

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
\$15,000

ADDRESS
0x1a2b...9f

TIMING
Monthly

B2B Settlements

Firm A



Firm B

DEAL SIZE
\$50M

PARTNERS
Visible

FREQUENCY
Trackable

Salary, bonus structure, employee wallets all PUBLIC

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

OUR SOLUTION

ZK + FHE Architecture



Zero-Knowledge Proof

Validates transaction without revealing sender, receiver, or amount

FHE Encrypted Audit

Homomorphic encryption enables queries on encrypted logs

$\text{SUM}(\text{Enc(amount)}) \text{ where } \text{Enc(sender)} = X$

MPC Threshold Decryption

3-of-5 nodes required for audit decryption

COMPLIANCE QUERY

"Sum of transfers from X > \$10K?"

FHE RESULT

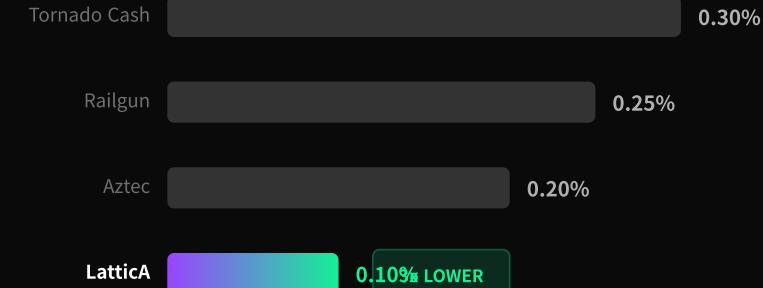
TRUE (computed on encrypted data)

MARKET OPPORTUNITY

Market Size & Go-To-Market



Transaction Fee Comparison



Go-To-Market Phases

Q1

Solana Payroll

Partner with crypto-native companies

Q2

B2B Settlements

Trading firms, DAOs, treasuries

Q3

DeFi SDK

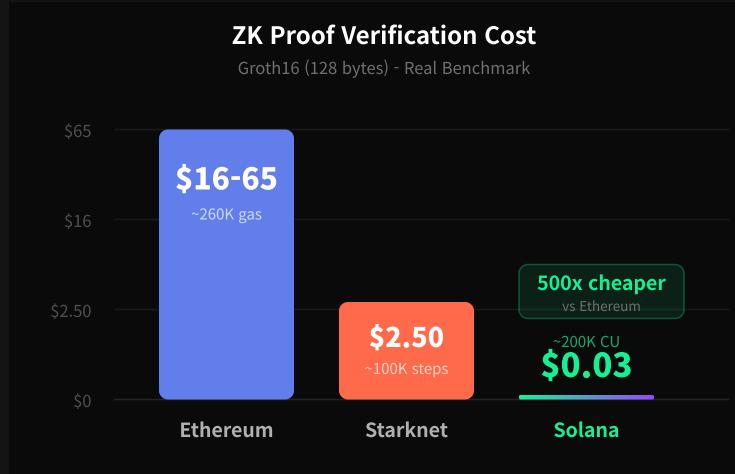
DEX, lending, yield protocols

Q4

Multi-Chain

Ethereum, Polygon expansion

Why Solana



\$0.03

ZK Verification

Groth16 proof (128 bytes) - 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

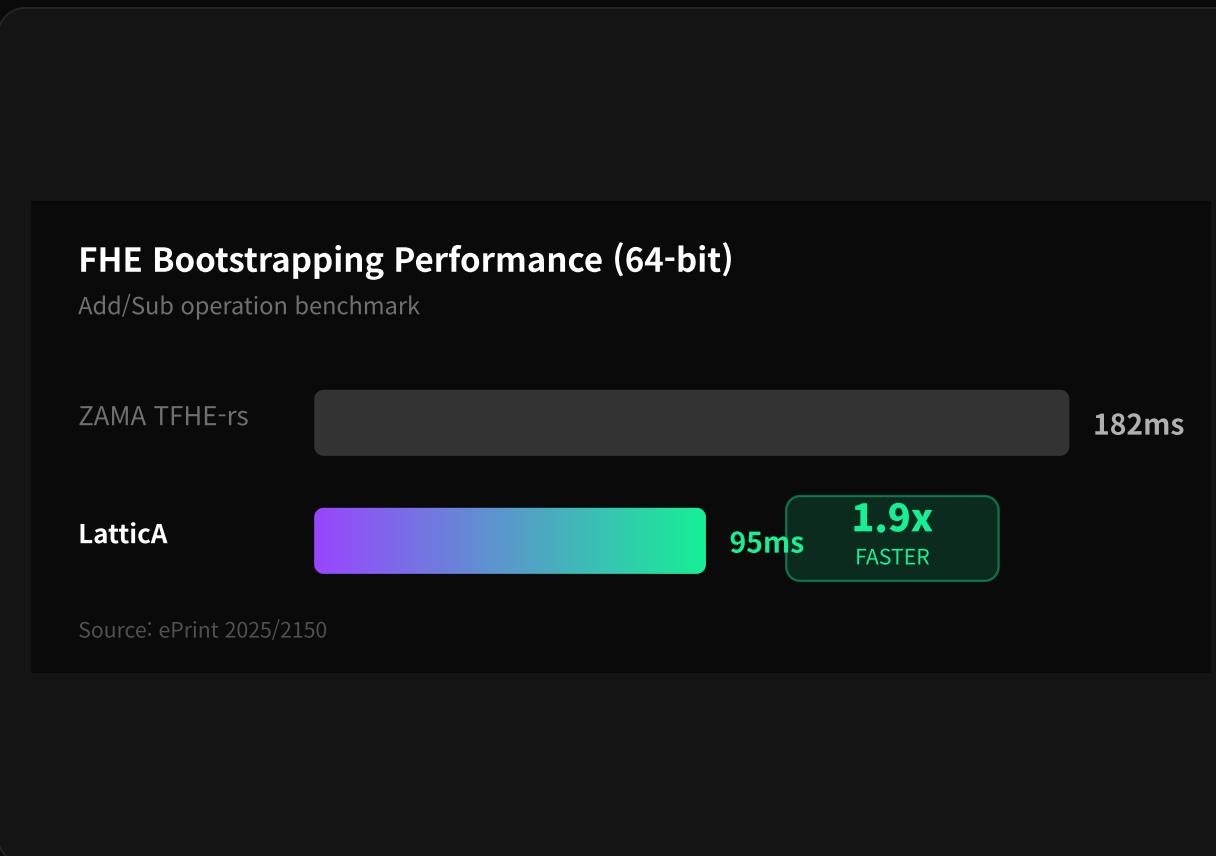
↗ DeFiLlama

↗ groth16-solana

↗ Token-2022

3.5GB

Why LatticA



01 Cross-Platform Determinism

CPU GPU FPGA

NTT-based computation (no FFT rounding errors)

02 Compliance-First Design

- AML/KYC Compatible
- Audit-Ready Logs
- Threshold Decryption

03 Production Ready

Solana Devnet Live Token-2022 Integration

[View Repository](#)

Ready to bring compliant privacy to your platform

[Contact Us](#)