ioBuilders

Privacy on Tokenized RWAs

a design choice, not a switch

INDEX

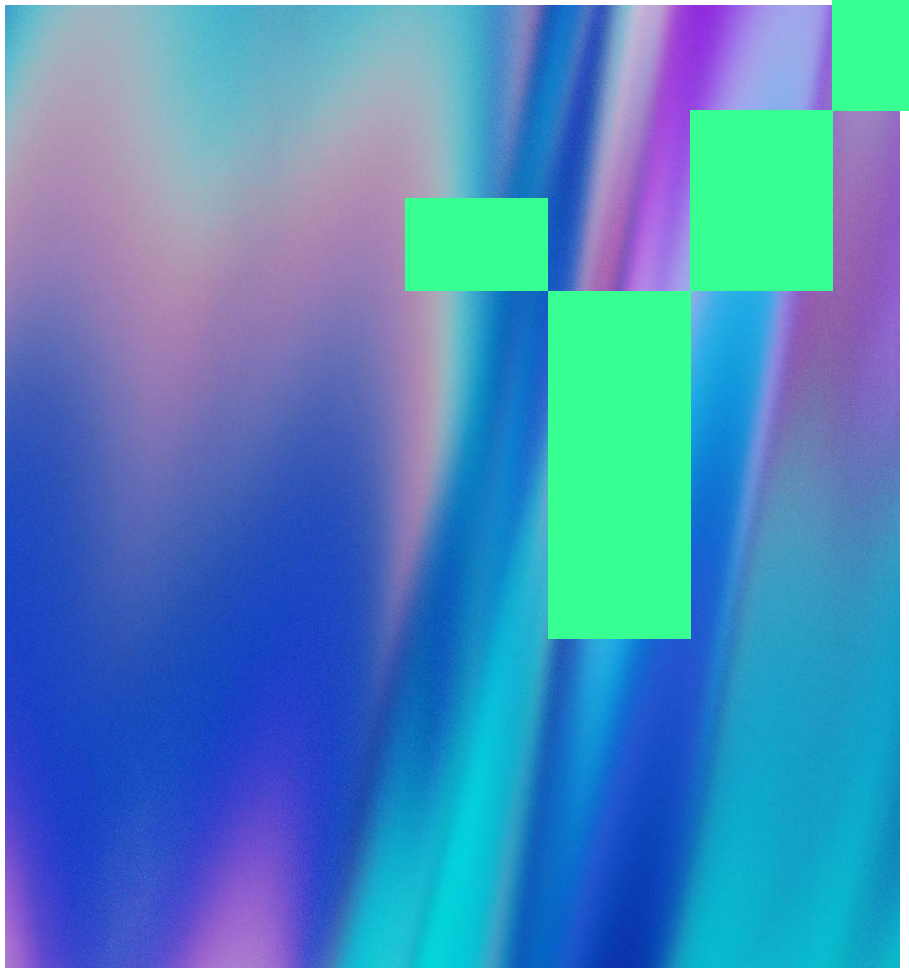
Content

01. Privacy Requirements

02. Privacy Solutions

03. The Asseto Product

04. How Privacy Affects Asseto



01

A precondition for tokenized RWAs, not a feature.

Privacy Requirements

Privacy vs. Auditability

HIDE

The privacy mandate

- Salaries, positions, order size & price
- Bookbuilding, OTC, cross-bank screening
- Hard requirements, not preferences

REVEAL

The auditability mandate

- Disclose under legal process (auditor / view keys)
- MiCA · MiFID II · Travel Rule · OFAC
- Hiding everything fails in regulated finance

The design principle: Auditability where required, privacy where desired.

PRIVACY REQUIREMENTS

The Privacy Spectrum

	Identity VISIBLE	Identity HIDDEN
Data VISIBLE	**Pseudonymity** *Default public-ledger state*	**Anonymity** *Shielded sender / receiver*
Data HIDDEN	**Confidentiality** *Encrypted amounts & data*	**Fully Private** *Confidential compute*

Source: ioBuilders;Solana Foundation's 2026 privacy report

02

Privacy Solutions

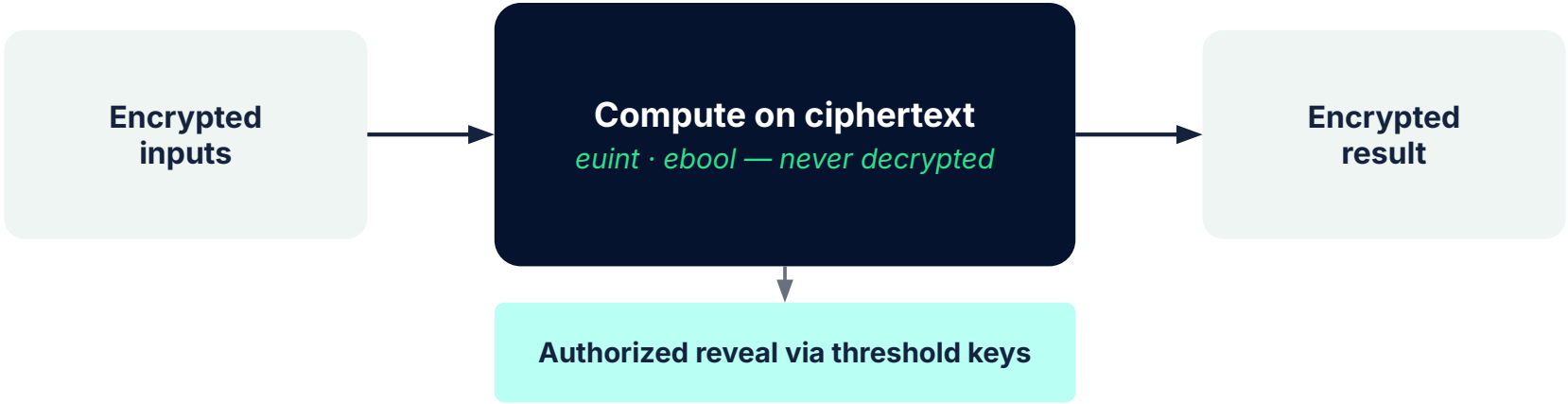
The technologies that matter for enterprise RWAs.

PRIVACY SOLUTIONS

Zama

Fully Homomorphic Encryption · fhEVM

Confidentiality



Native Solidity · any EVM

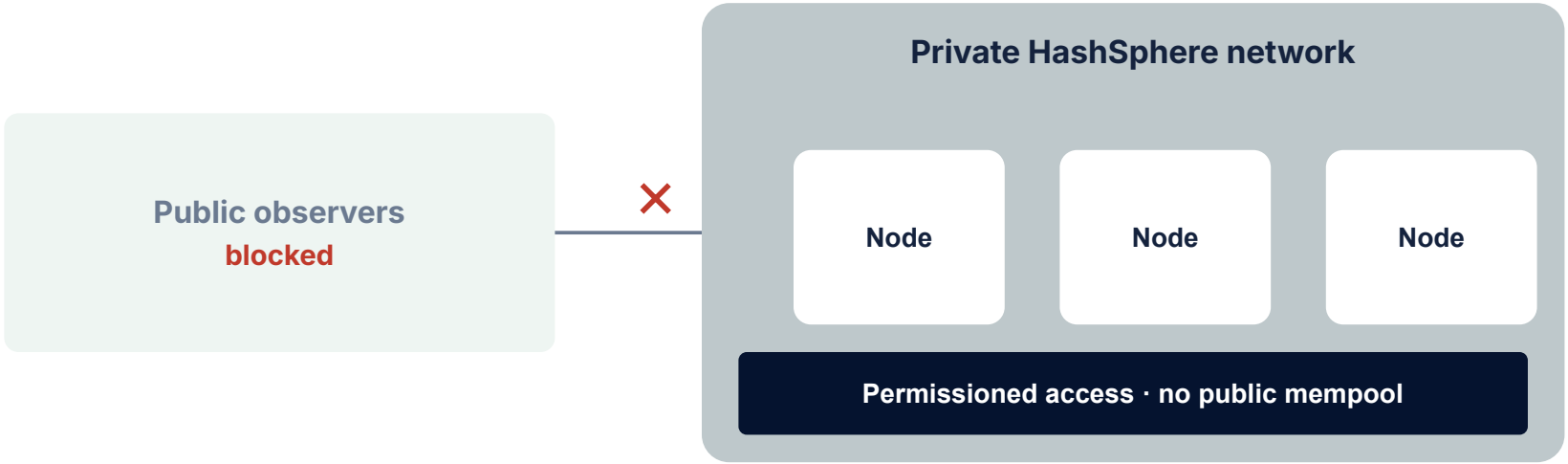
Cost: FHE is heavy

PRIVACY SOLUTIONS

HashSphere

Private permissioned network · Hedera

Fully private / Pseudonymity



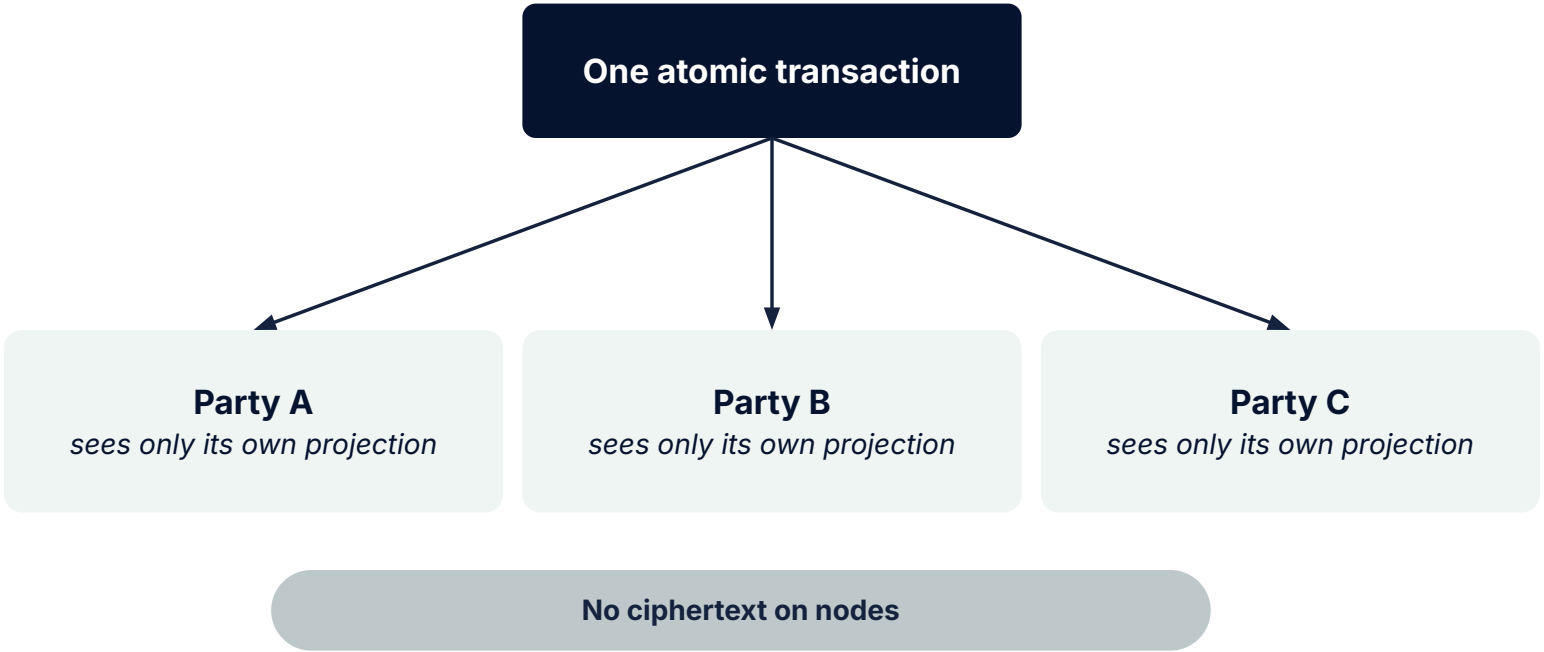
Access-control privacy (not cryptographic)

PRIVACY SOLUTIONS

Canton

DAML · sub-transaction privacy

Fully private



PRIVACY SOLUTIONS

Paladin

Programmable privacy domains on Evm

Fully private

Noto

Mechanism: Notary validation (no ZK)

Does: UTXO confidential tokens; notary writes validated hashes

Note: Full reliance on the notary

Zeto

Mechanism: Zero-knowledge proofs

Does: UTXO confidential tokens; ZK-anchored fungible tokens;

Note: Hard for auditability

Pente

Mechanism: Private EVM groups

Does: Standard EVM in a permissioned group; nodes filter who reads what

Note: Pseudonymity among group members

All three run on Evm and publish succinct anchors to the base chain.

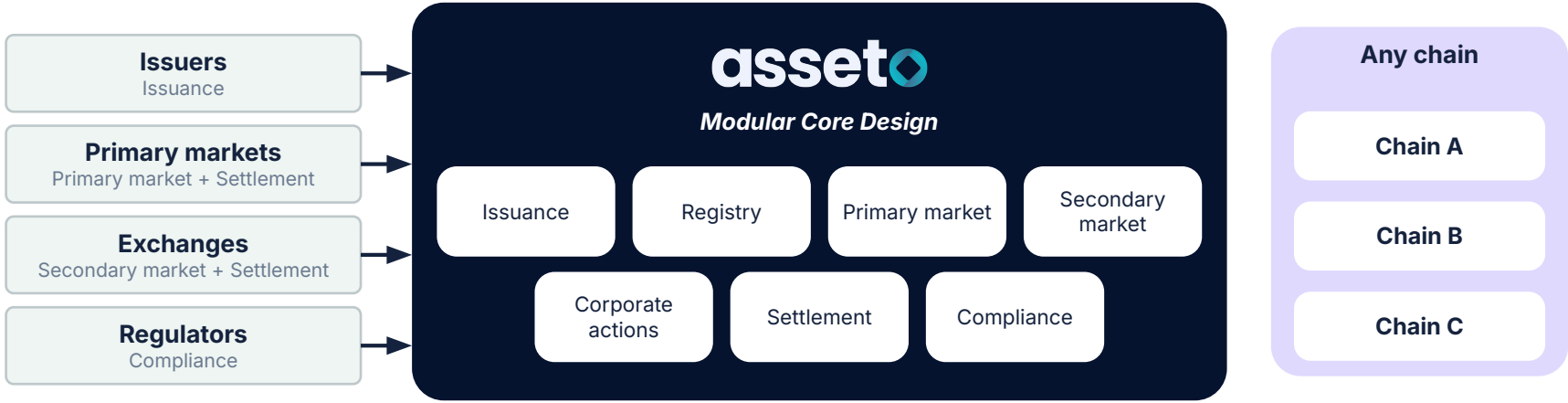
03

Asseto

End-to-end tokenization on a modular, chain-agnostic core.

Asseto Functionality

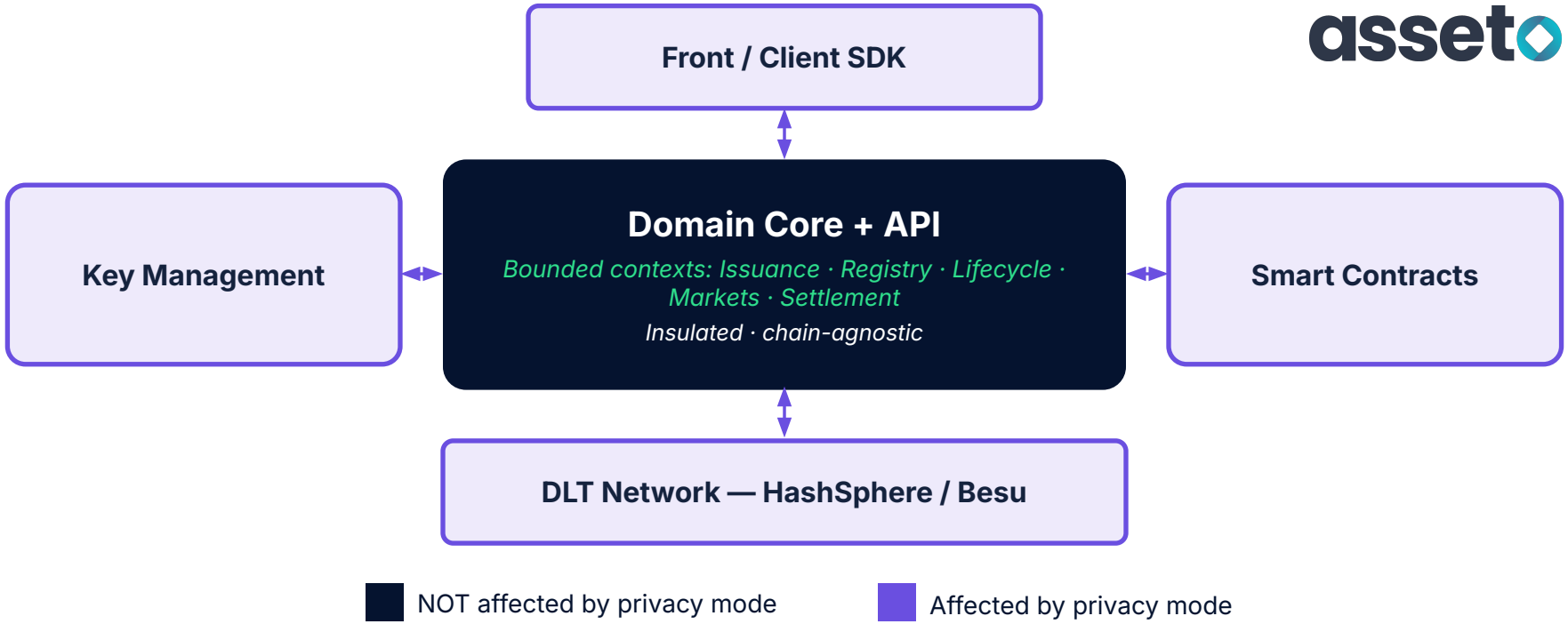
The all-in-one RWA tokenization platform



Each actor activates only the modules it needs

Asseto Architecture

Privacy touches only the 4 outer components — the core + API stay untouched.



04

How privacy affects Asseto

Domain logic untouched. Only four layers are affected.

Smart Contracts

How each privacy mode reshapes the contracts themselves.

Zama	Canton	Paladin	HashSphere
Solidity + encrypted types *euint · ebool · eaddress*	**New language: DAML** *full re-implementation*	**UTXO model** *commitments, not balances*	**Standard Solidity** *contracts unchanged*

Privacy is chosen before deploy — keep a set of contracts per privacy mode.

DLT & Network

Each mode restricts the selectable networks.

Zama	Canton	Paladin	HashSphere
fhEVM-enabled chain *FHE coprocessor* *EVM-compatible*	**Its own DLT** *DAML runtime* *NOT EVM-compatible*	**Runs on Evm** *privacy domains* *EVM-compatible*	**Hedera (HSCS)** *EVM-compatible*

All EVM-compatible ≠ interchangeable — switching privacy mode means a chain migration.

Key Management

Each mode introduces different key material.

Zama	Canton	Paladin	HashSphere
FHE keypair *+ threshold decryption network*	**Identity provider** *issues JWT tokens*	**ZK prover** *client-side proof generation*	**Standard keys / HSM** *no new crypto material*

Auditor & view keys become first-class compliance artefacts.

Front / Client SDK

The Buy-Side Tool is an active cryptographic participant, not a passive view.

Encrypted balances	Regulator disclosure	Shielded pools
Local decryption *client holds a key; RPC returns ciphertext*	**Proof from the wallet** *user holds a view key (distinct credential)*	**Deposit · transfer · withdraw** *new tx flow vs ERC-20 · distinct UX*

Each mode = deliberate SDK + UX work, not a backend toggle.

ioBuilders

Thank You

alberto@io.builders

