SOLANA | ZK PROOF | FHE

Compliance-Ready Confidential Transfer

Privacy-preserving transactions with regulatory compliance

Hide Amount

Hide Address

Hide Both

LatticA | ZK + FHE Infrastructure

THE PROBLEM

On-Chain Transparency Breaks Privacy

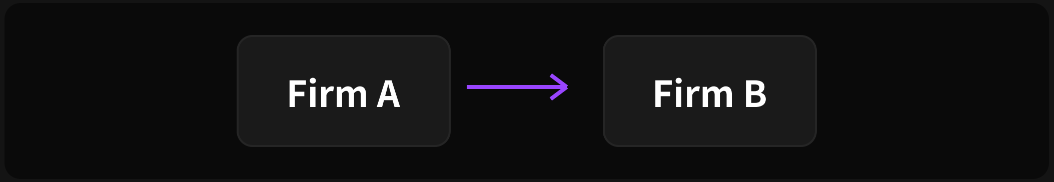
Corporate Payroll

Company Wallet → Employee

AMOUNT	ADDRESS	TIMING
$15,000	0x1a2b...9f	Monthly

Salary, bonus structure, employee wallets all PUBLIC

B2B Settlements


Firm A → Firm B

DEAL SIZE	PARTNERS	FREQUENCY
$50M	Visible	Trackable

Deal sizes, partnerships, trading volumes EXPOSED

100%
of on-chain transactions are public

$2.3B+
crypto payroll market exposed

0
compliant privacy solutions

CURRENT LANDSCAPE

Existing Solutions Fall Short

Feature	Solana Confidential	Dark Pools	LatticA
Amount Hidden	✓	✓	✓
Address Hidden	✗	✓	✓
Regulatory Compliance	Partial	✗	✓
Audit Capability	Limited	✗	✓

Tornado Cash Case Study

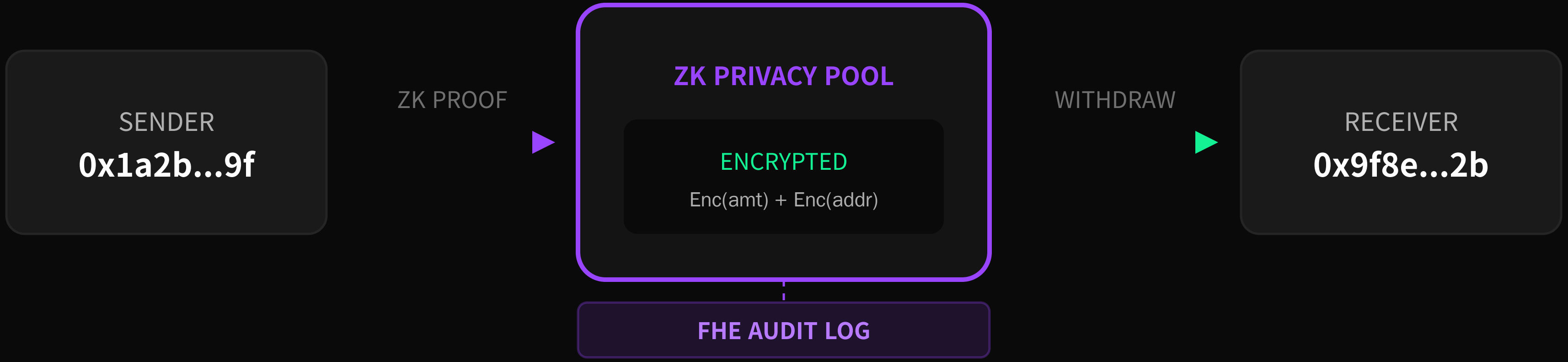
CEO sentenced to prison | $1B+ in regulatory fines | Protocol sanctioned

Privacy without compliance = Legal risk

DOJ Press Release   Treasury OFAC Sanctions

OUR SOLUTION

ZK + FHE Architecture



SENDER
0x1a2b...9f

ZK PROOF

ZK PRIVACY POOL

ENCRYPTED
Enc(amt) + Enc(addr)

WITHDRAW

RECEIVER
0x9f8e...2b

FHE AUDIT LOG

Zero-Knowledge Proof

Validates transaction without revealing sender, receiver, or amount

FHE Encrypted Audit

Homomorphic encryption enables queries on encrypted logs

```
SUM(Enc(amount)) where Enc(sender) = X
```

MPC Threshold Decryption

3-of-5 nodes required for audit decryption

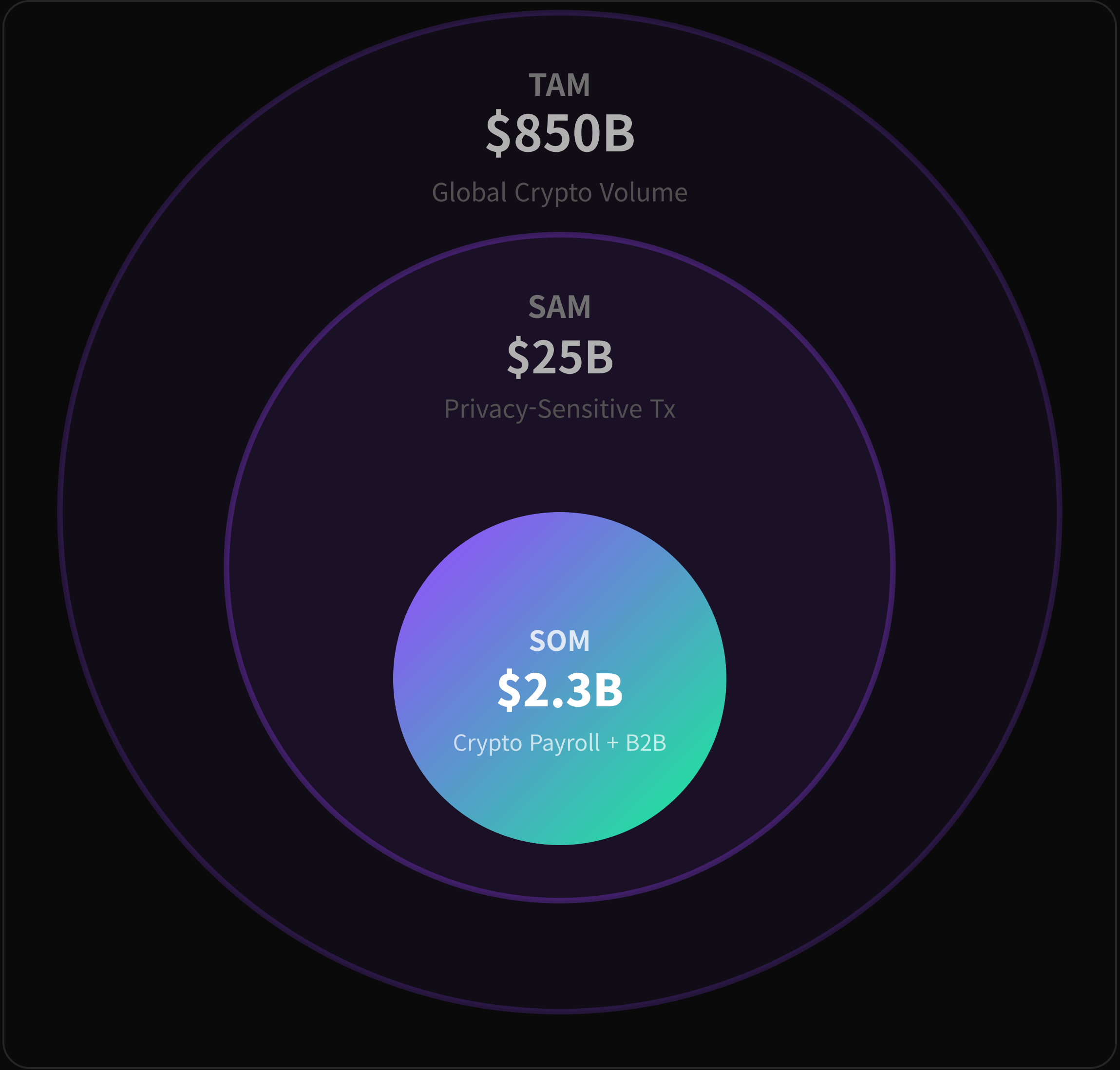
COMPLIANCE QUERY
"Sum of transfers from X > $10K?"

→

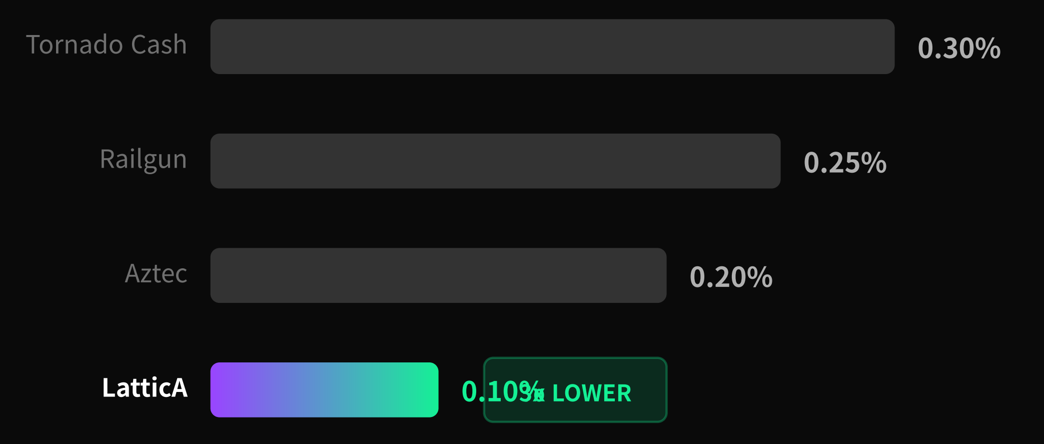
FHE RESULT
TRUE (computed on encrypted data)

MARKET OPPORTUNITY

Market Size & Go-To-Market



Transaction Fee Comparison



Go-To-Market Phases

Q1
Solana Payroll
Crypto-native companies

Q2
B2B Settlements
Trading firms, DAOs

Q3
DeFi SDK
DEX, lending protocols

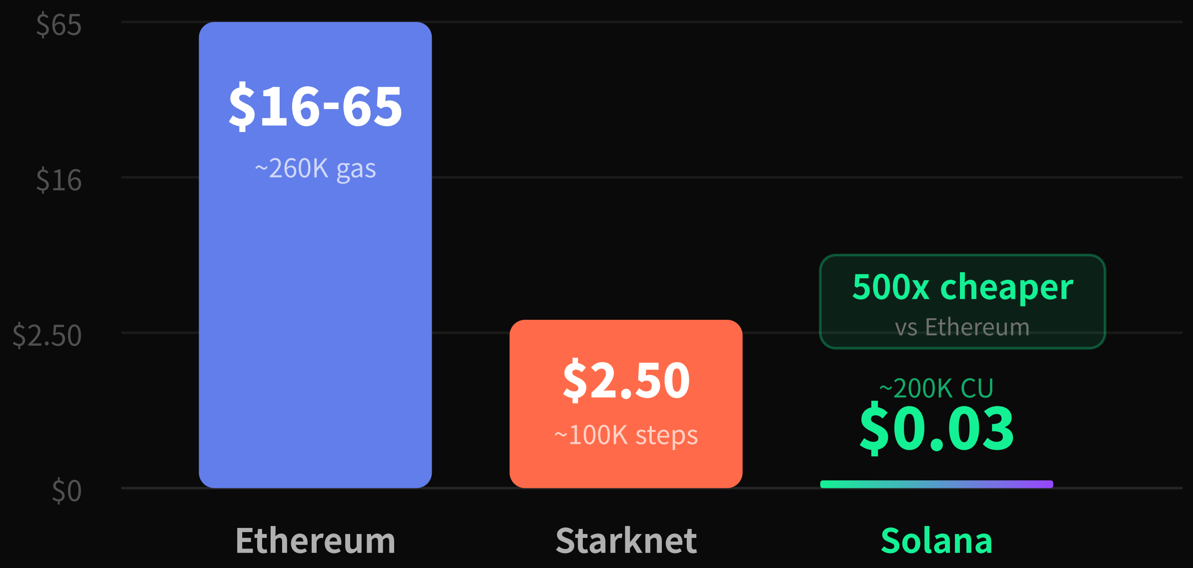
Q4
Multi-Chain
ETH, Polygon expansion

PLATFORM

Why Solana

ZK Proof Verification Cost

Groth16 (128 bytes) - Real Benchmark



$0.03

ZK Verification

Groth16 proof - 200K CU

400ms

Block Time

Near-instant finality

Token-2022

Native Extension

Built-in confidential transfer

Benchmark: Proving Time (M1 Mac)

4.0s	4.9s	5.1s	3.5GB
amount_audit	pool_identity	pool_transfer	Peak RAM

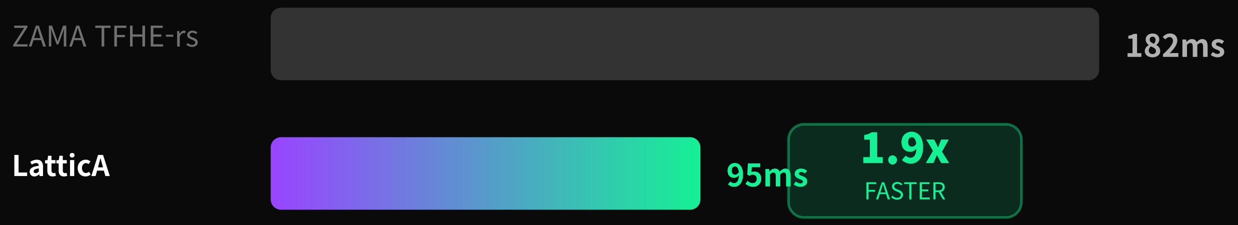
DeFiLlama groth16-solana Token-2022

COMPETITIVE EDGE

Why LatticA

FHE Bootstrapping Performance (64-bit)

Add/Sub operation benchmark



Source: ePrint 2025/2150

01 Cross-Platform Determinism

CPU GPU FPGA

NTT-based (no FFT errors)

02 Compliance-First Design

● AML/KYC ● Audit Logs ● Threshold Dec

03 Production Ready

Devnet Live Token-2022

Ready to bring compliant privacy to your platform **Contact Us**

Groth16 Paper Solana Explorer