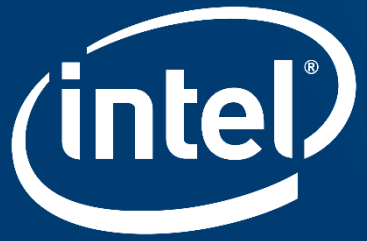


Blockchain and Trusted Execution Environments

Mic Bowman
Senior Principal Engineer, Intel Labs

Legal Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

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

No product or component can be absolutely secure.

Trusted Execution Environments

Confidentiality, integrity, attestation

AND side channels, single vendor, single root of trust, …

Blockchain

Immutable record, cryptographic assurance, trusted authority

AND… inefficient, redundant, complex key management

But More Than That…

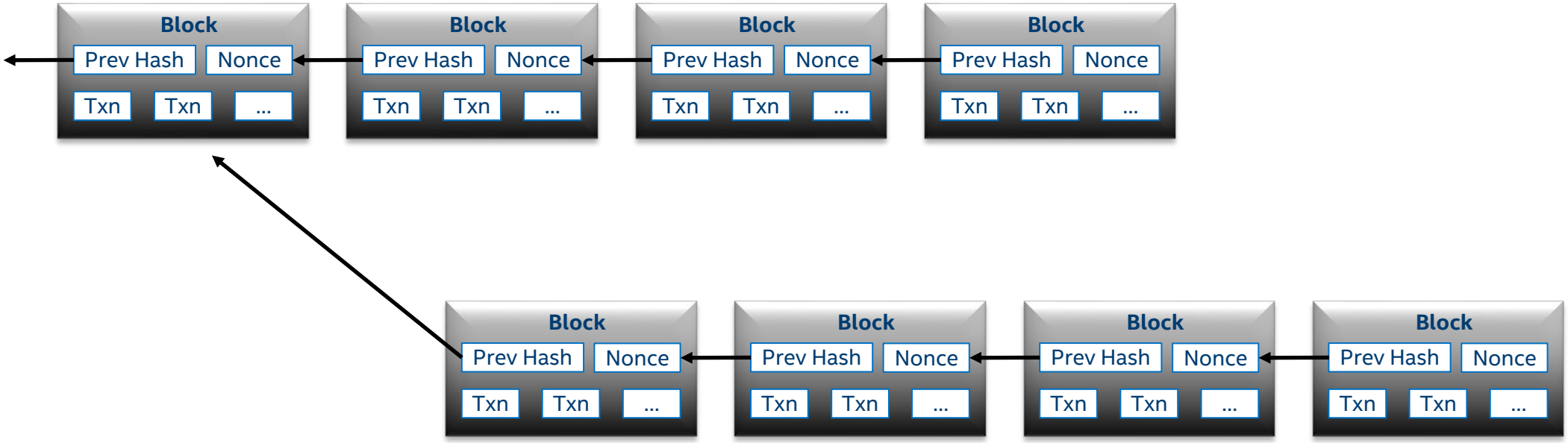
CoinDesk

Ethereum Classic Hit by Third 51% Attack in a Month

August has been an awful month for Ethereum Classic as the blockchain suffered yet another 51% attack.

By Zack Voell · Aug 29, 2020 at 5:00 p.m. MDT · Updated Sep 14, 2021 at 3:49 a.m. MDT

Coindesk, Sep 14, 2021
https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/



What Happens When the 51% Assumption Is Wrong?

(Or When There are More Than f Bad Actors?)

Why Use Blockchain If It Isn't Perfect?

Because Its Worth the Risk

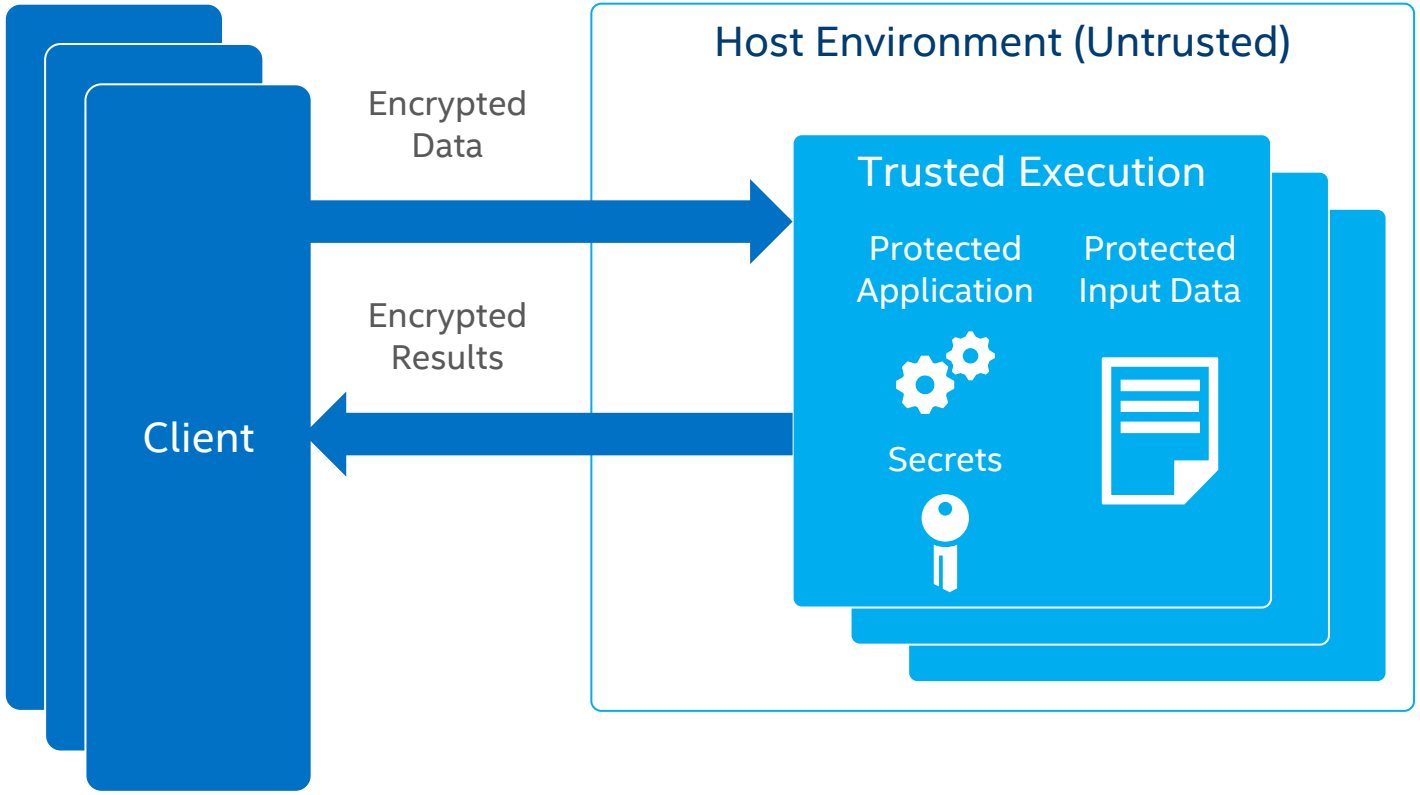
There Are No Perfect Solutions

Its always about managing risk (and the price that must be paid to reduce it)

TEE’s and Blockchain

TRUSTED EXECUTION ENVIRONMENTS (TEE)

A TEE provides software a protected place to execute without external interference.



CONFIDENTIALITY:

- **Protects sensitive execution** from platform software outside of the TEE
- **Secrets** (data/keys/et al) remain protected even when attacker has control of platform

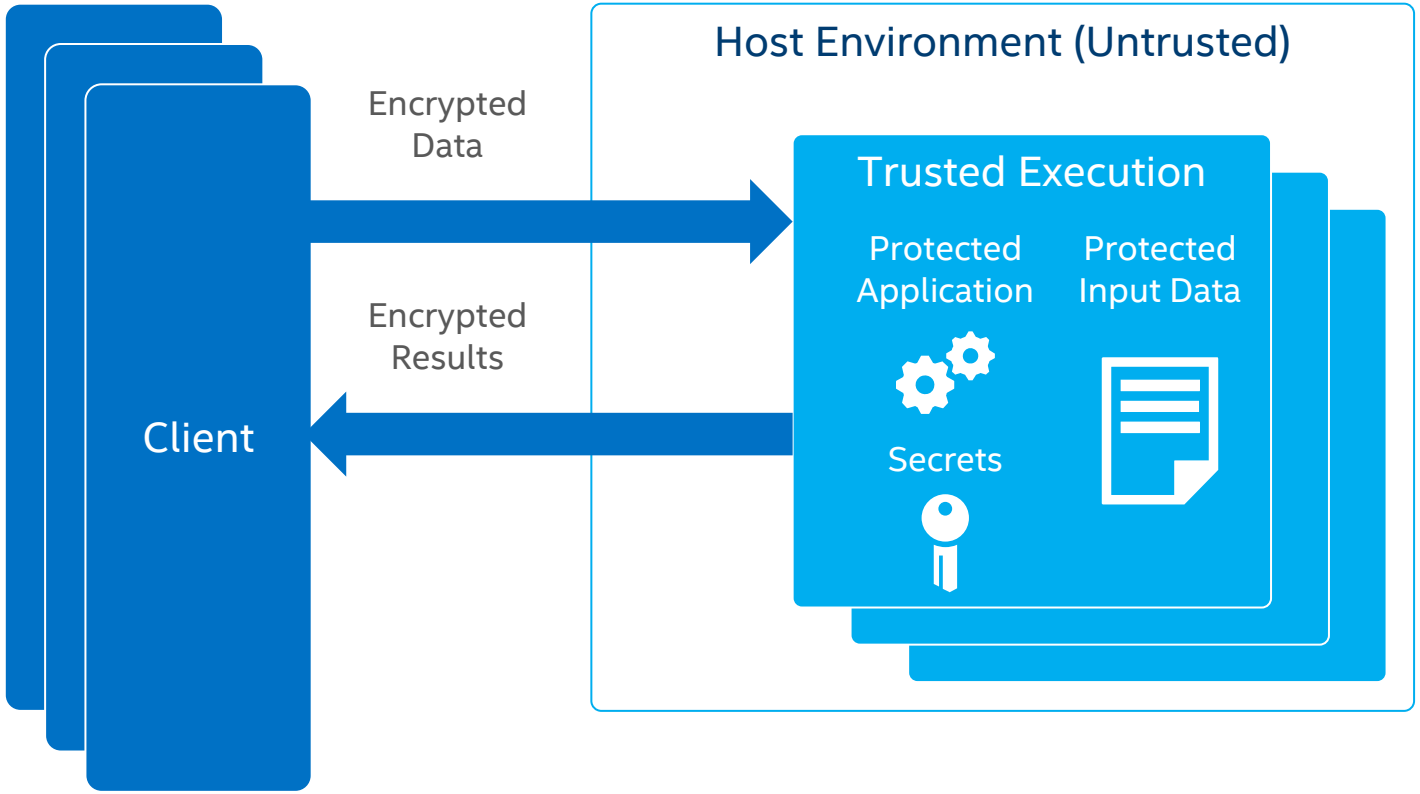
(VERIFIABLE) INTEGRITY

- **Prevent** select **hardware attacks** like memory bus snooping, memory tampering, and "cold boot" attacks against memory contents in RAM
- **Hardware-based attestation** capabilities to measure and verify valid code and data signatures

TRUSTED EXECUTION ENVIRONMENTS (TEE)

A TEE provides software a protected place to execute without external in

This is what matters to most TEE users



CONFIDENTIALITY:

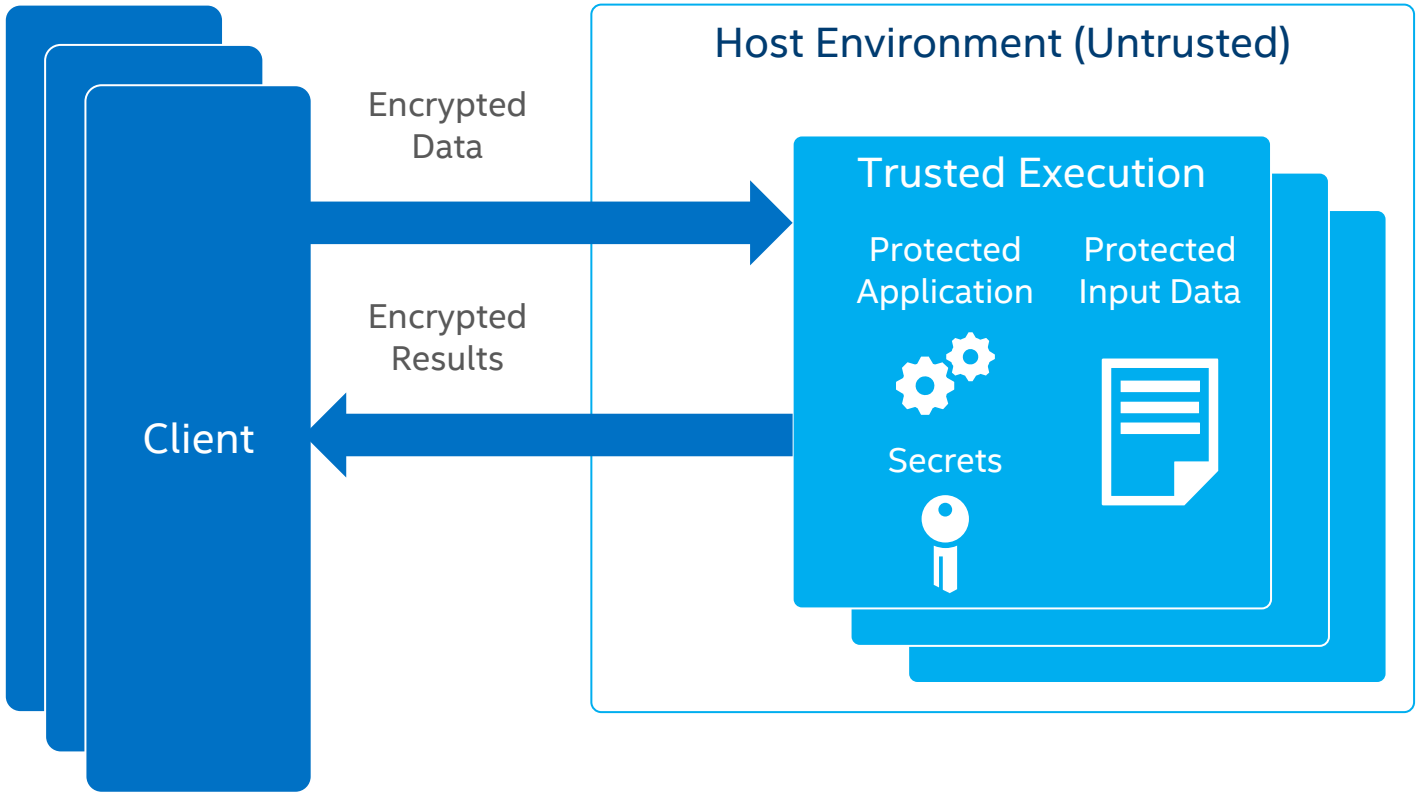
- **Protects sensitive execution** from platform software outside of the TEE
- **Secrets** (data/keys/et al) remain protected even when attacker has control of platform

(VERIFIABLE) INTEGRITY

- **Prevent** select **hardware attacks** like memory bus snooping, memory tampering, and "cold boot" attacks against memory contents in RAM
- **Hardware-based attestation** capabilities to measure and verify valid code and data signatures

TRUSTED EXECUTION ENVIRONMENTS (TEE)

A TEE provides software a protected place to execute without external interference.



CONFIDENTIALITY:

- **Protects sensitive execution** from platform software outside of the TEE
- **Secrets** (data/keys/et al) remain protected even when attacker has control of platform

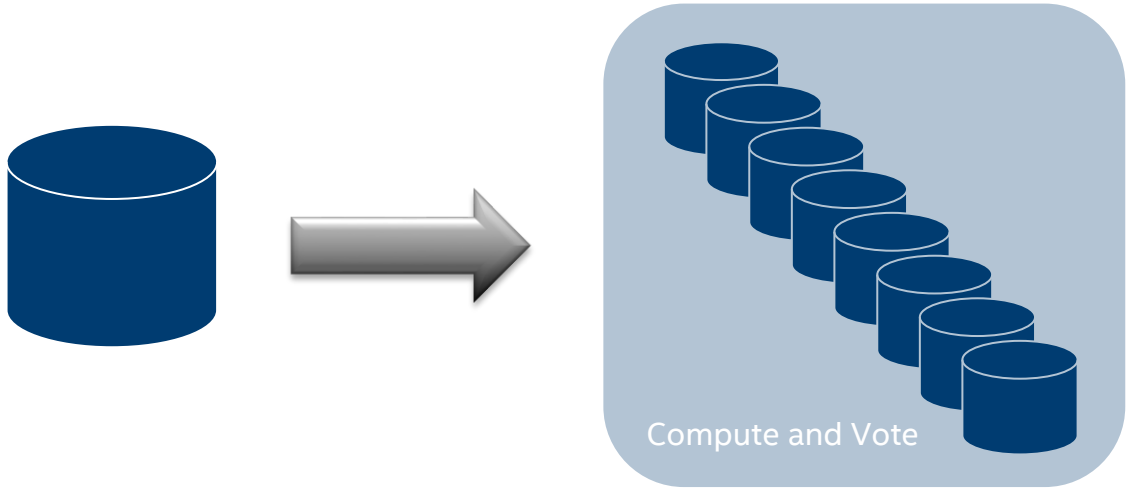
(VERIFIABLE) INTEGRITY

- **Prevent** select **hardware attacks** like memory bus snooping, memory tampering, and "cold boot" attacks against memory contents in RAM
- **Hardware-based attestation** capabilities to measure and verify valid code and data signatures

This is what matters for decentralized computing

Core Principle of Decentralized Compute

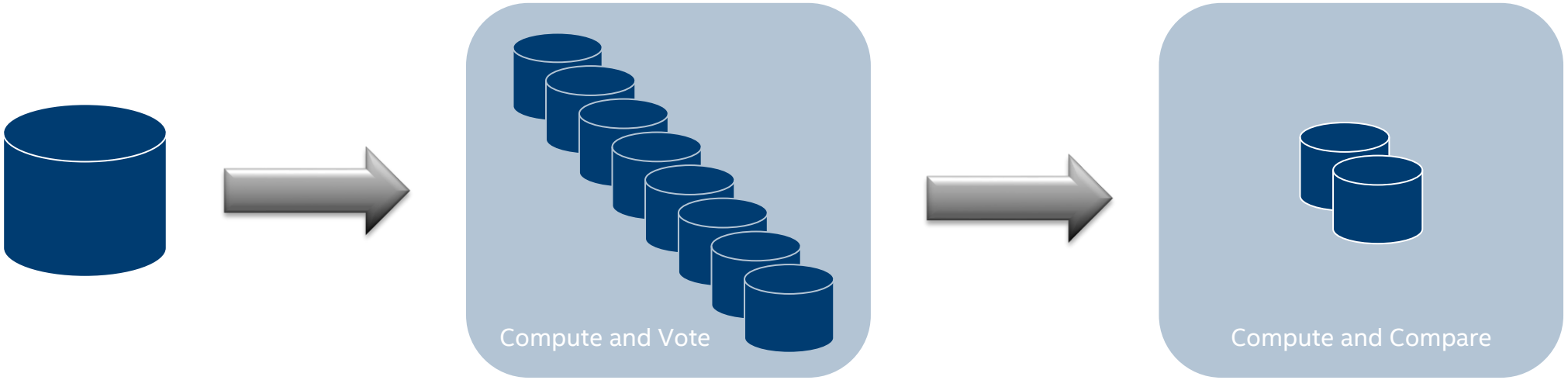
Redundant Compute Replaces Centralized Trust



Single Organization
Centralized Trust
Single Computation

Community Vote
Decentralized Trust
Redundant Computations and a Final Vote

Decentralized Compute with a TEE



Single Organization
Centralized Trust
Single Computation

Community Vote
Decentralized Trust
Redundant Computations and a Final Vote

HW-Based TEE
Efficient Decentralized Trust
Trusted Computation and Attestation

Private Data Objects

Smart Contracts for Data Access

Encrypt the data

- Not sufficient to just have the data
- Must have the key to access

Wrap data with a “smart contract”

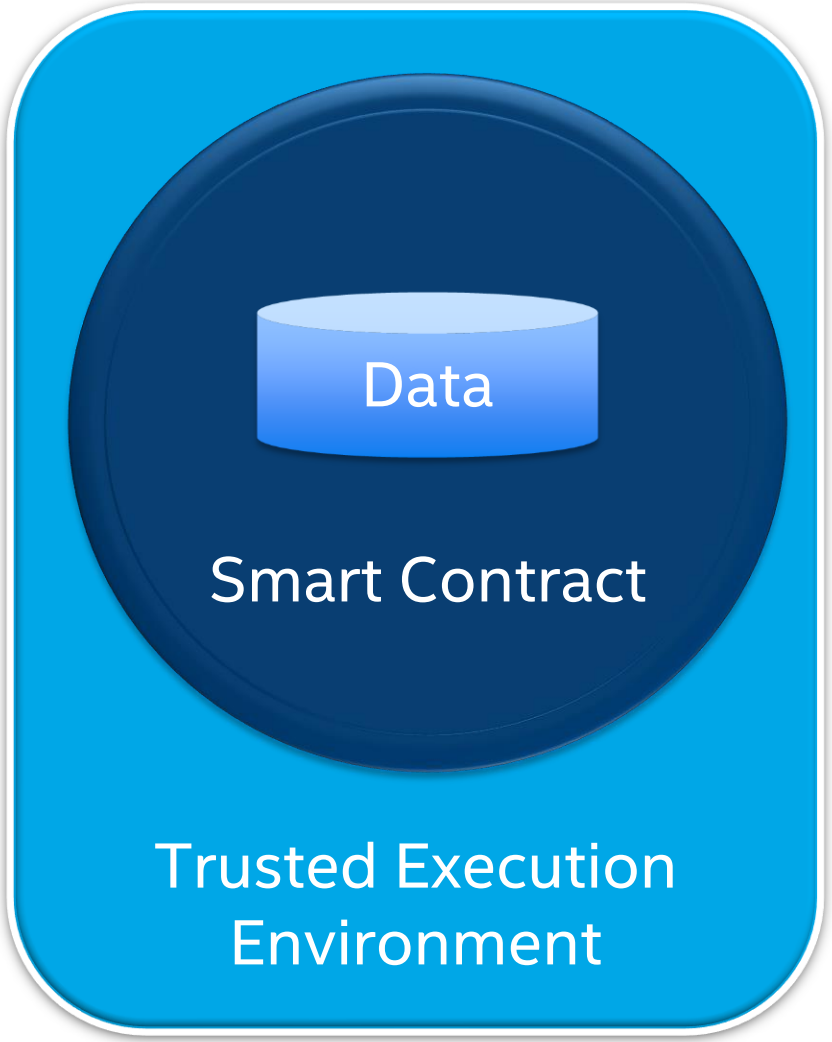
- Formalizes access and update policies
- Can express far more than “open”, “read”, “write”
- **Private Data Object**

Execute “smart contract” in a TEE

- Binds the key to the smart contract
- The ONLY way to access data is through the contract

Blockchain is the root of trust

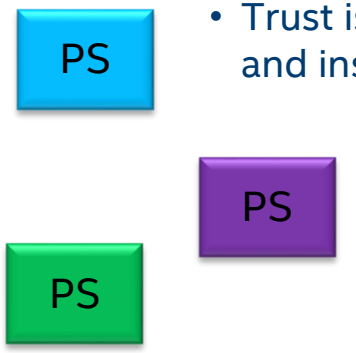
- Commitment: auditable record of agreements and policy
- Integrity: Identifies authoritative instances
- Coordination: Atomicity of transactional updates

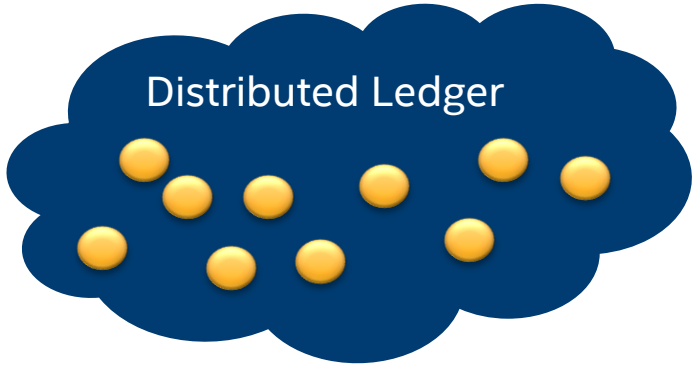


https://github.com/hyperledger-labs/private-data-objects

PDO Architecture

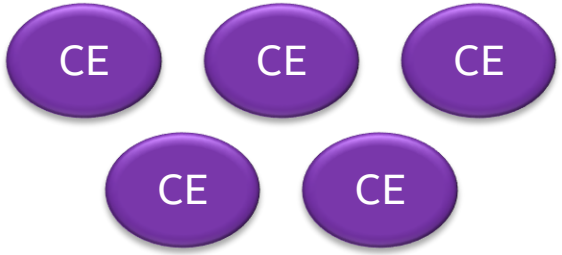
Contract Provisioning Svcs:
- Generate secrets for building state encryption keys
- Trust is both computational and institutional





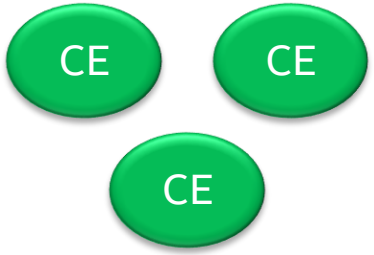
Distributed Ledger:
- Enclave Registry
- Decentralized commit log
- Contract Provisioning Record
- No contract semantics, blinded identities, and only encrypted state

Decentralized Storage Svcs:
- Guarantee state storage for a short period of time



Enclave Hosting Service

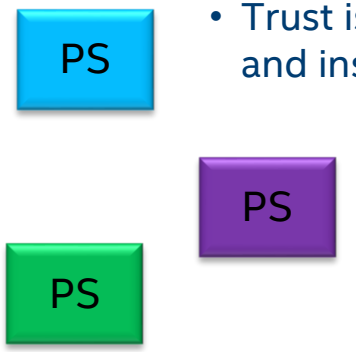
Contract Enclaves:
- Contract interpreter
- Executes within enclave

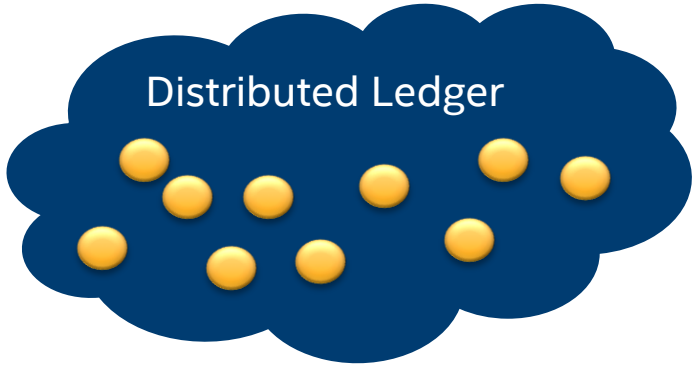


Enclave Hosting Service

PDO Architecture

Contract Provisioning Svcs:
- Generate secrets for building state encryption keys
- Trust is both computational and institutional





Distributed Ledger:
- Enclave Registry
- Decentralized commit log
- Contract Provisioning Record
- No contract semantics, blinded identities, and only encrypted state

Decentralized Storage Svcs:
- Guarantee state storage for a short period of time

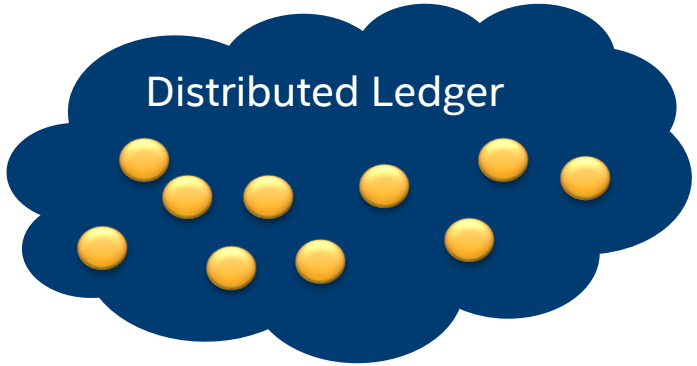
PDO Architecture

Contract Provisioning Svcs:
- Generate secrets for building state encryption keys
- Trust is both computational and institutional

PS

PS

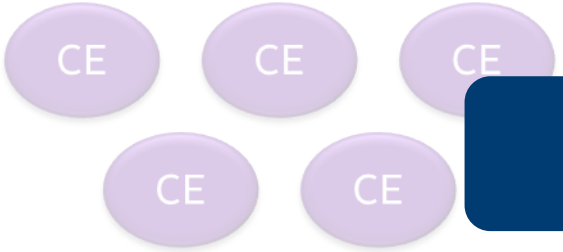
PS



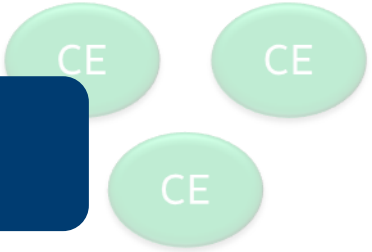
Distributed Ledger:
- Enclave Registry
- Decentralized commit log
- Contract Provisioning Record
- No contract semantics, blinded identities, and only encrypted state

Decentralized Storage Svcs:
- Guarantee state storage for a short period of time

Decentralized Contract State Storage



TEE-Based Contract Execution



Enclave Hosting Service

Enclave Hosting Service

PDO Architecture

Contract Provisioning Svcs:
- Generate secrets for building

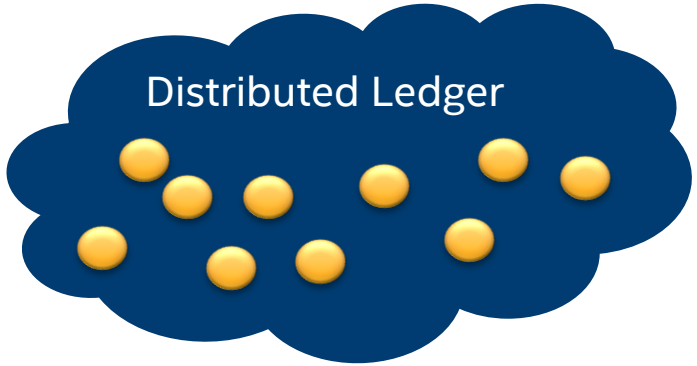
State Encryption Key Generation (MPC)

PS

PS

Decentralized Storage Svcs:
- Guarantee state storage for a short period of time

Decentralized Contract State Storage



Distributed Ledger:
- Enclave Registry
- Decentralized commit log
- Contract Provisioning Record
- No contract semantics, blinded identities, and only encrypted state

CE CE CE CE CE

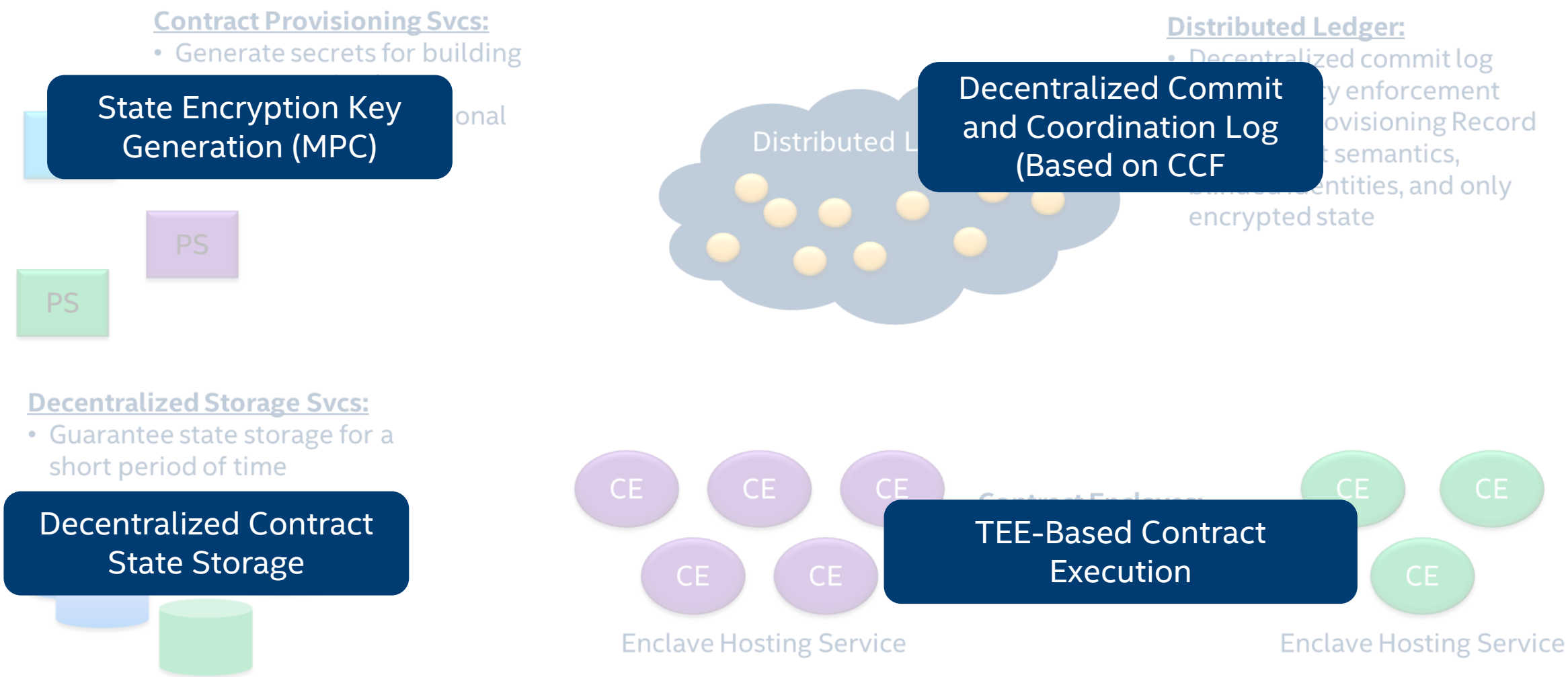
TEE-Based Contract Execution

CE CE CE

Enclave Hosting Service

Enclave Hosting Service

PDO Architecture



Attacks Happen…

Question: Why Should We Trust the TEE as the Sole Arbiter of Truth About Contract Execution?

Attacks Happen…

Question: Why Should We Trust the TEE as the Sole Arbiter of Truth About Contract Execution?

Answer: You Shouldn't!
(at least not blindly)

What Good is Trusted Execution?

Camp 1: It works and should be used everywhere!

Camp 2: It doesn't work and shouldn't be used anywhere!

The Middle Ground Assumptions
(In the language of risk)

Works Unless Explicitly Broken

Expensive to Break

Situated in a Larger System

TEE Security Design Principles

For Decentralized Systems

- Assume it works, then assume it doesn't.
  - A TEE can greatly improve performance, efficiency and confidentiality; but you need to figure out what to sacrifice to accommodate potential compromises
- Make sure there are no big targets.
  - For an adversary with a limited budget scalable attacks open the door to compromise the entire system
- Deployment is a fundamental part of the protocol definition.
  - TEE implementations vary widely in the attacks they are designed to prevent. Assumptions about deployment can dramatically strengthen claims about attack resiliency.

PDO Commit Policy

Principle	Realization
Assume It Works, Then Assume It Doesn't	Optimistic Commit: Commit on the claim of one TEE, allow revocation on claim of N TEEs
Make Sure There are No Big Targets	Explicit and limited provisioning of keys limits scalability of any attack
Deployment is a Fundamental Part of the Protocol	Everything about the system can be interrogated; risk can be assessed, and per-user policies applied

Why Use TEE If It Isn't Perfect?

Because Its Worth the Risk

Decentralized Computing in the Language of Risk

Be Cognizant of Hidden Assumptions: Be aware that there are always assumptions that can be attacked

Design for Failure: Any system must account for unexpected failures

Defense in Depth: A healthy view puts any security technology into a larger, operational context.

There Are No Perfect Security Technologies