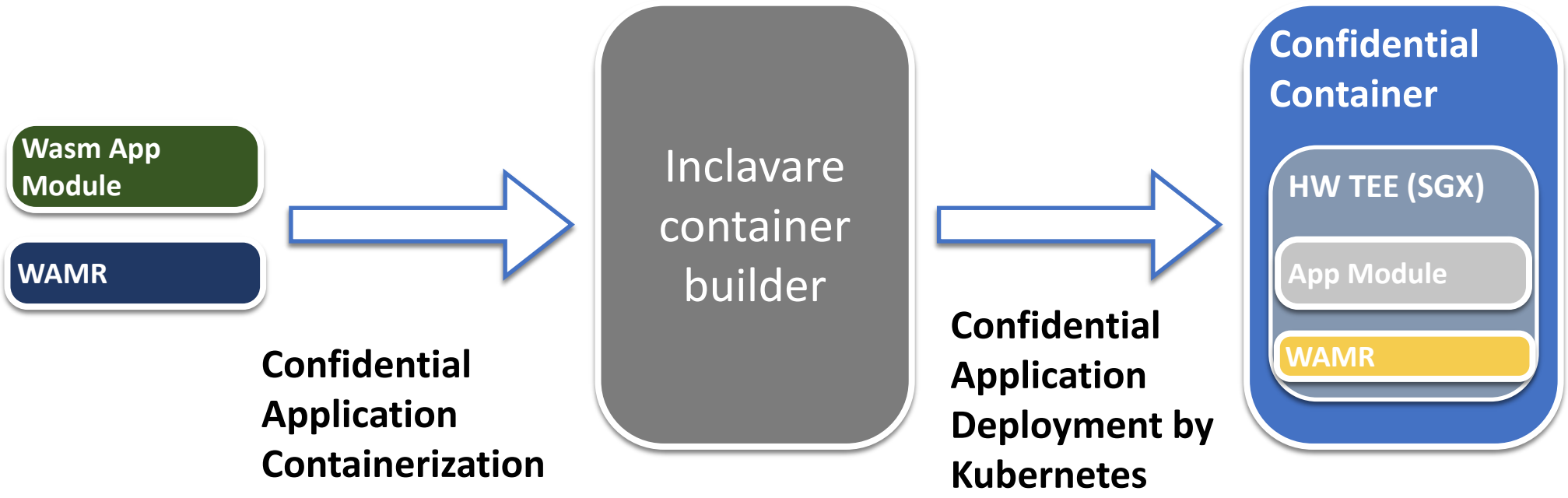
Wawaka Interpreter For Private Data Objects



Byte code – provided by the contract writer
WASM interpreter – provided by WAMR
Loader and Extensions – provided by PDO

https://github.com/hyperledger-labs/private-data-objects

Inclavare Container project: Build confidential containers with Wasm for SGX



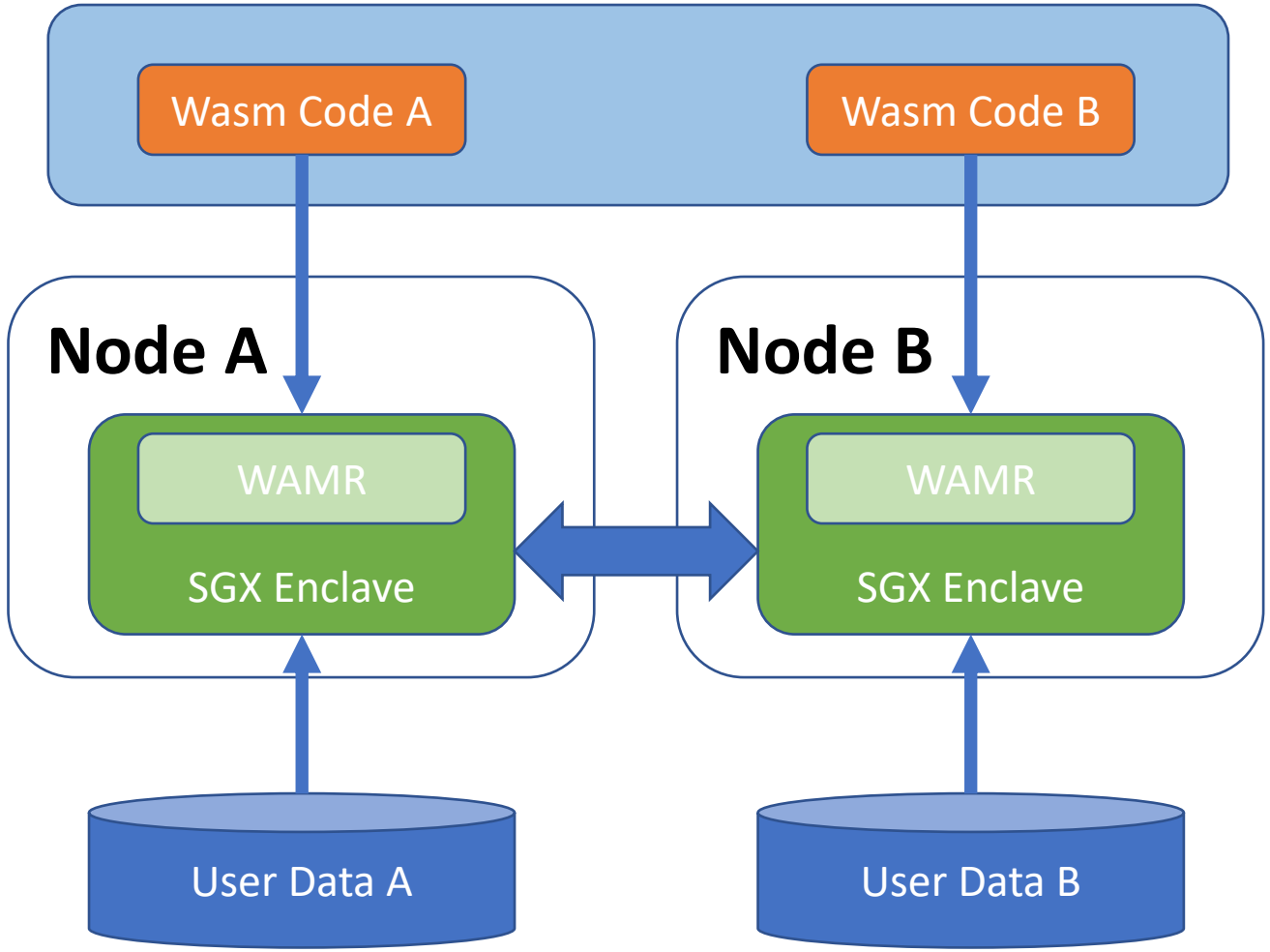
CLOUD NATIVE Wasm DAY

An infra that builds confidential containers for TEE and extend Kubernetes cross the TEEs

- Build confidential containers cross supporting multiple hardware-based TEEs
- Run unmodified application modules in hardware-based TEE
- Provide confidentiality, integrity, and attestation for the application modules

https://github.com/alibaba/inclavare-containers

A trusted multi-party computation usage



1. Each party creates a Wasm module serving data consumer or supplier
2. The source code of Wasm modules are multiparty reviewed and signed
3. The infra supports establishing trusted and secure channel between two Wasm apps
4. Ensured confidentiality and integrity through attestation by SGX

Call for action

Download WAMR from GitHub and try it out with SGX

https://github.com/bytecodealliance/wasm-micro-runtime