OpenZeppelin

openzeppelin.com

Privacy for Tokenized Finance

Options, trade offs, and standards for financial institutions

Jonathan Alexander
Chief Technology Officer

Developing privacy standards and solutions

Leaders in blockchain privacy that trust OpenZeppelin for design, development, standards, and security

- Zama - FHE coprocessor for EVM, coming to SVM
- Miden - ZK layer 2
- Stellar - ZK-enabled layer 1
- Midnight - ZK layer 1
- Zisk - ZK VM prover
- Privacy Boost - ZK TEE privacy pools



Bringing privacy to regulated digital assets on public chains

OpenZeppelin is working with T-REX and Zama to integrate ERC 7984 with ERC 3643, also on Stellar



ERC-7984: The New Confidential Token Standard

ERC-20 with confidential balances and transfers, compatible with FHE, ZK, or other encryption solutions

Encrypted by default

Balances and amounts live on-chain as bytes32 ciphertext handles, not readable numbers. The interface is technology-agnostic — handles can be backed by FHE, ZK, or secure enclaves (TEEs).

Private even during computation

When using FHE encrypted types (euint64): the contract checks, subtracts, and adds balances without ever decrypting them.

Selective disclosure & compliance

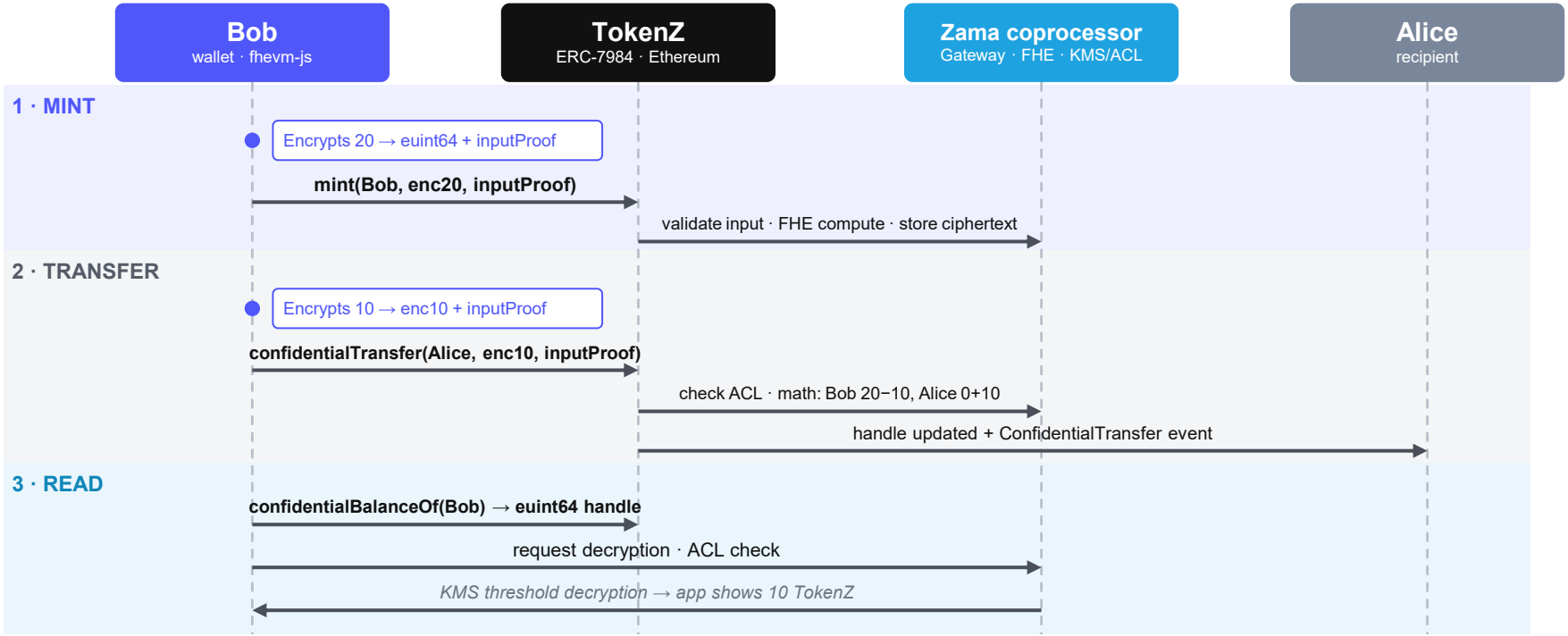
Owners can grant auditors or regulators decryption rights; optional modules add KYC/AML, freezing, and RWA compliance.

Audited & standardized

OpenZeppelin ships the canonical ERC-7984 reference implementation. OZ co-founded the Confidential Token Association with Zama and Inco — now 10+ members including Fhenix, Kaleido, Stellar, and Taurus.

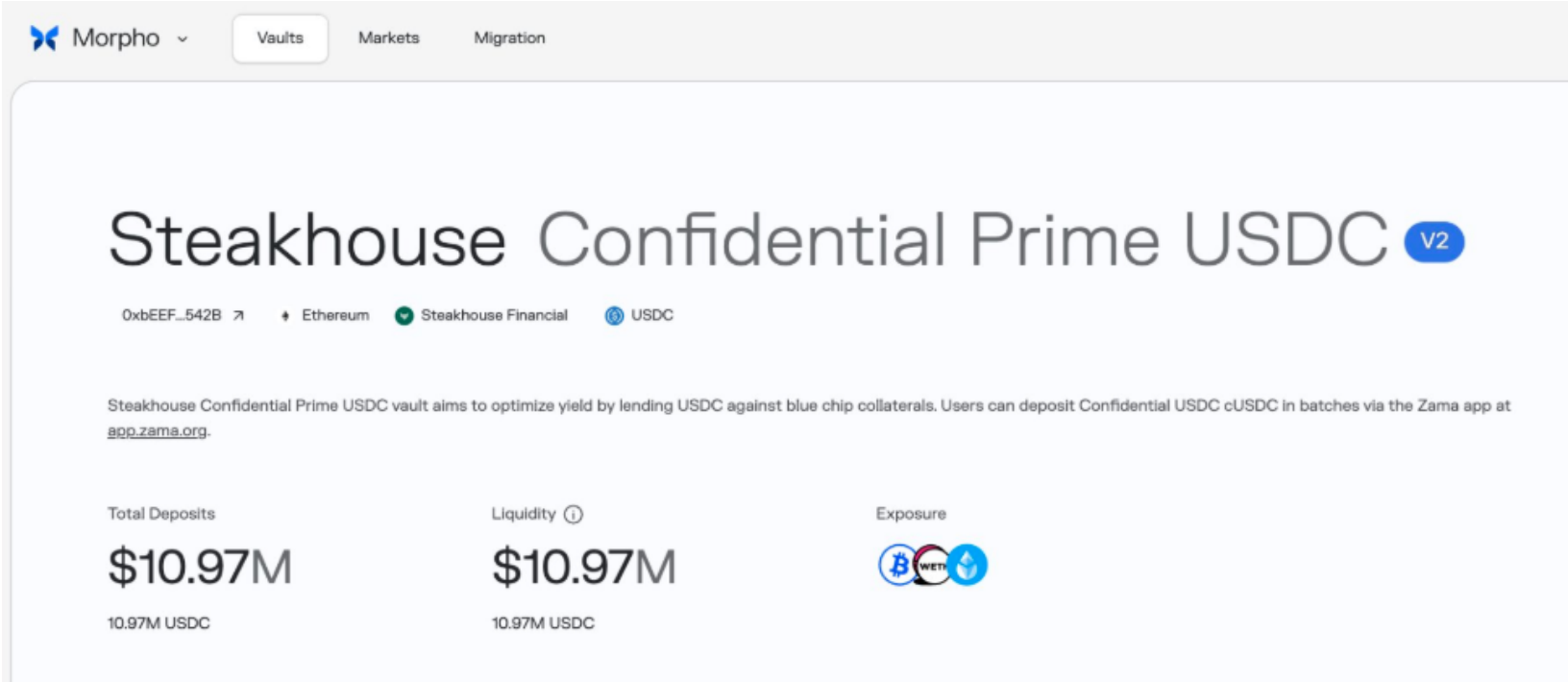
ERC-7984 - how it works

Bob mints 20, sends 10 to Alice, then reads his balance — every amount stays encrypted as ciphertext handles



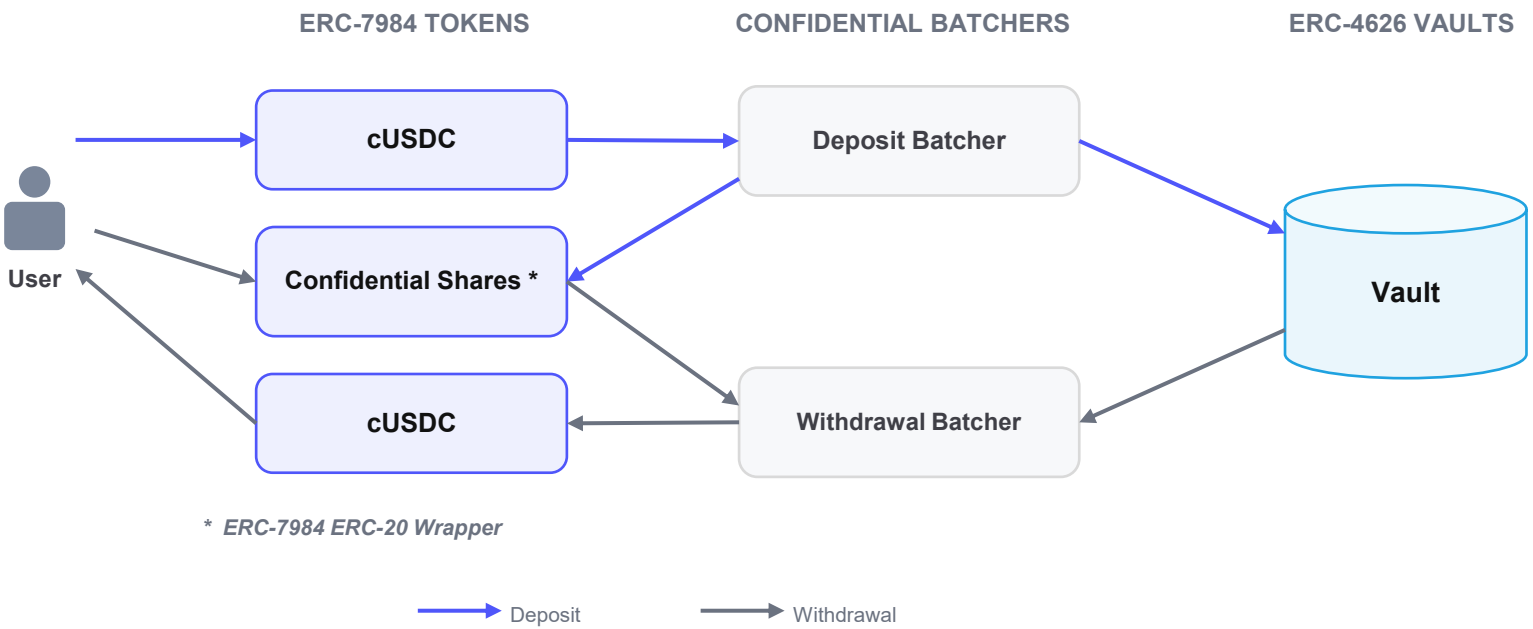
Morpho x Zama launched first confidential vault (June 23rd)

Utilizes ERC 7984 implementation and ConfidentialBatcher designed and implemented by OpenZeppelin



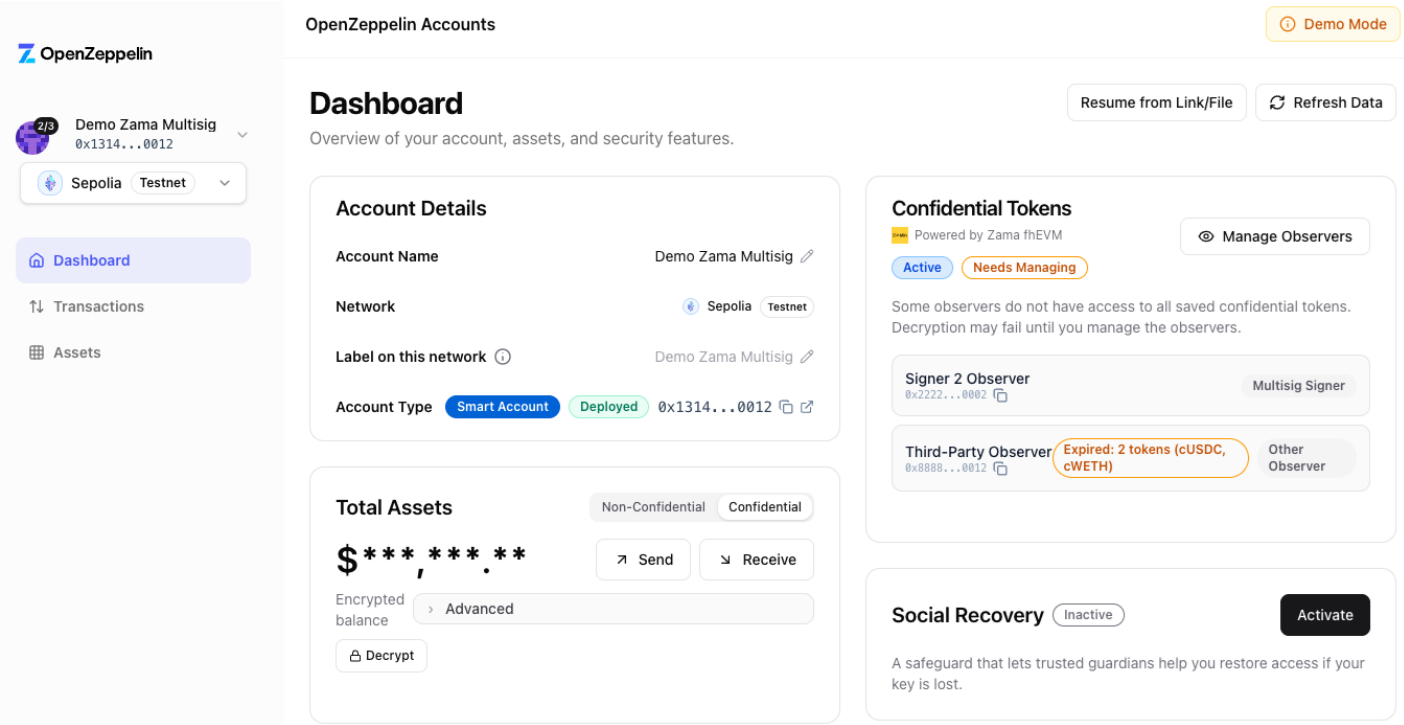
Private deposits into public DeFi with Confidential Batcher

Confidential ERC-7984 tokens flow through batchers into public ERC-4626 vaults — user positions stay private



Next: adding privacy and regulatory compliance to wallets

OpenZeppelin will soon launch ERC 7579 modular smart accounts with privacy features on Ethereum and Stellar



Guardian: Private State Manager (standards publication TBD)

Designed with Miden, OpenZeppelin implementation for Miden, Ethereum, Stellar integrated to ERC 7579 accounts

The challenge

When using ZK or other off-chain encryption/proofs, account state is private and held off-chain; only commitments reach the chain, so there is no public ledger to ensure state is immutable and coordinate shared accounts.

What it is

A coordination layer for private accounts: synchronization, backup, recovery, and multi-party signing — without custody or trust between parties.

How it works

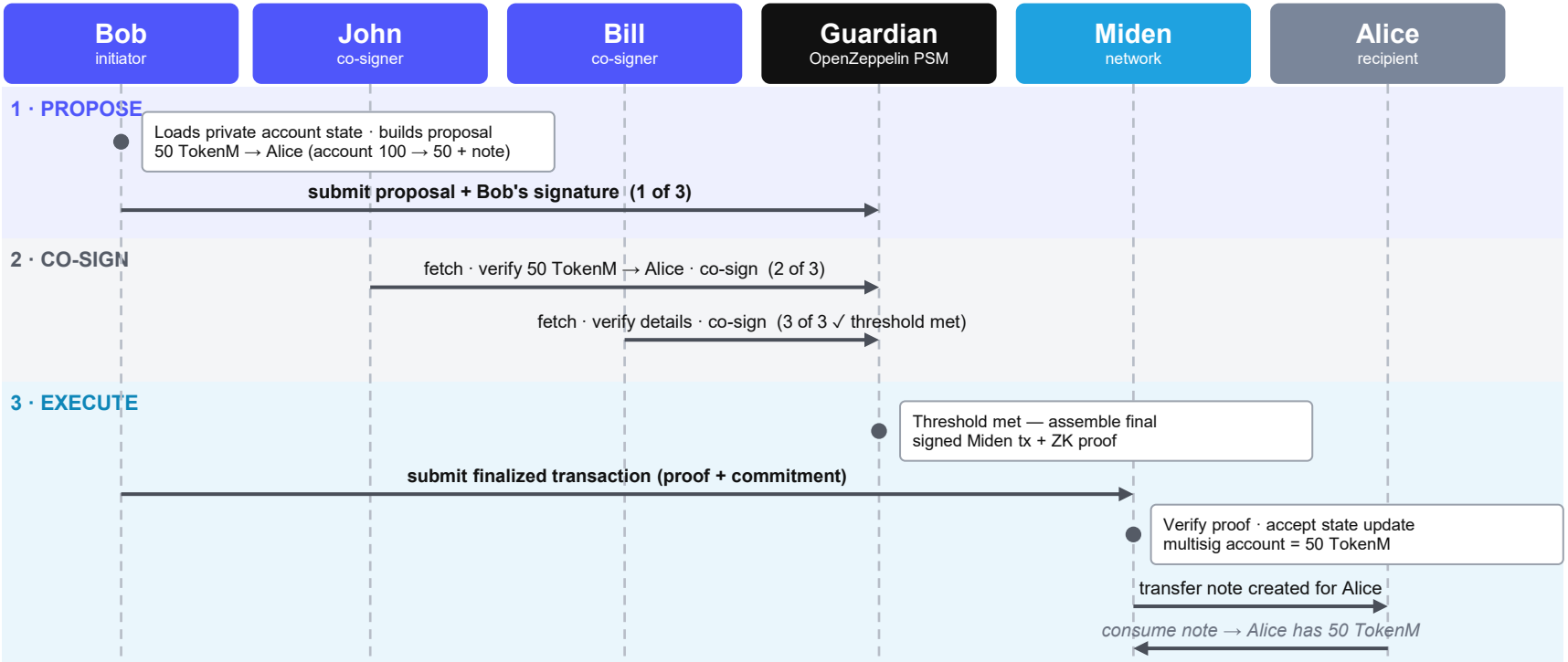
Coordinates private State snapshots and signed Deltas: relays updates, collects threshold approvals off-chain, and confirms via on-chain commitments.

Why it matters

Enables mutl-device and multi-signature privacy without exposing signers, thresholds, or the approval flow. Open-source, audited, and designed jointly with Miden.

Guardian - how it works

Bob, John & Bill co-sign sending 50 TokenM to Alice — Guardian coordinates signing; Miden verifies the proof



Satellite Architecture - Institutional privacy, public chains

Privacy and compliance for institutions using trusted satellite chains connected to shared and public chains

