THE PROBLEM

On-Chain Transparency Breaks Privacy

Payroll Exposure

BLOCKCHAIN

0xCorp -> 0xAlice $8,500

0xCorp -> 0xBob $12,000

My: $8,500
Bob: $12,000 !?

Employee

Coworker

Salary comparison visible to everyone

B2B Deal Exposure

VISIBLE
Partners

VISIBLE
Deal Size & Terms

VISIBLE
Frequency

Firm A

$50M Deal

Firm B

Competitor / Spy
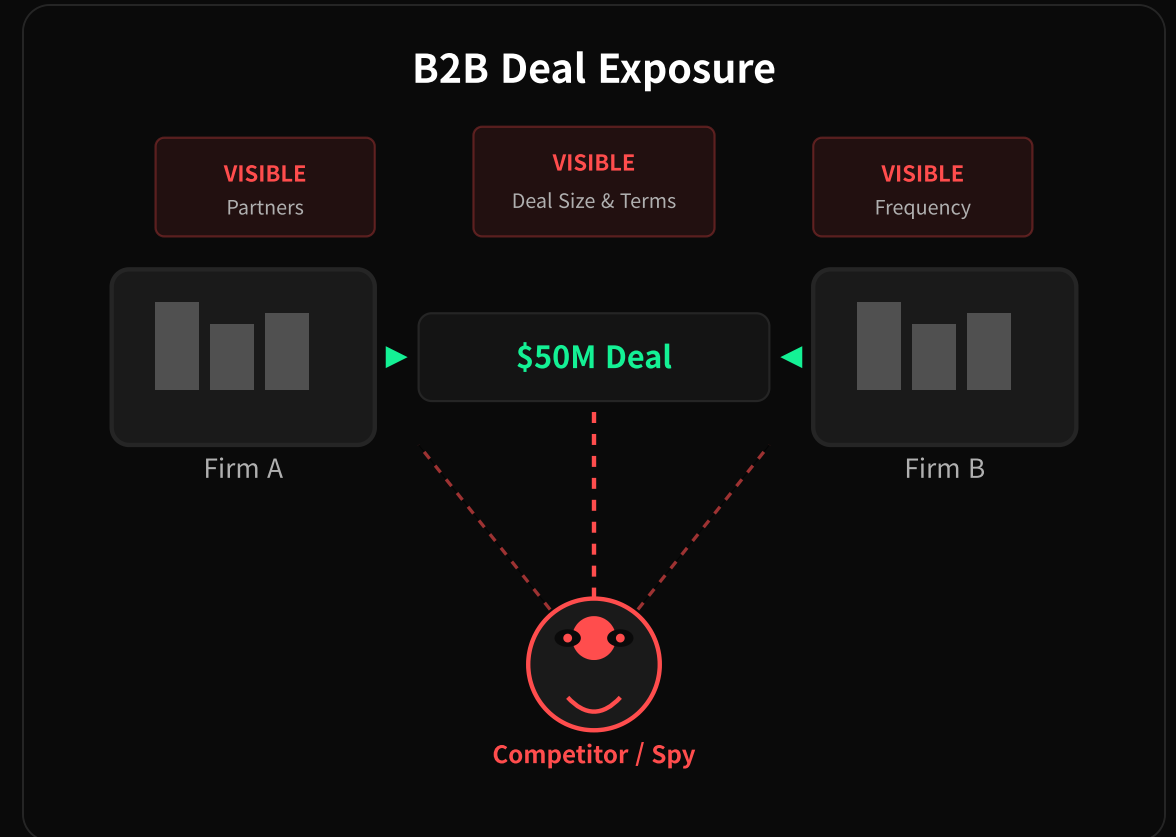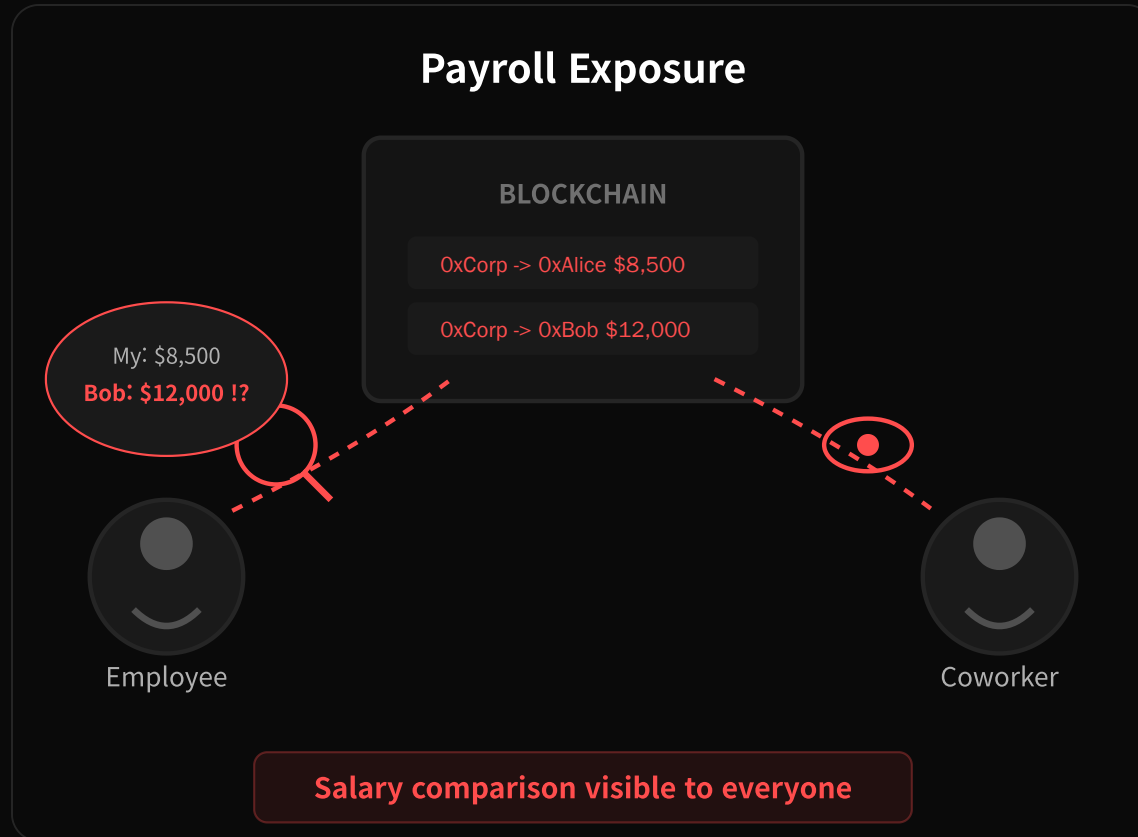
100%
of on-chain transactions are public

$2.3B+
crypto payroll market exposed

0
compliant privacy solutions

CURRENT LANDSCAPE

Existing Solutions Fall Short

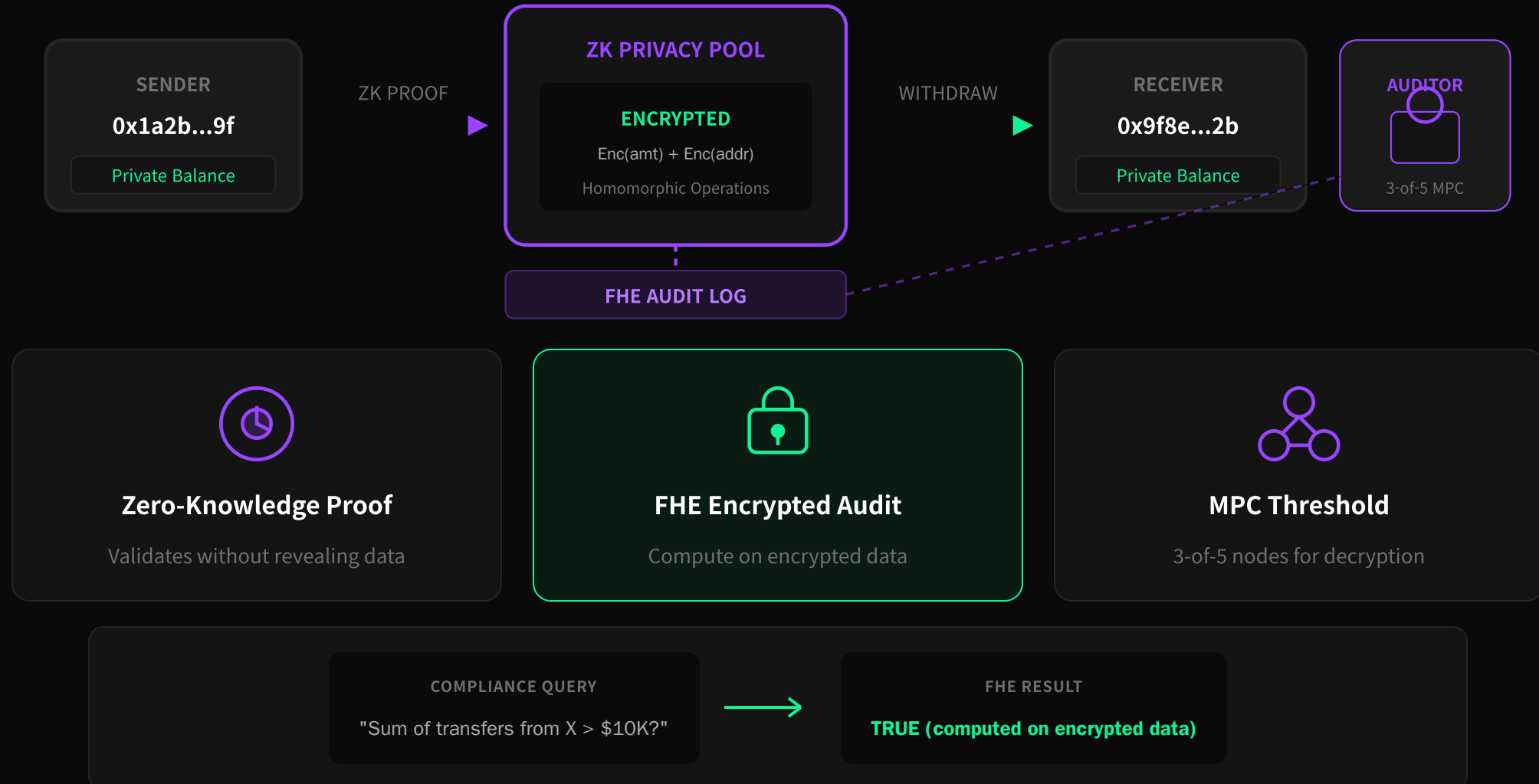| Feature	Solana Confidential	Dark Pools	LatticA
Amount Hidden	✔	✔	✔
Address Hidden	✘	✔	✔
Regulatory Compliance	Partial	✘	✔
Audit Capability	Limited	✘	✔

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

ZK PRIVACY POOL

SENDER

0x1a2b...9f

Private Balance

ZK PROOF

ENCRYPTED

Enc(amt) + Enc(addr)

Homomorphic Operations

WITHDRAW

RECEIVER

0x9f8e...2b

Private Balance

AUDITOR

3-of-5 MPC

FHE AUDIT LOG

Zero-Knowledge Proof

Validates without revealing data

FHE Encrypted Audit

Compute on encrypted data

MPC Threshold

3-of-5 nodes for decryption

COMPLIANCE QUERY

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

FHE RESULT

TRUE (computed on encrypted data)

MARKET OPPORTUNITY

Market Size & Go-To-Market

TAM
$850B
Global Crypto Volume

SAM
$25B
Privacy-Sensitive Tx

SOM
$2.3B
Crypto Payroll + B2B

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

Grand View Research   Chainalysis DeFi

Why Solana

ZK Proof Verification Cost
Groth16 (128 bytes) - Real Benchmark

$65

$16

$2.50

$0

$16-65
~260K gas

$2.50
~100K steps

500x cheaper
vs Ethereum

~200K CU
$0.03

Ethereum | Starknet | Solana
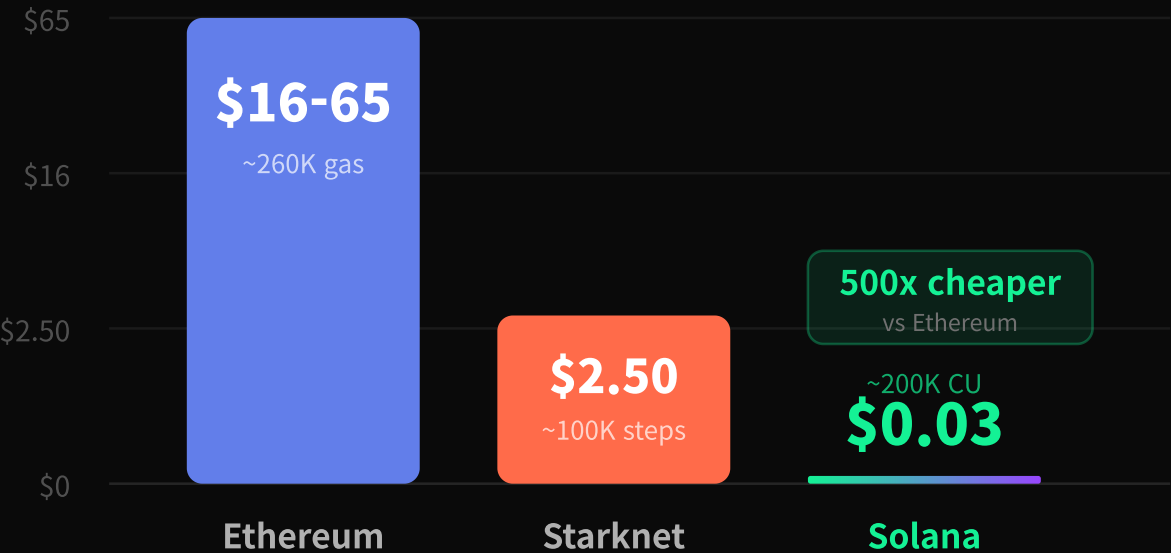
$0.03
ZK Verification
Groth16 proof - 200K CU

400ms
Block Time
Near-instant finality

Token-2022
Native Extension
Built-in confidential transfer

Benchmark: Proving Time (M1 Mac)

4.0s
amount_audit

4.9s
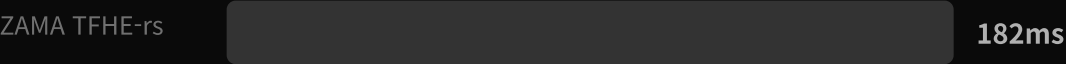pool_identity

5.1s
pool_transfer

3.5GB
Peak RAM

COMPETITIVE EDGE

Why LatticA

FHE Bootstrapping Performance (64-bit)

Add/Sub operation benchmark

ZAMA TFHE-rs   182ms

LatticA   95ms

1.9x
FASTER

Source: ePrint 2025/2150

Cross-Platform Determinism

CPU   **GPU**   **FPGA**

NTT-based (no FFT errors)

Compliance-First Design

AML/KYC   **Audit Logs**   **Threshold Dec**

Production Ready

Devnet Live   **Token-2022**

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